Microsoft

# Microsoft 365 Administrator

# Exam Ref MS-102

Orin Thomas

FREE SAMPLE CHAPTER |



Microsoft

# 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.



ISBN-13: 978-0-13-819946-3
ISBN-10: 0-13-819946-9

Library of Congress Control Number: 2023944921

**$PrintCode**



**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

# 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*

CHAPTER 2

# 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.

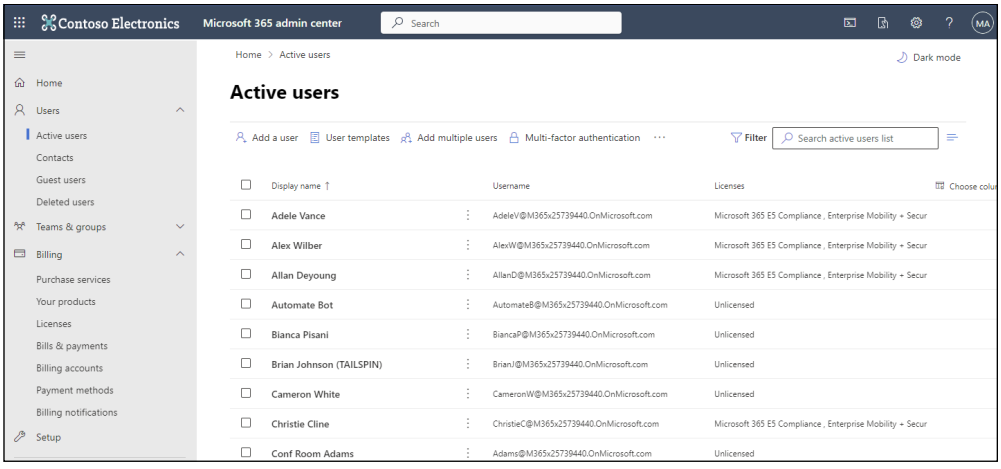


**FIGURE 2-1** Active Users

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.

