



2ND EDITION

Microsoft 365 Administration Cookbook

Boost efficiency, automate processes, and
enforce compliance with expert admin recipes

A decorative orange geometric shape, resembling a stylized 'L' or a corner bracket, located in the bottom left corner of the cover.

NATE CHAMBERLAIN

Foreword by Karuana Gatimu, Director, Microsoft 365 Customer Advocacy Group,
Collaborative Apps & Platform Engineering, Microsoft

Microsoft 365 Administration Cookbook

Boost efficiency, automate processes, and enforce compliance with expert admin recipes

Nate Chamberlain



Microsoft 365 Administration Cookbook

Copyright © 2024 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Group Product Manager: Dhruv Jagdish Kataria

Publishing Product Manager: Prachi Sawant

Book Project Manager: Ashwini Gowda

Senior Editor: Apramit Bhattacharya

Technical Editor: Nithik Cheruvakodan

Copy Editor: Safis Editing

Proofreader: Apramit Bhattacharya

Indexer: Manju Arasan and Subalakshmi Govindhan

Production Designer: Prashant Ghare

DevRel Marketing Coordinator: Marylou De Mello

First published: November 2020

Second edition: November 2024

Production reference: 2110625

Published by Packt Publishing Ltd.

Grosvenor House

11 St Paul's Square

Birmingham

B3 1RB, UK

ISBN 978-1-83588-802-5

www.packtpub.com

To my husband, William: your boundless love and encouragement are the secret ingredients in every recipe in this book. Thank you for adding zest to my life and our community.

Also, to our furry sous-chefs, Baxter and Lia, for bringing joy and comfort to my office and reminding me to take breaks and savor the small moments.

– Nate Chamberlain

Foreword

Welcome to a comprehensive guide for one of the most important roles in any organization, the Microsoft 365 tenant administrator. IT administration and service management of a variety of systems has been the cornerstone of my career for more than 25 years. The very many things required from this role in the modern era can feel daunting; systems are more complex, priorities and staffing are tight, and the consequences of inattentive management are high. That is why you have rightly picked up this valuable text in your hands.

Nate Chamberlain's dedication to empowering Microsoft 365 administrators is clear by the sheer volume of research, experience, and skill that has gone into compiling this volume. With a comprehensive approach to the guide the readers, this cookbook will provide you with the means to achieve the goal of a well-run, properly managed environment. Going beyond core tenant administration to incorporate management of essential tools like Exchange, OneDrive, Microsoft Teams, Power Platform, and more, this guide gives you a complete overview of essential tasks, PowerShell scale administrative tools, among other things.

Nate and I both count ourselves privileged to be a part of a far-reaching community of professionals that surround Microsoft 365, and we do all we can to create a supportive environment for continued learning. Your role as an administrator is not just technical – it is business critical. Nate and I know one thing for sure: the role will keep evolving, and your career journey can take you as far as you want to go. Use this guide and then expand your ongoing and real-world experience by participating in the technical community either via the Microsoft forums online at <https://aka.ms/techcommunity> or by attending free, local training events which you can find at <https://communitydays.org>. There you will meet people doing this work and more and you can continue to expand your experience with Microsoft 365.

At Microsoft, we take your commitment to our products seriously and thank you for the time you spend dedicating yourself to these. It is truly an honor to serve you while you are on your professional journey. Share your experience with us in the community and, most importantly, keep learning!

Karuana Gatimu

Director, Microsoft 365 Customer Advocacy Group

Collaborative Apps & Platform Engineering

Microsoft

Contributors

About the author

Nate Chamberlain is a Microsoft 365 expert from Kansas City, Missouri, specializing in training, business analysis, and Power Platform solution development. As a **Microsoft Certified Trainer (MCT)** and **Project Management Professional (PMP)**, he empowers individuals and organizations to maximize Microsoft 365 tools, including SharePoint, Power Platform, and Microsoft Teams.

Nate regularly contributes to the tech community through his books, website, and YouTube channel, sharing content and tutorials that have amassed millions of views, making complex topics more accessible.

Outside his professional endeavors, Nate volunteers at the Kansas City Zoo and Aquarium as a docent, educating visitors about wildlife and conservation.

Thank you to my team at Packt for making the writing and editing process so efficient and enjoyable. Your efforts have not gone unnoticed and are greatly appreciated. I'm proud to share this accomplishment with each of you.

About the reviewers

Greg Swart is a technology evangelist who has been working with Microsoft Modern Workplace tools and solutions for 12+ years and is passionate about business process transformation. He has worked in higher education, construction, and as a senior consultant to help companies get more out of their Microsoft 365 investments. He now works as a technology manager with an engineering enterprise using Microsoft 365 to support large-scale technical operations.

William Brand has worked for over 16 years in the information technology field, with a dedicated focus on Microsoft 365 for over 8 years. His multifaceted career has spanned roles as a developer, administrator, and analyst across diverse sectors, including finance, engineering, and energy. William holds an MSc from Napier University in Edinburgh and is a member of the **British Computer Society (BCS)**. He currently serves as a technical specialist at a prominent UK bank. His expertise encompasses Microsoft 365, Power Platform, Copilot, and AI. When he's not immersed in code and tech, he enjoys cherished moments with his family and dogs in Scotland. His diverse interests include music, hi-fi systems, literature, and 3D printing.

William extends his heartfelt gratitude to his wife, Margaret, and his daughters, Phoebe and Amelia, for their support and understanding of the demands of working in a field that is constantly changing. Sincere thanks are also extended to colleagues over the years, the entire tech community, and the team at Microsoft. Their collective passion has fueled his perpetual quest for knowledge and enjoyment of learning.

Table of Contents

1

Microsoft 365 Setup and Basic Administration 1

Technical requirements	2	There's more...	14
Accessing the admin centers	2	See also	17
Getting ready	2	Opening a service request	17
How to do it...	2	Getting ready	17
How it works...	5	How to do it...	17
See also	5	How it works...	20
Setting up PowerShell	5	Monitoring service request status	20
Getting ready	6	Getting ready	20
How to do it...	6	How to do it...	20
How it works...	7	How it works...	21
There's more...	8	There's more...	21
See also	8	Adding a domain	23
Viewing and filtering the Microsoft 365 roadmap	8	Getting ready	23
Getting ready	8	How to do it...	23
How to do it...	8	How it works...	24
How it works...	10	There's more...	25
See also	11	See also	25
Discovering upcoming changes via Microsoft 365 Message center	11	Changing the domain for users	26
Getting ready	11	Getting ready	26
How to do it...	11	How to do it...	26
How it works...	14	How it works...	27
		See also	27

Assigning a license to a user	28	Customizing navigation of the admin center	32
Getting ready	28	Getting ready	32
How to do it...	28	How to do it...	32
How it works...	29	How it works...	34
There's more...	30		
See also	30	Personalizing your admin center home page	34
Assigning a license to a group	30	Getting ready	34
Getting ready	30	How to do it...	34
How to do it...	30	How it works...	36
How it works...	31	There's more...	37
There's more...	32		
See also			

2

Microsoft 365 Identity and Roles **39**

Technical requirements	40	Enabling security defaults (MFA) in Entra ID	53
Creating a new user	40	Getting ready	53
Getting ready	40	How to do it...	53
How to do it...	40	How it works...	55
How it works...	43	There's more...	55
There's more...	43	See also	56
See also	44		
Importing users in bulk	44	Exporting users	56
Getting ready	44	Getting ready	56
How to do it...	44	How to do it...	56
How it works...	46	How it works...	59
There's more...	46	There's more...	59
See also	48	See also	60
Creating a new Microsoft 365 group	48	Managing guest users	60
Getting ready	48	Getting ready	60
How to do it...	48	How to do it...	60
How it works...	51	How it works...	63
There's more...	51	There's more...	64
See also	53	See also	64

Creating a user template	65	Assigning the User Administrator role	73
Getting ready	65	Getting ready	73
How to do it...	65	How to do it...	73
How it works...	67	How it works...	76
There's more...	68	There's more...	76
See also	68	See also	76
Restricting users from creating new Microsoft 365 groups	69	Managing admin roles in the Microsoft 365 admin center	76
Getting ready	69	Getting ready	76
How to do it...	69	How to do it...	76
How it works...	72	How it works...	78
There's more...	73	There's more...	79
See also	73	See also	80

3

Administering Microsoft 365 with PowerShell 81

Technical requirements	82	Changing user settings or profile information	89
Getting a list of all available commands	82	Getting ready	89
Getting ready	82	How to do it...	89
How to do it...	83	How it works...	89
How it works...	83	There's more...	90
There's more...	84	See also	91
See also	85	Getting a list of all users with user properties	91
Creating a user	85	Getting ready	91
Getting ready	85	How to do it...	91
How to do it...	85	How it works...	91
How it works...	86	There's more...	92
There's more...	86	See also	93
See also	87	Changing a user password	93
Disabling a user	87	Getting ready	93
Getting ready	87	How to do it...	93
How to do it...	87	How it works...	94
How it works...	87	There's more...	94
There's more...	88	See also	94
See also	88		

Connecting via PowerShell to SharePoint Online	94	Restoring a deleted OneDrive site	100
Getting ready	94	Getting ready	100
How to do it...	95	How to do it...	100
How it works...	95	How it works...	101
There's more...	95	There's more...	101
See also	96	See also	101
Creating a SharePoint Online site	96	Hiding Microsoft 365 groups from the Global Address List	102
Getting ready	96	Getting ready	102
How to do it...	96	How to do it...	102
How it works...	97	How it works...	102
There's more...	97	There's more...	103
See also	98	See also	103
Adding a new site admin to all SharePoint Online sites	98	Preventing external senders from emailing internal Microsoft 365 groups	103
Getting ready	98	Getting ready	103
How to do it...	98	How to do it...	103
How it works...	99	How it works...	104
There's more...	99	There's more...	104
See also	100	See also	104

4

Managing Exchange Online	105
Technical requirements	106
Creating a new user with a mailbox	106
Getting ready	106
How to do it...	106
How it works...	108
There's more...	109
See also	109
Creating a mail-enabled security group	110
Getting ready	110
How to do it...	110
How it works...	112
There's more...	114
See also	115
Creating an Exchange Online shared mailbox	115
Getting ready	116
How to do it...	116
How it works...	117
There's more...	118
See also	118
Creating a distribution list	119
Getting ready	119
How to do it...	119

How it works...	120	See also	132
There's more...	120		
See also	121		
Creating a dynamic distribution list	121	Configuring spam filter policies	132
Getting ready	121	Getting ready	133
How to do it...	121	How to do it...	133
How it works...	123	How it works...	135
There's more...	124	There's more...	136
See also	124	See also	136
Creating an Exchange-specific retention policy	124	Creating room and equipment resources	136
Getting ready	125	Getting ready	136
How to do it...	125	How to do it...	137
How it works...	127	How it works...	139
There's more...	128	There's more...	140
See also	128	See also	140
Creating a mail flow rule	128	Enabling ATP features	140
Getting ready	129	Getting ready	141
How to do it...	129	How to do it...	141
How it works...	131	How it works...	144
There's more...	132	There's more...	144
		See also	144

5

Setting Up and Configuring Microsoft Search 145

Technical requirements	146	There's more...	153
Creating an acronym	146	See also	154
Getting ready	146		
How to do it...	146	Importing bookmarks in bulk from CSV	155
How it works...	148	Getting ready	155
There's more...	149	How to do it...	155
See also	149	How it works...	156
Creating a bookmark	149	There's more...	157
Getting ready	150	See also	157
How to do it...	150	Adding a location	157
How it works...	152	Getting ready	158

How to do it...	158	There's more...	166
How it works...	159	See also	167
There's more...	160		
See also	160	Assigning Search Administrator and Search Editor roles	167
Adding a Q&A result	161	Getting ready	167
Getting ready	161	How to do it...	167
How to do it...	161	How it works...	168
How it works...	163	There's more...	169
There's more...	164	See also	169
See also	164	Using Search Insights dashboard reports	169
Setting up usage of Microsoft Search in Bing	164	Getting ready	169
Getting ready	164	How to do it...	170
How to do it...	164	How it works...	171
How it works...	166	There's more...	172
		See also	172

6

Administering OneDrive for Business 173

Technical requirements	174	Restricting sharing to specific domains	183
Enabling external sharing	174	Getting ready	183
Getting ready	174	How to do it...	183
How to do it...	174	How it works...	184
How it works...	179	There's more...	184
There's more...	179	See also	185
See also	179	Enabling local sync of files	185
Configuring external sharing permission levels	179	Getting ready	186
Getting ready	179	How to do it...	186
How to do it...	180	How it works...	187
How it works...	181	There's more...	189
There's more...	182	See also	190
See also	182		

Restricting local syncing to PCs on specific domains	190	Setting the default share link type	199
Getting ready	190	Getting ready	200
How to do it...	190	How to do it...	200
How it works...	191	How it works...	200
There's more...	192	There's more...	201
See also	193	See also	202
Setting up compliance safeguards	193	Adjusting all users' default storage allocation and retention periods	203
Getting ready	193	Getting ready	203
How to do it...	193	How to do it...	203
How it works...	195	How it works...	205
There's more...	195	There's more...	205
See also	196	See also	206
Providing individuals access to another user's OneDrive content	196	Migrating data using the SPMT	207
Getting ready	196	Getting ready	207
How to do it...	197	How to do it...	207
How it works...	197	How it works...	211
There's more...	198	There's more...	211
See also	199	See also	212

7

Configuring Power Platform 213

Technical requirements	214	How it works...	221
Creating a new Power Platform environment	214	There's more...	221
Getting ready	214	See also	221
How to do it...	214	Restricting certain connectors in Power Apps and Power Automate from accessing business data	221
How it works...	217	Getting ready	221
There's more...	218	How to do it...	222
See also	219	How it works...	223
Creating a Dataverse database	220	There's more...	224
Getting ready	220	See also	225
How to do it...	220		

Using Analytics to explore usage, failures, and performance in Microsoft Power Platform	225	Restricting Power BI's Publish to web (anonymous share) ability to specific security group members	236
Getting ready	225	Getting ready	236
How to do it...	225	How to do it...	236
How it works...	227	How it works...	237
There's more...	227	There's more...	238
See also	227	See also	238
Installing an on-premises data gateway	228	Auditing Power BI embed codes created by your organization	238
Getting ready	228	Getting ready	238
How to do it...	228	How to do it...	239
How it works...	230	How it works...	239
There's more...	232	There's more...	240
See also	233	See also	241
Restricting users from installing on-premises data gateways	233	Configuring a default logo, cover image, and theme for Power BI	241
Getting ready	234	Getting ready	241
How to do it...	234	How to do it...	241
How it works...	235	How it works...	242
There's more...	236	There's more...	242
See also	236	See also	242

8

Administering SharePoint Online	243
Technical requirements	244
Creating a new site	244
Getting ready	244
How to do it...	244
How it works...	247
There's more...	247
See also	248
Deleting a site	248
Getting ready	248
How to do it...	248
How it works...	249
There's more...	250
See also	250
Limiting external sharing abilities	250
Getting ready	251
How to do it...	251
How it works...	255
There's more...	255
See also	255

Setting stricter external sharing settings for a specific site	255	How to do it...	265
Getting ready	255	How it works...	267
How to do it...	255	There's more...	268
How it works...	256	See also	268
There's more...	257	Hiding the subsite creation button	268
See also	258	Getting ready	268
Setting the default share link type	258	How to do it...	268
Getting ready	259	How it works...	269
How to do it...	259	There's more...	270
How it works...	259	See also	270
There's more...	260	Designating a site as a hub site and associating other sites with it	270
See also	261	Getting ready	270
Configuring site collection storage	261	How to do it...	271
Getting ready	262	How it works...	272
How to do it...	262	There's more...	273
How it works...	264	See also	274
There's more...	264	Restricting access by IP address	274
See also	265	Getting ready	274
Importing data from network locations using the Migration Manager or SPMT	265	How to do it...	274
Getting ready	265	How it works...	275
		There's more...	276
		See also	276

9

Managing Microsoft Teams 277

Technical requirements	278	How to do it...	281
Creating a team	278	How it works...	282
Getting ready	278	There's more...	283
How to do it...	278	See also	283
How it works...	279	Configuring meeting settings	283
There's more...	280	Getting ready	283
See also	280	How to do it...	284
Creating a Team policy	281	How it works...	285
Getting ready	281	There's more...	285
		See also	285

Creating a Meeting policy	285	Configuring Teams setup policies	298
Getting ready	285	Getting ready	298
How to do it...	286	How to do it...	298
How it works...	287	How it works...	299
There's more...	287	There's more...	300
See also	287	See also	300
Creating an Events policy	288	Configuring external access	300
Getting ready	288	Getting ready	300
How to do it...	288	How to do it...	300
How it works...	289	How it works...	302
There's more...	290	There's more...	302
See also	290	See also	304
Creating a Messaging policy	290	Configuring guest access	304
Getting ready	290	Getting ready	304
How to do it...	291	How to do it...	304
How it works...	292	How it works...	305
There's more...	292	There's more...	305
See also	293	See also	305
Applying a policy (Team/Meeting/ Messaging) to specific users	293	Reviewing all teams and their owners	306
Getting ready	293	Getting ready	306
How to do it...	293	How to do it...	306
How it works...	294	How it works...	307
There's more...	294	There's more...	307
See also	297	See also	308

10

Managing Viva Engage	309	Pinning Viva Engage in Teams	313
Technical requirements	309	Getting ready	313
Understanding admin roles for Viva Engage	310	How to do it...	313
Getting ready	310	How it works...	315
How to do it...	310	There's more...	315
How it works...	311	See also	315
There's more...	312		
See also	313		

Assigning the Corporate Communicator role to a user	316	How it works...	322
Getting ready	316	There's more...	323
How to do it...	316	See also	323
How it works...	317	Creating a dynamic Viva Engage community	324
There's more...	317	Getting ready	324
See also	317	How to do it...	324
Customizing the look of your Viva Engage network	318	How it works...	326
Getting ready	318	There's more...	326
How to do it...	318	See also	326
How it works...	319	Restricting posts in the All Company community	327
There's more...	319	Getting ready	327
See also	320	How to do it...	327
Creating a Viva Engage community	320	How it works...	328
Getting ready	321	There's more...	329
How to do it...	321	See also	330

11

Configuring and Managing Users in Microsoft Entra ID 331

Technical requirements	332	There's more...	339
Creating and populating Microsoft Entra ID	332	See also	339
Getting ready	332	Adding a privacy statement to the Entra ID sign-in page	340
How to do it...	332	Getting ready	340
How it works...	335	How to do it...	340
There's more...	335	How it works...	340
See also	336	There's more...	341
Adding branding to the Entra ID sign-in page	337	See also	341
Getting ready	337	Adding SSO for an application	341
How to do it...	337	Getting ready	342
How it works...	339	How to do it...	342
		How it works...	344
		There's more...	344
		See also	344

Getting direct sign-on links for organizational apps	344	See also	351
Getting ready	344	Creating an Access review report in Entra ID	351
How to do it...	344	Getting ready	351
How it works...	345	How to do it...	351
There's more...	346	How it works...	356
See also	346	There's more...	357
Installing and connecting to the Microsoft Graph SDK via PowerShell	346	See also	357
Getting ready	346	Reviewing and completing an Access review report in Entra ID	358
How to do it...	346	Getting ready	358
How it works...	348	How to do it...	358
There's more...	348	How it works...	359
See also	349	There's more...	359
Adding/removing users via PowerShell in Microsoft Graph	349	See also	360
Getting ready	349	Enabling self-service password reset	360
How to do it...	350	Getting ready	360
How it works...	350	How to do it...	360
There's more...	350	How it works...	361
		There's more...	361
		See also	363

12

Understanding Microsoft Defender	365
Technical requirements	365
Creating a threat protection policy	366
Getting ready	366
How to do it...	366
How it works...	368
There's more...	369
See also	369
Setting up a Safe Links policy	369
Getting ready	369
How to do it...	369
How it works...	372
There's more...	372
See also	372
Setting up a Safe Attachments policy	373
Getting ready	373
How to do it...	373
How it works...	375
There's more...	375
See also	375
Accessing and reviewing an organization's Secure Score	375
Getting ready	376

How to do it...	376	There's more...	386
How it works...	378	See also	388
There's more...	379		
See also	379		
Complying with Secure Score security configuration recommendations	380	Monitoring Microsoft Defender reports	388
Getting ready	380	Getting ready	388
How to do it...	380	How to do it...	388
How it works...	382	How it works...	392
There's more...	383	There's more...	392
See also	384	See also	392
Assigning permissions for non-IT users to Microsoft Defender	384	Utilizing threat investigation and response capabilities	393
Getting ready	384	Getting ready	393
How to do it...	384	How to do it...	393
How it works...	386	How it works...	394
		There's more...	394
		See also	394

13

Understanding the Microsoft Purview Portal 395

Technical requirements	396	Creating a DLP policy to protect content with HIPAA-protected data detected	401
Viewing a report on all users who have accessed a specific SharePoint file	396	Getting ready	401
Getting ready	396	How to do it...	401
How to do it...	396	How it works...	405
How it works...	398	There's more...	406
There's more...	398	See also	406
See also	399	Using DLP to automatically report HIPAA incident reports	406
Accessing Microsoft's HIPAA business associate agreement	399	Getting ready	407
Getting ready	399	How to do it...	407
How to do it...	399	How it works...	410
How it works...	400	There's more...	410
There's more...	400	See also	411
See also	401		

Creating a custom sensitive information type based on keywords	411	How it works...	428
Getting ready	411	There's more...	429
How to do it...	411	See also	430
How it works...	415	Creating and using an eDiscovery case	430
There's more...	416	Getting ready	430
See also	417	How to do it...	430
Creating a DLP policy for content with custom keywords in the name or subject	417	How it works...	434
Getting ready	417	There's more...	434
How to do it...	417	See also	434
How it works...	422	Assigning permissions for non-IT users to Microsoft Purview	435
There's more...	422	Getting ready	435
See also	422	How to do it...	435
Tuning a DLP policy's sensitivity	422	How it works...	437
Getting ready	422	There's more...	437
How to do it...	422	See also	438
How it works...	424	Using Communication Compliance to identify potential policy violations in messages	438
There's more...	425	Getting ready	438
See also	425	How to do it...	438
Creating a retention policy to retain content for seven years	425	How it works...	440
Getting ready	425	There's more...	441
How to do it...	425	See also	442

14

Monitoring Microsoft 365 Apps and Services 443

Technical requirements	444	Creating alerts for specific activities performed by users in OneDrive	446
Finding at-risk users	444	Getting ready	446
Getting ready	444	How to do it...	446
How to do it...	444	How it works...	448
How it works...	445	There's more...	448
There's more...	445	See also	449
See also	445		

Reviewing mail handling to see spam and malware history	449	How to do it...	456
Getting ready	449	How it works...	457
How to do it...	450	There's more...	458
How it works...	450	See also	458
There's more...	450	Checking general usage data for Microsoft 365 apps and services	458
See also	451	Getting ready	458
Identifying your least active SharePoint sites	451	How to do it...	459
Getting ready	451	How it works...	460
How to do it...	451	There's more...	460
How it works...	452	See also	461
There's more...	452	Checking Teams usage and user activity	461
See also	452	Getting ready	461
Analyzing search activity throughout Microsoft 365	452	How to do it...	461
Getting ready	452	How it works...	462
How to do it...	452	There's more...	462
How it works...	454	See also	463
There's more...	455	Monitoring Power Apps and Power Automate usage and activity	464
See also	455	Getting ready	464
Checking service health status and known issues	456	How to do it...	464
Getting ready	456	How it works...	466
		There's more...	466
		See also	467
Appendix	469		
Purchase a subscription	469	Purchase licenses	470
Compare Microsoft 365 subscriptions	469	Upgrade a license	470
Compare additional services	470	Renew a license	471
		Useful resources	471
Index	473		
Other Books You May Enjoy	484		

Preface

Microsoft 365 Administration Cookbook is an essential resource for IT professionals looking to streamline their organization's Microsoft 365 management and administration tasks. This comprehensive guide covers a wide range of topics, from initial setup and configuration to advanced management techniques, providing step-by-step instructions and practical tips to help administrators efficiently manage their Microsoft 365 environment. The book is structured to facilitate easy understanding and quick implementation, making it an invaluable reference for both novice and experienced administrators.

Who this book is for

This book is designed for IT professionals, system administrators, and technical support staff responsible for managing Microsoft 365 environments. A basic understanding of Microsoft 365 and general IT administration concepts is assumed. Whether you are new to Microsoft 365 or looking to enhance your existing skills, this book provides the knowledge and tools necessary to effectively administer and optimize your organization's Microsoft 365 services.

What this book covers

Chapter 1, Microsoft 365 Setup and Basic Administration, guides you through the initial setup and configuration of your Microsoft 365 tenant, including domain setup, DNS configuration, and initial user and group licensing.

Chapter 2, Microsoft 365 Identity and Roles, looks at the management and automation of user accounts and groups, including tips for managing large numbers of users efficiently.

Chapter 3, Administering Microsoft 365 with PowerShell, introduces PowerShell scripting for automating common administrative tasks, saving time and reducing the potential for errors.

Chapter 4, Managing Exchange Online, provides detailed instructions for configuring and managing Exchange Online, including mailbox setup, email flow configuration, and security settings.

Chapter 5, Setting Up and Configuring Microsoft Search, focuses on setting up and managing Microsoft Search, including creating bookmarks, acronyms, and managing search results to enhance the user experience.

Chapter 6, Administering OneDrive for Business, delves into configuring OneDrive settings for individual user document storage and sharing, managing default settings, and migrating data from local network locations to OneDrive.

Chapter 7, Configuring Power Platform, covers the administration of Power Platform services such as Power BI, Power Automate, and Power Apps, providing insights into data visualization, automation, and app experiences.

Chapter 8, Administering SharePoint Online, discusses the creation and management of SharePoint sites, sharing abilities, and permissions, aimed at facilitating effective collaboration within your organization.

Chapter 9, Managing Microsoft Teams, explains how to set up and manage Microsoft Teams, including team creation, policy configuration, and integration with other Microsoft 365 services.

Chapter 10, Managing Viva Engage, introduces Viva Engage (formerly Yammer), focusing on creating communities, assigning roles, and customizing the user experience to foster a connected organizational culture.

Chapter 11, Configuring and Managing Users in Microsoft Entra ID, provides detailed instructions on using Microsoft Entra ID for advanced user management, access restrictions, group management, and licensing.

Chapter 12, Understanding Microsoft Defender, covers core security features and functions of Microsoft Defender within Microsoft 365, including monitoring your Secure Score and setting up threat protection policies.

Chapter 13, Understanding the Microsoft Purview Portal, focuses on data loss prevention and eDiscovery within Microsoft 365, ensuring the protection of sensitive data and compliance with legal standards.

Chapter 14, Monitoring Microsoft 365 Apps and Services, explains how to utilize various reporting and analysis tools available in Microsoft 365 to monitor user activities, service health, and app usage to ensure optimal performance.

To get the most out of this book

To fully benefit from this book, you should have a basic understanding of Microsoft 365 and general IT administration principles. Familiarity with the Microsoft 365 admin center, Microsoft 365 apps and services, and PowerShell will be advantageous. The book assumes a Windows, macOS X, or Linux operating system environment.

Note that Teams Desktop on Linux was retired in 2022, but you can still use the admin centers via a browser and PowerShell for administration.

Software/hardware covered in the book	OS requirements
PowerShell 7.0 or later	Windows 8.1 and later, macOS 10.13 and later, and Linux (various) – refer to https://learn.microsoft.com/en-us/powershell/ for more specifics.
Microsoft Teams desktop application	Windows 8.1 and later, one of the three most recent versions of macOS, one of the last four major versions of Android, one of the last two major versions of iOS – refer to https://learn.microsoft.com/en-us/microsoftteams/hardware-requirements-for-the-teams-app for more specifics.
Microsoft 365 apps and services	Any (web-based)

Conventions used

There are a number of text conventions used throughout this book.

Code in text: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. Here is an example: “The `-AllowClobber` parameter in PowerShell allows a new module, script, or command to be installed to overwrite an existing command or alias that has the same name.”

Any command-line input or output is written as follows:

```
Install-Module -Name Microsoft.Graph -Scope CurrentUser -AllowClobber
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: “Upon entry, explore the left-hand navigation pane, which presents various management options, including user and group management, **Billing**, **Settings**, and **Setup**.”

Tips or important notes

Appear like this.

Sections

In this book, you will find several headings that appear frequently (*Getting ready*, *How to do it...*, *How it works...*, *There's more...*, and *See also*).

To give clear instructions on how to complete a recipe, use these sections as follows:

Getting ready

This section tells you what to expect in the recipe and describes how to set up any software or any preliminary settings required for the recipe.

How to do it...

This section contains the steps required to follow the recipe.

How it works...

This section usually consists of a detailed explanation of what happened in the previous section.

There's more...

This section consists of additional information about the recipe in order to make you more knowledgeable about the recipe.

See also

This section provides helpful links to other useful information for the recipe.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, mention the book title in the subject of your message and email us at customercare@packtpub.com.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit www.packtpub.com/support/errata, selecting your book, clicking on the Errata Submission Form link, and entering the details.

Piracy: If you come across any illegal copies of our works in any form on the Internet, we would be grateful if you would provide us with the location address or website name. Please contact us at copyright@packtpub.com with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit authors.packtpub.com.

Share Your Thoughts

Once you've read *Microsoft 365 Administration Cookbook*, we'd love to hear your thoughts! Please click [here](#) to go straight to the Amazon review page for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Download a free PDF copy of this book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere?

Is your eBook purchase not compatible with the device of your choice?

Don't worry, now with every Packt book you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there, you can get exclusive access to discounts, newsletters, and great free content in your inbox daily

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the link below



<https://packt.link/free-ebook/978-1-83588-802-5>

2. Submit your proof of purchase
3. That's it! We'll send your free PDF and other benefits to your email directly

Microsoft 365 Setup and Basic Administration

Welcome to the second edition of *Microsoft 365 Administration Cookbook*. This comprehensive guide is designed to equip you with step-by-step instructions for navigating the spectrum of administration tasks within the Microsoft 365 ecosystem.

Tip

Due to this book's nature as a cookbook, you do not need to read it sequentially. You can jump around to recipes and subjects of interest throughout the book.

The initial stages of administration and tenant configuration might seem straightforward, yet they often involve critical decisions whose impact is challenging to reverse or modify at a later stage. This chapter will delve into essential topics, such as domain connection to your tenant, activation of PowerShell capabilities, and licensing users so they can begin to take advantage of all that Microsoft 365 has to offer your organization. Additionally, we will introduce fundamental navigation techniques and the routine tasks every administrator should adopt to maintain an efficient Microsoft 365 environment.

We will cover the following recipes in this chapter:

- Accessing the admin centers
- Setting up PowerShell
- Viewing and filtering the Microsoft 365 roadmap
- Discovering upcoming changes via Microsoft 365 Message center
- Opening a service request
- Monitoring service request status
- Adding a domain

- Changing the domain for users
- Assigning a license to a user
- Assigning a license to a group
- Customizing navigation of the admin center
- Personalizing your admin center home page

Technical requirements

This chapter requires administrative access within Microsoft 365. Users assigned the Global Administrator role will have the capability to execute all tasks presented. Those holding specific app or function administration roles will find many of these recipes within their reach. We will detail the recipes that necessitate particular administrative roles, all of which can be assigned by an existing Global Administrator through the Microsoft 365 admin center's **Users** section if not already in place.

Accessing the admin centers

The **Microsoft 365 admin center** is your gateway to administering your organization's Microsoft services and subscriptions. It's a unified platform where you can manage users, groups, billing, and much more. This first recipe is a guide on how to navigate and utilize the admin centers effectively.

Getting ready

To access the admin centers, you must hold a role with administrative privileges. The Global Administrator role grants you full access across all admin centers. Specific app administrator roles, meanwhile, allow access to relevant app-specific admin centers.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com/>. If you're already signed in to Microsoft 365, you can also access the admin center via the app launcher by selecting **Admin**, as shown in *Figure 1.1*.

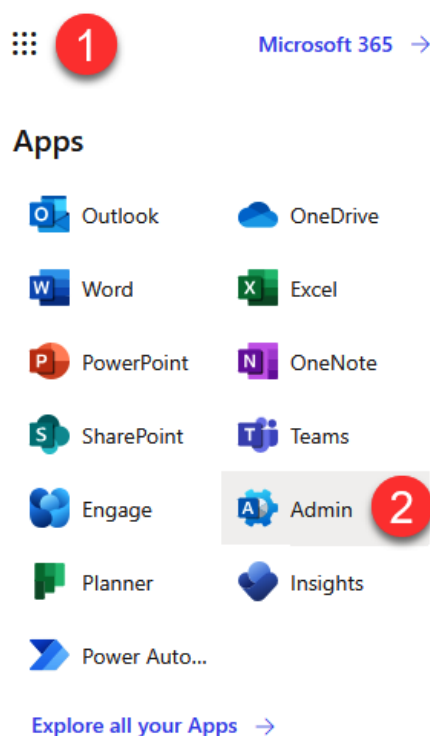


Figure 1.1 – Admin center location from the app launcher

2. Upon entry, explore the left-hand navigation pane, which presents various management options, including user and group management, **Billing**, **Settings**, and **Setup**. These options are your tools for customizing and managing the Microsoft 365 experience for your organization.

Tip

Settings is an important menu option where you can access most of your organization's configuration settings. Take time to explore the **Settings** menu to familiarize yourself with its various sections, such as **Domains**, **Search & intelligence** (for knowledge management), and **Org settings**, which offer a wide range of customization options for themes, organization information, specific app settings, and more.

3. Select **Show all**. You will now see all admin capabilities available to you. Other administrators can also access the Microsoft 365 admin center, but their options may differ if they're not also Global Administrators. For example, only Global Administrators and Billing Administrators may access **Billing**.

4. At the bottom of the navigation pane, you'll find the **Admin centers** section. Here, specialized admin centers for services such as **Exchange**, **SharePoint**, and Microsoft Entra ID (**Identity**) (formerly Azure **Active Directory (AD)**) are available, each providing a detailed suite of settings and options for the respective service.
5. Select **All admin centers**. Once again, depending on your admin roles, your options on this screen may differ. Global Administrators will see all admin centers, as shown in *Figure 1.2*.

















Name	Description
 Azure ATP	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
 Compliance	Use the Microsoft Purview compliance portal to meet your compliance and privacy goals. You'll find integrated solutions that help protect sensitive info, manage data lifecycles, reduce insider risks, safeguard personal data, and more.
 Dynamics 365 Apps	Use the Dynamics 365 admin center to manage your environment, manage capacity, monitor usage and perform other admin operations.
 Endpoint Manager	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
 Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
 Microsoft Entra	Use the Microsoft Entra admin center to manage identities, permissions, and network access.
 Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
 Power Apps	Use the Power Platform admin center to manage activity, licenses, and policies for user-generated Power Apps, which can connect to your data and work across web and mobile.
 Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up connections to web services, files, or cloud-based data and put them to work.
 Power BI	This admin center enables Power BI service admins to manage a Power BI tenant for your organization. The portal includes items such as usage metrics and settings.
 Search & intelligence	Manage Microsoft Search settings including services and content that are available for people in your organization. Make finding internal tools, documents, and people just as easy as searching the web in Bing.
 Security	Use Microsoft 365 Defender for unmatched visibility into threats to your network and your security posture. Respond to incidents, proactively hunt for threats, track your assets, and deploy policies to secure your identities, devices, Office 365 workspaces, apps, and more.
 SharePoint	Manage sites, sharing, storage, and more for SharePoint and OneDrive. Migrate files and sites to Microsoft 365.
 Stream	Choose how Microsoft Stream works for your organization.
 Teams	Configure messaging, conferencing, and external communication options for your users.
 Viva Engage	Manage your Yammer network, set a usage policy, control external network settings, and enable features like translation.

Figure 1.2 – All admin centers accessible via the Microsoft 365 admin center

6. From this screen, you can access all apps and services to adjust individual policies, settings, identities, and more to curate your organization's user experience. We'll explore several of these admin centers throughout this book, but take a moment to explore a couple to get an idea of what sorts of configurations are possible.

How it works...

By default, admin centers are *hidden* behind a **Show all** menu item in the Microsoft 365 admin center. You can pin any of the admin center navigation menu items to always appear in the navigation pane. This makes it so that you don't need to select **Show all** before accessing it next time. *Figure 1.3* shows where the **Pin** feature appears when hovering over a menu node.

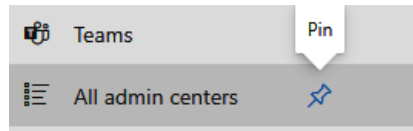


Figure 1.3 – The Pin option for Microsoft 365 admin center navigation options

Learn more about customizing the Microsoft 365 admin center navigation options in this chapter's *Customizing navigation of the admin center* recipe.

Remember that depending on your assigned roles, you may be unable to access certain admin centers. In this recipe, you've discovered where they're all listed and which of them are available to you.

Tip

Check out the last two recipes in this chapter, *Customizing navigation of the admin center* and *Personalizing your admin center home page*, to make your admin experience simpler and more specific to your role.

Also, as you become more familiar with the various admin centers, you'll notice other **uniform resource locators (URLs)** that will save you a couple of selections, such as `security.microsoft.com`, `compliance.microsoft.com`, `TenantName-admin.sharepoint.com`, `admin.powerplatform.microsoft.com`, and so on.

See also

- Learn more about the admin center at <https://learn.microsoft.com/en-us/microsoft-365/admin/admin-overview/admin-center-overview>
- Learn more about specific admin roles and their abilities at <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles>

Setting up PowerShell

PowerShell is a versatile scripting language that offers administrators a powerful toolset for managing Microsoft 365 environments. This recipe outlines the essential steps to prepare your PowerShell environment for administering Microsoft 365, ensuring you have the necessary setup to execute commands and scripts effectively.

Getting ready

Before beginning, ensure PowerShell is installed on your system. Most modern Windows versions come with PowerShell pre-installed. If you're using a different **operating system (OS)** or need to install PowerShell, find guidance relevant to your OS at <https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell>.

Verify your role as a Global Administrator or specific app administrator to ensure you have the necessary permissions to execute the task you wish to perform.

How to do it...

1. Search for **PowerShell** in your **Start** menu, right-click on it, and select **Run as administrator**, as shown in *Figure 1.4*, to open a session with elevated rights.

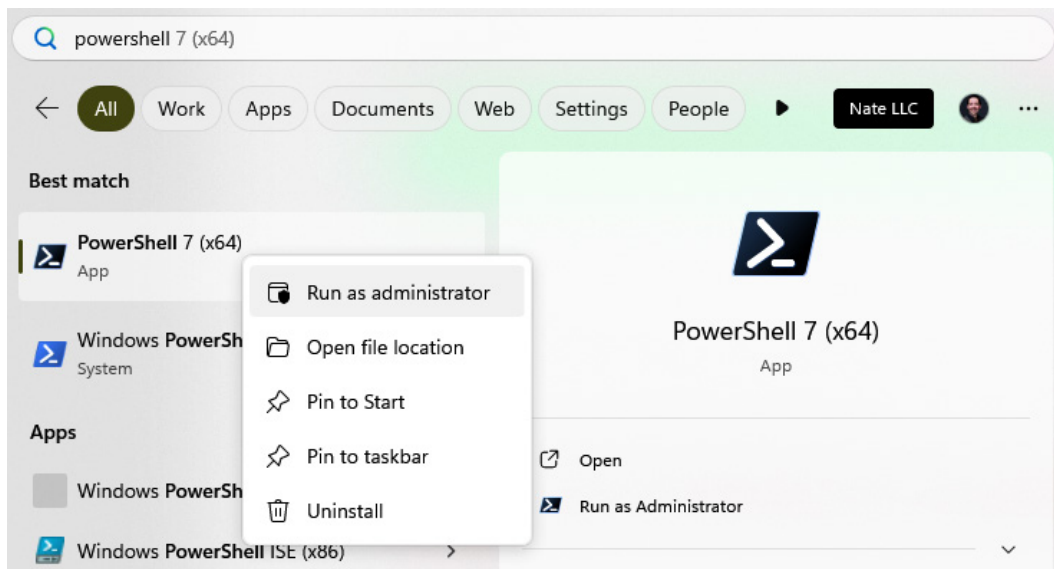


Figure 1.4 – The Run as administrator option appears when right-clicking PowerShell from Start

2. You'll need the **Microsoft Graph PowerShell Software Development Kit (SDK)** to manage Microsoft 365. Run the following command to install the module:

```
Install-Module -Name Microsoft.Graph -Scope CurrentUser  
-AllowClobber
```

If prompted about an untrusted repository, type *Y* and press *Enter* to continue.

Tip

The `-AllowClobber` parameter in PowerShell allows a new module, script, or command being installed to overwrite an existing command or alias that has the same name.

- Before executing management commands, establish a connection to your Microsoft 365 tenant with the following command:

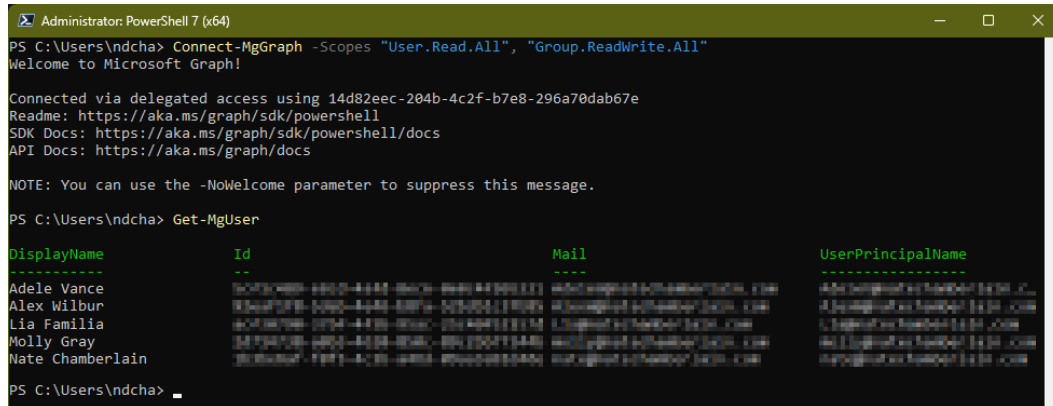
```
Connect-MgGraph -Scopes "User.Read.All", "Group.ReadWrite.All"
```

This command initiates a sign-in process where you'll enter your administrator credentials. If using **multi-factor authentication (MFA)**, which is a best practice and mandatory for some admin locations, such as Azure and Entra, you'll be prompted for additional verification. You'll also be asked to consent to Graph API permissions for yourself, or on behalf of your organization.

- To confirm that your connection is active, try retrieving a list of users or another simple query to ensure responses from the Microsoft 365 services:

```
Get-MgUser
```

Figure 1.5 shows the result of this cmdlet, displaying a list of your users, their GUIDs, email addresses, and user principal names.



```
Administrator: PowerShell 7 (x64)
PS C:\Users\ndcha> Connect-MgGraph -Scopes "User.Read.All", "Group.ReadWrite.All"
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Users\ndcha> Get-MgUser

DisplayName      Id                                     Mail                                     UserPrincipalName
-----
Adele Vance      14d82eec-204b-4c2f-b7e8-296a70dab67e 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com
Alex Wilbur      14d82eec-204b-4c2f-b7e8-296a70dab67e 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com
Lia Familia      14d82eec-204b-4c2f-b7e8-296a70dab67e 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com
Molly Gray       14d82eec-204b-4c2f-b7e8-296a70dab67e 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com
Nate Chamberlain 14d82eec-204b-4c2f-b7e8-296a70dab67e 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com 14d82eec-204b-4c2f-b7e8-296a70dab67e@ndcha.com

PS C:\Users\ndcha>
```

Figure 1.5 – Result of Steps 3 and 4, signing in and retrieving a list of your users

How it works...

With the evolution of Microsoft 365, PowerShell now leverages the Microsoft Graph PowerShell SDK for a more integrated and robust management experience, replacing the older `MSOnline` module. PowerShell 7 or later is recommended when working with Graph PowerShell SDK.

By installing the Microsoft Graph PowerShell SDK and connecting to Microsoft 365 using `Connect-MgGraph`, you gain access to a wide range of cmdlets designed for the efficient management of users, groups, and services within your organization. This setup differs from the older `MSOnline` module by providing a direct interface with Microsoft Graph, which is the unified API endpoint for Microsoft services.

See *Chapter 3, Administering Microsoft 365 with PowerShell*, to dive into the specific administrative actions you can now perform with PowerShell.

There's more...

The `Connect-MgGraph` command supports MFA by default, simplifying the process of connecting to Microsoft 365 in secure environments.

The `-Scopes` parameter in the `Connect-MgGraph` command can be adjusted to match the specific permissions your scripts require to execute their tasks within Microsoft 365.

See also

- Learn more about Microsoft Graph PowerShell at <https://learn.microsoft.com/en-us/powershell/microsoftgraph/overview>

Viewing and filtering the Microsoft 365 roadmap

The **Microsoft 365 roadmap** is a vital tool for administrators and IT professionals to stay informed about new updates, features, and changes across Microsoft 365 services. It is designed to help you manage change and prepare your organization for future updates. This recipe will help you leverage the roadmap to its fullest.

Getting ready

Access to the roadmap is straightforward, requiring only an internet connection. It is publicly available and does not necessitate a login, making it accessible to all for planning and strategic considerations.

How to do it...

1. Navigate to the Microsoft 365 roadmap at <http://roadmap.office.com>. This portal showcases upcoming features and updates across various Microsoft 365 services. *Figure 1.6* shows the landing page of the roadmap.

Microsoft 365 roadmap

Get the latest updates on our best-in-class productivity apps and intelligent cloud services. Rethink productivity, streamline business processes, and protect your business with Microsoft 365.

[Using this roadmap](#)

Search for a specific item:

Filter the items below:

Product Release phase Platform Cloud instance New or updated [Clear all](#)

Showing **1884** updates: [Download](#) | [Share](#) | [RSS](#)

☐ **657 In development** ■■■
Updates that are currently in development and testing

☐ **179 Rolling out** ■■■
Updates that are beginning to roll out and are not yet available to all applicable customers

☐ **1040 Launched** ■■■
Fully released updates that are now generally available for applicable customers

Sort by Rollout date Newest to oldest

> ■■■ **Microsoft Purview compliance portal: eDiscovery (Premium) - CMK (Customer Managed Keys) encryption support for data at-rest in Review sets**

Preview Available: December 2024
Rollout Start: March 2025

Figure 1.6 – Microsoft 365 roadmap landing page

2. Use the search and filters area to tailor the information according to your needs:
 - **Search bar:** Type in a product or feature to see if it's listed.
 - **Product:** As an example, you might select **SharePoint**, **Microsoft Teams**, and **OneDrive** to focus on updates relevant to these core applications.
 - **Release phase:** If your organization has a specific release cadence, such as **Current Channel** or **Targeted Release**, you can filter updates to match this schedule. The default release cadence is **Current Channel**.
 - **Platform:** Filter to specific mobile or desktop platforms.
 - **Cloud Instance:** Choose the cloud instance that applies to your organization, such as **DoD** (Department of Defense), **GCC (Government Community Cloud (GCC))**, or **Worldwide (Standard Multi-Tenant)**, to see features available for your subscription type.
 - **New or updated:** Filter to items new or changed within the last week or month to only see what you may have missed recently.
 - **In development, Rolling out, and Launched:** If you're particularly interested in only items currently rolling out, you can filter to display those only.

3. After applying the necessary filters, you can expand individual features to get more details. *Figure 1.7* shows a filtered roadmap with the first result expanded.

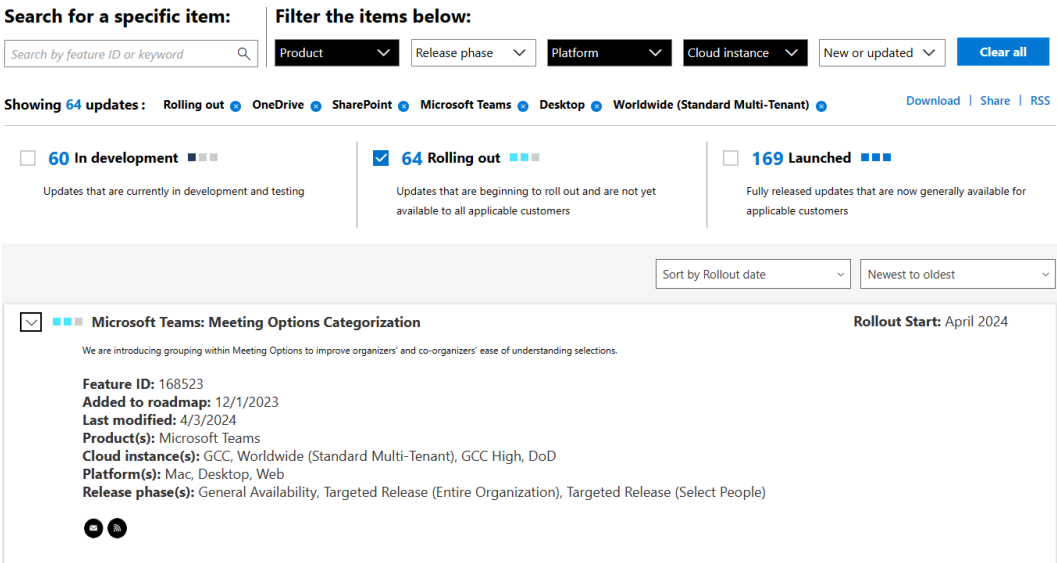


Figure 1.7 – A filtered roadmap with the first result expanded

4. You can view and download the roadmap information as a CSV file by selecting **Download**. This enables offline review and sharing within your organization.
5. Selecting **Share** copies the roadmap URL, including your current filters, so you can show others exactly what you're looking at.
6. **RSS** allows you to subscribe to roadmap updates, just as you might for a blog, so you can automatically post or share updates utilizing **Really Simple Syndication (RSS)** connectors.

How it works...

The roadmap is continuously updated, providing a dynamic look at the development and release process for Microsoft 365 features. Utilizing the provided filters helps narrow down the updates to those most pertinent to your organization's environment, subscription, and compliance requirements. For GCC customers, for example, the roadmap can filter out updates not applicable or features that aren't available due to government compliance restrictions.

See also

- Learn more about how to use the Microsoft 365 roadmap at <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15ouN>

Discovering upcoming changes via Microsoft 365 Message center

The **Microsoft 365 Message center**, accessible via the Microsoft 365 admin center, serves as a crucial hub for monitoring forthcoming changes, new functionalities, and scheduled maintenance tasks pertinent to your organization's deployment. Official communications from Microsoft, including a comprehensive overview and supplementary links for deeper insights, are disseminated through the Message center. This recipe guides you on how to utilize the Message center to stay ahead of upcoming changes.

Getting ready

Accessing the Message center in Microsoft 365 requires assignment to a role with the necessary permissions. While most administrative roles grant access to the Message center, there's also a specific role known as the **Message center reader** role. This particular role is tailored to users who need to view Message center communications but do not require broader administrative capabilities. This approach ensures that a wide range of personnel within your organization, from those with comprehensive administrative responsibilities to those focused solely on monitoring updates and announcements, have access to vital information. Such inclusive access enables your team to stay informed, provide non-technical users with clear expectations and information, and facilitate decision-making and strategic planning based on the latest Microsoft 365 developments and updates.

How to do it...

1. Navigate to the Microsoft admin center by visiting <https://admin.microsoft.com/>.
2. Locate and select **Message center** under the **Health** section, as shown in *Figure 1.8*. This directs you to a comprehensive list of all current announcements and notifications.

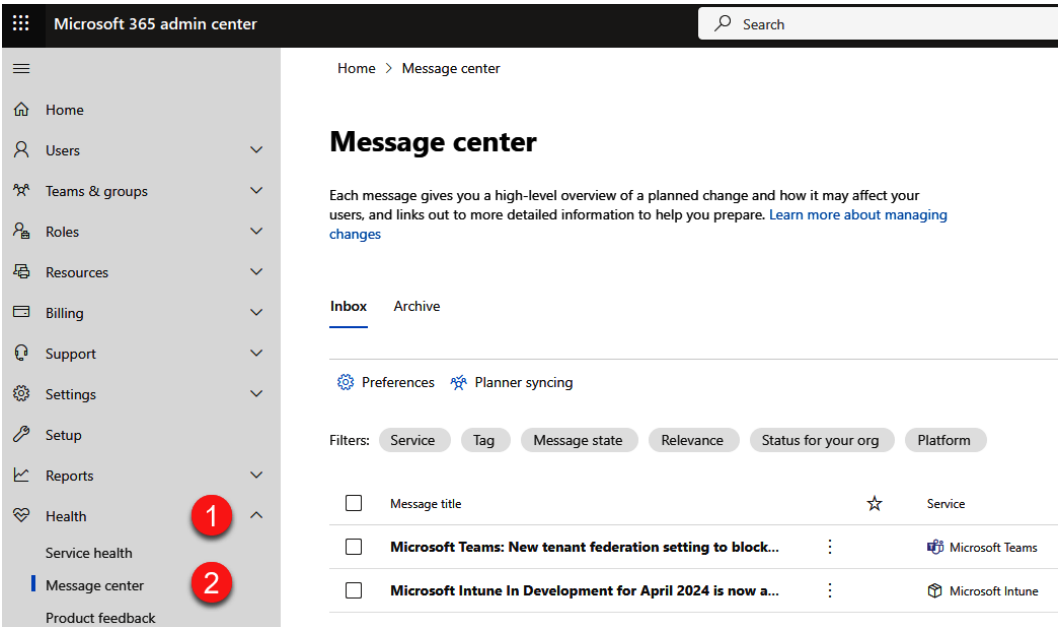


Figure 1.8 – Steps to access the Message center

3. Within the Message center, you can explore active messages, including those flagged as of high importance, or use filters to view messages that are unread or have been archived. You can filter by the following:
 - **Service** (specific apps and services)
 - **Tag** (Major update, Admin impact, User impact, New feature, Feature update, etc.)
 - **Message state** (Favorites, Unread, or Updated)
 - **Relevance** (High, Medium, or Low)
 - **Status for your org** (matches the Microsoft 365 roadmap statuses of **Scheduled**, **Rolling out**, and **Launched** and includes filters for **Changed within last week** and **Changed within last month**)
 - **Platform** (OSs or platform)
4. You can also sort messages to more easily find those of high importance or requiring action. The Message center includes the following sortable columns:
 - **Last updated** (date)
 - **Act by** (date by which action is required)
 - **Relevance** (High, Medium, or Low)

- **Status for your org** (matches the Microsoft 365 roadmap statuses of **Scheduled**, **Rolling out**, and **Launched**)

Select the column's header to sort ascending, and again for descending.

5. Selecting any message title will expand a detailed view on the right side of the screen, presenting in-depth information regarding the update or announcement. *Figure 1.9* is an example of a Microsoft Teams and Planner announcement.

↑ ↓ ×

The new Microsoft Planner app in Microsoft Teams

 Archive  Share  Copy link  Mark as unread

Summary

Microsoft Teams is updating the existing Tasks by Planner and To Do app to the new Microsoft Planner app, which will maintain all existing app functionality and add new options and features to help users be more productive. The new app will start rolling out in late March 2024 and expect to complete by early May 2024. Organizations should update any internal documentation that references the previous app name Tasks by Planner and To Do to use the new app name Planner. Supporting adoption resources will be available on this website starting early March 2024.

Is this summary helpful?  

The new Microsoft Planner is a single, unified work management experience. It brings together the simplicity of Microsoft To Do, the collaboration of Planner, the power of Microsoft Project, and the intelligence of Microsoft Copilot for Microsoft 365 into a single, simple solution that spans from individual task management and frontline task management to enterprise and professional project management.

We are updating the existing Tasks by Planner and To Do app in Microsoft Teams to the new Microsoft Planner app, which will maintain all existing app functionality and add new options and features to help users be more productive.

Learn more about the [new Microsoft Planner announced at Microsoft Ignite 2023](#).

This message is associated with Microsoft 365 Roadmap ID [186964](#).

When this will happen:

The new app will start rolling out in late March 2024 and expect to complete by early May 2024.



How this will affect your organization:

- We are updating the app name for the Tasks by Planner and To Do app in Microsoft Teams to Planner.
- Planner in Teams will maintain all existing functionality of the Tasks app while adding support to access all your plans, the power of Microsoft Project, and the intelligence of Copilot.

Relevance ⓘ

■■■ High

Service & monthly active users ⓘ

 Microsoft Teams (3)  Planner

Platform

Web

Message ID

MC718248

Roadmap ID

[186964](#)

Published

Feb 21, 2024

Tag

ADMIN IMPACT

FEATURE UPDATE

USER IMPACT

Figure 1.9 – A Message center announcement about Planner and Microsoft Teams

Messages often include a lot of information:

- Related roadmap item ID
- Services involved
- Description of the change
- When it will happen
- How it affects your organization
- How to prepare for the change
- Links to additional documentation

How it works...

The Message center is your gateway to the most current updates, feature releases, and maintenance notifications relevant to Microsoft 365 services. It's designed to provide administrators with a centralized overview of important information, facilitating informed decision-making and proactive management of the Microsoft 365 environment.

Upon selecting a message, various options become available. You can share insights directly from the Message center via the **Share** option, keep certain messages in focus by marking them as **Unread**, and express feedback through the **Like/Dislike** buttons. Moreover, it's possible to archive messages or explore further through additional links provided within each message for more comprehensive details.

There's more...

Leveraging the Message center reader role can be particularly effective for keeping key personnel within your organization informed about imminent changes, enabling them to prepare and respond appropriately.

For administrators on the move, the **Microsoft 365 Admin mobile app** offers access to the Message center, ensuring you remain informed regardless of your location. Download the app via <https://go.microsoft.com/fwlink/p/?linkid=627216>.

Also in the Message center, you may notice the button shown in *Figure 1.10* for **Planner syncing**.

Message center

Each message gives you a high-level overview of a planned change and how it may affect your users, and links out to more detailed information to help you prepare. [Learn more about managing changes](#)

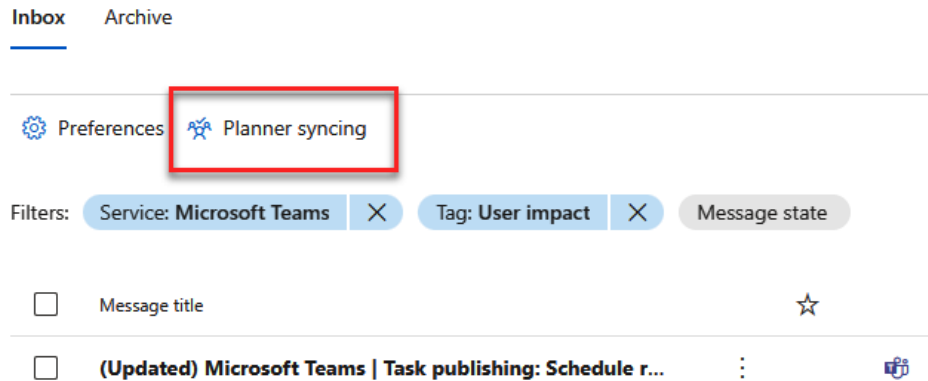


Figure 1.10 – Planner syncing option in Message center

Selecting this option opens a wizard where you can set up automatic creation of tasks for messages meeting your specified criteria (such as major updates only for specific services). *Figure 1.11* shows this screen of the wizard where you configure the message filter.

Planner syncing

☒ Plan

☒ **Messages**

☐ Import

☐ Finish

Choose which messages to sync

Messages that you sync become tasks in Planner. Data privacy messages won't sync to Planner.

☐ All updates
You can still exclude updates from specific categories, products, and services.

☒ Only major updates
Major updates are marked with a red exclamation mark (!). You can still exclude updates from specific categories, products, and services.
[Learn how major updates are defined](#)

Include messages in these categories *

☒ Prevent or fix issues
Messages about known issues that may require action to avoid disruptions.

☒ Plan for change
Messages about changes that will happen at least 30 days in the future and that may require action to avoid disruptions.

☒ Stay informed
Messages about new or updated features that don't require any action to prepare.

Include messages about these products or services *

☐ Azure Information Protection

☒ Basic Mobility & Security

☐ Dynamics 365 Apps

☒ Exchange Online

☒ General announcement

☒ Microsoft 365 Apps

Figure 1.11 – Choosing which messages to sync to Planner

Once tasks are created, you can assign them to individuals with deadlines. This is especially helpful for messages with **Act by** dates. You can create a new plan for these tasks or choose an existing plan. All Message center messages you choose to include during setup will be added to one chosen bucket of that Planner plan.

See also

- Learn more about the Message center, including which roles are included and excluded for access, at <https://learn.microsoft.com/en-us/microsoft-365/admin/manage/message-center>

Opening a service request

Service requests are the formal way of seeking Microsoft's assistance with any issues encountered in Microsoft 365. This process is essential for discussing and resolving problems effectively. This recipe will show you how to create a new service request.

Important note

Microsoft offers different levels of support with varying **service-level agreements (SLAs)**:

Standard Support: This offers a basic level of service with longer response times.

Unified Support: This provides enhanced SLAs, including faster response times and more comprehensive support options, often at an additional cost. This level of support is ideal for organizations with mission-critical needs that require rapid resolutions.

Understanding the differences in SLAs between Standard and Unified Support can help set expectations for response times and service quality when submitting a service request.

Getting ready

Creating service requests requires Microsoft 365 administrative privileges. Ensure you have an eligible admin role to proceed.

How to do it...

1. Start by visiting the Microsoft 365 admin center at <http://admin.microsoft.com>.
2. Select the teal **Help & support** button at the screen's lower-right corner or navigate through the left menu: **Show all** | **Support** | **Help & support**.
3. A side panel opens. Initially, you'll describe your issue to see if any available self-service documentation may solve your issue. Type in *Switch* subscription and press *Enter*.

4. The results will attempt to provide solutions or direct resources, as shown in *Figure 1.12*.

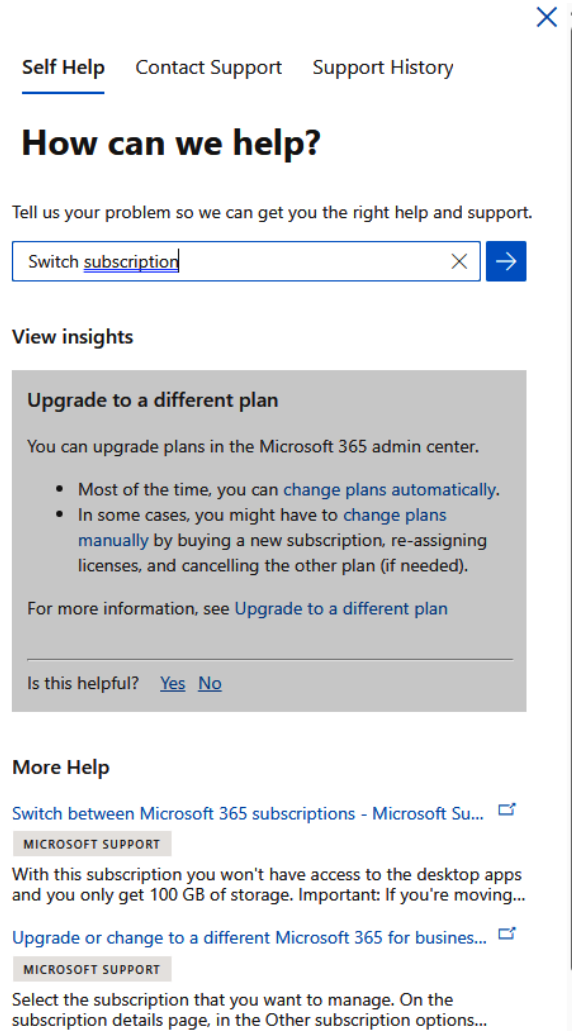


Figure 1.12 – Results for Switch subscription in Help & support

5. If the issue remains unresolved, you'll have the option to contact support by selecting the button in the lower-left corner of the panel. Select **Contact support**.
6. Fill in your service request's specifics, attaching any relevant screenshots or files. You can include the following information:
 - **Title**
 - **Description**

- Contact phone number
 - Authorized contact for Microsoft to work with
 - Call recording consent
 - **Preferred contact method (Phone or Email)**
 - **Attachments** (supports files, screenshots, or videos)
 - **Regional settings** (timezone and language)
 - **Accessibility settings** (open text for description of needs)
7. Select **Contact me** to submit your request. A confirmation of your request will be shown, as seen in *Figure 1.13*.

[Help](#) [Support History](#)

Service request

Switch subscription (#2404070040001857)

Open • Sev C

Created by Nate Chamberlain on 4/7/2024 at 03:22 PM

This is a test request ticket for demonstration purposes.

Service request opened

4/7/2024, 3:22:51 PM

A support agent is being assigned to your request.

Agent assigned

Issue resolved

Service request details

Name	Nate Chamberlain
Phone	+1-425-██████████
Email	██████████@██████████.com

[View case communications](#)

Timezone

(UTC-05:00) Central Time (US & Canada)

Alternate language

English (United States)

Figure 1.13 – Confirmation of service request submission

How it works...

This process is designed to expedite resolutions by first directing you through automated solutions, potentially saving time. If these initial steps don't address your concern, the option to engage directly with Microsoft support ensures you're not left without recourse. This method aims to use Microsoft's and your own time efficiently, streamlining the path to resolution.

Monitoring service request status

Once you've submitted a service request, managing and tracking its progress becomes crucial, especially when handling multiple requests. In this recipe, you'll find previously submitted service requests to check on their status or make changes.

Getting ready

Creating service requests requires Microsoft 365 administrative privileges. Ensure you have an eligible admin role to proceed.

How to do it...

1. In the Microsoft 365 admin center (<http://admin.microsoft.com>), go to **Show all | Support | View service requests**. You'll see all of your service requests listed along with their current status, as shown in *Figure 1.14*.

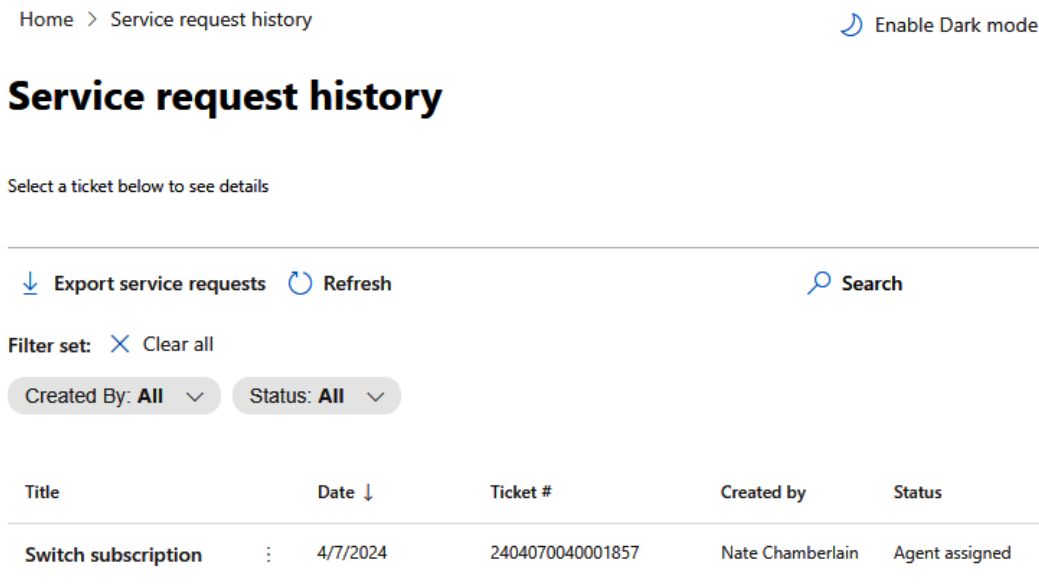








Figure 1.14 – Service request history



2. This screen allows you to export the last 13 months of service requests as CSV and search or filter your service requests, providing a clear view of their statuses.
3. By selecting a request, you can access detailed case notes and the request's history, including all communications, offering insights into the issue's resolution process. *Figure 1.15* shows the details for a request where you can also see the **Edit** option.


Home > Service request history > Switch subscription

 Enable Dark mode

Switch subscription

Ticket #	Date opened	Status	Description
2404070040001857	4/7/2024, 3:22:51 PM	Agent assigned	This is a test request ticket for demonstration purposes.
Created by	Phone	Email	
Nate Chamberlain	+1-425 	   	

 Refresh  Edit

 Expand all  Collapse all

Case notes

Subject	Sender	Received
Switch subscription - TrackingID#2404070040001857	support@mail.support.microsoft.com	4/7/2024, 3:24:20 PM
Case 2404070040001857 Your question was successfully submitted to Microsoft Support TrackingID#2404070040001857	support@mail.support.microsoft.com	4/7/2024, 3:22:57 PM

Figure 1.15 – Service request details

How it works...

The **Service request history** screen in the admin center facilitates easy tracking and management of your requests. It's designed to aid in identifying recurring issues, reporting on resolutions, and ensuring effective communication within your organization regarding service request outcomes.

There's more...

Editing an existing request is also straightforward. Here are the steps:

1. In the Microsoft 365 admin center (<http://admin.microsoft.com>), go to **Show all | Support | View service requests**.
2. Select your request.

3. Select **Edit** to provide additional information or update contact information. *Figure 1.16* shows the **Edit** panel with limited options to update.

[Help](#) [Support History](#)

Edit request

Switch subscription (#2404070040001857)

Open • Sev C

Created by Nate Chamberlain on 4/7/2024 at 03:22 PM

This is a test request ticket for demonstration purposes.

Attachments ?

[Add a file or screenshot or video](#)

Notes

Add a note

Confirm your number*

+1

425

Confirm email addresses of authorized contacts* ⓘ

Microsoft will work directly with contacts listed to resolve this service request.

Consent to the recording of all calls necessary to resolve this service request. This can be changed at any time.* ⓘ

No

Figure 1.16 – Edit options for an existing service request

You will be able to add additional notes at any time, as well as adjust your contact number, email, and recording consent preference.

4. Select **Save** to update the service request.

Adding a domain

To personalize or brand your tenant to your company, you can integrate a custom domain, such as `contoso.com`, with Microsoft 365. This elevates your organizational identity by replacing the generic `onmicrosoft.com` addresses (e.g., `nate@contoso.onmicrosoft.com`) with a branded email format (e.g., `nate@contoso.com`). This adjustment also extends to utilizing your domain with Microsoft 365 services, such as Outlook. In this recipe, we outline how to add the `natechamberlain.com` domain (or any custom domain) to your Microsoft 365 tenant.

Getting ready

To add a domain, having the Global Administrator role is required. It's not necessary to own a domain prior to this process, as there's an option to purchase during the setup.

How to do it...

1. Access the Microsoft 365 admin center by visiting `http://admin.microsoft.com`.
2. Navigate through **Show all | Settings | Domains**.
3. Here, as seen in *Figure 1.17*, you can either add an existing domain you own or purchase a new one. Select **Add domain** for this recipe.

Home > Domains

Domains

+ Add domain Buy domain Refresh		
Domain name ↑		Status
<input type="checkbox"/>	chambernate.onmicrosoft.com (Default)	✓ Healthy

Figure 1.17 – Domains screen of Microsoft 365 admin center

4. Submit the domain name you wish to add, for instance, `natechamberlain.com`, and then choose **Use this domain**.

5. To enable features such as email, you must update your **Domain Name System (DNS)** records at your domain registrar or hosting provider. Microsoft 365 can automate this for supported registrars (e.g., WordPress, GoDaddy). If this is possible for you, it will ask you to sign in to your registrar to verify before returning you to the wizard. You can also manually enter the required DNS records provided by Microsoft 365. The wizard screen shown in *Figure 1.18* will guide you to the appropriate action for your specific scenario if it can't be automated, or you choose not to use the automated method.

Domains > Add domain

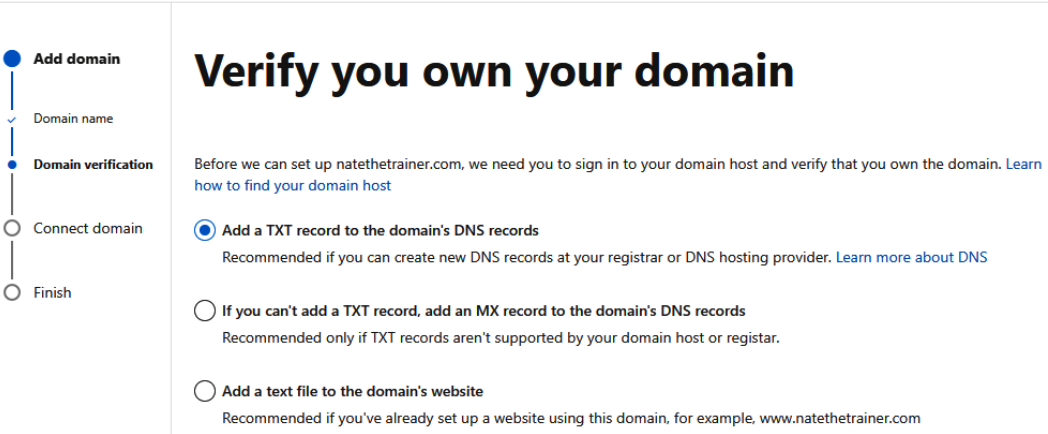


Figure 1.18 – Domain verification steps of adding a domain

6. After updating DNS records, proceed through the setup wizard to finalize the domain's integration with services such as Exchange and Teams, concluding by selecting **Done**.

How it works...

Adding your domain to Microsoft 365 directs your domain's email traffic to Microsoft 365, facilitating the use of Outlook for email services and allowing users to log in to Microsoft 365 services with your branded domain. This setup enhances your organizational presence and user experience.

Important note

For organizations with multiple domains or subdomains, Microsoft 365 supports the management of secondary email addresses, policies, and licenses. This flexibility is particularly useful in scenarios involving acquisitions, where integrating and managing new domains or creating specific subdomains (e.g., `staff.contoso.com`) is required.

There's more...

An alternative method to set up a custom domain you or your company already own is to follow these steps:

1. Access the Microsoft 365 admin center by visiting <http://admin.microsoft.com>.
2. Navigate through **Show all | Setup** and then select **Get your custom domain set up** from the **Sign-in and security** section, as shown in *Figure 1.19*.

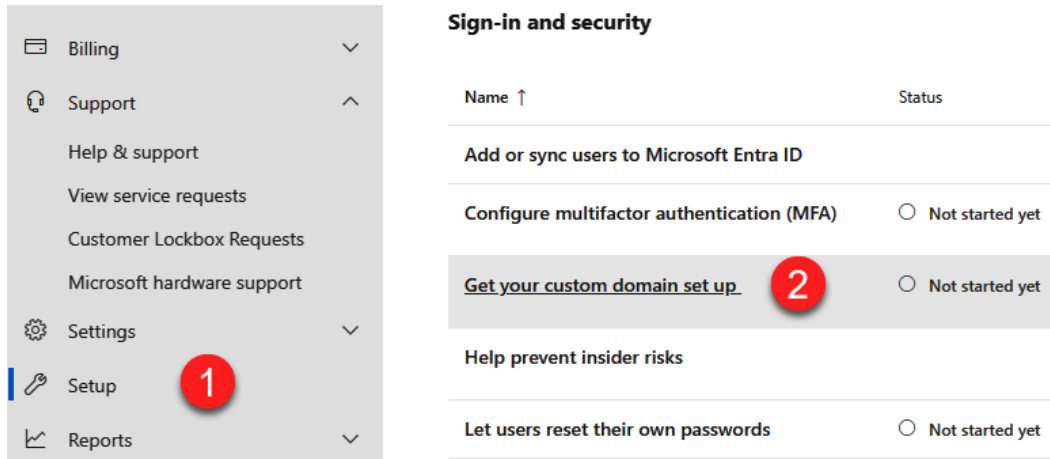


Figure 1.19 – Custom domain setup location

3. Select **Get started**. The same wizard from this section's recipe opens to guide you through the process of connecting your existing domain. All remaining steps are the same.

Note that this method does not permit you to purchase a new domain – only to connect your existing one.

See also

- For a comprehensive guide on adding a domain to your Microsoft 365 subscription, including detailed DNS configuration steps, visit <https://learn.microsoft.com/en-us/microsoft-365/admin/setup/add-domain>
- Complete a short learning module on custom domains where you can learn more about custom domains and DNS zones and records, as well as subdomains at <https://learn.microsoft.com/en-us/training/modules/add-custom-domain-microsoft-365/>

Changing the domain for users

After adding a custom domain to Microsoft 365, or in scenarios involving multiple domains, such as company acquisitions or rebranding, you may need to update the domains of existing users. This change affects users' email addresses and login credentials, which could impact scheduled meetings. Communication with affected users before making these changes is crucial for a smooth transition. For this recipe, you'll learn the process for updating the domain for selected users.

Getting ready

This task requires Microsoft 365 administrative privileges to modify user domain settings.

How to do it...

1. Begin by navigating to the Microsoft 365 admin center at `http://admin.microsoft.com`.
2. Proceed to **Users | Active users**. Here, you can change the domain for one or multiple users.
 - For one user, use the users ellipsis to select **Manage sign-in details**, as shown in *Figure 1.20*. Note you can also change their alias or, essentially, their entire email address this way.

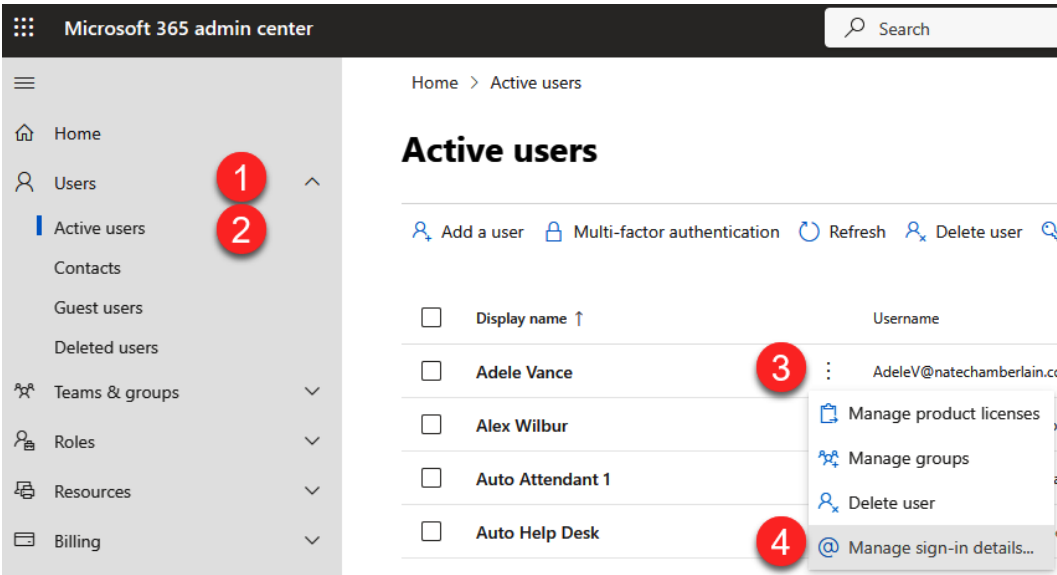


Figure 1.20 – Steps to change the domain for a single user


- For multiple users, multi-select the users whose domain you intend to change by selecting the checkbox next to their name, then select the **Change domains** option.

- When multi-selecting users to change domains, a panel opens on the side where you can choose from the available options to select the new domain for the users, as shown in *Figure 1.21*. A disclaimer highlighting the implications of this change will be shown.

Change domains

2 users selected ⓘ

Domain



Select a domain ▼

Select a domain

natechamberlain.com

natechamberlain.onmicrosoft.com

Figure 1.21 – The Change domains panel for multiple users

- After reviewing the disclaimer, confirm your decision by selecting **Save changes**.

How it works...

Changing a user's domain directly updates their associated email address and login credentials. Such modifications are relatively rare, and often reserved for significant organizational changes, such as mergers, rebranding, or internal reallocations. Upon confirmation, the update takes immediate effect, necessitating prompt communication with affected users to ensure they use their new login details and share the updated email addresses accordingly.

Important note

The previous domain, including the default onmicrosoft domain, can be retained as an email alias and fallback domain. This ensures that emails sent to the former address are automatically redirected to the new primary email, maintaining continuity of communication.

See also

- Read more about changing email addresses to use custom domains at <https://learn.microsoft.com/en-us/microsoft-365/admin/email/change-email-address>
- For further details on changing a user's name and email address, including step-by-step guidance and additional considerations, visit <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/change-a-user-name-and-email-address>

Assigning a license to a user

User capabilities within your Microsoft 365 environment are determined by the specific license types assigned to them. From fundamental operations, such as navigating the tenant and sending emails, to utilizing various applications, such as those in the Power Platform, licenses play a crucial role in enabling these functionalities. For example, E3 licenses do not include Power BI Pro licenses, whereas E5 licenses do. This recipe guides you on how to allocate product licenses to users efficiently through the Microsoft 365 admin center.

Getting ready

Assigning licenses necessitates having one of the administrative roles equipped to perform this action, such as Global Administrator or License Administrator.

All Microsoft 365 users in your tenant need to have a Microsoft 365 license assigned to them. These should be purchased through the Microsoft 365 admin center’s **Billing** section or your third-party provider. You can check your available license counts by going to **Billing | Licenses**.

How to do it...

1. Visit the Microsoft 365 admin center at `http://admin.microsoft.com`.
2. Navigate to **Users | Active users** and select the individuals you intend to assign licenses to, then opt for **Manage product licenses**. In *Figure 1.22*’s example, new employees Adele and Alex are selected.

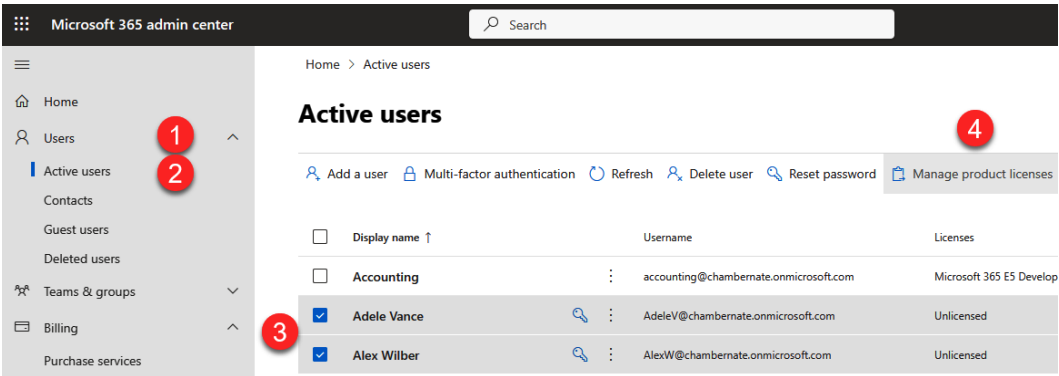


Figure 1.22 – Steps to manage product licenses for multiple users

3. A side panel will give you the **Replace**, **Assign more**, or **Unassign** options for the selected users. Since our new employees Adele and Alex don’t have any assignments currently, select **Assign more**.

4. Identify and select the desired product license for the user, confirming your choice by selecting **Save changes**.

Manage product licenses

2 users selected ⓘ

What would you like to do with the licenses for these users?

- ☐ Replace
Unassign existing licenses and assign new ones.
- ☒ Assign more
Keep the existing licenses and assign more.
- ☐ Unassign all

Licenses (1) ^

☐ **Microsoft Power Automate Free**
9994 of 10000 licenses available

☒ **Microsoft 365 E5 Developer (without Windows and Audio Conferencing)**
4 of 25 licenses available

Apps (71) ^

Show apps for:

All licenses v

☒ Select all

Save changes

Figure 1.23 – Product licenses being assigned to users

Note that Microsoft 365 licenses include many apps. As *Figure 1.23* shows, 71 apps are included by assigning a single Microsoft 365 E5 license. You can uncheck most of the 71 apps if you wish to restrict access to certain products, such as Power BI or Sway.

5. Select **Save changes**. A screen appears summarizing the actions taken.

How it works...

Through the **Users** section of the Microsoft 365 admin center, administrators have the ability to audit, allocate, or retract licenses for individual or multiple users. Opting for certain licenses, such as those for Enterprise plans, grants users access to a comprehensive suite of Microsoft products automatically. Alternatively, specific licenses allow for more granular control over app access, catering to diverse user needs within the organization.

There's more...

Managing licenses on an individual basis can be labor-intensive. For efficiency, Microsoft 365 supports bulk license assignments either through selecting multiple users simultaneously, importing a CSV file with user details, or executing PowerShell scripts. These bulk operations facilitate streamlined license management across your organization, significantly reducing the administrative overhead.

This approach to license assignment underscores the importance of understanding and managing Microsoft 365 licenses to ensure users have the necessary tools for their roles, while also offering administrators scalable solutions for license management.

See also

- Learn more about assigning and unassigning licenses for users at <https://learn.microsoft.com/en-us/microsoft-365/admin/manage/assign-licenses-to-users>
- Compare licenses at <https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products>

Assigning a license to a group

Assigning licenses to one or a few individuals is typical if a new hire is added or someone leaves the organization. However, for organizations of any size, managing licenses individually can be cumbersome when actions are needed in bulk. Utilizing groups for license assignment streamlines the process, especially for modifications that affect all members of a group. This recipe demonstrates the efficient assignment of licenses to groups, such as making sure all members of accounting have access to Power Automate.

Getting ready

Assigning licenses to a group requires administrative privileges, specifically roles such as Global Administrator or License Administrator. Additionally, your tenant must possess sufficient available licenses for assignment.

How to do it...

1. Navigate to Microsoft Entra admin center at <https://entra.microsoft.com>.
2. Within the Microsoft Entra ID section, locate and select **Billing | Licenses**.
3. Select **All products** to review the licenses your tenant has available.
4. Identify the desired license type and select it.

5. Proceed by selecting **Assign**, as shown in *Figure 1.24*.

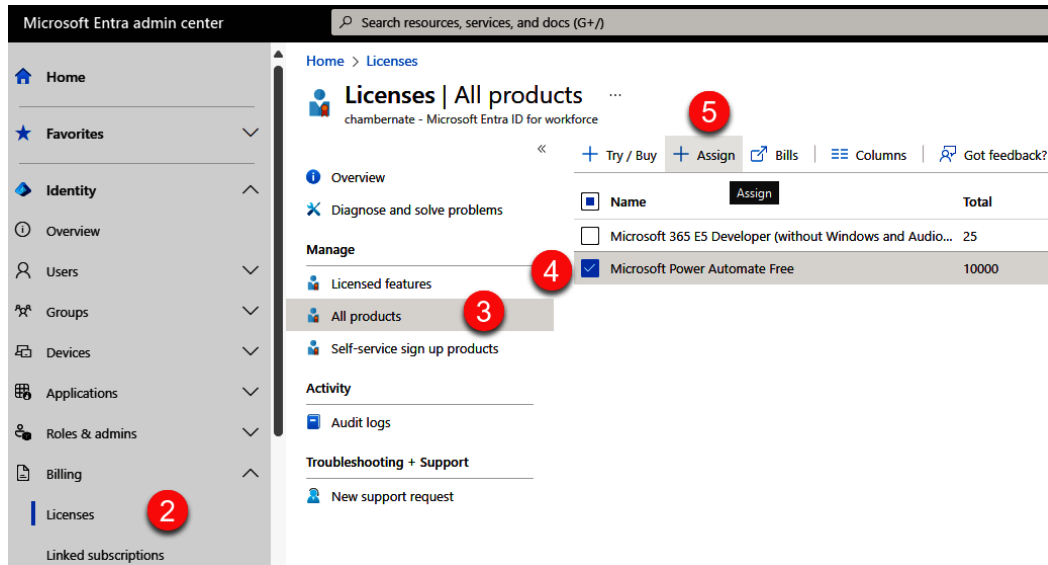


Figure 1.24 – Initial steps to assign product licenses to groups in Microsoft Entra admin center

6. Select **Add users and groups** under the **Users and groups** section, search and select the groups to which you wish to assign the license, and then confirm your selection by choosing **Select**.
7. Adjust any necessary assignment options to tailor the license features for the group. For example, you can turn **Common Data Service** (Dataverse) and **Flow Free** *on* or *off* when assigning the **Microsoft Power Automate Free** licenses.
8. Select **Review + assign**, review your pending action, and then complete the process by selecting **Assign**.

How it works...

By leveraging **Microsoft Entra ID** for group-based license assignments, the process is significantly expedited compared to individual assignments. Microsoft Entra ID automates the assignment, processing each group member sequentially. Depending on the group size, this may take some time, and usually applies within 15 minutes.

A completion notification will appear once the process concludes. Any issues encountered during the assignment, such as conflicts with existing licenses, are detailed in the notification for further review.

See also

- For verification of group license assignment completion, detailed guidance is available at <https://learn.microsoft.com/en-us/entra/identity/users/licensing-groups-assign#step-2-verify-that-the-initial-assignment-has-finished>
- To address and resolve license assignment issues, consult <https://learn.microsoft.com/en-us/entra/identity/users/licensing-groups-assign#step-3-check-for-license-problems-and-resolve-them>
- For information on known issues with group-based license management in Microsoft Entra ID, review <https://learn.microsoft.com/en-us/entra/identity/users/licensing-group-advanced>

Customizing navigation of the admin center

For administrators who frequently access specific admin centers within Microsoft 365, customizing the navigation menu of the Microsoft 365 admin center to make these links readily accessible can significantly enhance efficiency. This recipe focuses on ensuring that the Microsoft Entra, Exchange, and SharePoint admin centers are prominently displayed in your navigation menu without having to first select **Show all**.

Getting ready

To customize the admin center navigation, you must hold an administrative role, such as Global Administrator. Many administrator roles can access the admin center, but their options differ based on their specific role. For example, a SharePoint Administrator who is not also a Teams or Global Administrator will not see the Teams admin center option.

Note that customizations made to Microsoft 365 admin center navigation are specific to the logged-in user, so your customizations won't affect other administrators who may have made unique customizations to their own admin center navigation experience.

How to do it...

1. Visit the Microsoft 365 admin center at <http://admin.microsoft.com>.
2. Select the **Show all** link in the navigation pane.
3. Select the pushpin icons next to **Identity** (Microsoft Entra ID), **Exchange**, and **SharePoint**. *Figure 1.25* reflects this action.

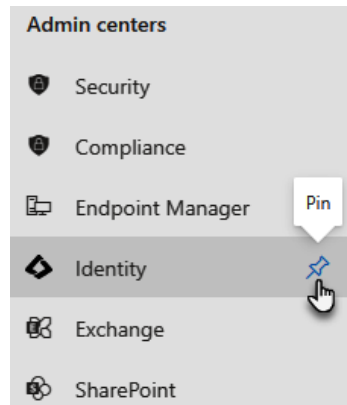


Figure 1.25 – Option to pin something normally hidden in the admin center navigation

4. When finished, your selected admin centers will be directly visible on the main navigation pane, as shown in *Figure 1.26* when visiting the admin center. The **Show all** link remains just as before as an option to expand and view additional admin centers and options that haven't yet been pinned.

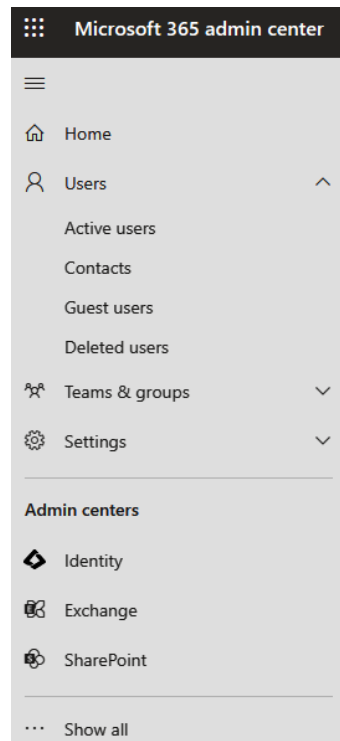


Figure 1.26 – Customized navigation in the Microsoft 365 admin center

How it works...

By choosing to pin and unpin nodes in the navigation pane, you effectively tailor the Microsoft 365 admin center to fit your specific administrative needs, ensuring quick access to frequently used admin centers, such as Microsoft Entra, Exchange, and SharePoint. *Figure 1.26* shows the result of pinning three admin centers and unpinning other nodes not needed as often (such as **Billing** and **Setup**). Notice how it makes their navigation less cluttered and easier to use on a regular basis for their most frequently needed items.

This personalization does not limit the visibility of other admin centers, as the **Show all** link will still allow you to explore the full range of admin centers available.

Customizing the admin center navigation streamlines your workflow by reducing the time spent searching for frequently used tools, making your administrative tasks more efficient and focused. This feature is especially beneficial in a growing ecosystem such as Microsoft 365, where the ease of access to necessary functions can significantly impact daily operations.

Personalizing your admin center home page

As the complexity and functionality of applications evolve, so does the necessity for streamlined access to vital tools and tasks. The Microsoft 365 admin center addresses this by allowing for a highly customizable home page, enhancing both accessibility and efficiency. This customization extends beyond aesthetic adjustments, providing practical shortcuts to frequent administrative tasks, such as adding users and resetting passwords. This recipe shows you how you can tailor your admin center home page to fit your specific needs.

Getting ready

To customize the admin center home page, you must hold an administrative role, such as Global Administrator. Many administrator roles can access the admin center, but their options differ based on their specific role.

Note that customizations made are specific to the logged-in user, so your customizations won't be visible to other administrators who may have made different customizations to their own admin center home page experience.

How to do it...

1. Start by navigating to the Microsoft 365 admin center at <http://admin.microsoft.com>.
2. You can first remove any existing card on your dashboard you don't always want there by selecting the ellipsis (...) in the upper-right corner of the card, and then selecting **Remove**. For this recipe, try removing all cards to start with a blank home page.

3. Next, look for the **Customize dashboard** option located on the ellipsis (...) along the top ribbon menu, as shown in *Figure 1.27*.

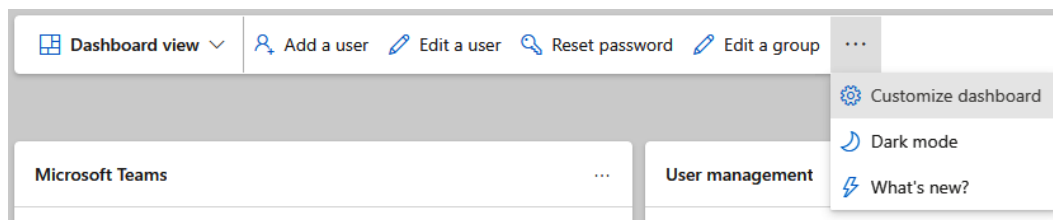


Figure 1.27 – Customize dashboard option location

4. You can personalize your dashboard by dragging and dropping your preferred cards or by selecting the plus sign (+) on a card to add it directly to your home page where you can drag to rearrange it as well. Card options include the following:
 - **App updates**
 - **Billing**
 - **Domains**
 - **Manage What's New messages**
 - **Message center**
 - **Microsoft 365 active users report**
 - **Microsoft 365 apps**
 - **Microsoft Entra**
 - **Role-based access for admins**
 - **Service health**
 - **Setup**
 - **Teams**
 - **Training and guides**
 - **Update Compliance Reporting**
 - **User management**