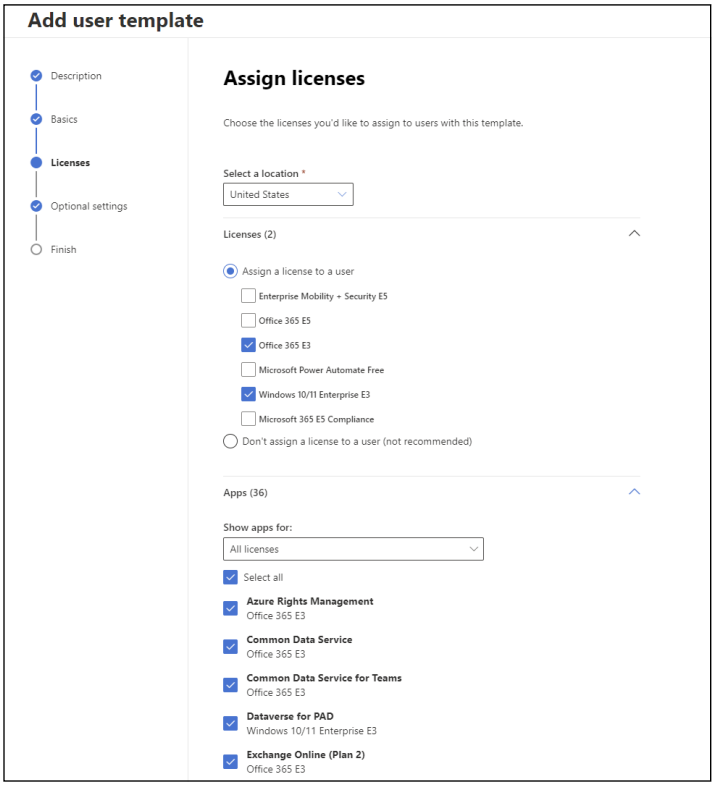


**FIGURE 2-2** Creating a new user template in the Microsoft 365 admin center

***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.

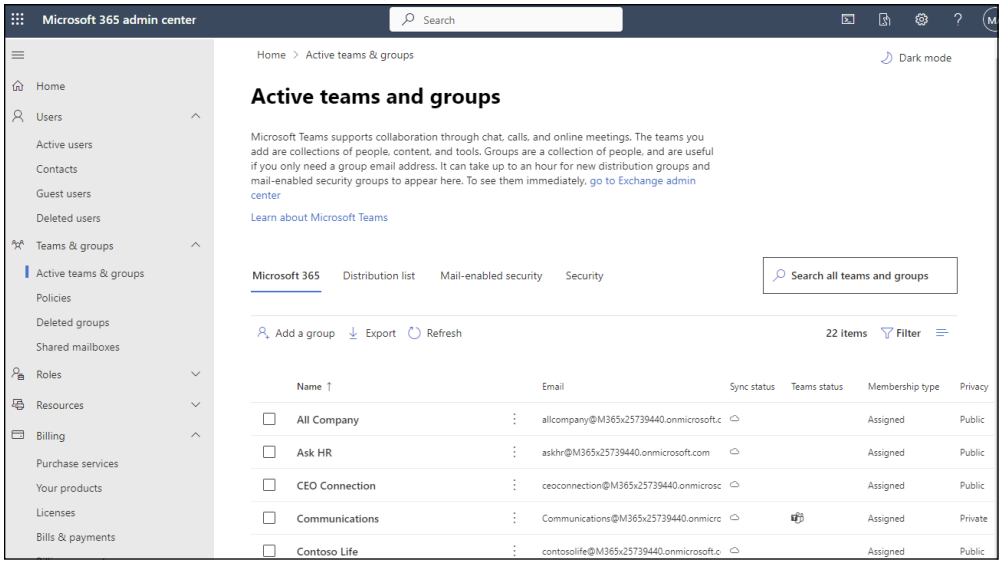


**FIGURE 2-3** The Active Teams And Groups page in the Microsoft 365 admin center

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.

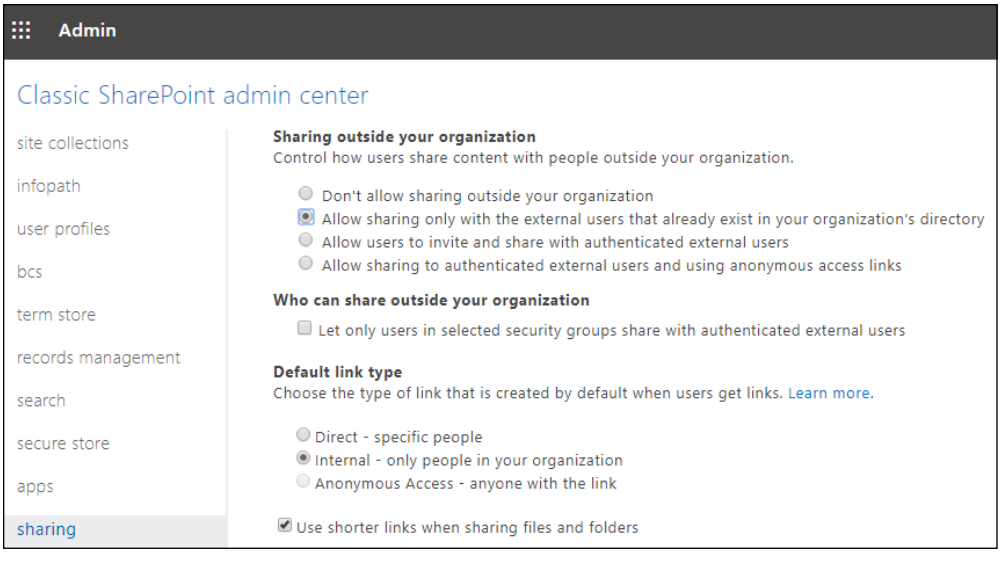


**FIGURE 2-4** SharePoint Online Sharing options

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.

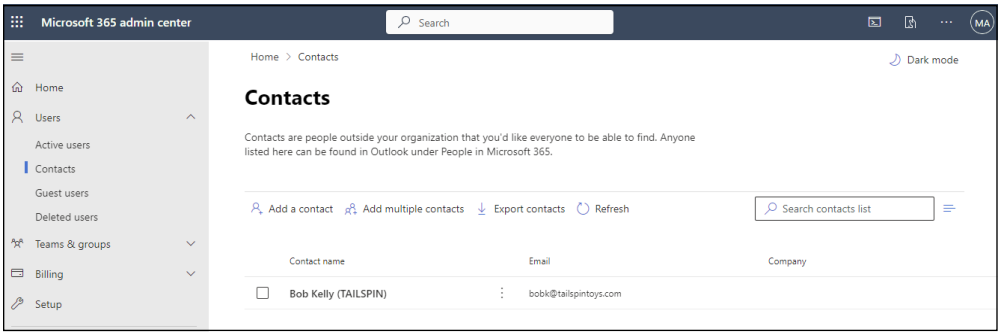


**FIGURE 2-5** Contacts

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.