5. Add the cards for **Message center**, **Microsoft Entra**, **Microsoft 365 active users report**, **Teams**, and **Service health**. Drag and drop them to arrange them how you wish.

6. Notice in *Figure 1.28* how this updated dashboard highlights upcoming changes and allows for easy user additions and edits, password resets, reports on user activity, and more. Your admin center dashboard can be specifically tailored to your responsibilities and interests.

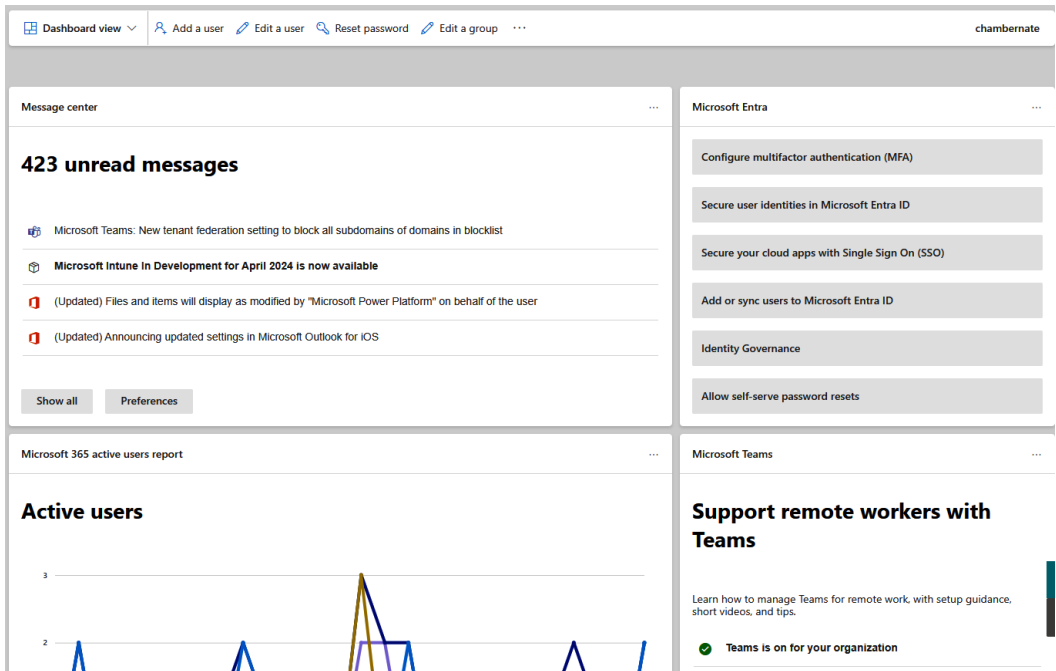


Figure 1.28 – Customized Microsoft 365 admin center home page

How it works...

By adding specific data cards to your home page, you gain instant access to the most relevant and frequently used information and functionalities without navigating or scrolling through multiple menus and irrelevant featured items. This level of customization allows for more efficient administration by centralizing crucial data and tasks.

While the customization options are bound by the preconfigured selections provided by Microsoft, these options cover a broad spectrum of administrative functionalities, enabling the creation of a comprehensive and powerful dashboard tailored to your operational needs with convenient shortcuts to your favorite places.

Tip

Administrators also have the capability to modify the overall theme of the tenant's admin center, including toggling between light and dark modes, further personalizing the user experience to suit preferences, and enhancing visibility.

By following the steps in the last two recipes of this chapter, you can significantly enhance your efficiency and ease of navigation within the Microsoft 365 admin center, ensuring that the most important tasks and information are always just a selection away.

There's more...

Your Microsoft 365 admin center home page defaults to **Dashboard view**. If you change the drop-down selection shown in *Figure 1.29* from **Dashboard view** to **Health**, you'll have an entirely separate home page experience that focuses on service health for your organization.

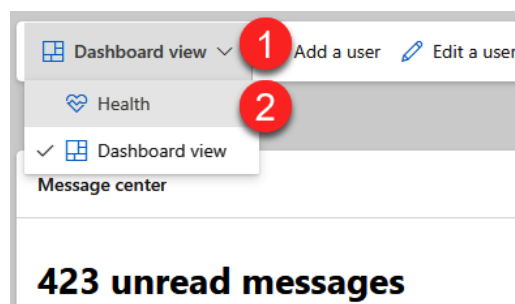


Figure 1.29 – Option to switch from Dashboard view to Health

Health can't be customized in the same way as **Dashboard view**, but it contains valuable information and cards, including the following:

- Critical alerts
- Service health and usage
- Microsoft 365 app updates
- Recommended actions

Tip

It's recommended to check service health daily for any ongoing Microsoft 365 issues that may be impacting your tenant and its users.

You can toggle back and forth between your custom **Dashboard view** and the standard **Health** view at any time.

2

Microsoft 365 Identity and Roles

At the heart of every administrative action within Microsoft 365 lie users and groups. They are not just elements within your administrative domain but are the foundation upon which security, licensing, and user experience enhancements are built. Thoughtful provisioning and management of these entities are important before embarking on policy creation or configuring specific features within the admin centers.

This chapter dives into the essentials of Microsoft 365 identity management, guiding you through the process of user and group creation and management. It will equip you with the knowledge to enhance your organization's security posture through measures such as enabling **multi-factor authentication (MFA)**. Additionally, we will navigate the assignment of administrative roles, a critical step in delineating responsibilities and access within your tenant.

The recipes we will explore in this chapter are as follows:

- Creating a new user
- Importing users in bulk
- Creating a new Microsoft 365 group
- Enabling security defaults (MFA) in Entra ID
- Exporting users
- Managing guest users
- Creating a user template
- Restricting users from creating new Microsoft 365 groups
- Assigning the User Administrator role
- Managing admin roles in the Microsoft 365 admin center

Technical requirements

This chapter requires that users possess administrative privileges within Microsoft 365. Individuals holding the Global Administrator role will have the ability to execute all tasks detailed in each recipe. Meanwhile, administrators assigned to specific applications or functions within the platform will find that they can perform a vast majority of the tasks outlined, and it will be noted when other roles may perform a function. There are no installations or downloads required to follow along with the recipes in this chapter.

Creating a new user

Setting up a new user in Microsoft 365 is an important task for administrators, enabling new employees or team members to access essential Microsoft services. In this recipe, you'll create a single new user in your organization via the Microsoft 365 admin center.

Getting ready

You need access to the Microsoft 365 admin center with a user role that allows you to add and configure new users, such as Global Administrator or User Administrator.

How to do it...

1. Access the Microsoft 365 admin center by navigating to `https://admin.microsoft.com`.
2. In the admin center, navigate to **Users | Active users**, then select **Add a user**, as shown in *Figure 2.1*.

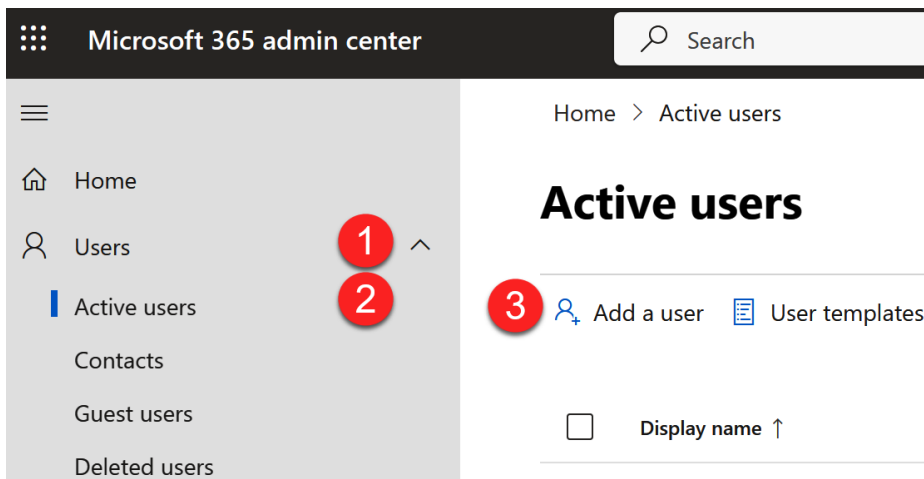


Figure 2.1 – Steps to add a user in the Microsoft 365 admin center

3. On the **Set up the basics** screen that appears, enter the user’s name, display name, and username. Also, specify the domain for the user’s account.

Note

The default domain for new tenants always ends in *.onmicrosoft.com*.

4. Choose **Automatically create a password** or create your own password and decide whether the user must change their password on the first login. You can also opt to send the password by email to the user. These options can be seen in *Figure 2.2*.

Add a user

● Basics

○ Product licenses

○ Optional settings

○ Finish

Set up the basics

To get started, fill out some basic information about who you're adding as a user.

First name

Last name

Nate

Chamberlain

Display name *

Nate Chamberlain

Username *

Domains

nate.chamberlain

@

chambernate.onmicrosoft.com

☒ Automatically create a password

☒ Require this user to change their password when they first sign in

☐ Send password in email upon completion

Next

Figure 2.2 – Set up the basics screen for adding a new user

5. Select **Next** to save and navigate to the **Assign product licenses** section. Here, select the appropriate licenses for the user, as shown in *Figure 2.3*. You can also modify the specific apps and services the user will have access to within the assigned licenses by expanding the **Apps** section and deselecting anything you want to remove.

Add a user

Basics

Product licenses

Optional settings

Finish

Licenses (1) *

☒ Assign user a product license

☒ **Microsoft 365 E5 Developer (without Windows and Audio Conferencing)**
1 of 25 licenses available

☐ **Microsoft Power Automate Free**
9988 of 10000 licenses available

☐ Create user without product license (not recommended)
They may have limited or no access to Microsoft 365 until you assign a product license.

Apps (72)

Show apps for:
All licenses

☒ Select all

☒ **Avatars for Teams**
Microsoft 365 E5 Developer (without Windows and Audio Conferencing)

Back Next

Figure 2.3 – Assign product licenses screen when adding a new user

Tip

The better practice for license assignment, rather than applying individually to users, is to assign licenses by using security groups. This will prove more efficient for administrators.

6. Select **Next** to save and navigate to the **Optional settings** screen. Here, you can expand the **Roles** section if you need to assign an administrative role to this user, and use the **Profile info** section to add additional details about the user, such as job title, department, office, phone number, and address.
7. Select **Next** to review the user's settings on the **Review and finish** screen, make any necessary adjustments, and then select **Finish adding**.

8. Finally, select **Close** on the confirmation screen shown in *Figure 2.4*.

Add a user

✓ Basics

✓ Product licenses

✓ Optional settings

✓ Finish

✓ **Nate Chamberlain added to active users**

Nate Chamberlain will now appear in your list of active users.

User details
Display name: Nate Chamberlain
Username: nate.chamberlain@chambernate.onmicrosoft.com
Password: ***** [Show](#)

Licenses bought
None

Licenses assigned
Microsoft Power Automate Free
Microsoft 365 E5 Developer (without Windows and Audio Conferencing)

Close

Figure 2.4 – New user addition confirmation screen

How it works...

This process registers the user in your organization's directory and assigns the specified roles and licenses, allowing them access to Microsoft 365 services based on the permissions granted.

There's more...

To add multiple users at once, navigate to **Users | Active users**, and select **Add multiple users**. You can enter up to 249 users via the wizard or upload a CSV file with user details to streamline this process. We'll cover this in the next recipe, *Importing users in bulk*.

Additionally, rather than assigning licenses individually to users, you can assign them to security groups. This method is more efficient, especially in larger organizations, as it allows you to manage licenses centrally. When users are added to or removed from these groups, their licenses are automatically updated accordingly, reducing the administrative overhead and ensuring consistency in license management.

See also

- *Add users and assign licenses at the same time:* <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/add-users>

Importing users in bulk

When setting up multiple users at once in Microsoft 365, importing users in bulk streamlines the administrative workload. This process involves preparing and uploading a formatted CSV file containing user details. This recipe will guide you through the steps involved. Check the *There's more...* section to learn about using the wizard to add multiple users instead.

Getting ready

Ensure you have administrative access to the Microsoft 365 admin center as a Global Administrator or User Administrator.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Navigate to **Users | Active users**, then select **Add multiple users**, as shown in *Figure 2.5*.

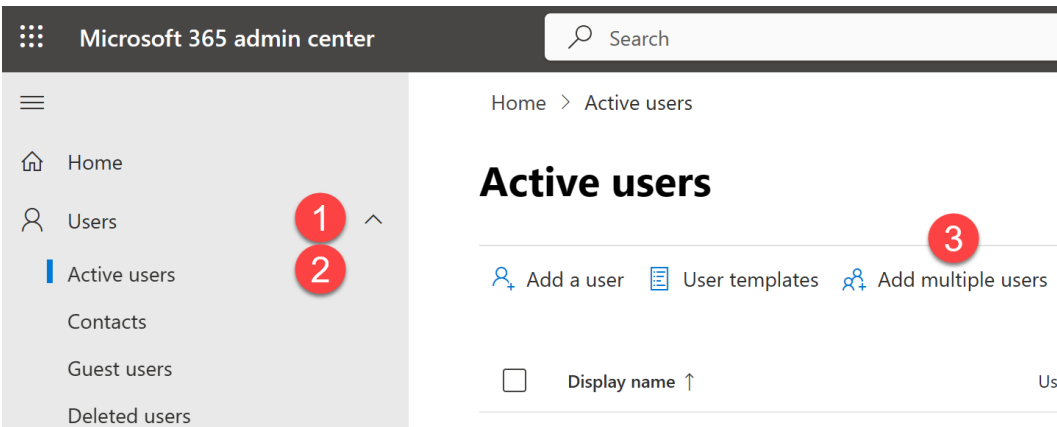


Figure 2.5 – Location of Add multiple users option

- On the **Add multiple users** screen, scroll down and select **I'd like to upload a CSV with user information**, then download the sample CSV file of your choice (with or without example user data). These steps and options are shown in *Figure 2.6*.

Active users > Add multiple users

Figure 2.6 – Steps to download a CSV template for bulk importing users

- Open your downloaded CSV file and populate it with your users' information.

	A	B	C	D	E	F	G
1	Username	First name	Last name	Display name	Job title	Department	Office number
2	samgreen@	Sam	Green	Sam Green	IT Manager	Information	123451
3	emilygold@	Emily	Gold	Emily Gold	IT Specialist	Information	123451
4	peterwhite@	Peter	White	Peter White	Helpdesk A	Information	123451
5	stephanier@	Stephanie	Redding	Stephanie R	Business A	Information	123451
6	tanyablue@	Tanya	Blue	Tanya Blue	CISO	Information	123451

Figure 2.7 – CSV file populated with user information

- In the admin center again, select **Browse** for **Upload CSV file with your user information**.
- Select **Next** to configure product license assignments. The same licenses must be applied to all users being imported. Later, you can add, remove, or adjust individuals' or smaller groups' assignments.

7. Select **Next** to review the users and licenses configured as shown in *Figure 2.8*, and select **Add users**.

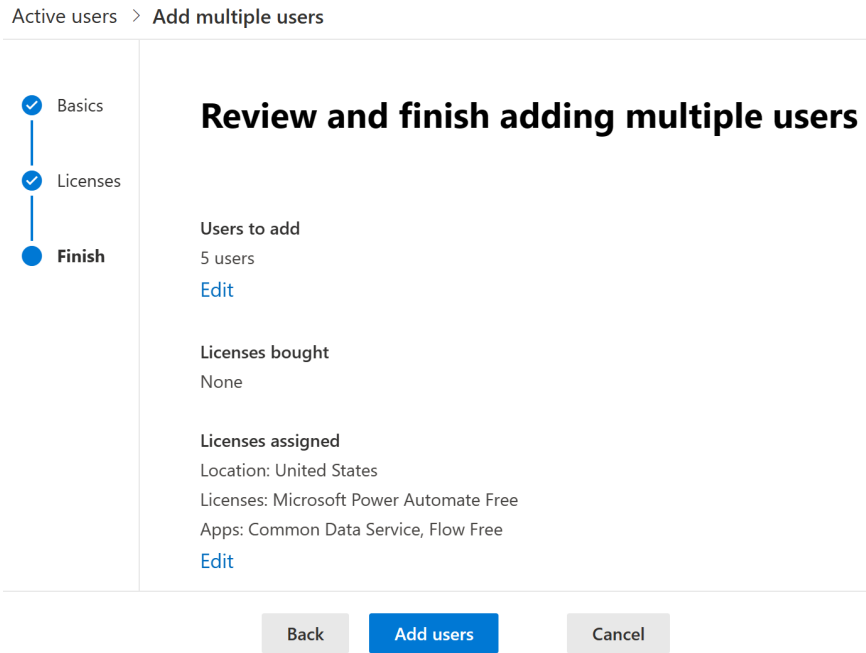


Figure 2.8 – Review screen when importing multiple users

8. On the final screen, you can optionally email sign-in details to one individual, download user details if needed, and select **Close** when finished.

How it works...

The system reads the CSV file, creates user accounts based on the information provided, and assigns roles and licenses as specified. This automated process ensures all users are set up simultaneously with consistent settings.

There's more...

Be prepared to correct any errors in the CSV file after you browse for and add it to the wizard. Common errors include formatting mistakes (such as usernames missing domains) or missing required fields (such as **Display name**). If there are errors, the wizard will allow you to view the specific errors per user, as shown in *Figure 2.9*.

View errors

Open your file, fix the errors for each row, and try again.

Row	Display name	Error message
2		Missing email address or display name.
3	Emily Gold	Email address incomplete or has invalid characters.

Figure 2.9 – Errors when importing users in bulk

Important note

Bulk upload will handle duplicate names by appending sequential numbers to their UPN.

After importing users, you may need to instruct them to complete profile setups, such as changing passwords or adding additional authentication methods.

Rather than download and fill in a CSV template, you can also opt to enter details for multiple users directly on the **Add multiple users** screen, as seen in *Figure 2.10*.

Active users > Add multiple users

● Basics

○ Licenses

○ Finish

Add list of users

Enter up to 249 users. All users are given temporary passwords.

+ Add row
- Remove row

First name	Last name	Username	Domain
Sam	Green	samg	@ chambernate.onmicro... ▼
Emily	Gold	emilyg	@ chambernate.onmicro... ▼
Tanya	Blue	tanyab	@ chambernate.onmicro... ▼
Heather	White	heatherw	@ chambernate.onmicro... ▼

Next

Cancel

Figure 2.10 – Manual entry of multiple users directly in the Add multiple users wizard

The downside to this wizard approach is you can't also enter details such as department, job title, and phone number. The CSV method gives you the best opportunity to bulk import many users with more details completed per user. Note that users can also be managed through Microsoft 365 groups, which we will cover in the next recipe.

See also

- *Add several users at the same time to Microsoft 365:* <https://learn.microsoft.com/en-US/microsoft-365/enterprise/add-several-users-at-the-same-time>

Creating a new Microsoft 365 group

Creating a group in Microsoft 365 allows you to manage email distribution, sharing permissions, and collaboration spaces efficiently across a set of users who have common interests. For example, you might create new Microsoft 365 groups for newly formed committees, departments, processes such as onboarding, or even groups with a social purpose, such as a company book club. These newly created groups will have access to a team in Microsoft Teams, the SharePoint site that supports the team, a notebook, a mailbox and calendar in Outlook, and more to help them collaborate and communicate throughout the life cycle of their objectives.

Getting ready

Many administrative roles, including Global Administrator, Groups Administrator, User Administrator, Teams Administrator, SharePoint Administrator, and Exchange Administrator, have the ability to create groups. For this recipe, you'll need an administrative role with access to the Microsoft 365 admin center.

How to do it...

1. Open the Microsoft 365 admin center by navigating to <https://admin.microsoft.com>.
2. From the left navigation pane, expand **Teams & groups** and select **Active teams & groups**.
3. Select **Add a Microsoft 365 group** to start the process.
4. Fill in the group's basic details on the **Set up the basics** screen, such as the name and, optionally, a description; then, select **Next**.
5. On the **Assign owners** screen shown in *Figure 2.11*, assign at least one owner who will manage the group; these individuals can change group settings and manage membership. Adding two owners is recommended for redundancy.

Home > Active teams and groups > Add a Microsoft 365 group



✓ Basics

Owners

○ Members

○ Settings

○ Finish

Assign owners

Group owners have unique permissions. They can add or remove members, delete conversations from the shared inbox, and change group settings. Group owners can also rename the group, update the description, and more.

ⓘ

You have to have at least one owner. We recommend adding two, so one can help out in the other's absence. If you plan to add Microsoft Teams to this group, all owners must have a license that includes Teams. [Learn more](#)

+ Assign owners

☐

Display name

Teams status

☐

EG

Emily Gold

emilygold@chambernate.onmicrosoft.com

☐

TB

Tanya Blue

tanyablue@chambernate.onmicrosoft.com

Back

Next

Figure 2.11 – Assign owners screen during Microsoft 365 group creation

6. Select **Next** to navigate to the **Add members** screen, where you can add users who will become members of the group. In Teams and SharePoint, these users will be able to post messages, create and share content, and add and manage lists and libraries by default. They will not be able to manage the group's membership or edit group settings.
7. Set up a unique email address for the group and configure privacy settings and Microsoft Teams integration on the **Edit settings** screen shown in *Figure 2.12*.

Edit settings

❗ You'll be able to change settings, like **Allow External Senders** or **Send Copies of Group Conversations to Members' Inboxes**, after the group is created. [Learn more about all settings](#)

Microsoft 365 groups allow teams to collaborate by giving them a group email and a shared workspace for conversations, files, and calendars. Choose settings for your Microsoft 365 group.

Group email address *

M365AdminCookbookAuthors @chambernate.onmicrosoft.com

Privacy ⓘ

Private

Role assignment

☐ Allow admin roles to be assigned to this group

This setting will be permanent for this group. [Learn more about assigning roles to groups](#)

Add Microsoft Teams to your group

Back Next

Figure 2.12 – Edit settings screen when creating a new Microsoft 365 group

Important note

Carefully choose between **Public** and **Private** for the privacy setting:

- **Public groups:** Anyone in your organization can see the group's content and become a member
- **Private groups:** Only approved members can see the group's content and join the group

The privacy setting also affects the associated SharePoint site. If the group is public, the site is accessible to everyone in the organization. Private groups restrict site access to group members only. Setting a group to public by mistake can lead to unintended exposure of sensitive information.

8. Select **Next** to review all the settings, and if everything is correct, select **Create group**.
9. Select **Close** on the confirmation screen shown in *Figure 2.13*.

Home > Active teams and groups > Add a Microsoft 365 group

✓ Basics

✓ Owners

✓ Members

✓ Settings

✓ Finish

✓ **M365 Admin Cookbook Authors group created**

M365 Admin Cookbook Authors group will appear in your list of Active teams & groups within 5 minutes.

Now that the group has been created, you can change these settings:

- Send copies of group conversations and events to group members' inboxes
- Let people outside the organization email this group
- Hide from my organization's global address list

Would you like to know more?
[Using groups to collaborate effectively](#)

Next steps

Close

Figure 2.13 – Group creation confirmation screen

How it works...

This process sets up a new Microsoft 365 group that includes features such as a team, group mailbox, calendar, and a SharePoint site. Owners manage the group, while members have access based on the permissions and settings set on various resources connected to the group.

Microsoft 365 groups are also widely used to manage roles and licenses for groups of users. Assigning licenses via groups can be more efficient, ensuring consistent access across similar users. Additionally, Microsoft 365 groups are heavily integrated with Viva Engage, where they manage communities and membership.

There's more...

After creating a group, you might want to add or remove members, change settings, or even delete the group if it's no longer needed. This can be done from the Microsoft 365 admin center's **Teams & groups | Active teams & groups** screen. Group owners can also handle these responsibilities from their respective resources. For example, they can manage their group's membership via Outlook or Teams.

You can also manage who outside your organization can send emails to the group and configure whether discussions in the group are saved to members' inboxes. Open an existing group from the admin center and select the **Settings** tab to configure the options as shown in *Figure 2.14*.

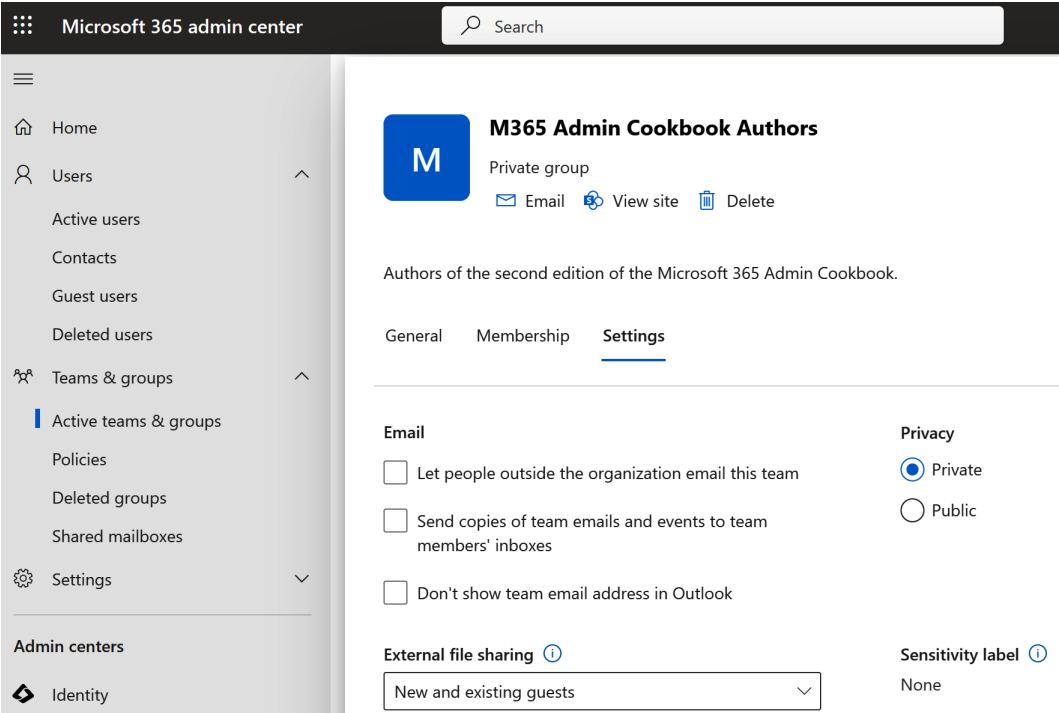


Figure 2.14 – Settings screen for an existing Microsoft 365 group in the admin center

From the Microsoft 365 admin center, you can also easily access and manage a variety of group types, including teams (Microsoft 365 groups), distribution lists, and security groups, as shown in *Figure 2.15*.

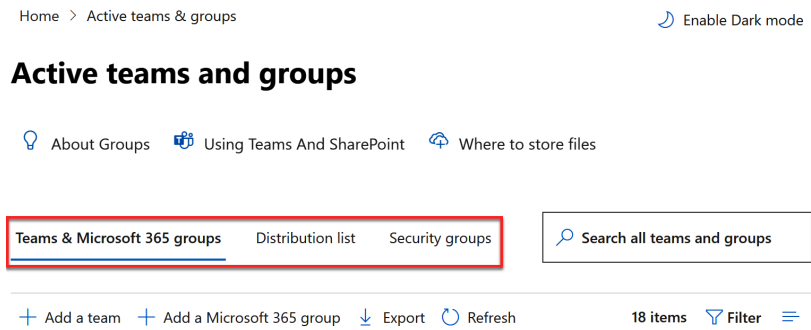


Figure 2.15 – Tabs for various group types in the Microsoft 365 admin center

The term *team* (as in a team within Microsoft Teams) is often used synonymously with *Microsoft 365 group* in administrative tasks, as you see in this recipe with options such as **Teams & groups** or **Teams & Microsoft 365 groups**. When a new team is created, it creates an underlying Microsoft 365 group, which powers its membership and connects its various resources, such as its team, SharePoint site, notebook, and any created Planner plans.

Distribution lists are exclusively used for communication with a group of individuals and cannot be used for team or site access. *Security groups*, by contrast, are used for configuring access to resources such as teams and sites. *Microsoft 365 groups* combine these abilities and can be used for communicating with members while also permitting access to the group's resources.

In addition to using the Microsoft 365 admin center to manage Microsoft 365 groups as we did in this recipe, you can use Microsoft Entra ID to create and manage groups. We'll explore Microsoft Entra ID more throughout this book, including in the next recipe.

See also

- *Overview of Microsoft 365 Groups for administrators*: <https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/office-365-groups>
- *Compare types of groups in Microsoft 365*: <https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups>
- *Create a group in the Microsoft 365 admin center*: <https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/create-groups>

Enabling security defaults (MFA) in Entra ID

Security defaults are preconfigured rules that include commonly configured security features, such as requiring MFA. Enabling **security defaults** is crucial for protecting your Microsoft 365 environment against common security risks to Microsoft 365, such as phishing or other identity-related attacks, by enforcing secure authentication methods recommended by Microsoft.

Getting ready

To enable security defaults, you need to have administrative privileges in the Microsoft 365 admin center. It's recommended to have the Security Administrator or Global Administrator role.

How to do it...

1. Sign in to the Microsoft Entra admin center by navigating to <https://entra.microsoft.com> or by selecting **Identity** from the list of admin centers in the Microsoft 365 admin center at <https://admin.microsoft.com>.

2. In the navigation pane, go to **Identity | Overview | Properties**, as shown in *Figure 2.16*.

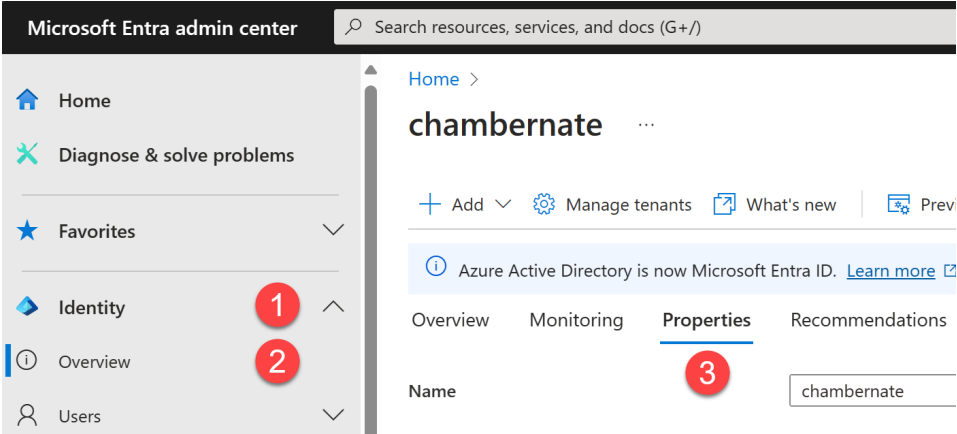


Figure 2.16 – Steps to navigate to Entra ID properties

3. Select **Manage security defaults** located at the bottom of the **Properties** page.
4. Set the **Security defaults** dropdown to **Enabled** and select **Save**, as shown in *Figure 2.17*.

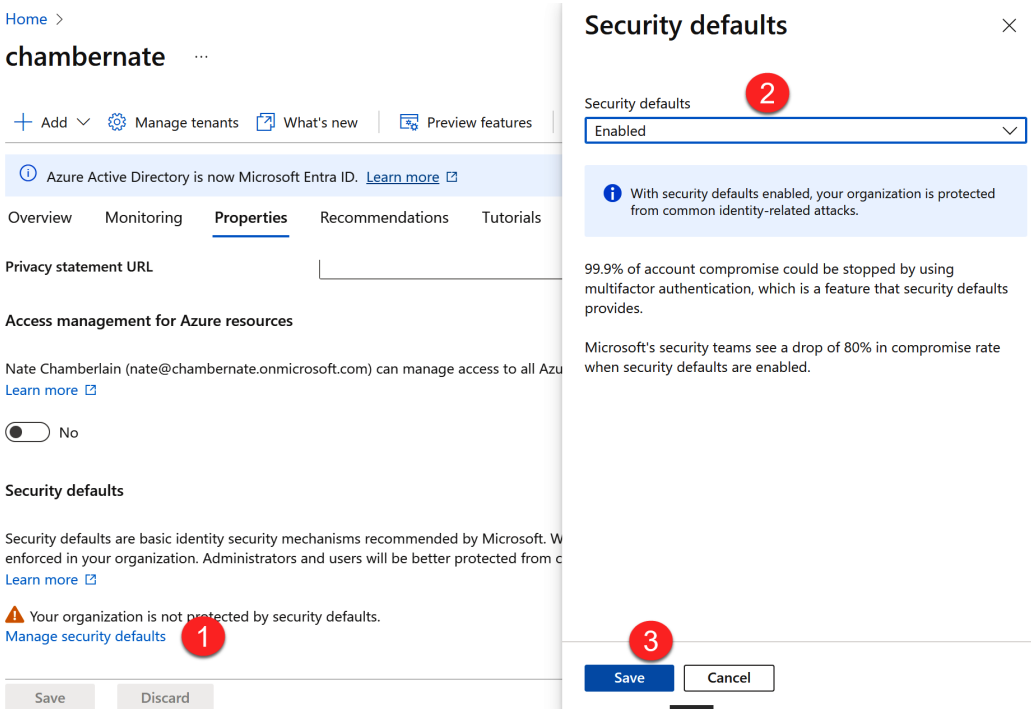


Figure 2.17 – Steps to enable Security defaults in Microsoft Entra ID

How it works...

Upon enabling security defaults, your Microsoft 365 environment will do the following:

- Require all users to register for and use MFA
- Block legacy authentication protocols that do not support MFA, such as SMTP, IMAP, and POP
- Require administrators to perform MFA on every sign-in

This setting ensures that basic but essential security measures are enforced across your organization, significantly improving your security posture against potential breaches.

Important note

Users who do not register for MFA within 14 days will be locked out and unable to access their accounts until they complete the registration process.

There's more...

Once security defaults are enabled, users will have 14 days to register for MFA. During this period, they will be prompted for additional authentication based on the security context of each sign-in. Some MFA options include, from least to most secure, the following:

- **SMS-based MFA:** Sends a verification code via text message to the user's mobile phone. This is the least secure option because SMS can be intercepted or spoofed.
- **Voice call MFA:** Delivers a code through an automated voice call to the user's phone. It is slightly more secure than SMS but still vulnerable to interception and spoofing.
- **Authenticator app (e.g., Microsoft Authenticator) with TOTP:** Uses a mobile app to generate a **time-based one-time password (TOTP)**. This method is more secure than SMS or voice because it's tied to a specific device, but still relies on the security of the mobile device.
- **Passwordless phone sign-in:** Allows users to sign in using the Microsoft Authenticator app with no password, where users approve a push notification to authenticate. This method reduces reliance on passwords and mitigates phishing risks, making it more secure than SMS, voice, or TOTP-based authentication.
- **Biometric methods (e.g., Windows Hello):** Uses biometric data such as facial recognition or fingerprint scanning for authentication. This method is highly secure as it uses unique physical characteristics that are difficult to replicate.

- **FIDO2 security keys:** Hardware-based authentication using FIDO2-compliant security keys. These keys provide the highest level of security by generating cryptographic keys that are resistant to phishing, man-in-the-middle attacks, and other common security threats.

It is also a good practice to revoke existing session tokens when enabling security defaults to force all users to re-authenticate under the new security settings.

See also

- *Security defaults in Microsoft Entra ID:* <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>

Exporting users

Exporting user data in Microsoft 365 can be essential for audits, compliance, reporting, or management purposes. This process allows you to generate and download reports that detail user activities, licensing, and other attributes.

Getting ready

Ensure you have administrative privileges to access the Microsoft 365 admin center with an assigned role such as Global Administrator, Global Reader, or Reports Reader in order to perform these actions.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com> and go to the **Reports | Usage** section. Note that this might be under **Show all** if you don't see it immediately. This area provides a variety of reports related to user activities and service usage, as seen in *Figure 2.18*.

Usage

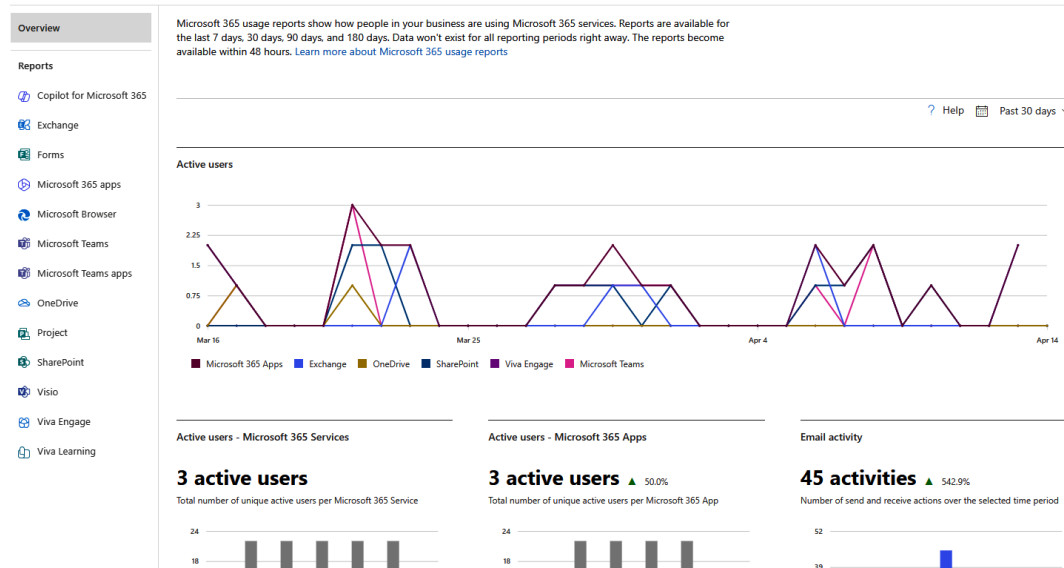


Figure 2.18 – Usage reports in the Microsoft 365 admin center

- Choose the specific report you are interested in, such as the **Active users** report, by selecting **View more** under the **Active users - Microsoft 365 Services** card, as shown in *Figure 2.19*. You can also navigate to this report by selecting **Microsoft 365 apps | Active users**. This report offers insights into product license usage, activity levels, and more over selectable periods.

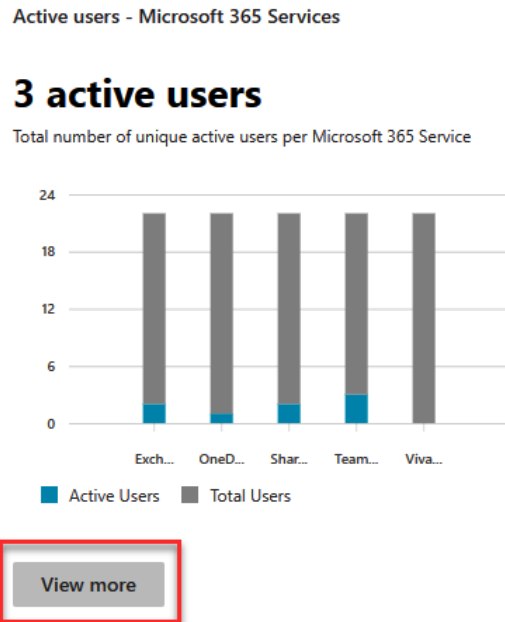


Figure 2.19 – Link to view the Active users report

3. You can customize what time span is shown in the report page's visuals by changing the date filter from **Past 30 days** to the past 7, 30, 90, or 180 days.
4. Look for an option to export the data behind a specific visual, available as a button or link near the top of the related visual on the page, as shown in *Figure 2.20*. Selecting this will allow you to download the data in a CSV format, which you can then open with Microsoft Excel for further analysis.

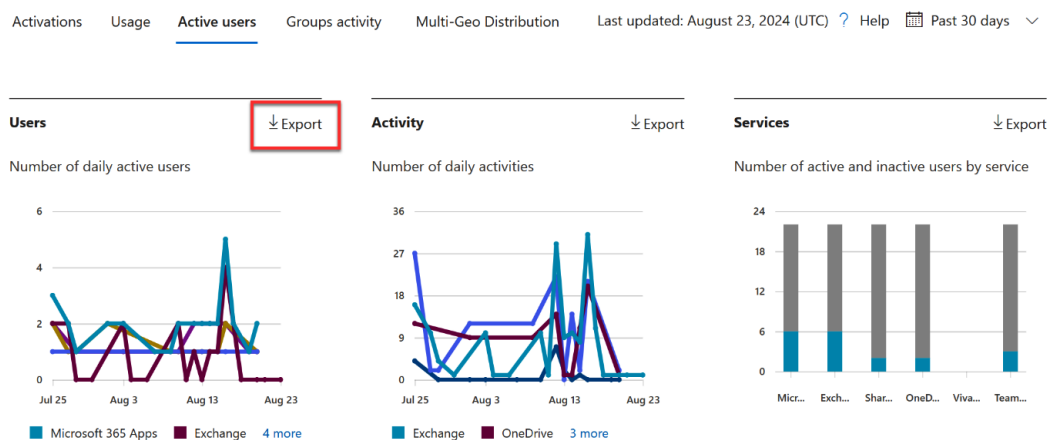


Figure 2.20 – Option to export the data for Users

For this recipe's example, to export a list of all of your users along with details such as assigned licenses and last activity dates, find the table on the **Active users** screen with some of these details and choose **Export** to get a CSV file with all details.

Important note

If you're only seeing ID numbers and no names in your CSV file, read the *There's more...* part of this recipe to learn how to show identifying details.

How it works...

Exporting the report generates a CSV file that includes user data as per the selected report type and your customization. This file can then be used for detailed analysis, record-keeping, or as required by organizational policies.

There's more...

By default, identifying information, including usernames, is concealed from reports to protect user privacy. To turn off this restriction and show user-specific details in all reports, a Global Administrator must navigate to **Settings | Org settings** from the Microsoft 365 admin center, select **Reports**, then uncheck the **Display concealed user, group, and site names in all reports** box. Then, click **Save**. This screen before unchecking is shown in *Figure 2.21*.

Reports

Reports found in the Microsoft 365 admin center provide information about your organization's usage data. Your organization's data is managed by trusted cloud security and privacy safeguards.

By default, reports conceal user information such as usernames, groups, and sites. You can decide to display concealed information if you prefer or if your organization's policies require it.

This setting applies to Microsoft 365 usage reports in Microsoft 365 admin center, Microsoft Graph and Power BI and the usage reports in Microsoft Teams admin center.

☒ Display concealed user, group, and site names in all reports

Microsoft 365 usage analytics

Usage data is analyzed and used to make charts and graphs to help you understand your organization's use of apps and services. Reports can be found in the Microsoft 365 admin center and in Power BI. [Learn how to get started with Power BI](#)

☐ Make report data available to Microsoft 365 usage analytics for Power BI

Save

Figure 2.21 – Option to conceal user info in all reports

See also

- *Microsoft 365 Reports in the admin center*: <https://learn.microsoft.com/en-US/microsoft-365/admin/activity-reports/activity-reports>
- *Assess the Microsoft 365 Active Users report*: <https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/active-users-ww>

Managing guest users

Managing guest users in Microsoft 365 allows organizations to collaborate securely with individuals outside their organization, such as partners, vendors, or consultants. These external users can be given access to various resources, such as Microsoft Teams and SharePoint, without being part of your organization's official directory.

Important note

Guests do not need a Microsoft 365 license to use Teams' and SharePoint's collaboration features. Other Microsoft 365 applications, however, may require licensing.

Getting ready

To manage guest users, you need appropriate administrative privileges in the Microsoft 365 admin center with a role such as Global Administrator or User Administrator.

How to do it...

1. Navigate to the Microsoft 365 admin center at <https://admin.microsoft.com> and select **Show all | Settings | Org settings**.
2. Under the **Services** tab, select **Microsoft 365 Groups**.
3. In the side panel that appears, you can enable or disable the ability for group owners to add guests and specify whether guests can access group content. These options are shown in *Figure 2.22*.

Microsoft 365 Groups

Choose settings for guests and ownerless groups.

Guests

Choose how guests from outside your organization can collaborate with your users in Microsoft 365 Groups. [Learn more about guest access to Microsoft 365 Groups](#)

- ☒ Let group owners add people outside your organization to Microsoft 365 Groups as guests
- ☒ Let guest group members access group content
If you don't select this, guests will still be listed as members of the group, but they won't receive group emails or be able to access any group content. They'll only be able to access files that were directly shared with them.

Ownerless groups

All groups must have an owner to add or remove members. Owners have unique permissions like the ability to change group settings.

- ☐ When there's no owner, email and ask active group members to become an owner

Save

Figure 2.22 – Options to manage guest invitations and guest access

4. To add an existing guest user to a group via the admin center, select **Teams & groups | Active teams & groups**.

5. Choose the group you want to add guests to, then select **Membership** | **Members** | **Add members**, as shown in *Figure 2.23*.

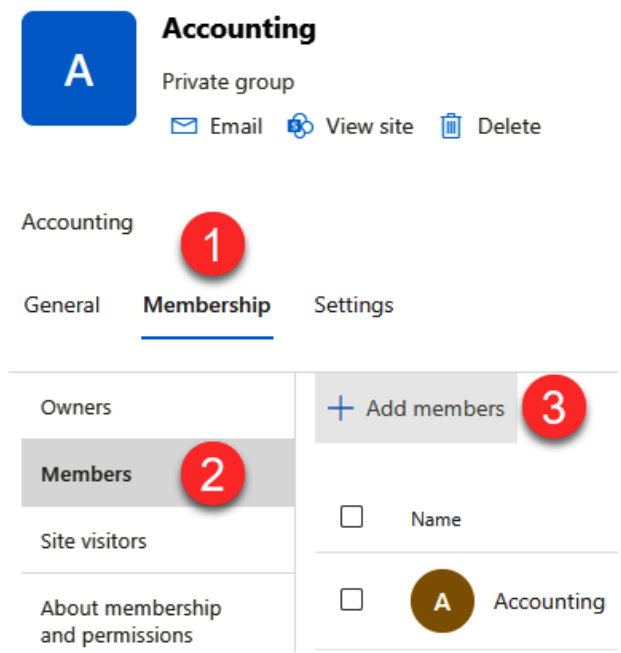


Figure 2.23 – Steps to add members to a group via the admin center

6. Search for the guest by name or email address and add them as a member. If the guest is not yet in your directory, you may need to add them first through Microsoft Entra ID. See the *There's more...* part of this section for guidance.
7. To change product licenses for a guest in your organization, go to **Users** | **Guest users**, select the guest, and then select **Manage product licenses**, as shown in *Figure 2.24*.

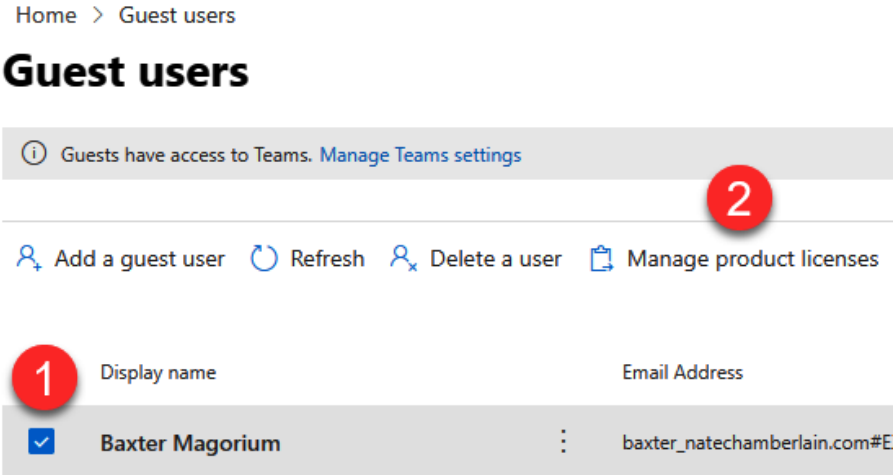


Figure 2.24 – Steps to manage product licenses for a guest user

8. To remove a guest from your organization, go to **Users | Guest users**, select the guest, then choose **Delete a user**, effectively revoking their access to any group resources.

How it works...

Enabling guest access allows guests to participate in teams and groups as if they were part of your organization, but with specific permissions that limit their access to resources. This is managed through a combination of Microsoft Entra ID, SharePoint, Microsoft Teams, and Microsoft 365 group settings.

Deleted guest users can be restored for up to 30 days by navigating to **Users | Deleted users**, selecting the deleted guest, and choosing **Restore user**.

There's more...

To add a new guest to your organization, navigate to **Users | Guest users** and select **Add a guest user**, as shown in *Figure 2.25*.

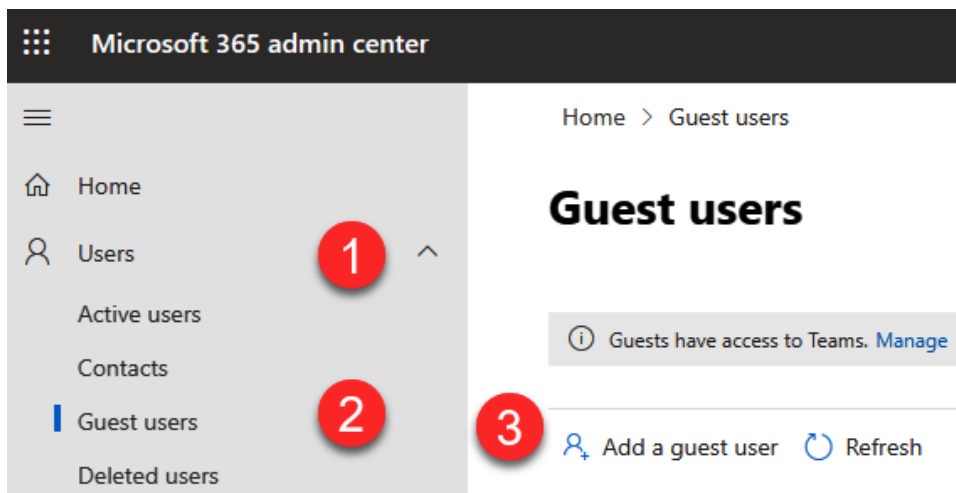


Figure 2.25 – Steps to add a guest user from the Microsoft 365 admin center

This redirects you to Microsoft Entra ID, where you can set up the new guest account. During account creation, or after being added, you'll be able to add the guest to groups, as covered in this section's recipe.

Regularly review the activities and permissions of guest users to ensure compliance with your organization's security policies. Utilize audit logs and access reviews for ongoing management.

Depending on the collaboration needs, you can customize the guest access permissions in SharePoint and Teams to restrict or grant access to certain information more granularly.

See also

- *Manage guest access in Microsoft 365 groups*: <https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/manage-guest-access-in-groups>

Creating a user template

Creating a user template in Microsoft 365 helps streamline the process of adding new users by predefining a set of properties that can be applied to multiple users. This is especially useful for onboarding employees in similar roles or departments efficiently and consistently.

Getting ready

Ensure you have administrative access to the Microsoft 365 admin center. User templates can only be created and managed by users with appropriate admin roles, such as a Global Administrator or User Administrator.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Navigate to **Users** | **Active users**, then select **User templates** near the top of the page, as shown in *Figure 2.26*.

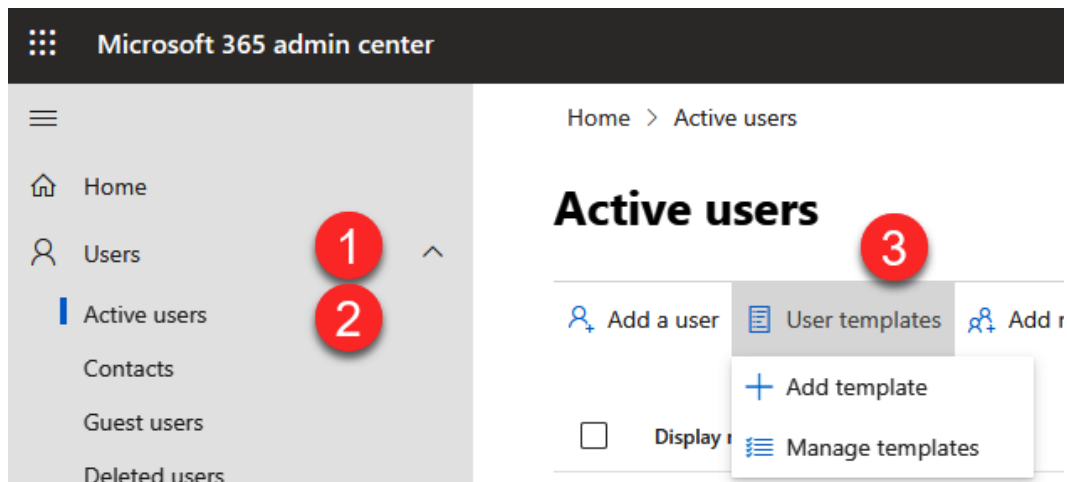


Figure 2.26 – Location of the User templates option in the Microsoft 365 admin center

3. Select **Add template** to create a new template. This opens a side panel wizard where you can enter the template's name and description, as shown in *Figure 2.27*.

Add user template

Description

Basics

Licenses

Optional settings

Finish

Set up your template

User templates allow you to quickly add new users with a saved configuration. To get started, fill out some basic information about the template you're creating.

Name your template *

Technical Business Analyst *

Add a description (recommended)

Full-time technical business analysts in the Midwest region.

Publish this template

☒ Make this template available to other admins who manage users.
If you want to un-publish a template, delete it. You can't change a template to private after it is published.

Next

Figure 2.27 – User template wizard

4. Select **Next** and continue configuring the template form with the default settings, such as domain, password settings (auto-generated or manual), licenses and apps, roles, and profile info.

Note

User-specific information, such as names and usernames, are not included in templates. Those details will be added for each user when this template is used for provisioning new accounts.

5. Save the template by selecting **Finish adding** on the review screen, as shown in *Figure 2.28*.

Add user template

✓ Description

✓ Basics

✓ Licenses

✓ Optional settings

Finish

Review and finish creating your template

Review the settings for your template. You can use this template immediately after you finish creating it.

Template description

Name: Technical Business Analyst

Description: Full-time technical business analysts in the Midwest region.

Publish status: Published

[Edit](#)

Domain

chambersgate.onmicrosoft.com

[Edit](#)

Password

Type: Require users to change password on first login

Require users to change password on first login

[Edit](#)

Product licenses

Back

Finish adding

Figure 2.28 – Review screen when configuring a new user template

- On the confirmation screen, you can select **Add a user using this template**, **Create another template**, or **Manage user templates**. Otherwise, select **Close** if finished for now.

How it works...

When a template is saved, it stores all the specified configurations, such as domain, licenses, and role settings. When adding new users, you can apply this template, and all the predefined settings will automatically populate, reducing the need to manually enter them each time.

Consider a scenario where you have a *Human Resources Specialist* template. The next time you onboard a new HR specialist, you'll choose your template, add the name, display name, and username, and be finished in very little time. See the *There's more...* part of this recipe to learn more about applying a user template.

There's more...

You can view, modify, or delete existing templates by navigating to **User templates** in the **Active users** section, and then selecting **Manage templates**.

To use a template, navigate to **Users | Active users | User templates**, then select the template you've created, as shown in *Figure 2.29*, to auto-fill the settings during the process.

Home > Active users

Active users

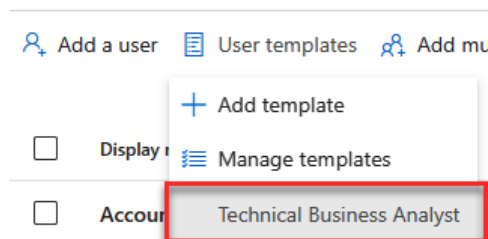


Figure 2.29 – Custom user template showing on the User templates menu

The only details left for you to specify that weren't configured in the template include the following:

- First and last names
- Display name
- Username
- Whether the password should be sent upon completion, and the email address if so

Select **Add user** when finished. Understandably, only having to configure four fields for a common role or user type saves administrators a significant amount of time.

See also

- *Create and use a template to add users*: <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/create-and-use-a-template-to-add-users>

Restricting users from creating new Microsoft 365 groups

In organizations utilizing Microsoft 365, administrators might need to restrict user capabilities to ensure data security and compliance. One such administrative control involves preventing non-admin users from creating new groups. This recipe provides a step-by-step guide on how to set up these restrictions.

Getting ready

Before you begin, ensure you have administrative access to the Microsoft 365 admin center as either Global Administrator or User Administrator. You must also be assigned a Microsoft Entra ID Premium P1 or P2 license. These licenses build upon the basic Entra ID Free license, offering expanded capabilities, such as enhanced control over user verification methods (beyond just the Authenticator app) and the activation of Conditional Access policies (P1) and Risk-based Conditional Access policies (P2).

How to do it...

1. First, we must create a security group of individuals who will be allowed to create new groups. Go to the Microsoft 365 admin center at <https://admin.microsoft.com/>, then select **Teams & groups** | **Active teams & groups** | **Security groups** | **Add a security group**, as shown in *Figure 2.30*.

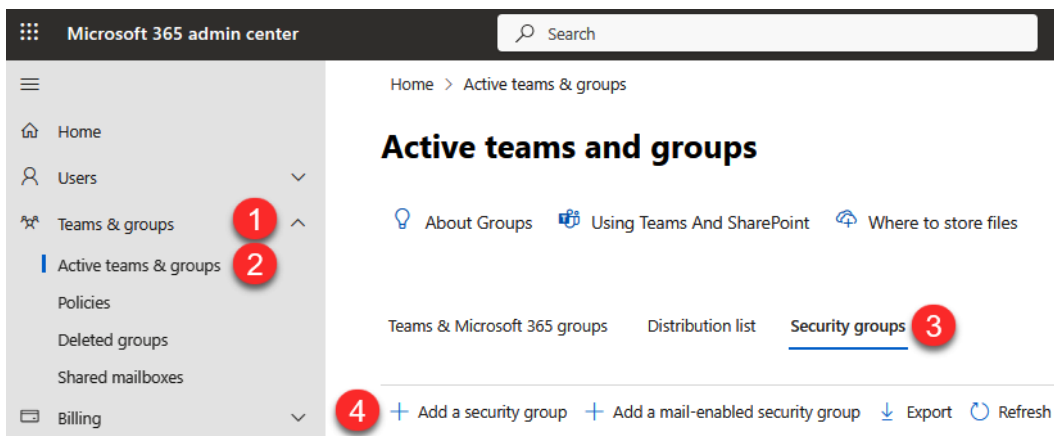


Figure 2.30 – Steps to navigate to and add security groups

2. Name and describe the group (such as *M365 Group Creators*), then select **Next**.
3. Select **Next** again, not opting for the ability for Entra ID roles to be assigned to the group since admin roles are not required for this specific group's purpose.
4. Review, then select **Create group** and **Close**.

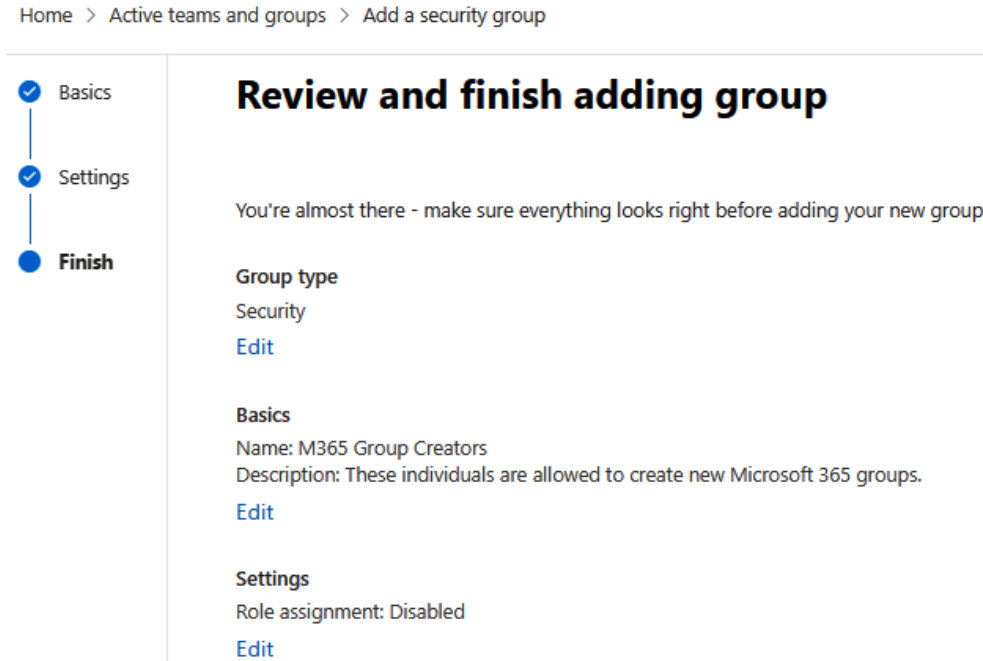


Figure 2.31 – New security group review screen

- Next, we need to restrict new group creation only to members of our new group. First, you need to install the Microsoft Graph PowerShell modules if you haven't already. This can be done by opening PowerShell as an administrator (right-click | **Run as administrator**) and running the following:

```
Install-Module Microsoft.Graph -Scope CurrentUser
Install-Module Microsoft.Graph.Beta -Scope CurrentUser
```

- Now, import and connect to Microsoft Graph PowerShell Beta by running the following commands. Note that you have the Global Administrator role to grant API consent:

```
Import-Module Microsoft.Graph.Beta.Identity.DirectoryManagement
Import-Module Microsoft.Graph.Beta.Groups
Connect-MgGraph -Scopes "Directory.ReadWrite.All", "Group.Read.All"
```

- Now, replace the group name in the first line of the following with your new group's name and press *Enter* to declare these values and retrieve the ID of the directory setting for group management:

```
$GroupName = "M365 Group Creators"
$AllowGroupCreation = "False"
$settingsObjectID = (Get-MgBetaDirectorySetting | Where-object
-Property Displayname -Value "Group.Unified" -EQ).id
```

8. Now, run the following PowerShell command:

```
if(!$settingsObjectID)
{
    $params = @{
        templateId = "62375ab9-6b52-47ed-826b-58e47e0e304b"
        values = @(
            @{
                name = "EnableMSStandardBlockedWords"
                value = "true"
            }
        )
    }
    New-MgBetaDirectorySetting -BodyParameter $params
```

9. Next, run this PowerShell command to retrieve the new directory setting ID for group management:

```
$settingsObjectID = (Get-MgBetaDirectorySetting | Where-object
-Property Displayname -Value "Group.Unified" -EQ).Id
}
```

10. And lastly, run this PowerShell command to enable the new group's members to create other groups:

```
$groupId = (Get-MgBetaGroup | Where-object {$_.displayname -eq
$GroupName}).Id
$params = @{
    templateId = "62375ab9-6b52-47ed-826b-58e47e0e304b"
    values = @(
        @{
            name = "EnableGroupCreation"
            value = $AllowGroupCreation
        }
        @{
            name = "GroupCreationAllowedGroupId"
            value = $groupId
        }
    )
}
Update-MgBetaDirectorySetting -DirectorySettingId
$settingsObjectID -BodyParameter $params
(Get-MgBetaDirectorySetting -DirectorySettingId
$settingsObjectID).Values
```

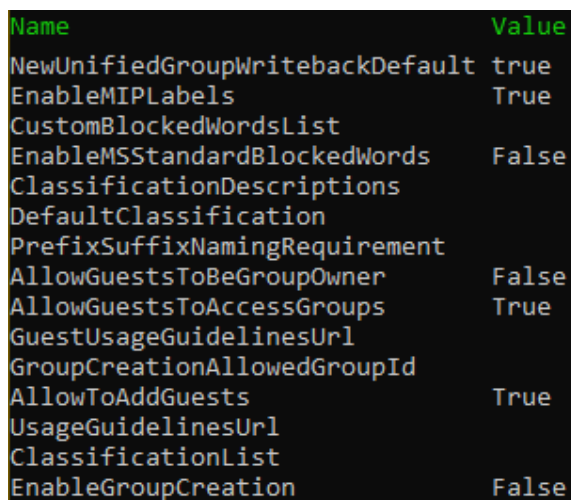

How it works...

This recipe restricts the group creation capability (which also prevents team creation) within your organization to only those added to your allowed security group. This helps in maintaining the organizational structure and prevents the uncontrolled sprawl of groups, which could potentially lead to data leaks or mismanagement. Your new group's members will be able to create Microsoft 365 groups, but everyone else who is not a member of that group will not.

Important note

Those with privileged roles such as Exchange Administrator, SharePoint Administrator, or Teams Administrator can create Microsoft 365 groups regardless of membership in the newly created exception group.

The output of the PowerShell command is as follows:

The image shows a PowerShell command output in a dark-themed console window. The output is a table with two columns: 'Name' and 'Value'. The 'Name' column lists various settings related to group creation, and the 'Value' column shows their current state (True or False).

Name	Value
NewUnifiedGroupWritebackDefault	true
EnableMIPLabels	True
CustomBlockedWordsList	
EnableMSStandardBlockedWords	False
ClassificationDescriptions	
DefaultClassification	
PrefixSuffixNamingRequirement	
AllowGuestsToBeGroupOwner	False
AllowGuestsToAccessGroups	True
GuestUsageGuidelinesUrl	
GroupCreationAllowedGroupId	
AllowToAddGuests	True
UsageGuidelinesUrl	
ClassificationList	
EnableGroupCreation	False

Figure 2.32 – Output of the PowerShell command for restriction of Microsoft 365 group creation

In the last line of the PowerShell output shown in *Figure 2.32*, `EnableGroupCreation` is `False`. This translates to only our security group's members being able to create Microsoft 365 groups. Running the PowerShell command again but with `$AllowGroupCreation` set to `"True"` will *undo* this, allowing all users to create new Microsoft 365 groups again.

There's more...

In addition to the administrator completing this recipe's steps needing a Microsoft Entra ID Premium P1 or P2 license, any members of the permitted security group must also have that license. Note that Entra ID Premium licenses are included with E3 (or equivalent) subscriptions and above.

Consider periodically reviewing these settings as your organization evolves or as roles change. Additionally, training for authorized personnel on responsible group management can further enhance your governance strategy.

See also

- *Manage who can create Microsoft 365 Groups*: <https://learn.microsoft.com/en-us/microsoft-365/solutions/manage-creation-of-groups>

Assigning the User Administrator role

Assigning the Microsoft 365 User Administrator role is essential for delegating user management tasks. The User Administrator role allows designated individuals to create and manage users, reset passwords, and manage user licenses without having full Global Administrator privileges.

Getting ready

Ensure you have access to the Microsoft 365 admin center with the Global Administrator role to be able to assign roles to other users.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. From the left navigation pane, select **Users | Active users**.
3. Choose the user to whom you want to assign the User Administrator role.

4. In the side panel that appears, within the user's **Account** tab, select **Manage roles** under the **Roles** header, as shown in *Figure 2.33*.

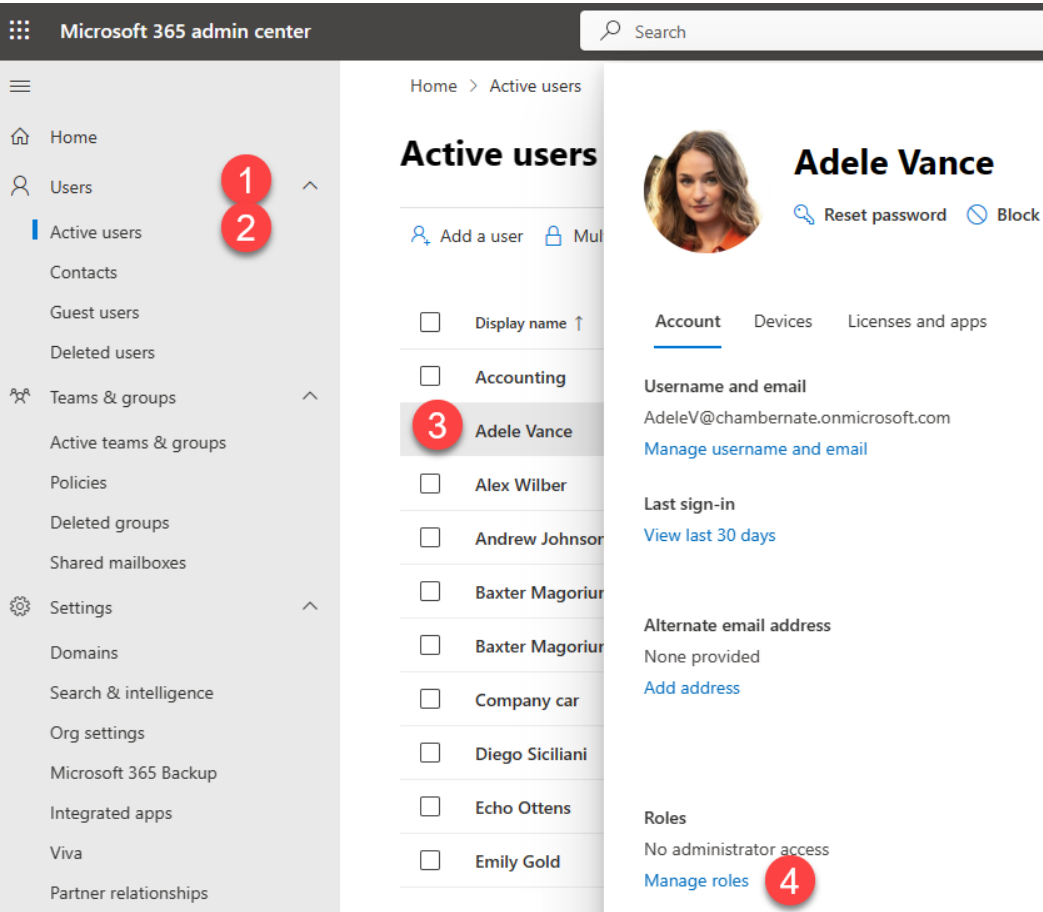


Figure 2.33 – Steps to manage roles for a user in the Microsoft 365 admin center

5. Select **Admin center access**, then select **User Administrator** from the list of available roles, as seen in *Figure 2.34*.

Manage admin roles

Adele Vance selected

Admin roles give users permission to view data and complete tasks. The least-permissive role is selected by default.

[Learn more about admin roles](#)

☐ User (no admin center access)

☒ Admin center access

Global readers have read-only access to admin centers, while other roles are more limited in what they can see and do.

☐ Exchange Administrator ⓘ

☐ Global Administrator ⓘ

☐ Global Reader ⓘ

☐ Helpdesk Administrator ⓘ

☐ Service Support Administrator ⓘ

☐ SharePoint Administrator ⓘ

☐ Teams Administrator ⓘ

☒ User Administrator ⓘ

☐ User Experience Success Manager ⓘ

Show all by category

Save changes

Figure 2.34 – User Administrator added to a user's roles

6. Select **Save changes**.

How it works...

By assigning the User Administrator role to a user, they gain the ability to manage other user accounts within the organization. This includes creating and editing users, resetting passwords, and assigning licenses, which are important tasks for day-to-day administration without granting full administrative rights to items such as **Billing** and **Org settings**.

There's more...

It's important to regularly review and audit the roles assigned to users to ensure that only the necessary permissions are granted. Over-privileging can lead to security risks. Microsoft recommends only having 2–4 Global Administrators.

To remove a role from a user, repeat *Steps 1–4* in this recipe, but then deselect the role and select **Save changes**.

See also

- *Microsoft Entra built-in roles*: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>
- *About admin roles in the Microsoft 365 admin center*: <https://learn.microsoft.com/en-US/microsoft-365/admin/add-users/about-admin-roles>

Managing admin roles in the Microsoft 365 admin center

Managing administrative roles in the Microsoft 365 admin center helps in maintaining security and ensuring that the right individuals have the appropriate access to perform their roles efficiently. This guide will walk you through the process of managing admin roles, helping you to delegate responsibilities securely within your organization.

Getting ready

To manage admin roles, you must have the Global Administrator or Privileged Administrator role assigned. Make sure you are signed in to the Microsoft 365 admin center with the appropriate permissions.

How to do it...

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. In the left navigation pane, select **Show all | Roles | Role assignments** to view the list of roles and descriptions, as shown in *Figure 2.35*.

The screenshot shows the Microsoft 365 admin center interface. The left sidebar contains navigation links: Home, Users, Teams & groups, Roles, Role assignments (selected), Administrative units, Resources, Billing, Support, Settings, Setup, and Reports. The main content area is titled 'Role assignments' and shows tabs for Microsoft Entra ID, Exchange, Intune, and Billing. Below the tabs, there is a description of Microsoft Entra ID roles and a link to learn more. A table lists several roles with checkboxes for selection, their names, and descriptions.

<input type="checkbox"/>	Name ↑		Description
<input type="checkbox"/>	Exchange Administrator	:	Full access to Exchange Online, creates and manages service health.
<input type="checkbox"/>	Global Administrator	:	Has unlimited access to all management features and settings.
<input type="checkbox"/>	Global Reader	:	Can view all administrative features and settings.
<input type="checkbox"/>	Helpdesk Administrator	:	Resets passwords and re-authenticates for requests, and monitors service health.

Figure 2.35 – Role assignments screen of the Microsoft 365 admin center

3. Select the name of the role you wish to manage. A side panel will appear with tabs for **General** (what this role does and how many individuals are currently assigned), **Assigned** (current individuals with this role), and **Permissions** (advanced view of specific privileges of the role).
4. To assign the role to a user, select **Add users** or **Add groups**, as seen in *Figure 2.36*, on the **Assigned** tab of the side panel.

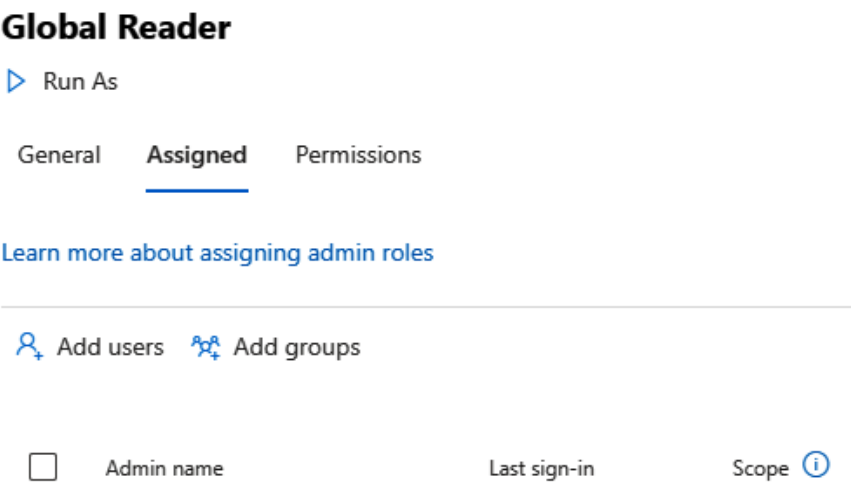


Figure 2.36 – Assigned tab of an admin role panel

- 5. Search for the user by name or email address, then select them from the list.
- 6. Select **Add** to assign the role to the selected user.
- 7. To remove an admin role from a user, repeat steps 1-3, then select the user from the **Assigned** tab and choose **Remove**.

How it works...

Assigning administrative roles through the Microsoft 365 admin center allows you to control who can manage specific services within your organization. Each role includes a set of permissions that define what the user assigned to that role can and cannot do, which helps limit access to sensitive information and critical functionalities to only those who need it.

Important note

While you can do much of your Microsoft 365 administration via the Microsoft 365 admin center these days, you'll find that you're able to complete similar tasks in other admin centers as well. For instance, the Microsoft Entra admin center (or **Identity**, which takes you to Microsoft Entra ID, from the Microsoft 365 admin center) will allow you to perform all user administration and group tasks in most cases. The decision of where to do administrative tasks often comes down to personal preference or, in the case of having limited privileges, allowed admin centers and screens.

There's more...

Regularly review the roles and the individuals assigned to them to ensure that access rights remain aligned with current job functions and organizational policies. Periodic audits can help prevent privilege creep and enhance security.

If you're unsure which role to assign to a user, you can multi-select up to three admin roles from **Roles | Role assignments**, then choose **Compare roles**. This allows you to view the selected roles side by side with abilities and features available to them, each marked as shown in *Figure 2.37*.

Compare roles

Compare permissions for up to 3 roles at a time so you can find the least permissive role to assign.

Export comparison	<input type="text" value="Search this list"/>	
Permissions	Global Administrator ⓘ	Global Reader ⓘ
Read basic properties on all resources in the Microsoft 365 admin center	●	●
Read usage reports in the Microsoft 365 admin center	●	●
Read and configure Service Health in the Microsoft 365 admin center	●	●
Read all network performance properties in the Microsoft 365 admin ce...	●	●
Read security messages in Message Center in the Microsoft 365 admin c...	●	●
Read messages in Message Center in the Microsoft 365 admin center, ex...	●	●
Read shipping status for open Microsoft hardware warranty claims	●	●

Figure 2.37 – Role comparison of Global Administrator and Global Reader

Also consider leveraging **administrative units (Roles | Administrative units)** to enhance role management in your organization. Administrative units allow you to divide your organization's users into logical groupings, such as by region or department, and assign administrative roles to individuals who can manage only users within specific administrative units. This can be particularly useful if you want, for instance, a User Administrator who is only able to modify user details or reset passwords for users in a specified administrative unit, such as the Southwest, without having access to modify details for users in the Northeast administrative unit. This setup helps maintain organizational structure and security by limiting administrative reach to specified segments of your organization.

See also

- *About admin roles in the Microsoft 365 admin center:* <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles>
- *Administrative units in Microsoft Entra ID:* <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units>

Administering Microsoft 365 with PowerShell

PowerShell extends the capabilities of Microsoft 365 Administrators far beyond the limitations of the admin centers and **graphical user interface (GUI)**. It enables the automation of complex and repetitive tasks, offers access to a suite of commands not always available in the GUI, and allows for the efficient management of multiple user accounts and licenses. This chapter delves into specific PowerShell recipes designed to enhance the efficiency and capabilities of Microsoft 365 Administrators.

In this chapter, we will cover the following PowerShell recipes:

- Getting a list of all available commands
- Creating a user
- Disabling a user
- Changing user settings or profile information
- Getting a list of all users with user properties
- Changing a user password
- Connecting via PowerShell to SharePoint Online
- Creating a SharePoint Online site
- Adding a new site admin to all SharePoint Online sites
- Restoring a deleted OneDrive site
- Hiding Microsoft 365 groups from the Global Address List
- Preventing external senders from emailing internal Microsoft 365 groups

Technical requirements

Before diving into the recipes, administrators must have PowerShell 5.1 or later installed on their systems. Both the command-line version and the **Integrated Scripting Environment (ISE)** are suitable for following along with the examples provided in this chapter. Administrators should ensure they possess valid credentials and appropriate roles, such as the Global Administrator role, to execute the tasks outlined.

For all recipes in this chapter, right-click **PowerShell** and select **Run as administrator** before you begin.

Your PowerShell script execution policy must be either remote-signed or less restrictive. Run the following to make it so:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
```

As a Microsoft 365 Administrator, you should install the Microsoft Graph and Microsoft Graph Beta PowerShell modules, which are compatible with PowerShell 5.1 or later, and work on Windows, macOS, and Linux platforms. Install them by running the following:

```
Install-Module Microsoft.Graph -Scope CurrentUser
Install-Module Microsoft.Graph.Beta -Scope CurrentUser
```

Important note

Beta modules are subject to change without notice from Microsoft.