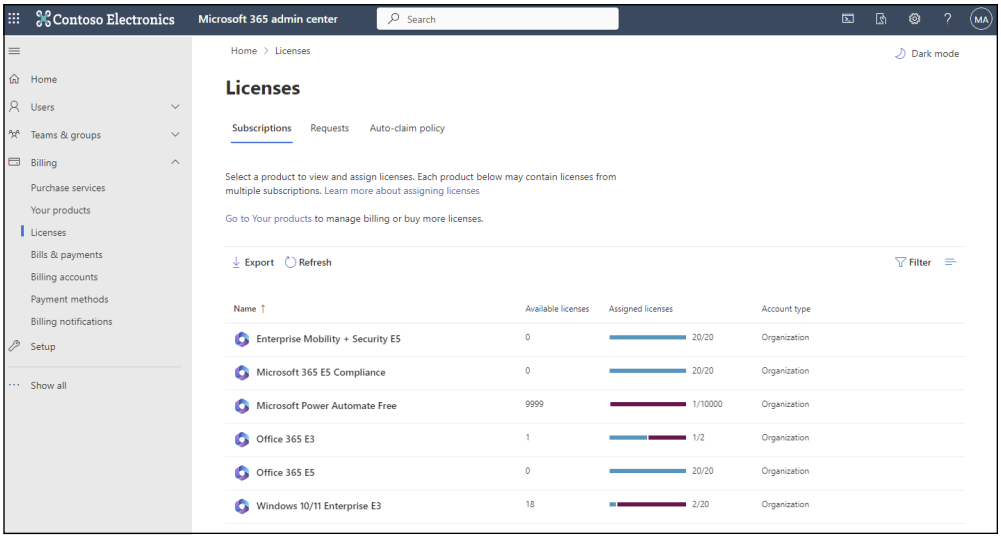


**FIGURE 2-6** The Licenses page

***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.

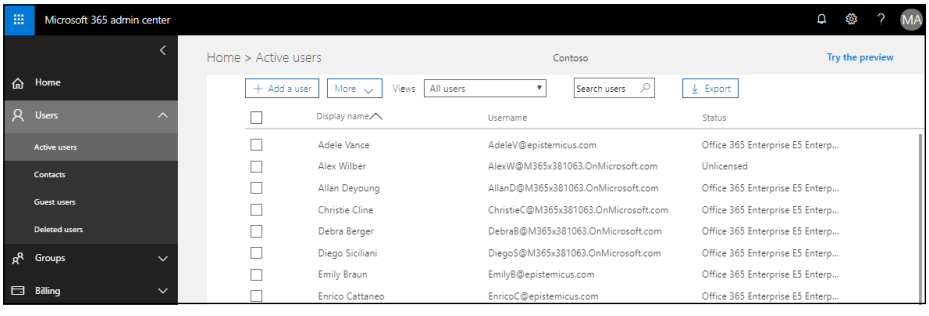


**FIGURE 2-7** The Active Users node

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.