Optionally, replace `CurrentUser` with `AllUsers` if you have admin rights and wish for all users to be able to utilize these modules.

Lastly, connect to your Microsoft 365 tenant using the following:

```
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"
```

Getting a list of all available commands

Becoming familiar with all of the available commands in Microsoft Graph PowerShell can help you effectively manage Microsoft services. This recipe guides you through how to list all the commands available in your environment using the Microsoft Graph PowerShell module.

Getting ready

Follow the guidance in the *Setting up PowerShell* recipe from *Chapter 1, Microsoft 365 Setup and Basic Administration*, to connect to your Microsoft 365 tenant via PowerShell. Ensure you have administrative privileges in your system.

How to do it...

1. After you've opened PowerShell and connected to your tenant, run the following cmdlet:

```
Get-Command -Module Microsoft.Graph*
```

2. Review the output in the PowerShell window (a small sample of which is shown in *Figure 3.1*) to see all the cmdlets available in the Microsoft Graph and Microsoft Graph Beta PowerShell modules.

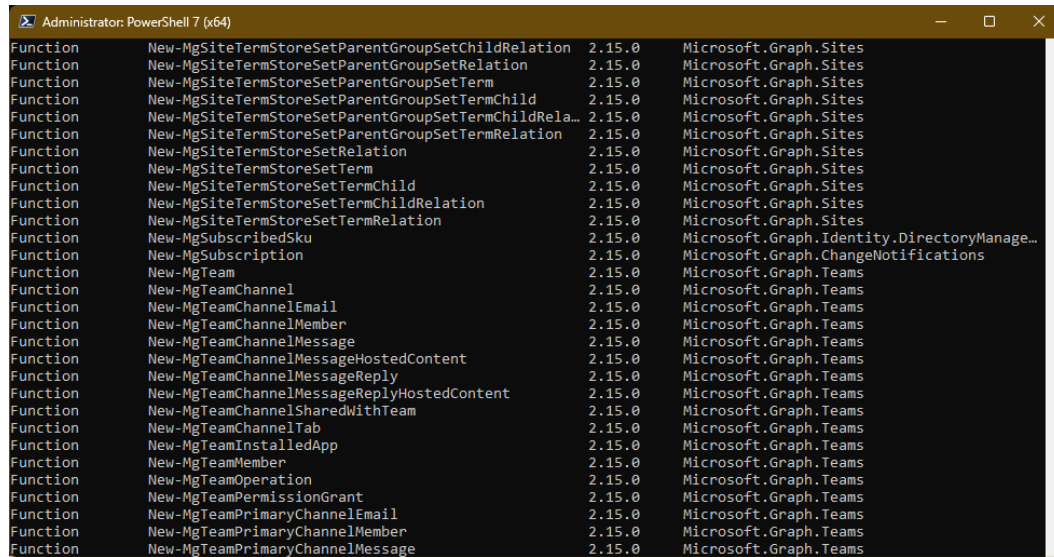


Figure 3.1 – Output of the Get-Command cmdlet

How it works...

The `Get-Command` cmdlet will display all the cmdlets available in the module(s) included in the `-Module` parameter. In this recipe, we used the Microsoft Graph and Microsoft Graph Beta PowerShell modules, which allow you to manage everything from users and devices to mail and calendars. The Microsoft Graph PowerShell module provides cmdlets that are auto-generated from the Microsoft Graph API, covering a broad spectrum of administrative functions. Commands follow a verb-noun naming convention, making them intuitive to use once you are familiar with PowerShell's syntax.

If you run `Get-Command` without a `-Module` parameter, it'll list all commands across all installed modules.

There's more...

In addition to listing commands, it's valuable to familiarize yourself with some of the most commonly used commands, or at least the commonly used patterns, within the Microsoft Graph PowerShell SDK. Here are a few key commands to know:

- `Connect-MgGraph`: Initiates a connection to Microsoft Graph, allowing you to start interacting with Microsoft 365 services. Authentication is required before executing other commands.
- `Get-MgUser`: Retrieves information about users in your organization. This command can be particularly useful for user management tasks such as reading properties and relationships of a user object.
- `Update-MgUser`: Allows you to update the properties of a user object, such as changing a user's job title or contact information.
- `New-MgUser`: Creates a new user in your Microsoft 365 tenant, enabling you to add users individually or in bulk.
- `Remove-MgUser`: Deletes a user, which is helpful in managing user accounts effectively, especially when offboarding employees.
- `Get-MgGroup`: Retrieves groups within the organization so that you can update them or use their details in other actions.
- `New-MgGroup`: Creates a new group in Microsoft 365, allowing you to specify details such as the group's display name, description, and membership type (e.g., dynamic or static).
- `Remove-MgGroup`: Deletes a group from Microsoft 365, which is useful for managing unused or obsolete groups and cleaning up resources.
- `Add-MgGroupMember` and `Remove-MgGroupMember`: These cmdlets manage members of a group, either adding new members or removing existing ones.

Tip

There are many commands you may utilize in the Microsoft Graph modules. Use the `Get - Help` cmdlet followed by any cmdlet to learn more about its purpose and use. For example, running `Get - Help Remove-MgGroup` will explain that it deletes a Microsoft 365 group that can be restored for 30 days until it's permanently deleted. It will also tell you all of the parameters you can use with the cmdlet and provide links to learn more.

Each of these commands utilizes the consistent and predictable patterns of the Microsoft Graph API, making them powerful tools for administrators.

See also

- *Get-Command*: <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/get-command>
- *Microsoft Graph PowerShell overview*: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/overview>

Creating a user

This recipe guides you through the process of creating a new user in your Microsoft 365 tenant using the Microsoft Graph PowerShell SDK. This is an essential task for administrators looking to onboard new employees into the organization's digital workspace.

Getting ready

Follow the guidance in the *Setting up PowerShell* recipe from *Chapter 1, Microsoft 365 Setup and Basic Administration*, to connect to your Microsoft 365 tenant via PowerShell. Ensure you have administrative privileges on your system, as well as administrative permissions to create user profiles in your Microsoft 365 tenant such as User Administrator or Global Administrator.

How to do it...

1. First, prepare the user details by defining the properties of the new user. In the simple example that follows, you'll define `DisplayName`, `UserPrincipalName`, `MailNickname`, and `Password` (be sure to update with your own values):

```
$userParams = @{
    DisplayName = "Echo Ottens"
    UserPrincipalName = "eottens@natechamberlain.com"
    MailNickname = "eottens"
    PasswordProfile = @{
        ForceChangePasswordNextSignIn = $true
        Password = "initialPassword123"
    }
    AccountEnabled = $true
}
```

2. Then, use the `New-MgUser` cmdlet along with your specified properties to create the user:

```
New-MgUser @userParams
```

How it works...

The `New-MgUser` cmdlet sends a request to Microsoft Graph to create a new user object with the properties defined in `$userParams`. This includes essential details such as the display name, **User Principal Name (UPN)** (synonymous with email address), and initial password settings. The cmdlet ensures that all required attributes are set, and the user account is enabled upon creation. The output of the command will confirm successful creation, like that shown in *Figure 3.2*:

```
PS C:\Users\ndcha> $userParams = @{
>>   DisplayName = "Echo Ottens"
>>   UserPrincipalName = "eottens@natechamberlain.com"
>>   MailNickname = "eottens"
>>   PasswordProfile = @{
>>       ForceChangePasswordNextSignIn = $true
>>       Password = "initialPassword123"
>>   }
>>   AccountEnabled = $true
>> }
>> New-MgUser @userParams

DisplayName Id                                     Mail UserPrincipalName
-----
Echo Ottens ccbcd199-48b2-4aa9-85ea-41cdf92478e8   eottens@natechamberlain.com
PS C:\Users\ndcha>
```

Figure 3.2 – Output of the `New-MgUser` cmdlet

You can run `Get-MgUser` afterward to double-check that the user has been created.

There's more...

We defined a few properties for our user in this recipe, but you can define even more in your actual `$userParams`, including common properties such as the following:

- `PreferredName`
- `Department`
- `JobTitle`
- `Photo`
- `EmployeeId`
- `BusinessPhones`

The `New-MgUser` cmdlet only works to create a new user and cannot be used again later to update that same user. See the *Changing user settings or profile information* recipe to learn how to update a user after creation.

See also

- *New-MgUser*: <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/new-mguser>
- *Working with users in Microsoft Graph*: <https://learn.microsoft.com/en-us/graph/api/resources/users>
- *Microsoft Graph PowerShell overview*: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/overview>

Disabling a user

This recipe explains how to disable a user in your Microsoft 365 tenant using the Microsoft Graph PowerShell SDK. Disabling a user is helpful for temporarily blocking sign-in to manage user access and security within your organization, such as when an employee may be on extended leave. Disabling a user may also be useful when an employee separates from your company but you don't want to delete the account entirely yet.

Getting ready

Follow the guidance in the *Setting up PowerShell* recipe from *Chapter 1, Microsoft 365 Setup and Basic Administration*, to connect to your Microsoft 365 tenant via PowerShell. Ensure you have administrative privileges on your system, as well as administrative permissions to modify user profiles in your Microsoft 365 tenant such as User Administrator or Global Administrator.

How to do it...

Run the following command to disable a user account by setting the `AccountEnabled` property to `$false`:

```
Update-MgUser -UserId "eottens@natechamberlain.com"  
-AccountEnabled:$false
```

How it works...

Setting `AccountEnabled` to `$false` blocks the user's sign-in but doesn't delete the account in case it needs to be re-enabled or used for other purposes, such as investigations, content recovery, or audits.

If you wish to confirm the account is disabled, you can check the user in the Microsoft 365 admin center to make sure their sign-in is blocked, as shown in *Figure 3.3*.

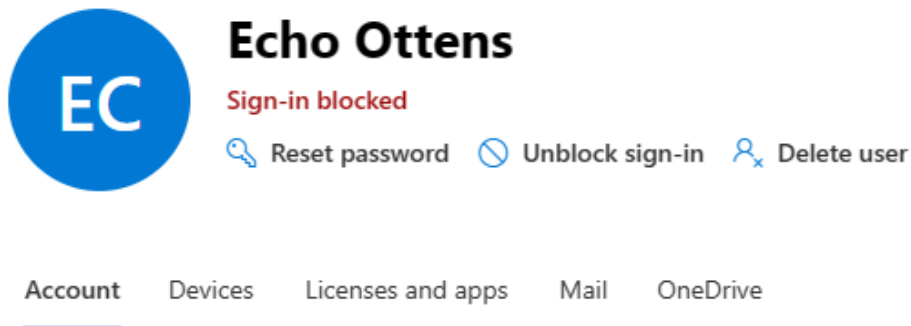


Figure 3.3 – A disabled user account in the admin center showing Sign-in blocked

Blocking sign-in by disabling the account will prevent access for that user, but it will not unlicense the account or reset their password. Those actions must be done separately.

There's more...

If you'd prefer to delete the user account entirely, use `Remove-MgUser` instead (be sure to update with your own values):

```
Remove-MgUser -UserId eottens@natechamberlain.com
```

Deleted accounts can be restored within 30 days.

See also

- *Update-MgUser*: <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/update-mguser>
- *Remove-MgUser*: <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/remove-mguser>
- *Working with users in Microsoft Graph*: <https://learn.microsoft.com/en-us/graph/api/resources/users>
- *Microsoft Graph PowerShell overview*: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/overview>

Changing user settings or profile information

This recipe describes how to change settings or profile information for a user in Microsoft 365 using the Microsoft Graph PowerShell SDK. Updating user details such as job roles or personal information is a common task for administrators.

Getting ready

Follow the guidance in the *Setting up PowerShell* recipe from *Chapter 1, Microsoft 365 Setup and Basic Administration*, to connect to your Microsoft 365 tenant via PowerShell. Ensure you have administrative privileges on your system, as well as administrative permissions to modify user profiles in your Microsoft 365 tenant such as User Administrator or Global Administrator.

How to do it...

Execute the `Update-MgUser` cmdlet to modify user settings. For example, to update a user's job title and department, use the following:

```
Update-MgUser -UserId "eottens@natechamberlain.com" -JobTitle "Senior  
Manager" -Department "Marketing"
```

How it works...

The `Update-MgUser` cmdlet modifies the specified properties of an existing user object in Microsoft Graph. By specifying the `-UserId` and the properties to update, this cmdlet sends a `PATCH` request (a method used to update specific properties of an existing resource without completely replacing it) to the Microsoft Graph API, applying the new values for the specified attributes.

You can verify your user's updated details in the Microsoft 365 admin center by checking their contact information, as shown in *Figure 3.4*.

Manage contact information

First name
Echo

Last name
Ottens

Display name *
Echo Ottens

Job title
Senior Manager

Department
Marketing

Figure 3.4 – The updated user's job title and department

There's more...

In addition to basic user profile information, you can also modify other attributes such as office location, contact information, and custom attributes if configured. For example, to change a user's office phone number and address, use the following:

```
Update-MgUser -UserId "eottens@natechamberlain.com" -BusinessPhones @
("123-456-7890") -StreetAddress "1234 Market St"
```

The list of available properties is quite extensive, but some other popular properties you might update via PowerShell include the following:

- GivenName (first name)
- Surname (last name)
- PreferredName (nickname)
- DisplayName

- Manager
- MailNickname

Check the resources in the *See also* section to find even more properties.

See also

- *Update-MgUser*: <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/update-mguser>
- *Working with users in Microsoft Graph*: <https://learn.microsoft.com/en-us/graph/api/resources/users>
- *Microsoft Graph PowerShell overview*: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/overview>

Getting a list of all users with user properties

This recipe outlines how to retrieve a list of all users in your Microsoft 365 tenant along with their user properties using the Microsoft Graph PowerShell SDK. This can be valuable for audits, compliance checks, or general administrative overviews.

Getting ready

Follow the guidance in the *Setting up PowerShell* recipe from *Chapter 1, Microsoft 365 Setup and Basic Administration*, to connect to your Microsoft 365 tenant via PowerShell. Ensure you have administrative privileges on your system, as well as administrative permissions to modify user profiles in your Microsoft 365 tenant such as User Administrator or Global Administrator.

How to do it...

Run the `Get-MgUser` cmdlet with selected properties to retrieve information about all users:

```
Get-MgUser -All | Format-Table DisplayName, UserPrincipalName,  
JobTitle, Department
```

How it works...

The `Get-MgUser` cmdlet fetches users from your Microsoft 365 tenant. You can specify which user properties to retrieve, helping to focus the output on relevant details. This cmdlet sends a GET request to Microsoft Graph, pulling data for each user based on the properties specified. `Format-Table` takes the value from the previous cmdlet (`Get-MgUser`) and provides the output in a table format.

The output of this command resembles the output shown in *Figure 3.5*:

```
PS C:\Users\ndcha> Get-MgUser -All | Format-Table DisplayName, UserPrincipalName, JobTitle, Department
```

DisplayName	UserPrincipalName	JobTitle	Department
Adele Vance	AdeleV@natechamberlain.com		
Alex Wilbur	AlexW@natechamberlain.com		
AutoAttendant	AutoAttendant_1601131652@natechamberlain.onmicrosoft.com		
Auto Help Desk	AutoHelpDesk@natechamberlain.com		
Conference Room A	ConferenceRoomA@natechamberlain.com		
Echo Ottens	eottens@natechamberlain.com	Senior Manager	
Heather Granger	heather@natechamberlain.com		

Figure 3.5 – Output of Get-MgUser

Notice how this could be helpful in quickly identifying users' missing properties such as JobTitle and Department.

There's more...

Add a -Filter parameter to limit the list of users returned. For example, to get only users whose DisplayName starts with S, you could run the following:

```
Get-MgUser -Filter "startsWith(DisplayName, 'S')" | Format-Table
DisplayName, UserPrincipalName, JobTitle, Department
```

Also, instead of Format-Table, you can try Format-List to see users in individual groups of properties, as shown in *Figure 3.6*.

```
DisplayName      : Echo Ottens
UserPrincipalName : eottens@natechamberlain.com
JobTitle         : Senior Manager
Department       :
```

Figure 3.6 – Output of Get-MgUser in list format

You may also wish to output the data to a CSV file instead for easier analysis and sharing. To do so, run `Get-MgUser -All | Select-Object DisplayName, UserPrincipalName, JobTitle, Department | Export-Csv -Path "C:\Path\To\Your\Folder\UsersList.csv" -NoTypeInfo` instead, updating the path to wherever you want the CSV file to be saved.

See also

- *Get-MgUser*: <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/get-mguser>
- *Working with users in Microsoft Graph*: <https://learn.microsoft.com/en-us/graph/api/resources/users>
- *Microsoft Graph PowerShell overview*: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/overview>

Changing a user password

This recipe outlines the procedure for changing a user's password in Microsoft 365, ensuring that you can manage user access and maintain security standards within your organization efficiently.

Getting ready

Follow the guidance in the *Setting up PowerShell* recipe from *Chapter 1, Microsoft 365 Setup and Basic Administration*, to connect to your Microsoft 365 tenant via PowerShell.

Ensure you have administrative privileges on your system, as well as administrative permissions to modify user profiles in your Microsoft 365 tenant such as User Administrator or Global Administrator.

Important note

Elevating privileges in a production environment requires careful consideration. You must have the appropriate API permissions and consent granted by an administrator for the following scope: `Connect-MgGraph -Scopes "Directory.AccessAsUser.All"`.

Before proceeding, ensure that your organization's security policies allow for this level of access. It's recommended to consult with your security team and understand the API permissions required by reviewing the information provided in the consent dialog.

How to do it...

Execute the following command to change the password for a specific user (be sure to update with your own values):

```
$userUPN="eottens@natechamberlain.com"
$newPassword="NewP@ssw0rd123"
$secPassword = ConvertTo-SecureString $newPassword -AsPlainText -Force
Update-MgUser -UserId $userUPN -PasswordProfile @{
  ForceChangePasswordNextSignIn = $true; Password = $newPassword }
```

How it works...

The `Update-MgUser` cmdlet is used to update the password for a user in Microsoft 365. The `ForceChangePasswordNextSignIn` parameter ensures that the user will have to change their password upon their next login, enhancing security, especially if the password reset is administrative.

There's more...

Consider implementing **multi-factor authentication (MFA)** and self-service password reset policies to enhance security further. These features empower users and reduce the administrative overhead of managing credentials. See the recipe titled *Enabling security defaults (MFA)* in *Chapter 2, Microsoft 365 Identity and Roles*, to learn more about these options included in security defaults.

See also

- *Update-MgUser*: <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/update-mguser>
- *Working with users in Microsoft Graph*: <https://learn.microsoft.com/en-us/graph/api/resources/users>
- *Microsoft Graph PowerShell overview*: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/overview>

Connecting via PowerShell to SharePoint Online

Microsoft Graph PowerShell provides a broad scope, interacting with various services across Microsoft 365, including SharePoint Online. It allows you to perform actions such as getting site information or managing SharePoint lists, but more specific administrative tasks (especially those that involve detailed configurations within SharePoint Online) might still require the SharePoint-specific cmdlets available in the **SharePoint Online Management Shell**.

This recipe will guide you through connecting to SharePoint Online using PowerShell, a necessary step for managing SharePoint Online via scripts.

Getting ready

Ensure you have administrative privileges on your system, as well as an administrative role as a SharePoint or Global Administrator to manage SharePoint Online.

To access SharePoint Online PowerShell cmdlets and functions, you must download and install the SharePoint Online Management Shell (link included in the *See also* section of this recipe).

How to do it...

1. Download and install **SharePoint Online Management Shell**.
2. Open **SharePoint Online Management Shell** from your start menu as administrator, as shown in *Figure 3.7*.

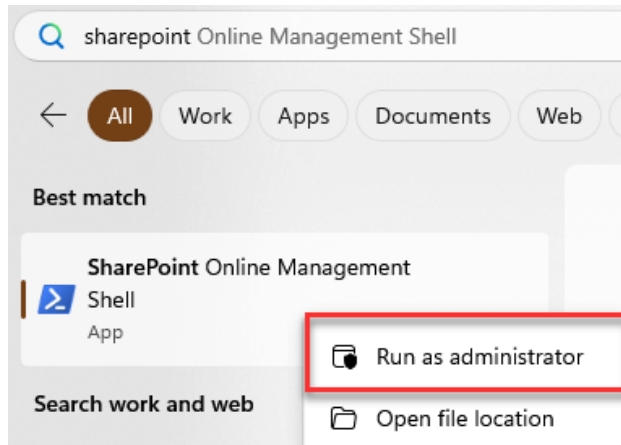


Figure 3.7 – SharePoint Online Management Shell

3. Run the following to sign in to the administrator account you wish to use, being sure to replace the URL with your own SharePoint admin center site URL:

```
Connect-SPOService -Url https://natechamberlain-admin.  
sharepoint.com
```

4. Sign in when prompted.

How it works...

The `Connect-SPOService` cmdlet establishes a connection to your SharePoint Online environment, allowing you to manage it through PowerShell. This connection is essential for executing further administrative commands within your tenant.

There's more...

Once connected, you can perform various administrative tasks such as creating and managing site collections, adjusting settings, and executing configurations. For instance, to list all site collections and their respective owners, you could use the following:

```
Get-SPOSite -Limit All
```


See also

- *Download SharePoint Online Management Shell*: <https://www.microsoft.com/en-us/download/details.aspx?id=35588>
- *Get started with SharePoint Online Management Shell*: <https://learn.microsoft.com/en-us/powershell/sharepoint/sharepoint-online/connect-sharepoint-online>

Creating a SharePoint Online site

This recipe will guide you through the process of creating a new site in SharePoint Online via the SharePoint Online Management Shell, an essential task for setting up collaborative and/or communication spaces efficiently for different teams or projects within your organization.

Getting ready

Ensure you have administrative privileges on your system, as well as an administrative role as a SharePoint or Global Administrator to manage SharePoint Online.

To access SharePoint Online PowerShell cmdlets and functions, you must download and install the SharePoint Online Management Shell (link included in the *See also* section of this recipe). Then, follow the instructions in the previous recipe, *Connecting via PowerShell to SharePoint Online*, to connect to your SharePoint Online environment.

How to do it...

1. Once connected to SharePoint Online via the SharePoint Online Management Shell, select the site template you wish to create from the options provided by running `Get-SPOWebTemplate` and take note of its name. Some of the most common are as follows:
 - **STS#3** | Team site (no Microsoft 365 group): Use this template when you need a team site without the overhead of a Microsoft 365 group and its associated apps such as a mailbox and calendar. This is particularly useful when you want to manage site permissions separately from a Microsoft 365 group.
 - **EHS#1** | Team site (with Microsoft 365 group): Ideal for scenarios where you want integrated collaboration features such as shared inboxes, calendars, and OneNote notebooks.
 - **SITEPAGEPUBLISHING#0** | Communication site: Perfect for building a site that is primarily used for broadcasting information across the organization, such as a department site that is part of your company's intranet.

2. Run the following command with your new site's specifications, including your chosen site template (be sure to update with your own values):

```
New-SPOSite -Url https://natechamberlain.sharepoint.com/sites/mynewsite -Owner eottens@natechamberlain.com -StorageQuota 1000 -Title "Echo Site" -Template SITEPAGEPUBLISHING#0
```

How it works...

The site creation process allows you to configure a new site collection with specific settings and properties tailored to your needs. This includes setting up the site's basic information, appearance, and functionality options, which will be immediately accessible and manageable by the designated site owner(s).

Utilizing PowerShell for creating SharePoint Online sites enhances efficiency, particularly beneficial in scenarios requiring multiple sites to be deployed simultaneously. PowerShell scripts allow for batch creation and automation of site setups, enabling consistent configurations across several sites without the repetitive manual input required in the SharePoint admin center. This method significantly streamlines the process, reducing both time and potential for error, and is ideal for large-scale deployments or routine maintenance tasks that include site creation.

There's more...

Expanding on the capabilities of PowerShell in managing SharePoint Online sites, administrators can leverage additional commands to further customize and automate tasks. For example, you can automate site configurations and permissions management:

- **Automate site configurations:** After creating a site, you might want to configure its settings automatically. You can use PowerShell scripts to set up navigation, site policies, and branding according to predefined company standards. For example, to update a site's logo and regional settings, replace the site URL, path to logo, and regional information with yours in the following:

```
Set-SPOSite -Identity https://natechamberlain.sharepoint.com/sites/mynewsite -LogoFilePath "path/to/logo.jpg" -TimeZoneId 13 -LocaleId 2057
```

- **Manage permissions efficiently:** PowerShell allows you to manage site permissions programmatically. This can be especially useful for large organizations where permissions need to be dynamically updated based on user roles or group memberships. The following example adds user@natechamberlain.com to the Team Site Members SharePoint permissions group for the mynewsite site:

```
Add-SPOUser -Site https://natechamberlain.sharepoint.com/sites/mynewsite -LoginName user@natechamberlain.com -Group "Team Site Members"
```

For more advanced automation scenarios, consider exploring **SharePoint PnP PowerShell**, which provides a library of PowerShell commands that are designed to perform complex provisioning and site management tasks more efficiently than the standard SharePoint Online Management Shell. Learn more about SharePoint PnP PowerShell at <https://learn.microsoft.com/en-us/powershell/sharepoint/sharepoint-pnp/sharepoint-pnp-cmdlets>.

See also

- *New-SPOSite*: <https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/new-sposite>
- *Get-SPOWebTemplate*: <https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/get-spowebtemplate>

Adding a new site admin to all SharePoint Online sites

This recipe details the process of assigning a new site administrator across all SharePoint Online sites using the SharePoint Online Management Shell. This approach is efficient for managing access across multiple sites simultaneously and will be useful for granting org-wide site access to site developers without granting the full SharePoint admin role.

Getting ready

Ensure you have administrative privileges on your system, as well as an administrative role as a SharePoint or Global Administrator to manage SharePoint Online.

To access SharePoint Online PowerShell cmdlets and functions, you must download and install the SharePoint Online Management Shell (link included in the *See also* section of this recipe). Then, follow the instructions in this chapter's earlier recipe, *Connecting via PowerShell to SharePoint Online*, to connect to your SharePoint Online environment.

How to do it...

1. Once connected to SharePoint Online via the SharePoint Online Management Shell, fetch all site collections where you want to add the new admin by running the following:

```
$sites = Get-SPOSite -Limit All
```

2. Loop through each site and add the new administrator. Replace `eottens@natechamberlain.com` with the actual email of the new admin:

```
foreach ($site in $sites) {  
    Set-SPOUser -Site $site.Url -LoginName "eottens@  
natechamberlain.com" -IsSiteCollectionAdmin $true  
}
```

Here is a breakdown of what's happening:

- The `foreach` loop iterates over each site collection stored in the `$sites` variable.
- The `$site` variable represents the current site collection in the loop during each iteration.
- The `Set-SPOUser` cmdlet is used to add the new site administrator. The `-Site` parameter specifies the URL of the site collection (accessed via `$site.Url`), and the `-LoginName` parameter specifies the new admin's email address.
- The `-IsSiteCollectionAdmin $true` parameter grants the specified user full administrative rights to the site collection.

This loop will process each site in your tenant, applying the new admin's permissions to all of them.

How it works...

SharePoint Administrators typically have extensive permissions across an organization but may lack the time or specific expertise to manage individual sites effectively. Instead of increasing the number of SharePoint Administrators, which can introduce security vulnerabilities, it's often more prudent to selectively elevate individuals with the necessary knowledge and skills. While it's uncommon to need a new administrator for all sites, certain situations make this action particularly advantageous. For instance, during organizational restructuring, roles and responsibilities among IT staff may shift. If a senior IT member is promoted to oversee all SharePoint operations, they would require administrative access to all sites. Utilizing PowerShell to assign this administrator across all sites not only streamlines the process but also ensures that access rights are uniformly applied, reducing potential disruptions and bolstering security during these transitions. This approach is essential for sustaining operational continuity and adhering to security standards in dynamic corporate settings.

There's more...

To achieve the opposite (removing a specific individual as a site admin for all sites), simply replace `$true` with `$false` in the `-IsSiteCollectionAdmin` parameter.

If you accidentally lock yourself out of SharePoint sites, you can follow these steps to regain access:

1. Navigate to the SharePoint admin center by going to the Microsoft 365 admin center (<https://admin.microsoft.com>) and then select **All admin centers | SharePoint**.
2. In the SharePoint admin center, select **Sites | Active Sites**.
3. Select the site(s) you need access to, and then select **Membership**.
4. Add yourself or the relevant admin back as a site admin or site owner.

This approach ensures you can regain control without needing to run additional scripts.

See also

- *Set-SPOUser*: <https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spouser>

Restoring a deleted OneDrive site

This recipe provides a step-by-step guide on how to restore a deleted OneDrive site in SharePoint Online, an important skill for administrators managing data continuity and recovery. Administrators may face this challenge when an employee departs the organization, leading to the automatic deletion of their OneDrive site after 30 days. However, if the site is needed again during the period between 30 to 93 days post-deletion, retrieving it can be more complex. This recipe aims to simplify that process, ensuring that critical data can be restored in a timely manner when necessary.

Getting ready

Ensure you have administrative privileges on your system, as well as an administrative role as a SharePoint or Global Administrator to manage SharePoint Online.

To access SharePoint Online PowerShell cmdlets and functions, you must download and install the SharePoint Online Management Shell (link included in the *See also* section of this recipe). Then, follow the instructions in this chapter's earlier recipe, *Connecting via PowerShell to SharePoint Online*, to connect to your SharePoint Online environment.

How to do it...

1. First, ensure you're connected to SharePoint Online with administrative credentials. Use the SharePoint Online Management Shell for this purpose (be sure to update with your own SharePoint admin center URL):

```
Connect-SPOService -Url https://natechamberlain-admin.sharepoint.com
```

2. You need to find the URL of the deleted OneDrive site. If you don't have it, you can list all deleted personal sites (OneDrive sites) with the following:

```
Get-SPODeletedSite -IncludeOnlyPersonalSite | Format-Table Url
```

3. Once you have the URL, you can restore the OneDrive site using the following:

```
Restore-SPODeletedSite -Identity URL_OF_DELETED_ONEDRIVE
```

Important note

If you receive an **Unable to find the deleted site** error message, check the URL. Do not include the final / at the end of the URL.

4. After restoration, assign a site collection administrator (such as the former employee's manager) so they can access and manage the OneDrive site:

```
Set-SPOUser -Site URL_OF_RESTORED_ONEDRIVE -LoginName manager@  
yourdomain.com -IsSiteCollectionAdmin $true
```

How it works...

When a user is deleted, their OneDrive is retained according to the retention settings specified in the SharePoint admin center, typically 30 days by default. After this period, OneDrive enters a deleted state for 93 days, during which it can be restored.

Accessing the **Deleted sites** screen of the SharePoint Online admin center allows administrators to review and restore these sites within this time frame. Restoring the site reinstates the user's OneDrive with all its files and configurations intact as they were before deletion.

There's more...

Consider setting up alerts or logs to monitor deletions, which can help in understanding patterns or preventing accidental deletions. Additionally, regularly backing up important data from OneDrive sites can provide an extra layer of security against data loss.

See also

- *Restoring a deleted OneDrive for Business site:* <https://support.microsoft.com/en-us/office/restoring-a-deleted-onedrive-for-business-site-c5595183-a1ef-4931-8201-48a62134f5af>

Hiding Microsoft 365 groups from the Global Address List

This recipe will show you how to hide Microsoft 365 groups from the **Global Address List (GAL)** using PowerShell. This can be useful for reducing clutter or keeping specific groups hidden from general visibility in your organization.

Getting ready

You need to be a Global Administrator or Exchange Administrator or have equivalent permissions to perform these steps. Run PowerShell as a System Administrator to complete the steps in this recipe.

How to do it...

1. Install the ExchangeOnline PowerShell module if you haven't already by running `Install-Module -Name ExchangeOnlineManagement`.
2. Use the `Connect-ExchangeOnline` cmdlet to establish a session with your Exchange Online environment (be sure to update it with your own UPN):

```
Connect-ExchangeOnline -UserPrincipalName admin@example.com  
-ShowProgress $true
```

3. Use the `Set-UnifiedGroup` cmdlet to hide the group. Replace `GroupName` with the name of the group you wish to hide:

```
Set-UnifiedGroup -Identity "GroupName"  
-HiddenFromAddressListsEnabled $true
```

How it works...

The `Set-UnifiedGroup` cmdlet is used to configure the properties of Microsoft 365 groups. The `-HiddenFromAddressListsEnabled` parameter specifically controls whether the group is visible in the GAL. Setting this parameter to `$true` ensures the group will not be listed, thereby keeping it hidden from general user visibility. Upon running the script, you won't see a confirmation but will simply be able to continue submitting PowerShell commands, as shown in *Figure 3.8*.

```
PS C:\Windows> Set-UnifiedGroup -Identity "FilesDemo" -HiddenFromAddressListsEnabled $true  
PS C:\Windows>
```

Figure 3.8 – Output of hiding a group from the GAL

There's more...

Consider periodically reviewing which groups are hidden to ensure that new members or changes in policy are reflected. Hiding groups can be reversed by setting the `-HiddenFromAddressListsEnabled` parameter to `$false` if needed in the future.

This process is particularly beneficial for managing clutter in the GAL and maintaining privacy for certain groups, such as executive teams or specific project groups, within large organizations.

See also

- *Connect to Exchange Online PowerShell*: <https://learn.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps>
- *Set-UnifiedGroup*: <https://learn.microsoft.com/en-us/powershell/module/exchange/set-unifiedgroup>

Preventing external senders from emailing internal Microsoft 365 groups

This recipe provides the necessary steps for preventing external senders from emailing internal Microsoft 365 groups, enhancing control over email communication, and improving security.

Getting ready

Ensure you are an Exchange Administrator or Global Administrator. This task requires the use of the Exchange Online PowerShell module, which should be installed (`Install-Module -Name ExchangeOnlineManagement`).

How to do it...

1. Use the `Connect-ExchangeOnline` cmdlet to establish a session (be sure to update it with your own UPN):

```
Connect-ExchangeOnline -UserPrincipalName admin@example.com  
-ShowProgress $true
```

2. Use the `Set-UnifiedGroup` cmdlet to restrict external senders. Replace `GroupName` with the name of your Microsoft 365 group:

```
Set-UnifiedGroup -Identity "GroupName"  
-RequireSenderAuthenticationEnabled $true
```


How it works...

The `Set-UnifiedGroup` cmdlet configures the properties of Microsoft 365 groups. The `-RequireSenderAuthenticationEnabled` parameter set to `$true` ensures that only authenticated senders within your organization can send emails to the group, thus blocking external emails. Internal group members are still able to send emails externally, however.

This configuration helps maintain secure and controlled communication within Microsoft 365 groups, preventing unauthorized external entities from sending potentially harmful or spam emails to group members.

There's more...

Before implementing this change, you might want to inform group members, owners, and other stakeholders about the update to manage their expectations of communication flow. Additionally, you should regularly review these settings to adapt to any changes in your organization's communication policies or security requirements.

See also

- *Set-UnifiedGroup*: <https://learn.microsoft.com/en-us/powershell/module/exchange/set-unifiedgroup>

4

Managing Exchange Online

Exchange Online offers robust email management capabilities tailored to modern enterprise needs. This chapter guides administrators through the essential tasks and optimizations for their Exchange Online environment, ensuring effective and secure email communication across an organization.

We will explore the updated features of the **Exchange admin center**, which is the primary tool for managing Exchange Online settings. The Exchange admin center has been designed to align closely with the overall Microsoft 365 admin experience, providing a more user-friendly and unified management interface. From mailbox and group management to migration tools and security protocols, this chapter covers the essential administrative tasks to enhance operational efficiency and security.

We will cover the following recipes in this chapter:

- Creating a new user with a mailbox
- Creating a mail-enabled security group
- Creating an Exchange Online shared mailbox
- Creating a distribution list
- Creating a dynamic distribution list
- Creating an Exchange-specific retention policy
- Creating a mail flow rule
- Configuring spam filter policies
- Creating room and equipment resources
- Enabling **Advanced Threat Protection (ATP)** features

Technical requirements

To manage Exchange Online effectively, administrators need a Microsoft 365 subscription that includes an Exchange Online plan (there are two), and they must be assigned either the Global Administrator or Exchange Administrator roles within the Microsoft 365 admin center. These roles provide the necessary permissions to manage email settings, security protocols, and compliance features.

Creating a new user with a mailbox

Creating a new user with a mailbox in Exchange Online involves using the Microsoft 365 admin center or Exchange Online PowerShell. This process not only sets up the mailbox but also integrates it within your Microsoft 365 environment, ensuring that the user is ready to communicate and collaborate.

Getting ready

Before starting, ensure that you have administrative access to the Microsoft 365 admin center. You will also need a valid Microsoft 365 license that includes Exchange Online to assign to the user.

Important note

While the Exchange admin center can be used for many things related to mailboxes, user mailboxes can only be created or deleted from the Microsoft 365 admin center.

How to do it...

1. Log into the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Navigate to **Users | Active Users**.
3. Select **Add a user** and fill in the user details, such as name, username, and domain.
4. Set up the password options and decide whether to auto-generate a password or create one manually. Also, choose whether the new user should be required to create a new password upon signing in. This screen is shown in *Figure 4.1*.

Add a user

● Basics

○ Product licenses

○ Optional settings

○ Finish

To get started, fill out some basic information about who you're adding as a user.

First name

Pippin

Last name

Vinyard

Display name *

Pippin Vinyard

Username *

pvinyard

Domains

@ chambernate.onmicrosoft.com

☒ Automatically create a password

☒ Require this user to change their password when they first sign in

☐ Send password in email upon completion

Next

Figure 4.1 – The new user creation screen in the Microsoft 365 admin center

5. Select **Next**, and then assign a Microsoft 365 license that includes Exchange Online to automatically create the mailbox.

Important note

The preceding action does not just create a mailbox but also sets up a new user profile in Microsoft 365. The mailbox is created because a Microsoft 365 license that includes Exchange Online is assigned directly to the user during this process.

6. Select **Next** to then configure any optional settings, such as administrative role assignments, or additional profile information, such as department and job title. Then, select **Next** again.

7. Review the new user's details on the confirmation screen. Then, select **Finish adding**, as shown in *Figure 4.2*, to create the user and, by extension, as they've been assigned a license with Exchange Online included, their mailbox.

Add a user

✓ Basics

✓ Product licenses

✓ Optional settings

● **Finish**

Review and finish

Assigned Settings
Review all the info and settings for this user before you finish adding them.

Display and username
Pippin Vinyard
pvinyard@chambernate.onmicrosoft.com
[Edit](#)

Password
Type: Auto-generated
[Edit](#)

Product licenses
Location: United States
Licenses: Microsoft 365 E5 Developer (without Windows and Audio Conferencing)
Apps: Defender Platform for Office 365, Immersive spaces for Teams, Purview Discovery, 69 more
[Edit](#)

Back

Finish adding

Figure 4.2 – The new user confirmation screen

How it works...

When you create a user mailbox through the admin center, assigning a Microsoft 365 license automatically initiates the mailbox setup in Exchange Online.

While this recipe describes a direct license assignment, it's important to note that this method might not be the most efficient for enterprise environments. Assigning licenses via security groups is a more common and scalable approach in large organizations. This method allows for easier management and automation of license assignments based on roles, departments, or other criteria, reducing the administrative overhead of managing licenses on an individual basis.

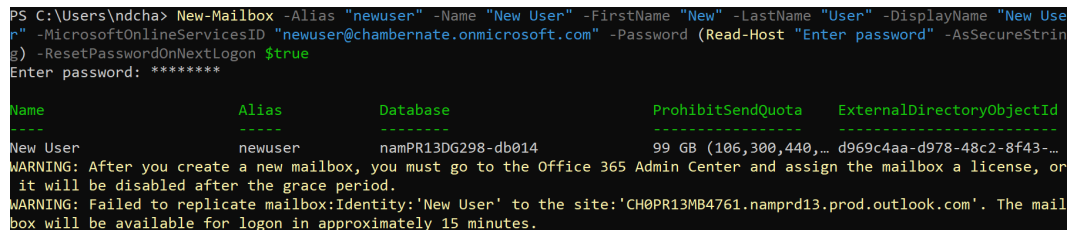
There's more...

You can also create mailboxes using PowerShell by following these steps:

1. Open PowerShell as an administrator.
2. Install the ExchangeOnlineManagement module if you haven't already by running `Install-Module -Name ExchangeOnlineManagement`.
3. Connect to Exchange Online via PowerShell by running `Connect -Exchange` and signing in with your administrator account.
4. Execute the command to create a new mailbox and user account, such as the following:

```
New-Mailbox -Alias newuser -Name 'New User' -FirstName
'New' -LastName 'User' -DisplayName 'New User'
-MicrosoftOnlineServicesID 'newuser@yourdomain.com'
-Password (Read-Host "Enter password" -AsSecureString)
-ResetPasswordOnNextLogon $true
```

5. A prompt to enter a password will appear. After entering the password, the mailbox and user account are created, and you must then assign the new account a Microsoft 365 license that includes Exchange Online. The output of this PowerShell command is shown in *Figure 4.3*.



```
PS C:\Users\ndcha> New-Mailbox -Alias "newuser" -Name "New User" -FirstName "New" -LastName "User" -DisplayName "New User" -MicrosoftOnlineServicesID "newuser@chambersnate.onmicrosoft.com" -Password (Read-Host "Enter password" -AsSecureString) -ResetPasswordOnNextLogon $true
Enter password: *****

Name                           Alias       Database              ProhibitSendQuota  ExternalDirectoryObjectId
-----
New User                        newuser     namPR13DG298-db014    99 GB (106,300,440,... d969c4aa-d978-48c2-8f43-...
WARNING: After you create a new mailbox, you must go to the Office 365 Admin Center and assign the mailbox a license, or it will be disabled after the grace period.
WARNING: Failed to replicate mailbox:Identity:'New User' to the site:'CH0PR13MB4761.namprd13.prod.outlook.com'. The mailbox will be available for logon in approximately 15 minutes.
```

Figure 4.3 – The output of PowerShell command used to create a new user and mailbox

In PowerShell, the `New-Mailbox` cmdlet combines user creation and mailbox setup in one step, streamlining the process and linking it directly to the license assignment.

After creating the mailbox, consider setting up additional configurations such as email forwarding, mailbox permissions, or advanced features such as archiving and retention policies, depending on the user's role and your organization's compliance needs.

See also

- *Create user mailboxes in Exchange Online:* <https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/create-user-mailboxes>
- *Manage user mailboxes in Exchange Online:* <https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-user-mailboxes/manage-user-mailboxes>

Creating a mail-enabled security group

Creating a **mail-enabled security group** in Microsoft 365 is a versatile function for organizations. It functions similarly to a distribution list in that it allows you to send emails to multiple recipients using a single email address. However, unlike a standard distribution list, a mail-enabled security group also enables you to control access to resources, such as files and hardware, within your organization. This dual functionality makes it highly valuable for managing both communication and permissions efficiently, without the additional features of a Microsoft 365 group, such as a SharePoint site and OneNote notebook that may not be needed for all teams or projects.

Getting ready

Before you begin, ensure that you have admin rights in the Exchange admin center as a Global or Exchange Administrator. You can also be a non-administrator with the Organization Management or Recipient Management roles assigned to you via **Role-Based Access Control (RBAC)**.

Tip

RBAC in Microsoft 365 is a security mechanism that assigns permissions to users based on their role within an organization. This system allows administrators to control access to resources, ensuring that users have the appropriate level of access for their roles, which simplifies management and enhances security across Microsoft 365 services without designating too many individuals as administrators (which often include more permissions than necessary).

How to do it...

1. Log into the Exchange admin center at `https://admin.exchange.microsoft.com`.
2. In the Exchange admin center, select **Groups** from the left navigation menu.
3. Select **Add a group** at the top of the screen.
4. Choose the type labeled **Mail-enabled security** from the group types available, as shown in *Figure 4.4*.

Home > Groups > Add a group

Group type

Basics

Owners

Members

Settings

Finish

Choose a group type

Choose the group type that best meets your team's needs. [Learn more about group types](#)

☐ **Microsoft 365 (recommended)**
Allows teams to collaborate by giving them a group email and a shared workspace for conversations, files, and calendars. In Outlook, these are called Groups.

☐ **Distribution**
Creates an email address for a group of people.

☒ **Mail-enabled security**
Sends messages to all members of the group and gives access to resources like OneDrive, SharePoint and admin roles

Next **Cancel**

Figure 4.4 – The Mail-enabled security option selected for a new group configuration

5. Enter the group name and description; then, select **Next**.
6. Click **Assign owners** and enter the names or email addresses of the owners you wish to include in the group. Having at least two owners is recommended per group.
7. Click **Next** and then **Add members** and enter the names or email addresses of the members you wish to include in the group. Members will receive an email after being added.
8. Select **Next**; then, add the group's email address, and choose whether external persons can email the new group and whether approval is required to join the group, as shown in *Figure 4.5*.

Home > Groups > Add a group

✓ Group type

✓ Basics

✓ Owners

✓ Members

Settings

○ Finish

Edit settings

Mail-enabled security group

Has all the functionality of a distribution list and additionally can be used to control access to OneDrive and SharePoint.

Group email address *

M365Admins

Domains

@ chambernate.onmicrosoft.com

Communication

☐ Allow people outside of my organization to send email to this Mail-enabled security group

Approval

☒ Require owner approval to join the group

Back

Next

Cancel

Figure 4.5 – The settings screen for a new mail-enabled security group

9. Select **Next** to review the settings and select **Create group** to create the mail-enabled security group.

How it works...

A mail-enabled security group combines the properties of a security group and a distribution list. This type of group not only simplifies email communication by allowing you to send an email to multiple users at once; it also provides an additional layer of security by restricting access to resources.

Your owners will be able to manage the membership of a group, and any members added will receive an email notification. Once the group is created, the assigned owners have specific responsibilities and capabilities, including the following:

- **Managing membership:**
 - Owners can add or remove members from a group. This can be done directly in the Exchange admin center by navigating to the group's settings and adjusting the membership list.
 - They can also approve or deny requests to join the group if it is configured to require approval for new members.
- **Configuring group settings:**
 - Owners can modify group settings, such as whether external senders can email a group or whether it requires approval to join
 - They can change the group's display name, email address, and description to ensure that it remains relevant and appropriately labeled
- **Delegating permissions:**
 - Owners can assign additional owners to a group, ensuring that there is always someone available to manage the group even if the original owner is unavailable.
 - They can also configure who has permission to send emails on behalf of the group, which is useful for scenarios where certain individuals need to communicate on behalf of the team or project that the group represents.
- **Monitoring group activity:**
 - Owners can review group activity and usage through the Exchange admin center. This helps in understanding how frequently a group is used for communication and whether it fulfills its intended purpose.

Note that it can take up to an hour before a new mail-enabled security group shows up in users' group lists.

There's more...

When it comes to groups in Microsoft 365, you'll choose between **mail-enabled security groups**, normal **security groups**, **distribution lists**, or **Microsoft 365 groups**. *Table 4.1* compares the features and abilities of each to help you to decide which is most suitable for each situation.

Feature	Mail-enabled security group	Security group	Distribution list	Microsoft 365 group
Purpose	Used for security permissions and email distribution.	Used to grant access permissions to resources.	Used primarily for email distribution without any security permissions.	Used for collaboration between users, integrating various Microsoft 365 services.
Email capability	Yes, it can receive emails as a group.	No email capabilities.	Yes, it can receive emails as a group.	Yes, it comes with an email inbox and a calendar, and it integrates with other Microsoft 365 apps. It can function as a distribution list with configuration.
Security permissions	Yes, it can be used to assign permissions to resources.	Yes, it is used to assign permissions to resources.	No, it does not provide security permissions.	Yes, it can be used to control access to group resources such as SharePoint sites and Planner.
Integration with Microsoft 365	Limited to email functionality and security permissions.	Limited to security permissions.	Limited to email distribution capabilities.	Extensive, and integrates with SharePoint, Teams, Planner, and so on.
Membership visibility	Can be viewed and managed in the Exchange admin center and Entra ID.	Managed through Entra ID.	Can be viewed and managed in the Exchange admin center and Entra ID.	Can be viewed and managed in Entra ID and across various Microsoft 365 admin centers.

Feature	Mail-enabled security group	Security group	Distribution list	Microsoft 365 group
Use case examples	Granting access to a SharePoint site and sending group emails to its members.	Restricting access to a network folder or SharePoint site only to group members.	Sending newsletters to a large number of employees.	Collaborating on a project, with shared resources such as files, calendars, and tasks.
Creation and management	Created and managed through the Exchange admin center or Azure AD.	Created and managed via Entra ID.	Created and managed through the Exchange admin center.	Created and managed via the Microsoft 365 admin center or through apps such as Teams.

Table 4.1 – A feature comparison for different group types

See also

- *Manage mail-enabled security groups in Exchange Online:* <https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-mail-enabled-security-groups>
- *Create and manage distribution list groups in Exchange Online:* <https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-distribution-groups/manage-distribution-groups>
- *Manage a group in the Microsoft 365 admin center:* <https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/manage-groups>
- *Manage user mailboxes in Exchange Online:* <https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-user-mailboxes/manage-user-mailboxes>

Creating an Exchange Online shared mailbox

A shared mailbox in Microsoft 365 allows multiple users to read and send emails from a common email address, such as `info@yourcompany.com`, without requiring a Microsoft 365 group. This setup is ideal for teams that require access to a common mailbox without the additional features of a group, such as a SharePoint site or team, for real-time communication among its members.

Getting ready

Ensure that you have administrative rights to access the Exchange admin center within Microsoft 365, as you will need these to set up the shared mailbox.

How to do it...

1. Log into the Exchange admin center at `https://admin.exchange.microsoft.com`.
2. Once in the Exchange admin center, select **Recipients | Mailboxes** in the left navigation menu, as shown in *Figure 4.6*.

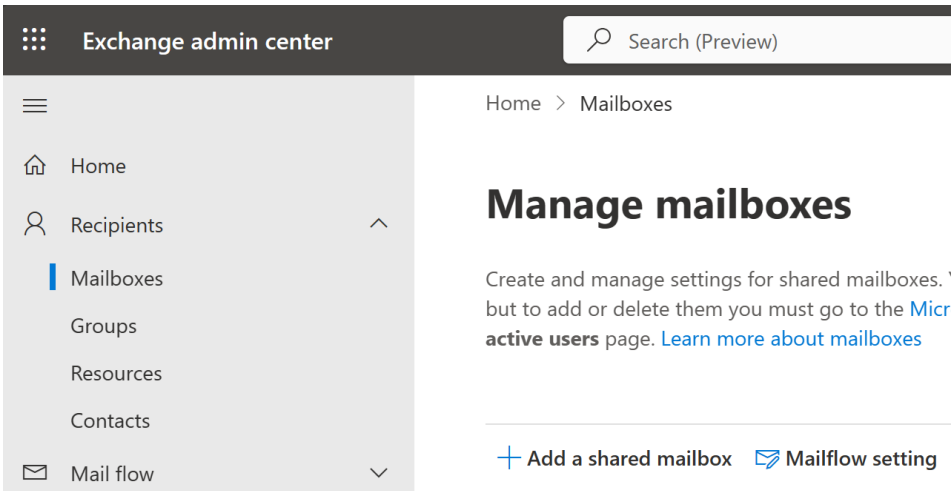


Figure 4.6 – The location of mailbox management in the Exchange admin center

3. Select **Add a shared mailbox**.
4. Fill in the required fields, such as **Display name**, **Email address**, and **Alias**, and select the desired domain for the shared mailbox, as shown in *Figure 4.7*.

Add a shared mailbox

Email can be sent to and from the name and email address of the shared mailbox, rather than an individual. After you create the shared mailbox, you can add members who can read and reply to email.

Display name *

Email address *

@



Alias

Create

Figure 4.7 – The shared mailbox detail configuration screen

5. Click **Create**; then, click **Add users to this mailbox | Add members**. Here, you can specify the users who will have full access to the mailbox. Full access allows users to send emails as the mailbox identity itself (e.g., a user sends an email to the entire organization but it appears to come from human resources) and grants them full permissions as the mailbox owner to manage its settings. To specify users who will have full access, search for and select users, and then click **Save** and **Confirm**.

How it works...

The shared mailbox does not require a license and provides a cost-effective solution for team email communication. Users given access can read and send emails as the mailbox identity, share the calendar, and coordinate appointments without individual ownership.

Important note

The individuals you add as delegates during the initial setup in this recipe are given full access as the mailbox owner(s). If you want to limit member permissions to only sending as the mailbox, add those members after creation instead.

Note that it may take up to an hour for the new shared mailbox to appear.

There's more...

While a shared mailbox does not have a direct login, users can access it through their own Outlook profiles, provided they have the necessary permissions. This setup is particularly useful for customer service and support teams.

After creating the mailbox, you can select it from the **Manage mailboxes** screen, and then select **Delegation**, as shown in *Figure 4.8*, to modify permissions, including adding members who can only send as the mailbox without having full access.

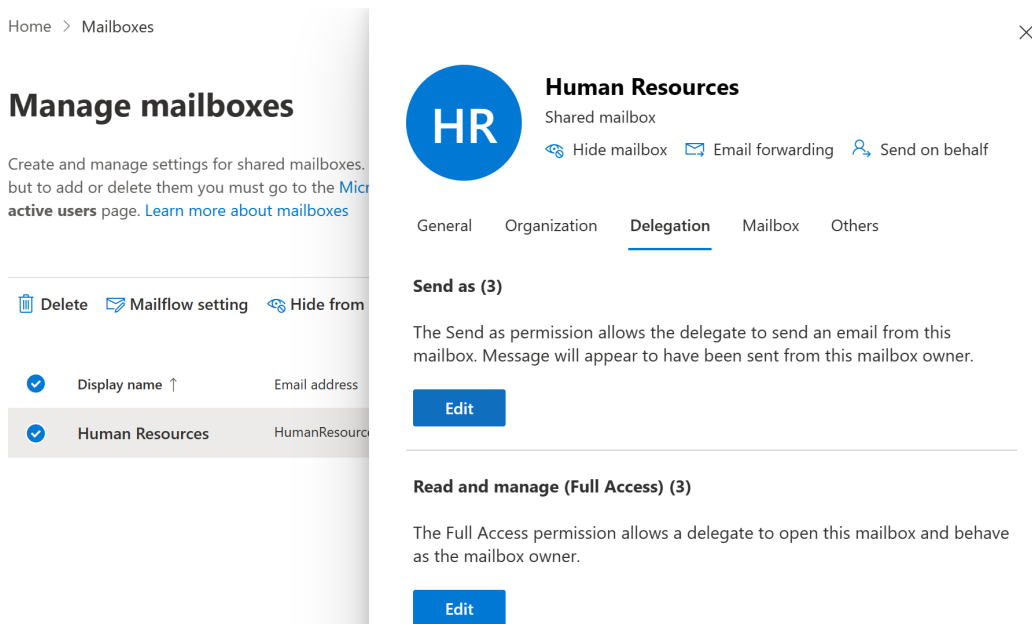


Figure 4.8 – The mailbox Delegation tab

See also

- *Manage permissions for recipients in Exchange Online:* <https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-permissions-for-recipients>
- *Shared mailboxes in Exchange Online:* <https://learn.microsoft.com/en-us/exchange/collaboration-exo/shared-mailboxes>

Creating a distribution list

A distribution list in Microsoft 365 is a type of email group used to send notifications to a group of people. It's an effective tool for email communication within an organization, especially for sending updates and information to a specific department or team.

Getting ready

Ensure that you have administrative rights to access the Exchange admin center within Microsoft 365. Specifically, you will need to be assigned the Exchange Administrator role or another role that includes the necessary permissions to create and manage distribution lists. Simply having access as a reader will not allow you to execute this recipe.

How to do it...

1. Log into the Exchange admin center at <https://admin.exchange.microsoft.com>.
2. Once in the Exchange admin center, select **Recipients | Groups** in the left navigation menu, as shown in *Figure 4.9*.

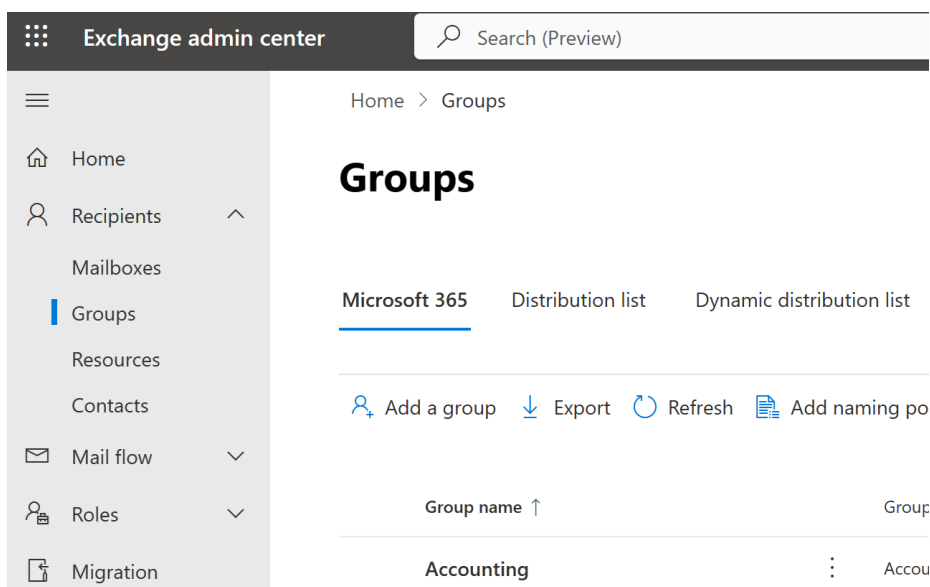


Figure 4.9 – The Groups screen in the Exchange admin center

3. Select **Add a group** and then **Distribution** from the list of options.

4. Click **Next** to go to the **Basics** screen, and then enter the name and description of your distribution list.
5. Click **Next** to go to the **Owners** screen, and then search for and add owners who will have the ability to rename the group, manage its membership, and change group settings.
6. Click **Next** to go to the **Members** screen, and then search for add members who will be recipients of any messages sent to the new distribution list.
7. Click **Next** to go to the **Settings** screen, and then specify the group settings, including the following:
 - **Group email address and Domain**
 - Whether external persons can email your distribution list
 - Whether internal persons can opt to join the list without owner approval or invitations from existing members
 - Whether members can opt to leave the list without owner approval
8. Click **Next** to go to the **Finish** screen to review the new distribution list's configuration; then, click **Create group** when finished.

How it works...

The distribution list allows emails to be sent to multiple recipients under a single email address, streamlining communications. It does not have its own mailbox but acts as a mail forwarding service to distribute messages among members. This option is useful in disseminating information to a consistent group of individuals who don't need additional features, such as a team in Teams or a site in SharePoint.

Distribution lists are simple to manage by non-IT staff and can be modified or updated to add or remove members as team dynamics change. They are ideal for situations where group collaboration is not needed and only email communication is required.

There's more...

Beyond the essential steps of creating a distribution list, you can utilize other functionalities and management options to enhance your distribution list's effectiveness and compliance, such as the following:

- **Dynamic distribution groups:** Unlike the standard distribution lists, dynamic distribution groups include recipients based on specific filters and conditions, rather than a fixed set of members. We will learn how to create these in the next recipe, *Creating a dynamic distribution list*.

- **Mail tips:** Configure mail tips to alert users before sending emails to large distribution lists or external recipients. This can help to prevent unintended information disclosure and manage email flow more effectively. Get started in the Exchange admin center by navigating to **Recipients | Mailboxes** and selecting your distribution list. Once there, select the **Other** tab and then **Manage mail tip** under **Mail tip**. You can enter up to 175 characters to be shown to a user before they email this list.

Note that these features are also available for dynamic distribution lists and mail-enabled security groups.

See also

- *Create and manage distribution list groups in Exchange Online:* <https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-distribution-groups/manage-distribution-groups>

Creating a dynamic distribution list

A dynamic distribution list in Microsoft 365 automatically updates its membership based on specific user attributes, such as department or location. This functionality ensures that emails are always sent to current members who meet the criteria, without the need for manual updates by list owners. For example, an accounting department could rest assured that their newest hires are included on distribution list communications, simply because the new hires' department attribute is set to **Accounting**.

Getting ready

Ensure that you have administrative rights to access the Exchange admin center within Microsoft 365. Specifically, you will need to be assigned the Exchange Administrator role or another role that includes the necessary permissions to create and manage distribution lists. Simply having access as a reader will not allow you to execute this recipe.

How to do it...

1. Log into the Exchange admin center at <https://admin.exchange.microsoft.com>.
2. Once in the Exchange admin center, click **Recipients | Groups** in the left navigation menu, as previously shown in *Figure 4.9*.

3. Click **Add a group**, and then select **Dynamic distribution** from the list of options, as shown in *Figure 4.10*.

Home > Groups > Add a group

Group type

Basics

Users

Settings

Finish

Choose the group type that best meets your team's needs. [Learn more about group types](#)

☐ **Microsoft 365 (recommended)**

Allows teams to collaborate by giving them a group email and a shared workspace for conversations, files, and calendars. In Outlook, these are called Groups.

☐ **Distribution**

Creates an email address for a group of people.

☐ **Mail-enabled security**

Sends messages to all members of the group and gives access to resources like OneDrive, SharePoint and admin roles

☒ **Dynamic distribution**

Sends email to all members of the list. The group's membership list is updated every 24 hours, based on the filters and conditions you set.

Next

Cancel

Figure 4.10 – Dynamic distribution selected in the new group configuration screen

4. Click **Next** to go to the **Basics** screen, and then enter the **Name** and **Description** of your dynamic distribution list.
5. Click **Next** to go to the **Users** screen, and then search for and add owners who will have the ability to rename the group, manage its membership, and change group settings.
6. On the same **Users** screen, search for and add members who will be recipients of any messages sent to the new distribution list. As demonstrated in *Figure 4.11*, this will consist of specifying an attribute and/or conditions under which a member qualifies for automatic addition to a group. In this example, any member of the *Accounting*, *Contracting*, or *Finance* departments will automatically be a member of the new dynamic distribution list.

Home > Groups > Add a group

☒ Group type

☒ Basics

☒ **Users**

☐ Settings

☐ Finish

Members

Specify the type of recipients that will be members of this group.

☒ All recipient types

☐ Only the following recipient types

☐ Users with Exchange mailboxes

☐ Mail users with external email addresses

☐ Resource mailboxes

☐ Mail contacts with external email addresses

☐ Mail-enabled groups

Membership in this group will be determined by the rules you set below

Department ▾

Accounting, Finance, Contracting

Add another rule

Back

Next

Cancel

Figure 4.11 – The member configuration for a new dynamic distribution list

- Click **Next** to go to the **Settings** screen, specify **Group email address**, and select **Domain** for the new list.
- Click **Next** to go to the **Finish** screen to review the new dynamic distribution list's configuration, and then click **Create group** when finished.

How it works...

A dynamic distribution list uses recipient filters and conditions to automatically include or exclude users. As user properties in your organization change, the list membership adjusts accordingly, ensuring that the list is always up to date with relevant recipients.

Dynamic distribution lists are particularly useful for large organizations or rapidly changing environments where groups need to be dynamically adjusted without manual intervention.

There's more...

You can enable message approval for your dynamic distribution list, where emails sent to the list must be approved by designated group moderators. This feature is particularly useful in controlling the content and quality of the messages circulated through the distribution list.

To get started with configuring message approval, select your dynamic distribution list by navigating to the Exchange admin center and then **Recipients | Groups | Dynamic distribution list**. Find and select the list for which you wish to enable moderation, and then select **Other | Edit message approval** in the **Message approval** section. From there, you can specify moderators and add individuals who can bypass approval.

Note that this feature is also available for normal distribution lists and mail-enabled security groups.

Another way to enhance your usage of dynamic distribution lists is to utilize nested groups. You can incorporate nested groups into your dynamic distribution list by using dynamic rules. This allows you to add a manual membership group to a dynamic group, ensuring that specific members are always included regardless of the dynamic criteria. For example, you might have a static group for senior management that should always be included in a department-based dynamic distribution list. By nesting the senior management group within the dynamic list via a dynamic rule, you ensure consistent communication with both dynamic and static members.

See also

- *Create and manage dynamic distribution groups in Exchange Online*: <https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-dynamic-distribution-groups/create-manage-dynamic-distribution-groups>
- *Mail flow rule conditions and exceptions (predicates) in Exchange Online*: <https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/conditions-and-exceptions>

Creating an Exchange-specific retention policy

Implementing an Exchange-specific retention policy in Microsoft 365 helps manage the life cycle of emails and other mailbox items, by specifying how long messages are kept and when they are automatically deleted. This is crucial for compliance with legal or regulatory requirements, and for managing data effectively within an organization.

Getting ready

Make sure you have access to Microsoft Purview as a Global or Compliance Administrator, which is necessary to create and manage retention policies.

How to do it...

1. Log into Microsoft Purview at <https://purview.microsoft.com>.
2. Navigate to **All solutions | Data Lifecycle Management**.
3. Navigate to **Policies | Retention policies**, as shown in *Figure 4.12*.

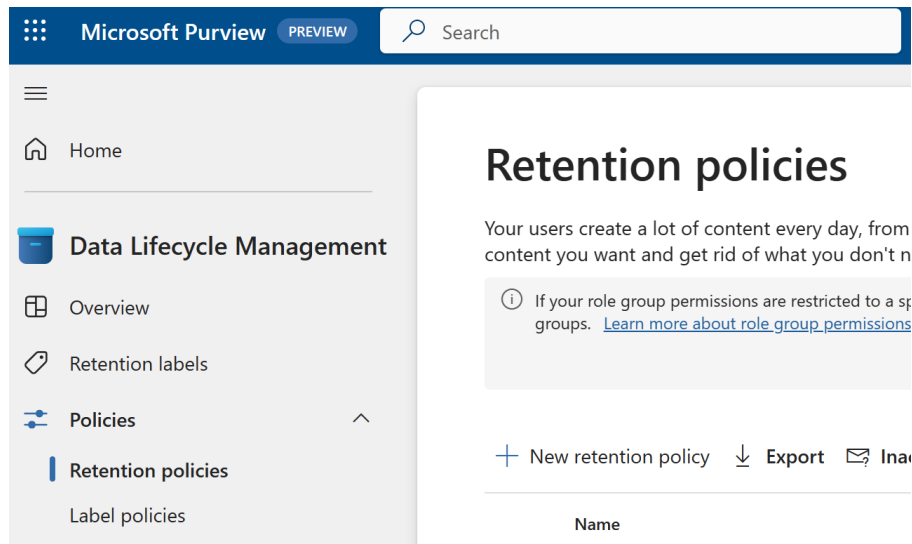



Figure 4.12 – Retention policies in Microsoft Purview




4. Select **New retention policy**, and then enter a name and description for the retention policy that clearly indicates its purpose and scope, such as `7-year email retention`.
5. If this policy should only apply to specific administrative units, add those and click **Next**; otherwise, click **Next** without making changes to apply the policy to the entire directory.
6. Choose whether this policy should be **Adaptive** (e.g., specific departments or sites matching a query, such as those containing a keyword) or **Static**, which will require manual updates as sites and departments are added or changed. For this Exchange-specific recipe, let's choose **Static**.

7. Click **Next**, and then deselect everything other than **Exchange mailboxes**, as shown in *Figure 4.13*.

Choose where to apply this policy

The policy will apply to content that's stored in the locations you choose.

 You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. [Set up now](#)

Status	Location	Applicable Content	Included	Excluded
<input checked="" type="checkbox"/> On	 Exchange mailboxes	Items in user, shared, and resource mailboxes: emails, calendar items with an end date, notes, and tasks with an end date. Doesn't apply to items in Microsoft 365 Group mailboxes. More details	All mailboxes Edit	None Edit
<input type="checkbox"/> Off	 SharePoint classic and communication sites	Files in classic sites or communication sites or team sites that aren't connected to a Microsoft 365 group, and files in all document libraries (including default ones like Site Assets). More details		
<input type="checkbox"/> Off	 OneDrive accounts	All files in users' OneDrive accounts. More details		

Back

Next

Cancel

Figure 4.13 – Retention policy locations

8. Click **Next**, and then choose the retention period details that should pertain to this Exchange-specific retention policy. In this recipe, choose to automatically delete items after retaining them for seven years, as shown in *Figure 4.14*.

Decide if you want to retain content, delete it, or both

☒ **Retain items for a specific period**
Items will be retained for the period you choose.

Retain items for a specific period

7 years

Start the retention period based on

When items were created

At the end of the retention period

☒ **Delete items automatically**

☐ **Do nothing**

☐ **Retain items forever**
Items will be retained forever, even if users delete them.

☐ **Only delete items when they reach a certain age**
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Back Next Cancel

Figure 4.14 – Retention period details

9. Click **Next** to review your policy, and then click **Submit** to create it.

Important note

In this specific policy, items that are already older than the defined retention period will be deleted upon policy submission. Take extra care to communicate with users before submitting a policy, and work with appropriate parties to prepare them for the impact of this change.

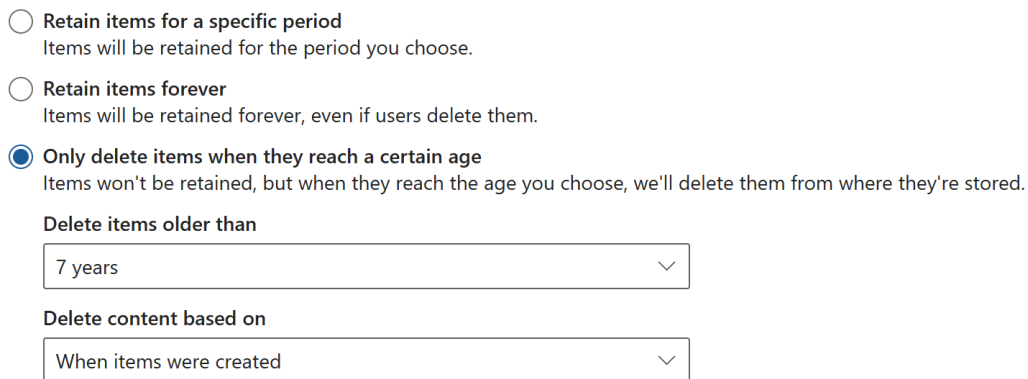
How it works...

Retention policies in Exchange Online are vital for ensuring that your organization remains compliant with applicable record schedules. These policies automate the management of email data, ensuring both compliance and a reduced risk of data loss. After you initiate a policy, it can take up to a week to fully implement across an organization. Once active, the policy governs the retention and deletion of emails for specified users and locations automatically, according to the set parameters.

There's more...

Retention policies play an important role in the data governance framework of Microsoft 365, allowing organizations to manage the storage and life cycle of information in accordance with both industry regulations and internal policies. In the example discussed, we configured a policy to retain data for seven years before deletion. However, it is possible to set up policies that either preserve content indefinitely or allow user-initiated deletion before the maximum retention period ends. As depicted in *Figure 4.15*, users can delete items before reaching the seven-year threshold, but automatic deletion will occur once the period expires, thus overriding the retention setting.

Decide if you want to retain content, delete it, or both



☐ Retain items for a specific period
Items will be retained for the period you choose.

☐ Retain items forever
Items will be retained forever, even if users delete them.

☒ Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Delete items older than

7 years

Delete content based on

When items were created

Figure 4.15 – A retention policy set to delete items at a certain age

See also

- *Create a retention policy for Exchange Online:* <https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-retention-policy>

Creating a mail flow rule

Mail flow rules in Microsoft 365, also known as transport rules, allow administrators to manage how emails are processed within an organization's email environment. These rules can help enforce compliance requirements, manage data security, and improve operational efficiencies by automatically taking action on emails that meet specified conditions.

Getting ready

You need to have access to the Exchange admin center as an administrator to create and manage mail flow rules. Specifically, you will need to be assigned the Exchange Administrator role or another role that includes the necessary permissions to create and manage mail flow rules.

How to do it...

1. Log into the Exchange admin center at <https://admin.exchange.microsoft.com>.
2. Once in the Exchange admin center, select **Mail flow | Rules** in the left navigation menu, as shown in *Figure 4.16*.

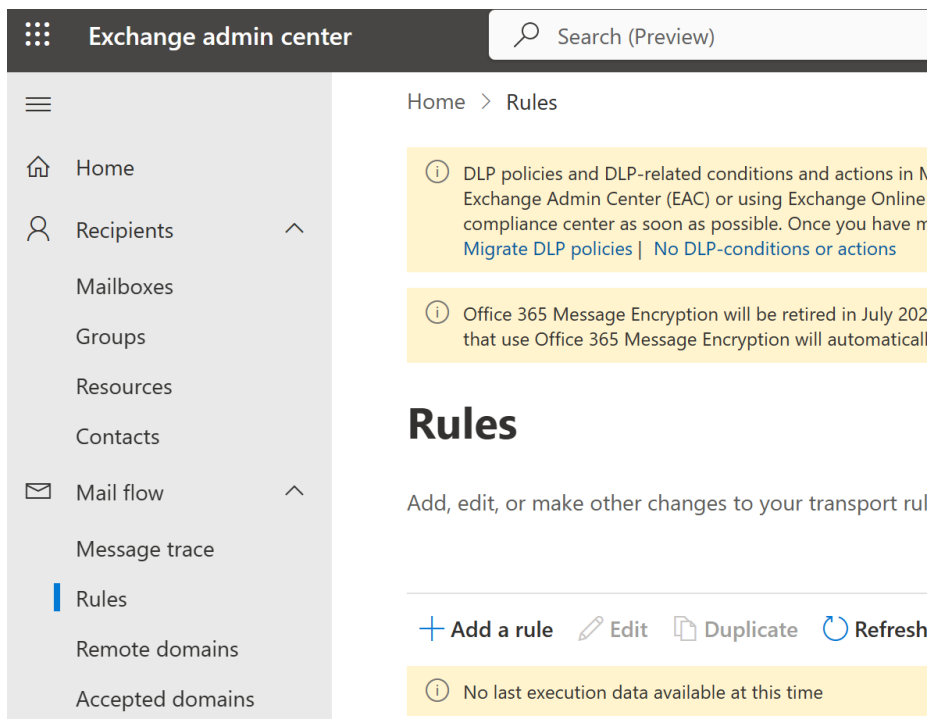


Figure 4.16 – The Mail flow rules screen in the Exchange admin center

3. Click **Add a rule** and choose **Create a new rule** from the drop-down menu.
4. On the first screen of the wizard that appears, **Set rule conditions**, provide a name for your rule that describes its function clearly and concisely.

5. On the same screen, set the conditions for the rule. For example, you can specify criteria such as emails from a certain sender, emails that contain specific keywords, or emails that have attachments. In this recipe, let's create a rule that prepends a disclaimer to messages received from external senders, as shown in the **Apply this rule if** section shown in *Figure 4.17*.

New transport rule

● Set rule conditions

○ Set rule settings

○ Review and finish

Set rule conditions

Name and set conditions for your transport rule

Name *

External email caution disclaimer

Apply this rule if *

The sender

is external/internal

+

The sender is located 'NotInOrganization'

Do the following *

Apply a disclaimer to the message

prepend a disclaimer

+

Prepend

['This message originated outside our organization. Use caution when opening links and review our records management schedule before sharing any data outside the organization.'](#)

and fall back to action 'Wrap' if the disclaimer can't be inserted

Except if

Select one

Next

Select one

+

🗑

Figure 4.17 – The Set rule conditions screen of a new mail flow rule

6. On the same screen, after **Do the following**, define the actions to be taken when an email meets the specified conditions. Actions can include redirecting an email to another address, adding or removing recipients, blocking a message, or applying a message classification. As previously shown in *Figure 4.16*, we'll prepend a disclaimer if the condition is met.
7. Configure any exceptions to the rule, if necessary. Exceptions allow emails that meet certain criteria to bypass the rule, despite meeting the initial conditions.
8. Click **Next**, and then adjust the settings, such as adding a priority to the rule. If multiple rules exist, decide whether the rule will be enforced immediately or during a scheduled period, as shown in *Figure 4.18*, where we enforce the rule immediately and apply a low severity.

New transport rule

- ✓ Set rule conditions
- Set rule settings**
- Review and finish

Set rule settings

Set settings for your transport rule

Rule mode

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

Severity *

Low

☐ Activate this rule on

5/4/2024 - 12:30 AM

☐ Deactivate this rule on

5/4/2024 - 12:30 AM

Back **Next**

Figure 4.18 – The Set rule settings screen of a new mail flow rule

9. Click **Next** to review the rule, and then click **Finish** to save.

How it works...

Mail flow rules process incoming and outgoing emails based on the conditions and actions defined. When an email matches the specified conditions, the defined actions are automatically applied, allowing for real-time email management and enforcement of policies.

In our recipe, an email received from outside the organization will appear with our prepended disclaimer, as shown in *Figure 4.19*.

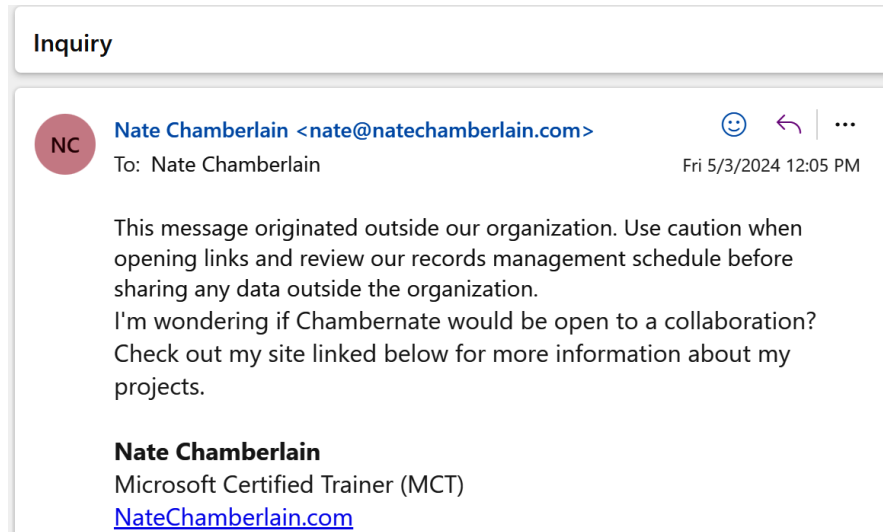


Figure 4.19 – An email received with a disclaimer prepended

There's more...

Regularly review and test mail flow rules to ensure that they work as expected. Update them as necessary to adapt to any changes to an organization's operational needs or compliance requirements.

See also

- *Mail flow rules (transport rules) in Exchange Online*: <https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules>
- *Mail flow best practices for Exchange Online, Microsoft 365, and Office 365 (overview)*: <https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/mail-flow-best-practices>

Configuring spam filter policies

Configuring spam filter policies in Microsoft 365 is essential for protecting your organization's email communication, by filtering out unwanted or harmful emails. These policies help manage and mitigate the risks associated with spam and phishing attacks.

Getting ready

Ensure that you have administrative rights to Microsoft Defender as a Global or Security Administrator, as you will need these to configure and manage spam filter policies.

How to do it...

1. Access Microsoft Defender at <https://security.microsoft.com>, and then navigate to **Email & collaboration** | **Policies & rules** | **Threat policies** | **Anti-spam**, as shown in *Figure 4.20*.

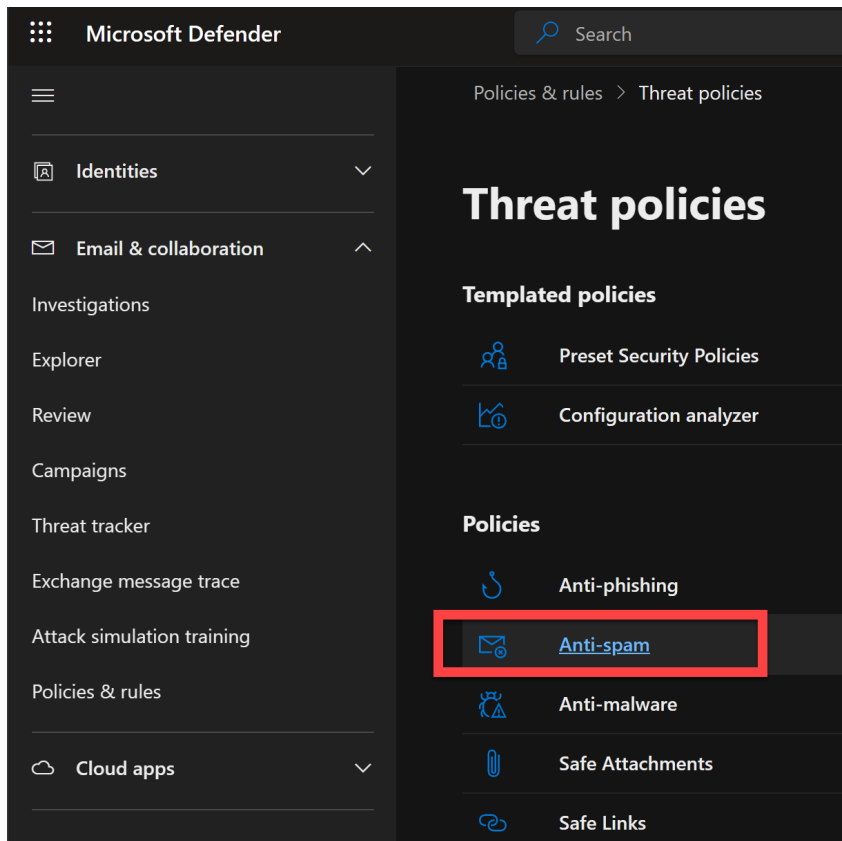


Figure 4.20 – The location of Anti-spam in Microsoft Defender

2. Select **Create policy** and choose **Inbound**.
3. Name your policy and provide a description that outlines its purpose.