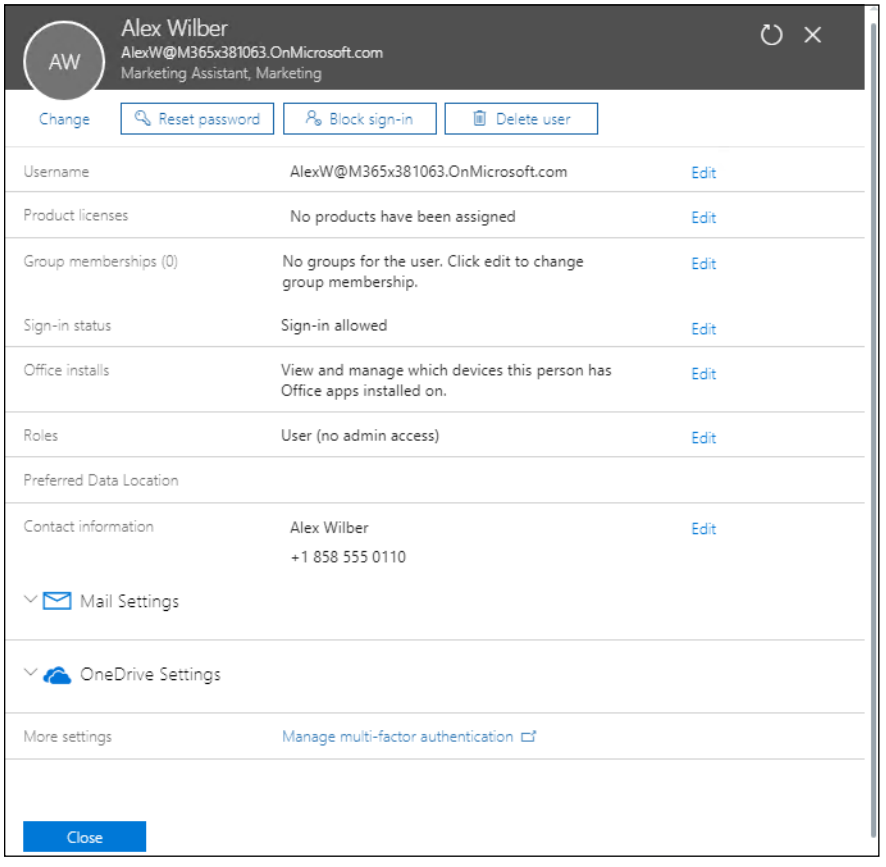


**FIGURE 2-8** User properties page

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.

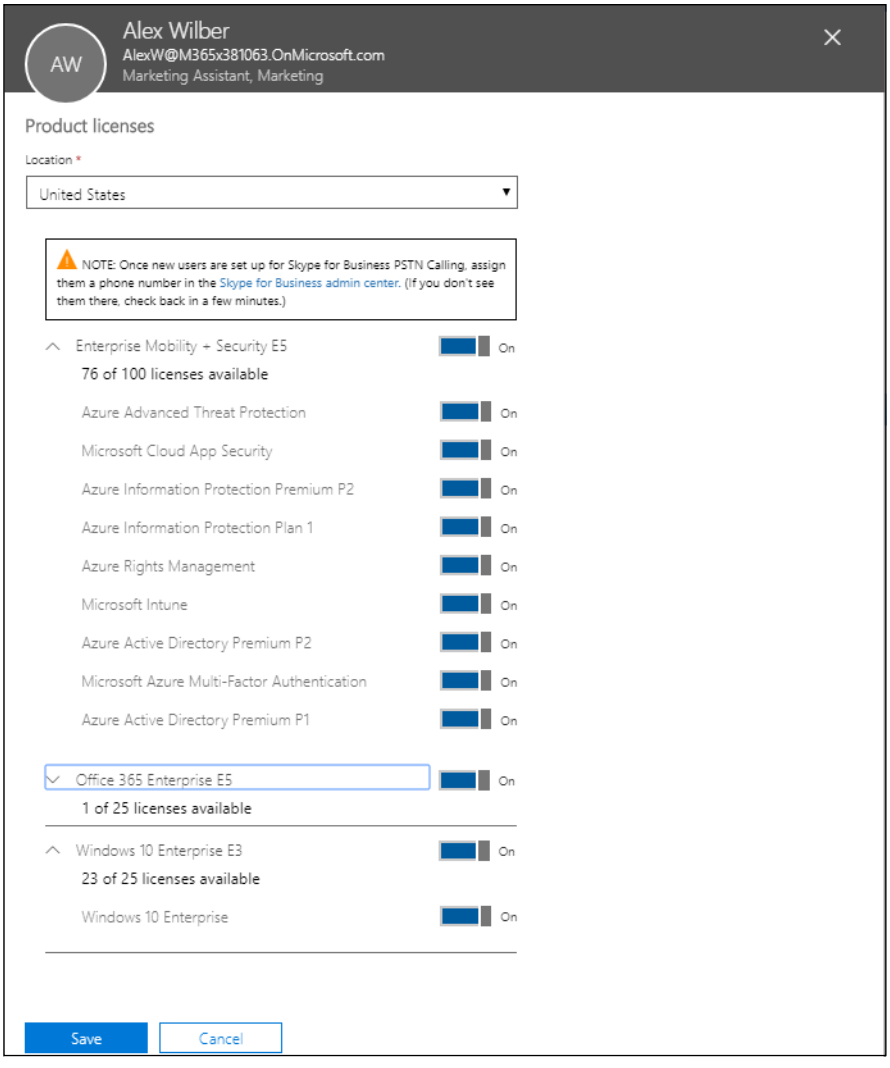


**FIGURE 2-9** The Product Licenses page

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

## B



## C



## D

# E

## F



## G



## H



## I



## K

# L



# M

## N



## O



## P

## Q



## R

# S



# T

## U



## V



## W



## Y