4. Click **Next**, and then configure which users, groups, and domains to include or exclude. For example, you may wish to exclude certain users who receive more spam-like materials, such as public relations or marketing teams. For these users, you may wish to create a more lenient anti-spam policy specifically for them.
5. Click **Next** to set conditions to detect spam, such as a bulk email threshold (spam confidence level) or specific characteristics of email messages, such as included keywords, links to remote locations, or emails sent from certain geographic territories.
6. Click **Next**, and then specify the actions to be taken when an email is flagged as spam, such as deleting the message, sending it to quarantine or the Junk Email folder, or prepending the subject line with text such as [SPAM] or [BULK EMAIL]. You can also configure actions for different levels of threats, such as phishing or high confidence spam. This screen is shown in *Figure 4.21*.

Policies & rules > Threat policies > Create anti-spam inbound policy

Actions

Set your actions for this policy.

Message actions

Spam

Move message to Junk Email folder

High confidence spam

Move message to Junk Email folder

Phishing

Prepend subject line with text

High confidence phishing

Quarantine message

Back **Next**

Figure 4.21 – Actions taken in an anti-spam policy configuration

7. On the same screen, decide how long messages will be retained in quarantine before they are automatically deleted. The default setting is typically 15 days, but this can be adjusted.
8. At the bottom of the **Actions** screen, adjust the settings to provide end users with safety tips or notify administrators of detected threats.
9. Click **Next** to specify which senders or domains are blocked or allowed, as shown in *Figure 4.22*. This helps to refine the filtering process and reduce false positives or negatives.

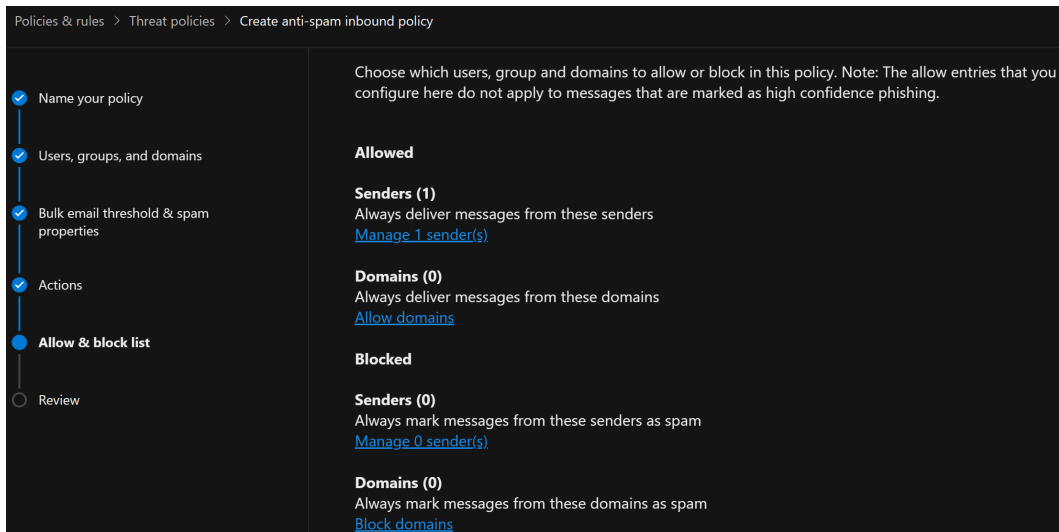


Figure 4.22 – Allowed and blocked senders and domains in an anti-spam policy

10. Click **Next** to review all the settings to ensure that they meet your organization's requirements. Then, click **Create** to implement the new policy.

How it works...

Spam filter policies in Microsoft 365 use defined criteria to inspect incoming and outgoing emails for signs of spam and phishing. When an email meets these criteria, the specified actions are automatically applied, helping to keep unwanted messages out of user inboxes and maintain email security.

Users can check their **Junk Email** folder in Outlook or quarantine to retrieve anything inadvertently marked as spam that they need.

There’s more...

After creating your spam filter policy, monitor its effectiveness and adjust the settings as required, based on the performance and any feedback from users regarding the handling of spam and phishing attempts.

Users can also add their own blocked senders and domains in addition to your policy configuration. *Figure 4.23* shows a user’s **Junk email** settings in Outlook, where they’ve added two blocked senders.

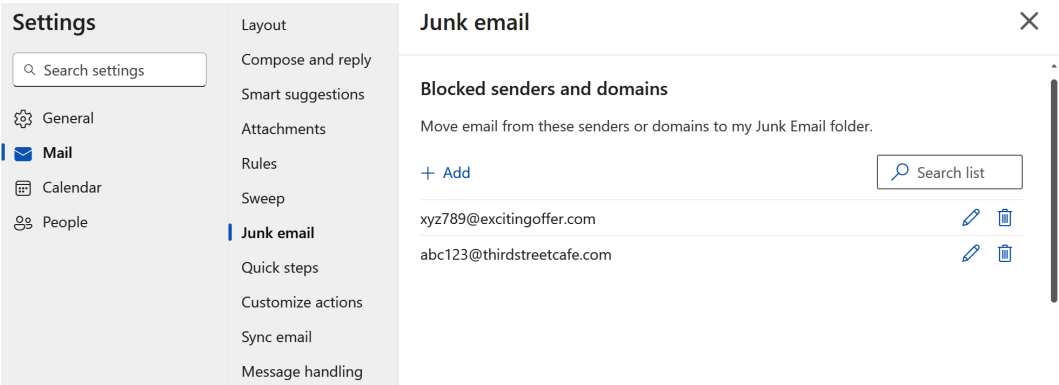


Figure 4.23 – A user’s Junk email settings in Outlook

See also

- *Configure anti-spam policies in EOP:* <https://learn.microsoft.com/en-us/defender-office-365/anti-spam-policies-configure>

Creating room and equipment resources

Creating room and equipment mailboxes in Microsoft 365 allows your organization to reserve and manage resources, such as conference rooms or equipment, through Outlook. This setup facilitates efficient scheduling and the shared usage of organizational assets.

Getting ready

To start, you need administrative access to the Exchange admin center in Microsoft 365.

How to do it...

1. Log into the Exchange admin center at <https://admin.exchange.microsoft.com>.
2. Once in the Exchange admin center, select **Recipients | Resources** in the left navigation menu, as shown in *Figure 4.24*.

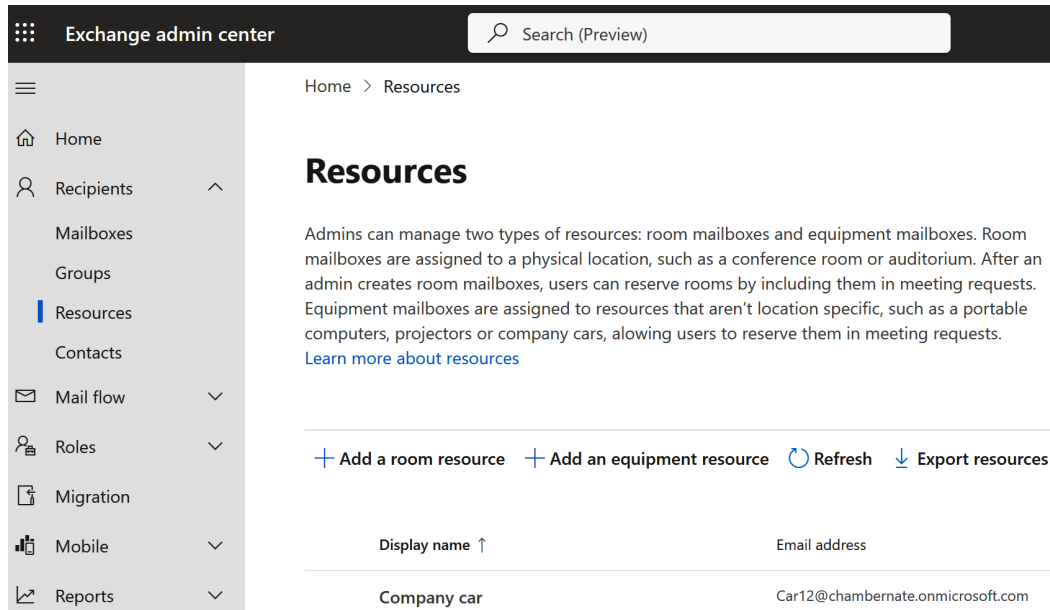


Figure 4.24 – The Resources screen in the Exchange admin center

3. Create a new resource mailbox by selecting the specific type you need:
 - For a room mailbox (e.g., conference room), select **Add a room resource**.
 - For an equipment mailbox (e.g., company vehicle, camera, or display), choose **Add an equipment resource**.
4. Enter the necessary details, such as the name, email address, and domain.

5. Click **Next**, and then enter resource details such as **Capacity**, **Location**, and **Department** (if applicable), as shown in *Figure 4.25*. Everything on the **Set properties** screen is optional.

New resource mailbox

- ✓ Resource Setup
- **General Information**
- Booking options
- Review resource

Set properties

Set properties for this scheduled resource.

Capacity

Location

Phone number

Department

Company

Figure 4.25 – The Set properties screen of a new resource account

6. Click **Next** to specify additional settings, as shown in *Figure 4.26*, including the following:
- **Allow repeating meetings**
 - **Allow scheduling only during work hours**
 - **Automatically decline meetings outside of the booking limits below:**
 - **Booking window (days)** (how far in advance you can reserve a resource)
 - **Maximum duration (hours)**
 - An automatic reply sent to the organizer
 - Delegate settings, including automatic acceptance or manual approval by specified individuals

New resource mailbox

- ☒ Resource Setup
- ☒ General Information
- ☒ **Booking options**
- ☐ Review resource

Booking delegate settings

Booking options

Choose when and how this resource should be scheduled.

- ☒ Allow repeating meetings
- ☐ Allow scheduling only during work hours
- ☒ Automatically decline meetings outside of booking limits below

Booking window (days)

Maximum duration (hours)

Enter an automatic reply to be sent to meeting organizers (optional)

Figure 4.26 – The Booking delegate settings screen of a new resource account

7. Click **Next** to review the configuration, and then click **Create** to save.

How it works...

Room and equipment mailboxes in Microsoft 365 serve as dedicated resources that can be reserved and managed through Outlook. These mailboxes are not associated with individual users but, rather, represent shared organizational resources such as conference rooms or equipment, including projectors and vehicles. When these mailboxes are created, they are configured with a calendar. This calendar becomes an essential component, as it stores the booking details and availability of a resource, making it visible to all users within an organization who wish to book the resource.

Administrators can configure settings to specify how a resource can be booked – for example, whether the resource can accept recurring meetings, whether booking is allowed only during specific hours, and setting maximum booking durations. This functionality is integrated directly into Outlook, allowing users to book resources similarly to how they'd schedule a meeting.

Important note

This recipe focuses on creating and managing room and equipment mailboxes through the Exchange admin center, which is essential for handling detailed configurations related to booking and calendar management across Microsoft 365 services. However, it's important to recognize that for Teams-specific devices such as Teams Rooms, phones, and displays, resource accounts can also be created and managed directly in the Teams admin center. This growing flexibility allows for easier integration and management within Teams environments without the need to use the Exchange admin center, depending on your organization's needs.

There's more...

Beyond the Exchange admin center, room and equipment mailboxes can be configured and managed using PowerShell commands. This approach is particularly useful for bulk operations, such as creating multiple mailboxes or modifying properties for several resources at once. PowerShell scripts can be written to automate these tasks, saving time and reducing the potential for manual errors.

Room and equipment mailboxes can be integrated with other Microsoft 365 services such as Microsoft Teams. For example, a room mailbox can be linked to a Teams meeting room, allowing seamless virtual meeting setups.

Users can benefit from features such as the Scheduling Assistant in Outlook, which helps to find available times for a resource based on participants' availability and resource policies. Moreover, users can view detailed attributes of each resource, such as capacity and equipment details, directly from Outlook, aiding in decision-making when booking.

See also

- *Manage resource mailboxes in Exchange Online:* <https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-resource-mailboxes>
- *Create Microsoft 365 room and equipment mailboxes:* <https://learn.microsoft.com/en-us/microsoft-365/admin/manage/room-and-equipment-mailboxes>

Enabling ATP features

This recipe guides you through configuring **safe attachments** and **safe links** settings in **Microsoft 365 Defender**, formerly known as Microsoft Defender for Office 365, empowering administrators to minimize vulnerabilities and enhance overall data security.

Getting ready

For this recipe, you'll need permissions within the Microsoft 365 Defender portal to manage security settings. These permissions are included in roles such as Global Administrator or Security Administrator. These roles enable administrators to create and configure policies for safe attachments and safe links, essential for enhancing an organization's security posture.

How to do it...

1. Go to Microsoft Defender at <https://security.microsoft.com>.
2. Navigate to **Email & collaboration** | **Policies & rules** | **Threat policies** on the left navigation menu, as shown in *Figure 4.27*.

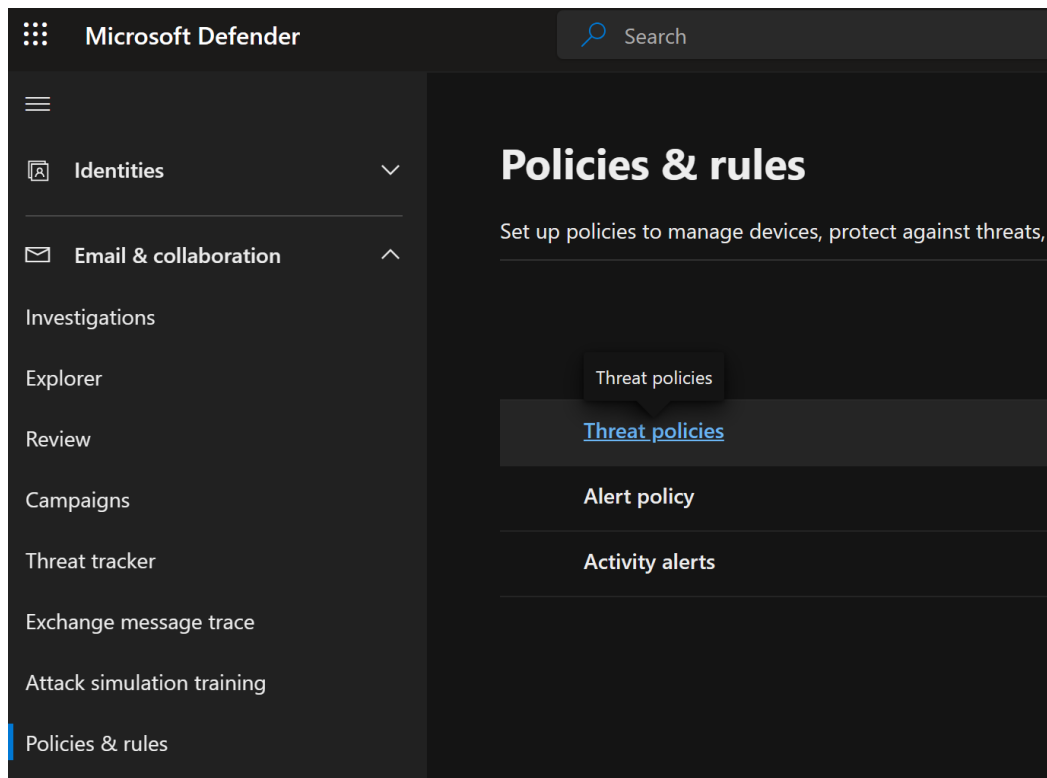


Figure 4.27 – The location of Threat policies in Microsoft Defender

3. Select **Safe Attachments**, and then click **Create**.
4. Name and describe your custom safe attachments policy, and then click **Next**.

5. On the **Users and domains** screen, choose the recipients to whom this policy applies or those who should be excluded, as shown in *Figure 4.28*.

The screenshot shows the 'Create Safe Attachments policy' wizard. The left sidebar has four steps: 'Name your policy' (checked), 'Users and domains' (selected), 'Settings', and 'Review'. The main area is titled 'Users and domains' and contains two sections. The first section, 'Include these users, groups and domains', has input fields for 'Users' and 'Groups'. The 'Users' field contains a red pill with 'AL' and the text 'All Company' with a close button. Below this is an 'And' label. The second section has input fields for 'Groups' and 'Domains', followed by another 'And' label. At the bottom, there is a checked checkbox for 'Exclude these users, groups and domains' and a 'Users' label.

Figure 4.28 – The Users and domains screen of a safe attachments policy

6. Click **Next**, and then choose a malware response method, as shown in *Figure 4.29*. For instance, select **Dynamic Delivery** to reduce email delivery delays while still scanning attachments for malware.

The screenshot shows the 'Settings' screen for a safe attachments policy. The title is 'Settings'. Below it is the section 'Safe Attachments unknown malware response'. The text says 'Select the action for unknown malware in attachments. [Learn more](#)'. There is a 'Warning' section with a list of bullet points: 'Monitor and Block actions might cause a significant delay in message delivery. [Learn more](#)', 'Dynamic Delivery is only available for recipients with hosted mailboxes.', and 'For Block or Dynamic Delivery, messages with detected attachments are quarantined and can be released only by an admin.' Below the warning is a list of radio button options: 'Off - Attachments will not be scanned by Safe Attachments.', 'Monitor - Deliver the message if malware is detected and track scanning results.', 'Block - Block current and future messages and attachments with detected malware.', and 'Dynamic Delivery (Preview messages) - Immediately deliver the message without attachments. Reattach files after scanning is complete.' The 'Dynamic Delivery' option is selected.

Figure 4.29 – The Settings screen of a safe attachments policy

7. Scroll down on the same screen and specify the Quarantine policy to apply, as well as whether you want to redirect monitored messages with attachments to a specific address.
8. Click **Next** to review the policy, and then click **Submit** to implement it.
9. Next, navigate to **Safe Links** in Microsoft Defender by navigating to **Email & collaboration | Policies & rules | Threat policies**, as previously shown in *Figure 4.27*.
10. Click **Create**.
11. Name and describe your new safe links policy, and then click **Next**.
12. On the **Users and domains** screen, choose the recipients to whom this policy applies or those who should be excluded.
13. On the **URL & click protection settings** screen, specify which settings you wish to enable, as shown in *Figure 4.30*. These settings are as follows:
 - **Email** (URLs are rewritten, but this can be turned off)
 - URLs that should not be rewritten
 - **Teams** (on/off): Check links against known, malicious links (URLs are not rewritten)
 - **Office 365 Apps** (on/off): Check links against known, malicious links (URLs are not rewritten)
 - **Click protection settings** (on/off):
 - ♦ Allow users to click through to original links
 - ♦ Display organization branding on warning pages

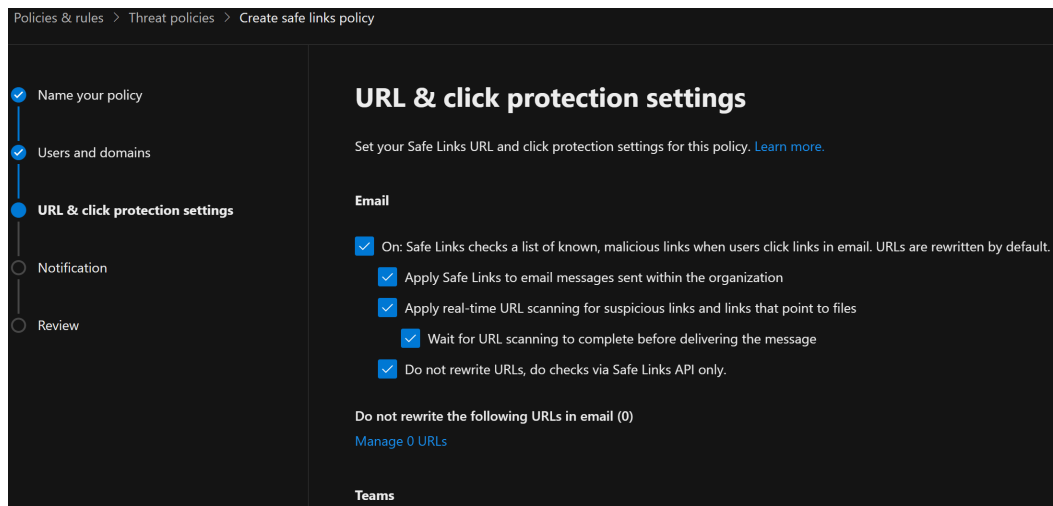


Figure 4.30 – The URL & click protection settings screen of a safe links policy

14. Click **Next**, and then choose either the default notification text or write your own custom notification text.
15. Review your policy, and then click **Submit** to implement it.

How it works...

In this recipe, you utilized Microsoft 365 Defender to create safe attachments and safe links policies. These policies ensure that any attached files and URLs in email messages are scanned for malicious content, enhancing your organization's security posture.

Important note

Consider alternative options such as **Monitor**, **Block**, and **Replace** for emails with attachments, depending on specific group or condition requirements.

There's more...

Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvements that could potentially be made. By implementing and configuring safe attachments and safe links, as described in this recipe, you contribute positively to your organization's Secure Score, making it a useful tool for monitoring and improving your security measures over time.

Implementing safe attachments and safe links policies as part of your security strategy helps protect against sophisticated malware and phishing attacks, which are key metrics in Microsoft Secure Score evaluations.

You'll learn more about Microsoft Secure Score and how to access it in *Chapter 12, Understanding Microsoft 365 Defender*.

See also

- *Safe Attachments in Microsoft Defender for Office 365*: <https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-about>
- *Safe Links in Microsoft Defender for Office 365*: <https://learn.microsoft.com/en-us/defender-office-365/safe-links-about>

5

Setting Up and Configuring Microsoft Search

In this chapter, we explore knowledge management through the capabilities of Microsoft Search, a core tool for any organization utilizing Microsoft 365. This powerful feature not only streamlines the search experience across various applications and services within the Microsoft ecosystem but also enhances productivity by allowing users to quickly find documents, data, and answers within their organization's digital environment. Through detailed setups and configurations, we aim to harness the full potential of Microsoft Search to create a more connected and efficient workplace. This chapter provides the necessary guidance on configuring search settings, content, and features that are tailored to meet the specific needs of your organization, ensuring that users have immediate access to the answers and resources they require with precision and ease.

We will cover the following recipes in this chapter:

- Creating an acronym
- Creating a bookmark
- Importing bookmarks in bulk from CSV
- Adding a location
- Adding a Q&A result
- Setting up usage of Microsoft Search in Bing
- Assigning Search Administrator and Search Editor roles
- Using Search Insights dashboard reports

Important note

The first edition of this book discussed floor plans, which were previously accessible in the **Answers** section of the Search & Intelligence admin center. These floor plans have now been phased out since 2023. In their place, Microsoft is rolling out **Microsoft Places**, a new feature available with additional licensing designed to assist with needs such as wayfinding and desk booking. Although not yet widely available at the time of writing, you can access Microsoft Places at <https://outlook.office.com/places>. For more information about Microsoft Places, visit <https://www.microsoft.com/en-us/microsoft-365/blog/2022/10/12/introducing-microsoft-places-turn-your-spaces-into-places>.

The first edition also covered importing SharePoint-promoted results as bookmarks, but SharePoint-promoted results have also been deprecated since 2021. This chapter covers the new method of achieving the same results by utilizing bookmarks.

Technical requirements

This chapter requires administrative access to Microsoft 365. Users assigned either the Global Administrator or Search Administrator role will have the capability to execute all tasks presented.

Creating an acronym

Creating acronyms in Microsoft Search helps users in your organization quickly become familiar with abbreviated terms specific to your environment, such as *CMO*, which, depending on your industry, might mean *Chief Marketing Officer* or *Chief Medical Officer*. Providing these definitions directly within the search results can be significantly helpful in avoiding confusion, especially when common acronyms have multiple meanings across different contexts or when new employees join your company.

Getting ready

Ensure you have the necessary administrative rights; either a Global Administrator, Search Administrator, or Search Editor role is required to execute these steps.

How to do it...

1. Navigate to the Search & intelligence admin center at <https://admin.microsoft.com/#/MicrosoftSearch> or by navigating to the Microsoft 365 admin center (<https://admin.microsoft.com>) and then **Settings | Search & intelligence**.

Tip

In addition to the previously mentioned ways of accessing Search & intelligence, you will also find it as its own admin center by navigating to the Microsoft 365 admin center (<https://admin.microsoft.com>) and then **All admin centers | Search & intelligence**.

2. Once inside the admin center, select **Answers** and then **Acronyms** from the top and left navigation menus, respectively, as shown in *Figure 5.1*.

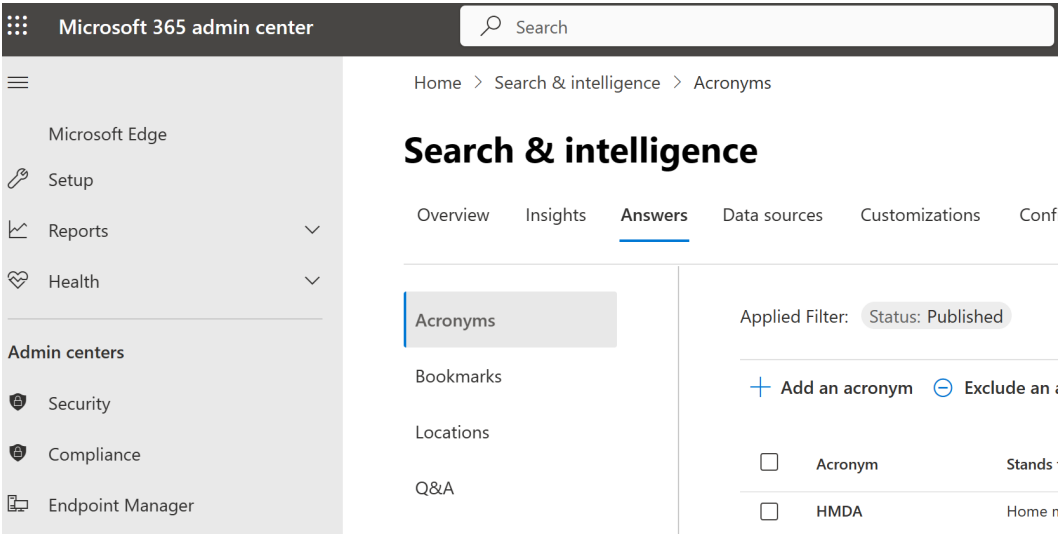


Figure 5.1 – Acronyms screen of the Search & intelligence admin center

3. Select **Add an acronym** to start creating a new acronym.
4. Input the acronym and its meaning. You can also add a description and a source or reference URL if available. *Figure 5.2* shows an acronym created with its meaning, description, and reference URL entered. As you enter the details, a preview of how the acronym will appear in the search results will be updated in real time.

Add an acronym

HMDA

Acronym • 1 result

Home Mortgage Disclosure Act

The Home Mortgage Disclosure Act (HMDA) is a federal law that requires mortgage lenders to keep records of key pieces of information regarding their lending practices. Lenders must submit these records to regulatory authorities.

Published by chambernate : <https://www.investope...>

Acronym *

HMDA

Stands for *

Home Mortgage Disclosure Act

Description

The Home Mortgage Disclosure Act (HMDA) is a federal law that requires mortgage lenders to keep records of key pieces of information regarding their lending practices. Lenders must submit these records to regulatory authorities.

Publish

Save to Draft

Figure 5.2 – Creating a new acronym screen

- 5. To finalize, select **Publish**.

How it works...

The acronym feature in Microsoft Search allows the organization to define specific abbreviations to enhance understanding and clarity for end users. After adding an acronym, it might take up to a day for it to become searchable in the system. When an acronym appears in search results, it will be at the top of the search results page, as shown in the example in *Figure 5.3*.

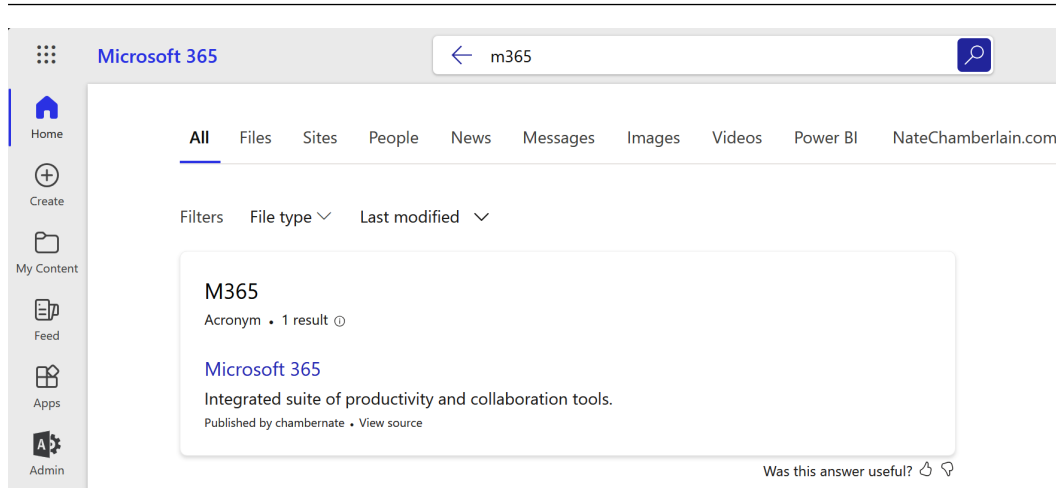


Figure 5.3 – An acronym search result in Microsoft Search

There's more...

If you need to add multiple acronyms, you can use the **Import** function to upload them in bulk via a CSV file. This method is efficient for large sets of data, especially if you're just getting started with implementing improved search experiences.

Microsoft Search also automatically uncovers acronyms across user emails and documents throughout Microsoft 365 to deliver system-curated acronyms to users so admins don't have to manually add and continually update them. These automatic acronyms are only shown to users who have access to the emails or documents in which the acronym was discovered.

See also

- *Manage Acronym answers in Microsoft Search:* <https://learn.microsoft.com/en-us/microsoftsearch/manage-acronyms>

Creating a bookmark

Creating bookmarks in Microsoft Search allows administrators to guide users directly to specific resources, either within the Microsoft 365 environment or to external sites. Bookmarks can improve the search experience by ensuring that important resources, such as official org charts, forms, policies, or procedures, are prominently displayed in search results.

Getting ready

Ensure you have the necessary administrative rights; either a Global Administrator, Search Administrator, or Search Editor role is required to execute these steps.

How to do it...

1. Navigate to the Search & intelligence admin center at `https://admin.microsoft.com/#/MicrosoftSearch` or by navigating to the Microsoft 365 admin center (`https://admin.microsoft.com`) and then **Settings | Search & intelligence**.
2. In the Search & intelligence admin center, choose **Answers** from the top menu and then select **Bookmarks** from the left navigation menu.
3. Select **Add bookmark**, as shown in *Figure 5.4*, to create a new bookmark.

Home > Search & intelligence > Bookmarks

Search & intelligence

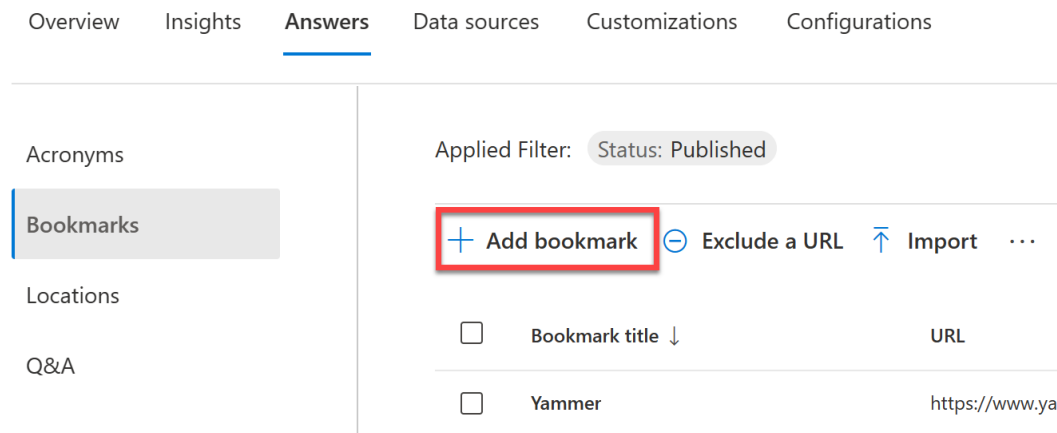



Figure 5.4 – Option to create a new bookmark

4. In the bookmark creation form, enter the following information:
 - A. **Title:** Provide a concise title that clearly describes the bookmark.
 - B. **URL:** Enter the URL of the resource.
 - C. **Description:** Add a brief description of the resource.
 - D. **Keywords:** Specify keywords that will trigger the appearance of the bookmark in search results.

- E. **Reserved keywords:** These are unique to this bookmark (they cannot be used for others) and ensure this bookmark appears when these terms are searched, whereas normal keywords can be shared among other bookmarks.
5. As you fill out these fields, a live preview of the search result card will display how it will appear to users, as shown in *Figure 5.5*.

NateChamberlain.com Website

 **NateChamberlain.com Website**
<https://www.natechamberlain.com>
Microsoft 365 blog posts, videos, books, and resources to help with your digital workplace solutions.

Title * Characters: 27 / 60

URL *

Description Characters: 101 / 300

Keywords * ⓘ

× × × ×

Enter search terms commonly used to find this page

☒ Automatically match similar keywords

Reserved keywords ⓘ

×

Categories: ⓘ

× ×

Bookmark settings
Choose when and where this result should be published

Figure 5.5 – An example of the bookmark creation form’s live preview

6. Optional settings to refine when and how the bookmark appears can be configured at the bottom of the form:
 - A. **Dates:** Set specific dates if the bookmark should only appear during a certain period.
 - B. **Country or region, Groups, Device & OS:** These settings allow you to target the bookmark to specific users based on location, group membership, or device type.
 - C. **Targeted variations:** Adjust the bookmark's content based on a user's device or location. For example, you may wish to send international employees to a variation of a policy intended for that audience, such as one that is translated to that geographic location's primary language.
 - D. **PowerApp:** Embedding an app directly in the search results can allow for interactive engagements.
7. Review your configurations and select **Publish** to make the bookmark live. You can alternatively choose **Save to draft** if you wish to resume configuration at a later time.

How it works...

This process creates a targeted shortcut in the Microsoft Search results, directing users to important resources based on the defined criteria. The changes are typically reflected almost immediately in the search index, allowing for rapid accessibility to users.

Bookmark results will appear immediately as suggestions when a user types the bookmark's keyword into the search bar before they hit *Enter*, as shown in *Figure 5.6*.

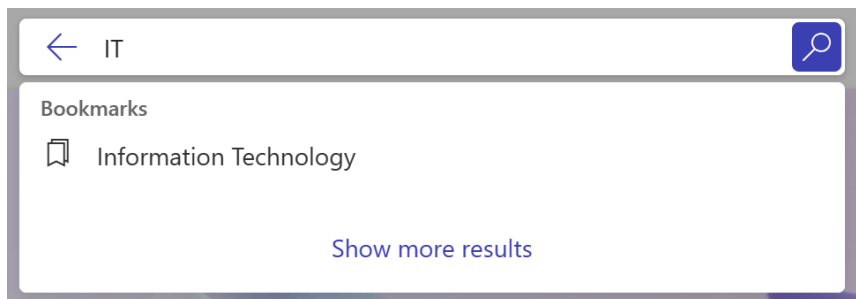


Figure 5.6 – A bookmark suggestion appearing immediately upon keyword match

If a user hits *Enter* on a search query, they will also see bookmarks listed at the top of the results page, as shown in *Figure 5.7*.

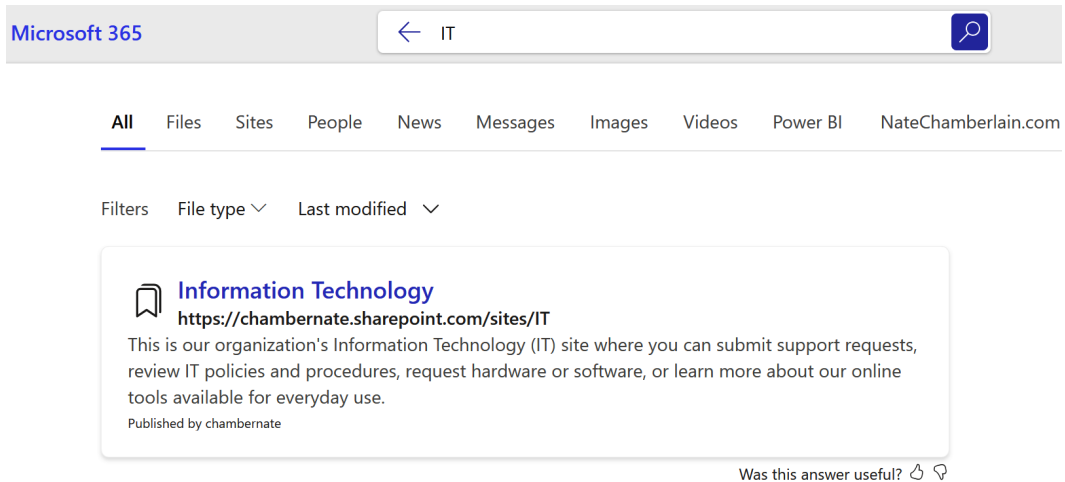


Figure 5.7 – A bookmark result shown at the top of the results page

There's more...

In addition to being able to add bookmarks manually, Microsoft will suggest bookmarks based on popular needs as well as specific search activity in your organization. Filter your bookmarks screen to only show those with the **Suggested** status (not **Draft** or **Published**) to find these and customize them prior to publishing.

Microsoft auto-publishes recommended bookmarks by default. You can change this setting by selecting the ellipsis (...) on the ribbon menu of the **Bookmarks** screen, then **Manage settings**. The setting is shown in *Figure 5.8*.

Bookmark settings

Recommended bookmarks

Microsoft Search analyzes which internal sites are visited most often by people in your organization and can recommend them as new bookmarks every 30 days. You can automatically publish these bookmarks in search results or manually select which bookmarks to publish from the **suggested** status list.

[Learn more about recommended bookmarks](#)

- ☒ Allow Microsoft Search to recommend bookmarks
- ☐ Automatically publish recommended bookmarks for your users.
- ☒ Manually select recommended bookmarks to publish for your users.

Figure 5.8 – Option to manually select or automatically publish recommended bookmarks

If you leave auto-publishing on, you may wish to exclude some URLs that may not be well suited for higher visibility, such as image asset libraries or archives. Use the **Exclude** option from the ribbon menu of the **Bookmarks** screen to add URLs that should not be recommended.

To add multiple bookmarks at once, the **Import** option allows administrators to upload a CSV file containing bookmark data. This is ideal for deploying large numbers of bookmarks systematically. We will cover this process in the next recipe, *Importing bookmarks in bulk from CSV*.

Post-implementation, use the search **Insights** dashboard to monitor the performance of bookmarks, adjusting strategies based on user engagement and search behaviors. We will review this dashboard in this chapter's final recipe, *Using Search Insights dashboard reports*.

See also

- *Manage bookmarks*: <https://learn.microsoft.com/en-us/microsoftsearch/manage-bookmarks>

Importing bookmarks in bulk from CSV

Importing bookmarks in bulk using a CSV file is an efficient method for administrators to add multiple search bookmarks at once in Microsoft Search. This capability is especially useful when deploying a large set of resources that need to be quickly accessible across the organization through search.

Getting ready

Ensure you have the necessary administrative rights; either a Global Administrator, Search Administrator, or Search Editor role is required to execute these steps.

How to do it...

1. Navigate to the Search & intelligence admin center at <https://admin.microsoft.com/#/MicrosoftSearch> or by navigating to the Microsoft 365 admin center (<https://admin.microsoft.com>) and then **Settings | Search & intelligence**.
2. In the Search & intelligence admin center, choose **Answers** from the top menu and then select **Bookmarks** from the left navigation menu.
3. Select the **Import** option shown in *Figure 5.9* to start the bulk upload process.

Home > Search & intelligence > Bookmarks

Search & intelligence

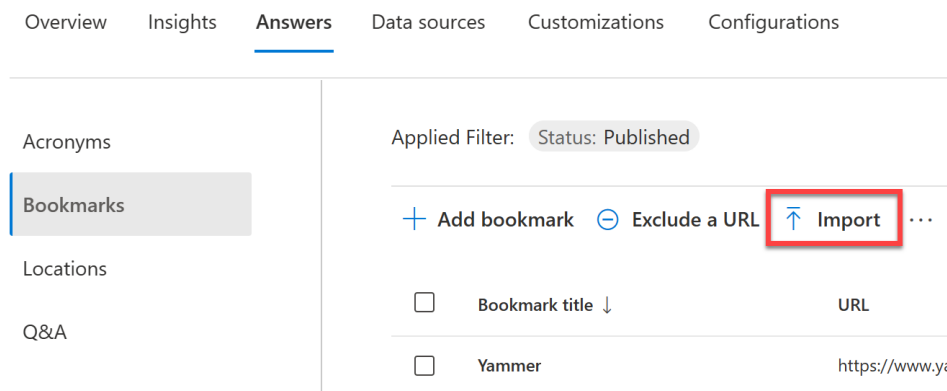


Figure 5.9 – Import option on the Bookmarks screen of Microsoft Search

4. On the side panel that opens, download the CSV template provided by Microsoft Search by selecting **Download bookmarks template (.csv)**. This will ensure proper formatting.

5. Open the downloaded CSV template, then fill out the file with the bookmark details, such as **Title**, **Url**, **Description**, **Keywords**, and any optional, applicable settings, such as **Country/Region**, **Groups**, and **Device & OS**.
6. Once your CSV file is prepared and saved, select **Browse** in the import dialog to upload your CSV file.
7. Review the import summary below the file path box that indicates how many bookmarks will be added or updated. Confirm the details and proceed by selecting **Import**.

How it works...

The import process reads the CSV file and creates or updates bookmarks based on the data provided. This batch operation streamlines the addition of multiple bookmarks, making them available nearly instantaneously to end users searching for related terms. Once bookmarks have been successfully imported, the side panel will display how many bookmarks were successfully added or updated, as shown in *Figure 5.10*.

Import bookmarks

Import using a CSV file

Download a copy of the bookmarks template to make sure any items you're importing are in the correct format. When you're ready to import, come back here and upload your file.

Download CSV template

[↓ Download bookmarks template \(.csv\)](#)

Upload the completed template

Browse

☑ Import complete:
Bookmarks: 1 added, 0 updated

Done

Figure 5.10 – Success message after bulk upload

There's more...

Should there be any issues with the CSV format or the data provided, Microsoft Search will provide error messages detailing the issues to be corrected. These specific errors can be accessed by selecting **Open file details** after attempting the import, as shown in *Figure 5.11*. This helps in ensuring that all bookmarks are uploaded correctly without any missing information.

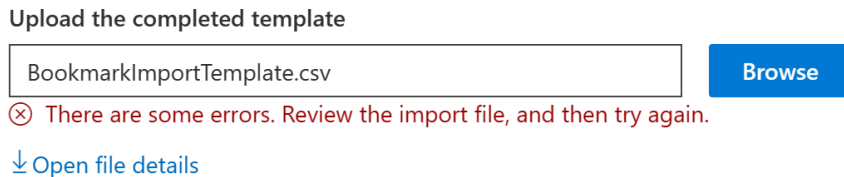


Figure 5.11 – Error message when importing bookmarks

After importing, it is advisable to review the bookmarks in the admin center to ensure all entries are correctly implemented and appear as expected. Adjustments can be made manually from within the Search & intelligence admin center if necessary.

See also

- *Manage bookmarks*: <https://learn.microsoft.com/en-us/microsoftsearch/manage-bookmarks>

Adding a location

In Microsoft Search, adding a location allows users to quickly find directions and details about key places within your organization, such as offices, campuses, and meeting rooms. This feature enhances the search experience by integrating geographical information directly into your enterprise search results. It's particularly useful for large organizations with multiple locations, helping employees and visitors navigate effectively.

Getting ready

Ensure you have the necessary administrative rights; either a Global Administrator, Search Administrator, or Search Editor role is required to execute these steps.

How to do it...

1. Navigate to the Search & intelligence admin center at `https://admin.microsoft.com/#/MicrosoftSearch` or by navigating to the Microsoft 365 admin center (`https://admin.microsoft.com`) and then **Settings | Search & intelligence**.
2. In the Search & intelligence admin center, choose **Answers** from the top menu and then select **Locations** from the left navigation menu.
3. Select **Add location**, as shown in *Figure 5.12*, to begin creating a new location entry.

Home > Search & intelligence > Locations

Search & intelligence

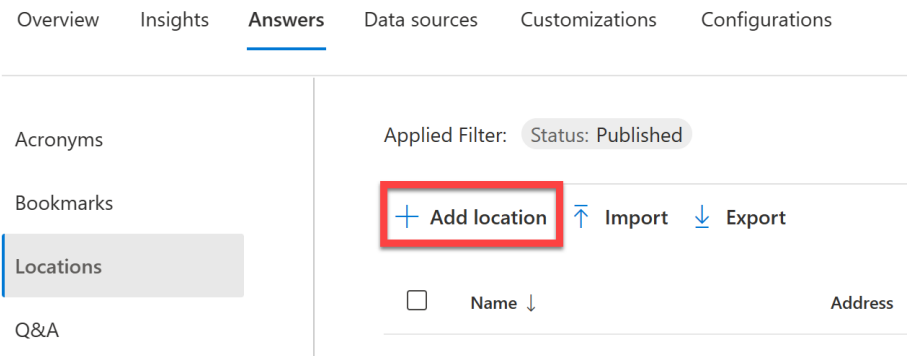


Figure 5.12 – Add location option in the Search & intelligence admin center

4. Fill in the details for the location, such as **Name**, **Country or region**, **Address**, and **Keywords**, as shown in *Figure 5.13*.

Building 252

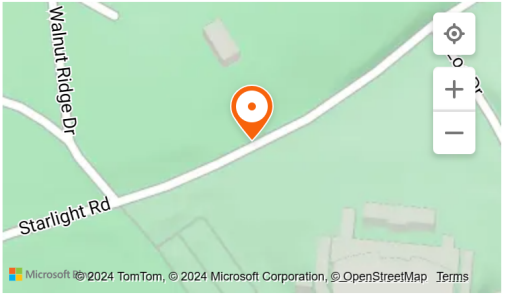
EditHistory

Building 252

Starlight Rd Kansas
City MO United States
64132

Get Directions

Expand map



Name *

Building 252

Country or region *

United States

Address

Starlight Rd. Kansas Ctv. MO 64132

Publish

Save to draft

Figure 5.13 – A new location being configured in the Search & intelligence admin center

5. After reviewing all the information, select **Publish** to publish the location to Microsoft Search.

How it works...

When you add a location to Microsoft Search, it creates a searchable entry that appears in search results when users query relevant terms. This feature utilizes the details you provide, such as name, address, and keywords, to offer directional guidance and basic information about the location within the organization’s search index. These entries help streamline navigation and increase operational efficiency by allowing users to quickly find and visualize places of interest within the company. An example of a result for the fictional *Building 252* is shown in *Figure 5.14*. Note the inclusion of a **Get directions** option alongside an interactive map.

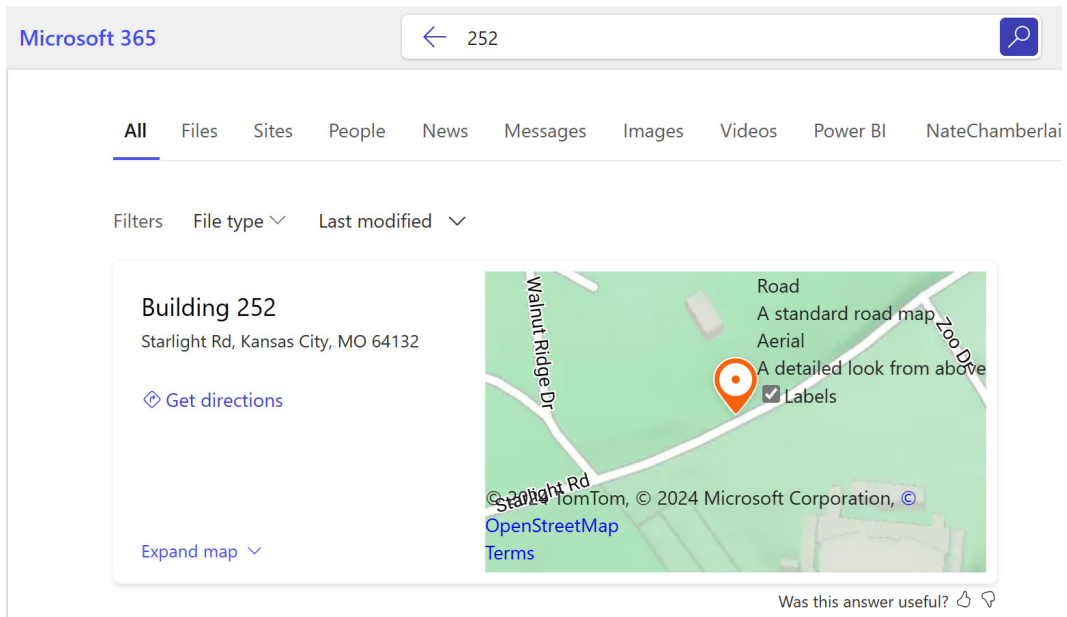


Figure 5.14 – A location search result with a map visual and directions link

There's more...

Just like adding multiple bookmarks at once, you can also import several locations simultaneously using the **Import** feature instead of **Add location**. Here's how:

1. First, on the **Locations** screen, select **Import** and download the provided CSV template.
2. Fill out the template with the necessary location details.
3. Upload the completed CSV template. This process is very similar to importing bookmarks in bulk, allowing you to efficiently add multiple locations to your Microsoft Search configuration at once.

By maintaining accurate and comprehensive data on your locations, you help ensure that employees and visitors can reliably find the places they need without manual assistance.

See also

- *Manage locations*: <https://learn.microsoft.com/en-us/microsoftsearch/manage-locations>

Adding a Q&A result

Adding a Q&A result in Microsoft Search allows you to directly answer common queries from users within your organization. This feature can guide users to the right information quickly and effectively by providing an answer directly in the search result itself, reducing clicks and the time spent browsing, thereby increasing productivity. It is especially useful for frequently asked questions about internal processes, HR inquiries, IT support, and more.

Getting ready

Ensure you have the necessary administrative rights; either a Global Administrator, Search Administrator, or Search Editor role is required to execute these steps.

How to do it...

1. Navigate to the Search & intelligence admin center at <https://admin.microsoft.com/#/MicrosoftSearch> or by navigating to the Microsoft 365 admin center (<https://admin.microsoft.com>) and then **Settings | Search & intelligence**.
2. In the Search & intelligence admin center, choose **Answers** from the top menu and then select **Q&A** from the left navigation menu, as shown in *Figure 5.15*.

Home > Search & intelligence > Q&A



Search & intelligence

Overview Insights **Answers** Data sources Customizations Configurations

Acronyms

Bookmarks

Locations

Q&A

Applied Filter: Status: Published

+ Add question

↕ Import

↓ Export

2 items

<input type="checkbox"/>	Title	Answer description
<input type="checkbox"/>	Where are the expense reports?	#Where to find Expense repc
<input type="checkbox"/>	Who is my department's timekeeper?	Your department's timekeep

Figure 5.15 – Location of Q&A results in the Search & intelligence admin center

3. Select **Add question** to begin adding a new Q&A result to Microsoft Search.
4. Enter a title (the question), URL (a reference with more information), and answer description (the answer), as shown in *Figure 5.16*.

When is the benefits enrollment deadline?

[When is the benefits enrollment deadline?](https://chambernate.sharepoint.com/sites/Benefits)
<https://chambernate.sharepoint.com/sites/Benefits>

The benefits enrollment deadline for 2025 is October 31, 2025. Ensure you have completed your enrollment forms and submitted to HR prior to this date to guarantee coverage for the upcoming year.

Title * Characters: 41 / 60

When is the benefits enrollment deadline?

URL

<https://chambernate.sharepoint.com/sites/Benefits>

Answer description *

The benefits enrollment deadline for 2025 is October 31, 2025. Ensure you have completed your enrollment forms and submitted to HR prior to this date to guarantee coverage for the upcoming year.

Publish **Save to draft**

Figure 5.16 – A new Q&A result being entered in Microsoft Search

5. Enter keywords and reserved keywords:
 - A. **Keywords:** Specify keywords that will trigger the appearance of the Q&A result in search results
 - B. **Reserved keywords:** These are unique to this Q&A result (they cannot be used for others) and ensure this result appears when these terms are searched, whereas normal keywords can be shared among other results

6. As you fill out these fields, a live preview of the search result card will display how it will appear to users, as previously shown in *Figure 5.16*.
7. Optional settings to refine when and how the Q&A result appears can be configured at the bottom of the side panel:
 - A. **Dates:** Set specific dates if the bookmark should only appear during a certain period.
 - B. **Country or region, Groups, Device & OS:** These settings allow you to target the Q&A result to specific users based on location, group membership, or device type.
 - C. **Targeted variations:** Adjust the Q&A result content based on a user's device or location. For example, you may wish to send international employees an answer that includes specific information or requirements for international employees that domestic employees may find irrelevant.
8. Review your configurations and select **Publish** to make the bookmark live. You can alternatively choose **Save to draft** if you wish to resume configuration at a later time.

How it works...

By adding a Q&A result, you embed a direct answer into the search engine that is triggered by specific user queries. This functionality supports the quick resolution of common questions, providing immediate answers without the need for users to navigate through multiple documents or pages. The search system indexes these Q&A entries by their keywords and displays them as top results when relevant queries are made, ensuring efficient information retrieval.

An example Q&A result for the query *open season* is shown in *Figure 5.17*.

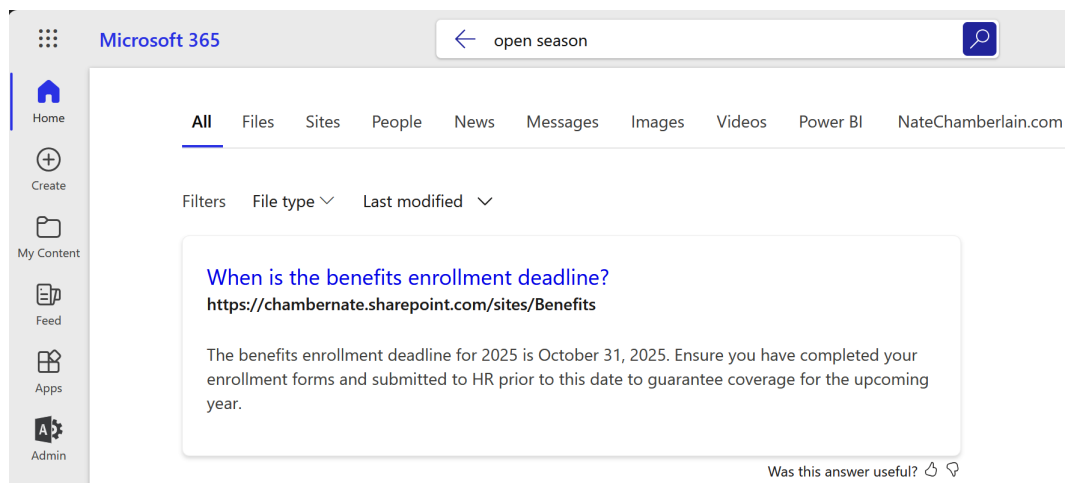


Figure 5.17 – Example Q&A result shown in search results

There's more...

You can enhance the Q&A results by linking to detailed articles or internal resources that provide more comprehensive information on the topic. If your Q&A result shares a benefits enrollment deadline primarily, your URL might be a SharePoint page that links to more information, including benefits package descriptions, eligibility criteria, and/or pricing. Additionally, consider regularly reviewing and updating your Q&A results to reflect changes over time (such as annual dates) or relevance (such as deprecated offerings, events, and procedures).

See also

- *Manage Q&As*: <https://learn.microsoft.com/en-us/microsoftsearch/manage-qas>

Setting up usage of Microsoft Search in Bing

Integrating Microsoft Search with Bing allows your organization's users to find relevant work results alongside public web results when they search using the Bing search engine at <https://bing.com>. This makes it easier for users to remain in the flow of work without the need to switch contexts, tabs, or applications to find the information they need from a single query. Employees may use this convenience to find internal documents, conversations, contacts, and more (just as they would from an office.com or SharePoint search) without leaving their web search engine, fostering a seamless integration of web and organizational resources.

Getting ready

Ensure you have the necessary administrative rights; either a Global Administrator, Search Administrator, or Search Editor role is required to execute these steps.

How to do it...

1. Navigate to the Search & intelligence admin center at <https://admin.microsoft.com/#/MicrosoftSearch> or by navigating to the Microsoft 365 admin center (<https://admin.microsoft.com>) and then **Settings | Search & intelligence**.
2. In the Search & intelligence admin center, choose **Configurations**, then select **Change** under **Microsoft Search in Bing setting**, as shown in *Figure 5.18*.

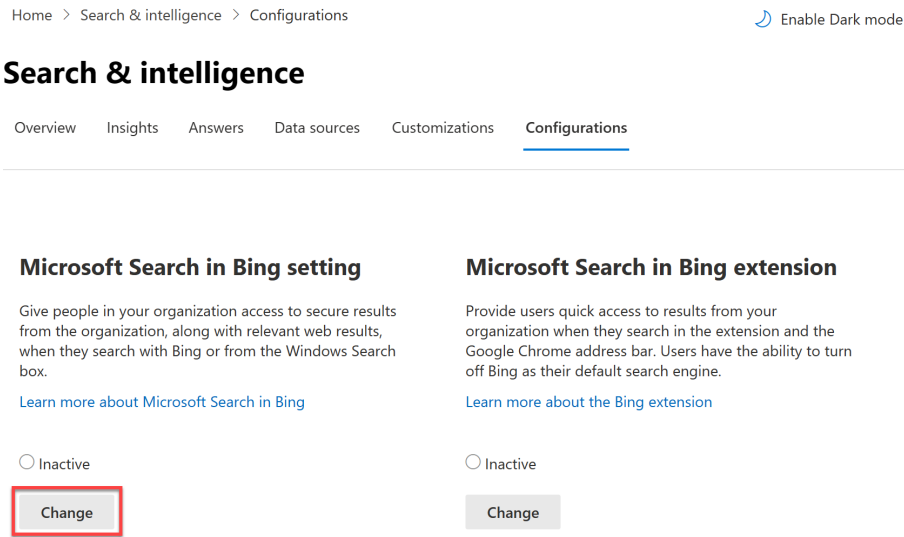


Figure 5.18 – Option to enable Microsoft Search in Bing

3. Check the box next to **Enable Microsoft Search in Bing for your organization**, then select **Next**.
4. Select the radio button next to **Enable Microsoft Search in Bing, Windows search, and Microsoft Edge**, then select **Save**, as shown in *Figure 5.19*.

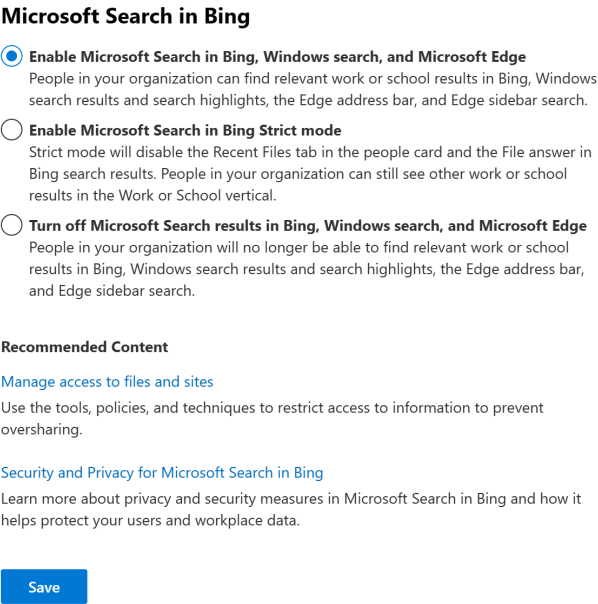


Figure 5.19 – Setting options when enabling Microsoft Search in Bing

How it works...

Integrating Microsoft Search with Bing allows organizational content to surface alongside web results in Bing searches. This setup uses Microsoft 365 authentication to securely fetch and display internal documents, files, and other resources in the search results, provided the user has the appropriate permissions. This dual-scope search capability ensures that employees can access all necessary information from a single search query, blending public and private data seamlessly.

Once you enable this setting, it may take up to 24 hours for changes to propagate across all users depending on the size of your organization.

There's more...

There are related settings you can configure from the Search & intelligence admin center under **Configurations**, including **Microsoft Search in Bing shortcut** and **Microsoft Search in Bing extension**.

Microsoft Search in Bing shortcut, as shown in *Figure 5.20*, will enable a keyword users can use in the Edge browser bar, such as *work*, which will only return work results rather than the usual work and public web results.

Microsoft Search in Bing shortcut

This shortcut lets people in your organization search for work content directly from the address bar in their Microsoft Edge browser, by using the default shortcut keywords **work** and **chamberbate**.

[Learn more about Microsoft Search in Bing shortcut](#)

☒ Enable the Microsoft Search in Bing shortcut

You can add 1 or 2 more shortcut keywords of your choice. [Learn more about search keywords](#)

Enter shortcut keywords

Figure 5.20 – Microsoft Search in Bing shortcut setting

Microsoft Search in Bing extension will set the default search engine for Google Chrome users to Bing and enable the Bing extension. Users can choose to search from either location (their Google Chrome address bar or the Bing extension) to retrieve work and public results side by side.

See also

- *Overview of Microsoft Search in Bing*: <https://learn.microsoft.com/en-us/microsoftsearch/overview-microsoft-search-bing>
- *Microsoft Search in Bing*: <https://support.microsoft.com/en-us/office/microsoft-search-in-bing-c49752ef-d00c-4e35-9f8b-840222d55cc0>

Assigning Search Administrator and Search Editor roles


Assigning the right administrative roles in Microsoft Search is crucial for managing search settings and configurations effectively. Search admins can manage all aspects of Microsoft Search, including modifying the search schema and setting up connectors, while Search editors are primarily responsible for creating and managing content such as bookmarks and Q&As. This role distribution ensures that the management of search capabilities is scalable and secure.

Getting ready




Ensure you have the necessary administrative rights; either a Global Administrator or User Administrator role is required to execute these steps.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. From the left navigation pane, select **Users | Active users**.
3. Choose the user to whom you want to assign the Search Administrator or Search Editor role.
4. In the side panel that appears, within the user's **Account** tab, select **Manage roles** under the **Roles** header, shown in *Figure 5.21*.



Alex Wilber

 Reset password  Block sign-in  Delete user

[Change photo](#)

Username and email

AlexW@chambernate.onmicrosoft.com

[Manage username and email](#)

Aliases

[Manage username and email](#)

Last sign-in

[View last 30 days](#)

Sign-out ⓘ

Sign this user out of all Microsoft 365 sessions.

[Sign out of all sessions](#)

Alternate email address

None provided

[Add address](#)

Groups

Information Technology

Mark8 Project Team

Nate LLC

[Manage groups](#)

Roles

Global Reader

[Manage roles](#)

Manager

Miriam Graham

[Edit manager](#)

Figure 5.21 – Option to manage roles for a user in the Microsoft 365 admin center

5. Select **Admin center access** and then select **Show all by category**.
6. Under the **Collaboration** heading, you'll find the Search Administrator and Search Editor roles. Check the box next to the role you wish to assign to the user and then select **Save changes**.

How it works...

Assigning specific roles such as Search Administrator and Search editor in Microsoft Search helps define and distribute the management responsibilities of your organization's search capabilities. Search Administrators have broad control over search configurations and settings, while Search editors focus on content creation and management. This role-based access control ensures that search settings and sensitive data are managed safely and effectively, maintaining system integrity and compliance.

Professionals who have worked in IT administration or knowledge management roles may have used these roles to manage enterprise search configurations effectively, especially in large organizations where search capabilities are critical to daily operations. For example, in roles where maintaining a consistent user experience across a global company is paramount, Search admins and Search editors ensure that localized content, such as bookmarks and Q&As, are up to date and relevant to different departments or regions.

There's more...

Note that if someone is assigned the Global Administrator role, they can already perform all functions of the Search Administrator role, so there is no need to assign the additional role. Similarly, if someone is a Search Administrator, they can already perform all functions of the Search Editor role.

For enterprise-scale management, assigning roles directly to individual users may not be the most efficient approach. Instead, consider assigning these roles through security groups. By doing so, you can manage role assignments more easily and ensure consistency across the organization. For instance, create a security group for Search Administrators and another for Search editors, and then assign the respective roles to these groups. This method aligns with best practices for role-based access control in large organizations, providing a scalable and maintainable solution.

In larger organizations, security group assignments are often the preferred method for managing permissions because they allow for easier scaling and management. This is particularly useful in scenarios where the organization is growing, and IT Administrators need to maintain control over access rights without manually updating individual user roles.

Regularly review the roles and permissions assigned to ensure they still align with your organizational policies and needs. Adjustments may be necessary as roles within your organization change or as Microsoft updates its platform capabilities.

See also

- *Set up Microsoft Search*: <https://learn.microsoft.com/en-us/microsoftsearch/setup-microsoft-search#step-1-assign-search-admin-and-search-editor>

Using Search Insights dashboard reports

The **Search Insights** dashboard in Microsoft Search is a powerful tool for administrators to analyze search behaviors and trends within their organization. By leveraging this dashboard, administrators can gain insights into what users are searching for, identify gaps in content, and optimize the search experience to better meet user needs.

Getting ready

Ensure you have the necessary administrative rights; either a Global Administrator, Search Administrator, or Search Editor role is required to execute these steps.

How to do it...

1. Navigate to the Search & intelligence admin center at <https://admin.microsoft.com/#/MicrosoftSearch> or by navigating to the Microsoft 365 admin center (<https://admin.microsoft.com>) and then **Settings | Search & intelligence**.
2. In the Search & intelligence admin center, select **Insights** from the top menu.
3. You will be presented with the Search Insights dashboard, which contains several reports along the left navigation menu, as shown in *Figure 5.22*.

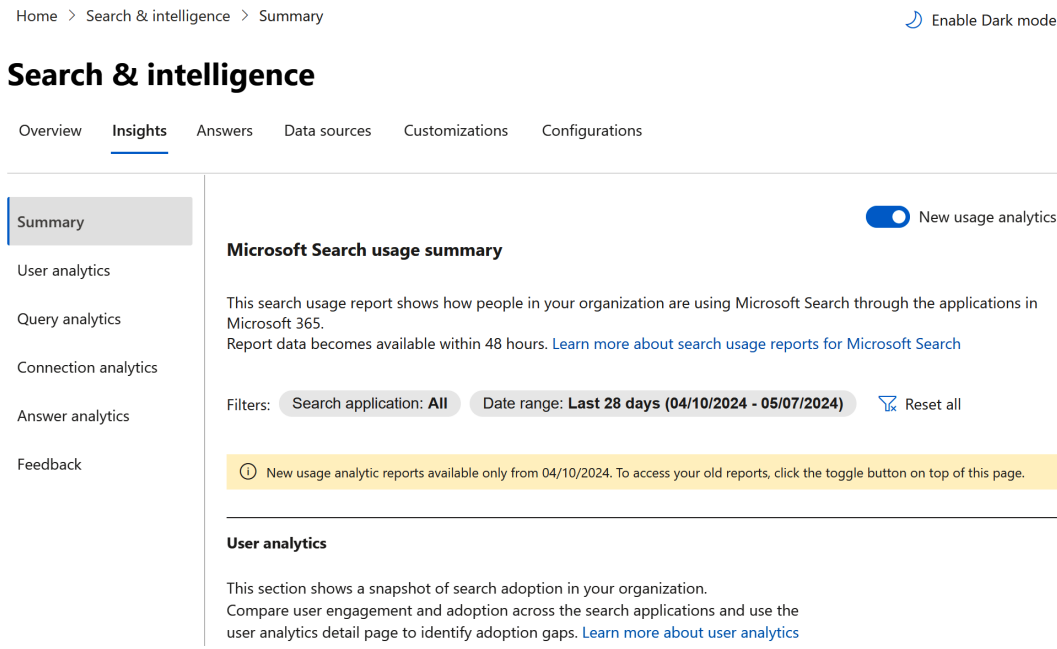


Figure 5.22 – Search insights dashboard in the Search & intelligence admin center

4. Along the left navigation menu, select the various reports to review the data they contain, including **Summary**, **User analytics**, **Query analytics**, **Connection analytics**, **Answer analytics**, and **Feedback**.
5. Use the filter options at the top of each report, such as those for **Query analytics** shown in *Figure 5.23*, to refine the data by date range, specific application, or other relevant criteria to focus on specific insights.

Query analytics

Here are the top queries by people in your organization who use search regularly, along with queries that returned no results or were abandoned by the user without selecting any search results. (If any filters show data for 5 or less individuals, those results will not be included in any report, to protect privacy.) [Learn more about query analytics.](#)

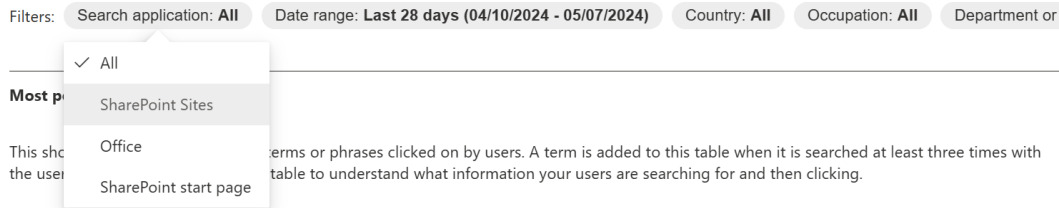


Figure 5.23 – Filter options for the Query analytics report

- Analyze the data presented to understand search patterns and potential areas for improvement in your search setup. You can also download several reports using the **Download Report** option in the upper-right corner of specific visuals. This will download a CSV file you can archive or import into other software, such as Power BI, to visualize your data however you would like.

How it works...

The Search Insights dashboard provides administrators with a comprehensive view of how search is being used within the organization. It aggregates data on search frequency, success, and user engagement, presenting these metrics in various reports and charts. Administrators can use this information to track search performance, understand user needs, and identify areas where search results can be optimized to enhance usability and relevance, ultimately improving the overall search experience within the organization.

Professionals in roles such as knowledge manager, IT Administrator, or business analyst often rely on search analytics to drive decisions about content management and user experience improvements. For instance, identifying common search queries that yield no results can highlight gaps in the organization's knowledge base, prompting the creation of new content to better serve employees.

The various reports available can help you focus on specific metrics:

- Summary:** Provides an overview of key metrics across the entire search landscape within your organization, including total searches, top queries, and click-through rates. This report offers a quick snapshot to gauge general search activity and effectiveness.
- User analytics:** Details individual user engagement with the search system, tracking metrics such as the number of searchers and non-searchers and searches by department, geography, and occupation. This report helps in understanding how different users interact with the search tools.

- **Query analytics:** Analyzes the search queries themselves, showing data on the most common queries and the success of queries in returning useful results. It's useful for identifying trends in what information users are frequently seeking.
- **Connection analytics:** Examines how users interact with various data sources connected to Microsoft Search, such as databases or external websites. It tracks which connections are used most and how effectively they contribute to successful search outcomes.
- **Answer analytics:** Focuses on the performance of configured answers in Microsoft Search, such as acronyms, bookmarks, and Q&A. It provides metrics on how often answers are shown and selected, helping to measure their relevance and accuracy.
- **Feedback:** Displays user feedback on search results, including ratings and comments. This report is crucial for continuous improvement, allowing administrators to adjust and enhance the search experience based on direct user input.

There's more...

Consider scheduling regular reviews of the Search Insights reports to continually refine and enhance your organization's search experience. Insights from these reports can help inform decisions on additional content creation, adjustments in search configurations, and targeted user training sessions to improve search effectiveness.

Regularly reviewing Search Insights can be a key responsibility for someone in a knowledge management role. This practice not only supports the continuous improvement of the search experience but also contributes to overall organizational efficiency. By using data-driven insights to optimize search configurations, professionals ensure that employees can find the information they need quickly and easily, which is essential in fast-paced business environments.

Please note that the Search Insights dashboard has a data retention limit of 12 months. To preserve older data for historical analysis and long-term trends, it's advisable to periodically download reports. This approach ensures continued access to past data, which can be valuable for conducting advanced analytics in Power BI or other similar tools.

See also

- *Microsoft Search Usage Reports:* <https://learn.microsoft.com/en-us/microsoftsearch/usage-reports>

6

Administering OneDrive for Business

This chapter equips Microsoft 365 Administrators with essential techniques for managing and securing OneDrive for Business, a cloud storage service that provides a secure space for individual users to store, share, and collaborate on files across multiple devices. This chapter covers a range of practices, from enabling external sharing and syncing files across devices to setting stringent compliance safeguards and managing data migrations using the **SharePoint Migration Tool (SPMT)**. The focus is on deploying practical, security-conscious strategies that enhance collaboration without compromising the integrity and privacy of organizational data. By mastering these administrative controls, you will be able to effectively enhance productivity and ensure that your organization's data handling aligns with industry standards and security protocols.

Important note

Since OneDrive for Business is built on SharePoint, many of these recipes will apply to both applications. In fact, OneDrive for Business doesn't have its own admin center – it is administered mostly via the SharePoint admin center.

We will cover the following recipes in this chapter:

- Enabling external sharing
- Configuring external sharing permission levels
- Restricting sharing to specific domains
- Enabling local sync of files
- Restricting local syncing to PCs on specific domains
- Setting up compliance safeguards
- Providing individuals access to another user's OneDrive content

- Setting the default share link type
- Adjusting all users' default storage allocation and retention periods
- Migrating data using the SPMT

Technical requirements

This chapter requires administrative access within Microsoft 365. Users assigned the Global Administrator role will have the capability to execute all tasks presented. Those holding the SharePoint Administrator role will find most of these recipes within their reach. We will detail the recipes that necessitate particular administrative roles, all of which can be assigned by an existing Global Administrator through the Microsoft 365 admin center's **Users** section if not already in place.

Enabling external sharing

External sharing in SharePoint and OneDrive for Business allows your organization to share content with people outside of your organization, such as partners or customers. This can facilitate collaboration on projects with external stakeholders without needing to give them full access to your internal sites.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint** as shown in *Figure 6.1*.

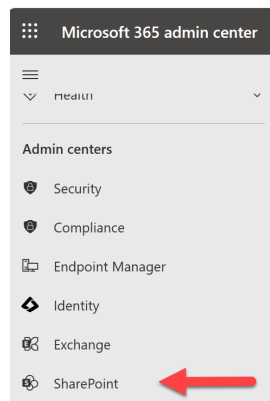


Figure 6.1 – SharePoint admin center location in Microsoft 365 admin center

2. In the left navigation menu of the SharePoint admin center, select **Policies | Sharing**.

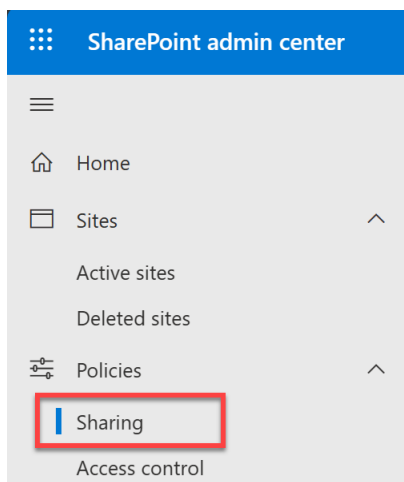


Figure 6.2 – External sharing settings location in the SharePoint admin center

3. Here, you can define the permitted scope of sharing throughout your organization. These settings apply to both SharePoint and OneDrive for Business. The sharing options are shown in *Figure 6.3* and described here:
 - A. **Anyone:** This allows users to share files and folders using links that do not require sign-in. It is best used for non-sensitive information, as this will make the information discoverable outside your organization.
 - B. **New and existing guests:** This setting supports sharing with guests who are either new to your directory or already exist within it. They must sign in to access the shared item(s).
 - C. **Existing guests:** This only supports guest members who already exist in your directory but will not support the addition of new guest members.

- D. **Only people in your organization:** This disables external sharing throughout your organization and restricts sharing to directory members with a Microsoft 365 license.

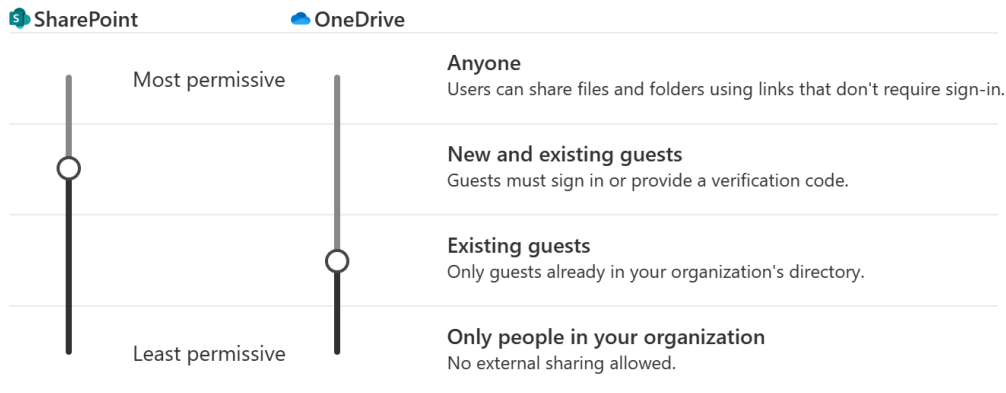
Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive.

[Learn more about managing sharing settings](#)

External sharing

Content can be shared with:



You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

Figure 6.3 – External sharing settings for SharePoint and OneDrive

4. Further down, select **More external sharing settings**. Here, you can adjust a number of settings, shown in *Figure 6.4*, that further protect your SharePoint and OneDrive (and, by extension, Teams) content. These settings allow you to do the following:
 - A. **Restrict sharing based on users' domains:** Control which domains your organization can share with by specifying allowed or blocked domains.
 - B. **Restrict external sharing to certain security groups:** If necessary, limit external sharing capabilities to specified security groups. This does not affect sharing through Microsoft 365 Groups or Teams.
 - C. **Authentication requirements for guests:** This setting ensures that guests sign in with the account to which an invitation was sent, adding an extra layer of security.

- D. **Sharing permissions for guests:** Determine whether guests can share items they don't own and set policies on automatic expiration of guest access and reauthentication requirements for users using verification codes. The three settings related to this topic are the final three shown in *Figure 6.4*.

More external sharing settings ▾

- ☐ Limit external sharing by domain
- ☒ Allow only users in specific security groups to share externally

1 security group: Marketing Members

Manage security groups

- ☒ Guests must sign in using the same account to which sharing invitations are sent
- ☒ Allow guests to share items they don't own
- ☒ Guest access to a site or OneDrive will expire automatically after this many days
- ☒ People who use a verification code must reauthenticate after this many days [Learn more](#) ⓘ

Figure 6.4 – More external sharing settings for SharePoint and OneDrive

5. Scroll down and configure the rest of the settings on the page shown in *Figure 6.5*. Note that when configuring the default link types (anyone, people in your org, etc.) and permissions (**Edit** versus **View**), your options are limited to those specified at the top site level for SharePoint and OneDrive permission settings.

Tip

Using **View** as the default link permission will help restrict access to items' version history as well, adding an additional level of protection to your content. Users can change the link's permission from **View** to **Edit**, but users in a hurry who stick with the default will have better-protected content.

File and folder links

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

- ☐ Specific people (only the people the user specifies)
- ☒ Only people in your organization
- ☐ Anyone with the link

Choose the permission that's selected by default for sharing links.

- ☐ View
- ☒ Edit

Other settings

- ☒ Show owners the names of people who viewed their files in OneDrive
- ☒ Let site owners choose to display the names of people who viewed files or pages in SharePoint
- ☒ Use short links for sharing files and folders

Figure 6.5 – File and folder link and other settings for SharePoint and OneDrive

The **Specific people** option (shown as **People you choose** to users outside the admin center) for link type is most appropriate and secure if you anticipate the need to share files and folders with guests on a regular basis.

The last three checkboxes under **Other settings** in *Figure 6.5* provide additional customization options for how file and folder links are managed in SharePoint and OneDrive. The first checkbox, **Show owners the names of people who viewed their files in OneDrive**, allows file owners to see who has accessed their files, offering transparency and insight into file engagement. The second checkbox, **Let site owners choose to display the names of people who viewed files or pages in SharePoint**, gives SharePoint site owners control over whether viewers' names are shown when files or pages are accessed, helping to manage visibility and privacy within the organization. The third checkbox, **Use short links for sharing files and folders**, enables the creation of concise, easily shareable URLs when files and folders are shared, simplifying link distribution and improving user experience.

6. Select **Save**.

Important note

It's important to remember that these settings apply at an organizational level for SharePoint, and they determine the settings available at the individual site level. The individual site settings cannot be more permissive than the organization-wide settings.

How it works...

Enabling external sharing in OneDrive for Business allows users to share documents and folders with individuals outside the organization. This feature is particularly useful when collaborating on projects with external partners, clients, or contractors. By setting this up, administrators can choose the extent to which users can share, including options such as allowing sharing with anyone who has the link or restricting sharing to guests who sign in or are provided access explicitly. The ability to share externally can significantly boost productivity and facilitate seamless collaboration on various projects across organizational boundaries. Administrators must carefully configure these settings, balancing the need for collaboration with the need to protect sensitive information.

There's more...

Check out this chapter's recipes titled *Setting the default share link type* and *Configuring external sharing permission levels* to learn how you can further customize external sharing abilities, including the following:

- Choose default link permissions (view or edit) and set expiration dates for links if needed to help make sure access to files is limited to defined time periods
- Restrict external sharing to users within specific security groups

See also

- *Manage sharing settings for SharePoint and OneDrive in Microsoft 365*: <https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>

Configuring external sharing permission levels

Configuring external sharing permission levels for SharePoint and OneDrive for Business is important for maintaining control over how files and folders are shared outside your organization. This setup helps in safeguarding sensitive information while facilitating collaboration with external partners and clients.

Getting ready

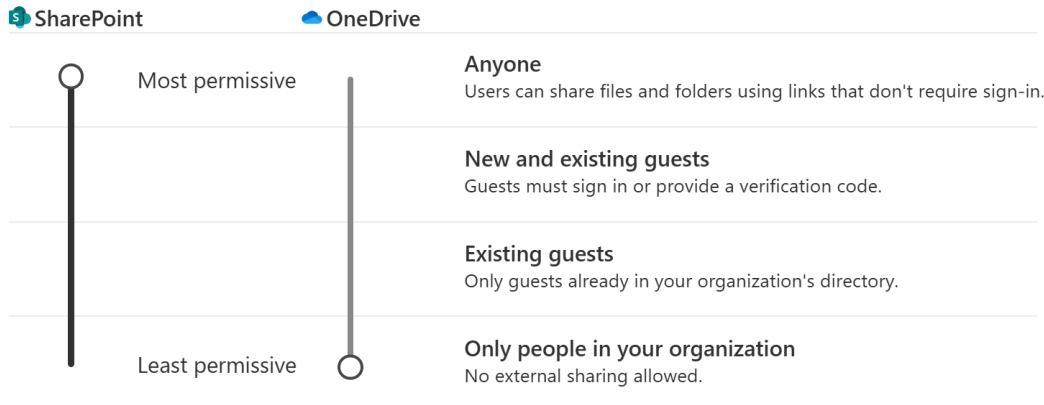
In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Policies | Sharing** from the left navigation menu.
3. Choose **External sharing** levels, as shown in *Figure 6.6*. You can select from several options, such as the following:
 - **Anyone:** This allows sharing with links that anyone can use without signing in. You can set these links to expire and limit them to view-only access by scrolling down and configuring those settings under **Choose expiration and permissions options for Anyone links**.
 - **New and existing guests:** This requires guests to sign in or verify their identity. This setting allows for more controlled access.
 - **Existing guests:** This restricts sharing to guests who are already in your organization's directory.
 - **Only people in your organization:** This disables all external sharing.

External sharing

Content can be shared with:



You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

Figure 6.6 – External sharing levels

Important note

OneDrive's permission level cannot be more permissive than SharePoint's, but it can be less. For example, you may allow SharePoint content to be shared with anyone but choose to restrict individual OneDrive content sharing to only people in your organization.

4. Expand **More external sharing settings**, as shown in *Figure 6.7*, to limit sharing by domain, specify which security groups can share externally, or set link expiration and permission levels.

More external sharing settings ▾

- ☒ Limit external sharing by domain

Add domains

- ☒ Allow only users in specific security groups to share externally

Manage security groups

- ☐ Guests must sign in using the same account to which sharing invitations are sent

- ☒ Allow guests to share items they don't own

- ☒ Guest access to a site or OneDrive will expire automatically after this many days

60

- ☐ People who use a verification code must reauthenticate after this many days [Learn more](#) ⓘ

30

Figure 6.7 – More external sharing settings

5. Confirm all changes by selecting **Save** to ensure the new settings are applied across SharePoint and OneDrive for Business.

How it works...

Configuring external sharing permission levels in OneDrive for Business allows administrators to define and limit how (and with whom) files can be shared outside the organization. This setup involves specifying different levels of access, such as allowing files to be shared with anyone, only with external users who authenticate, or only with existing external guests. This helps maintain control over the data shared externally, mitigating the risk of data exposure to unauthorized parties. By carefully managing these permissions, organizations can facilitate necessary collaborations without compromising their data security protocols, ensuring that only intended recipients have access to sensitive information.

There's more...

Note that the configuration you make in this recipe is the maximum allowed throughout the organization. No individual SharePoint site can have unique sharing settings that exceed the permission level specified at the org-wide level, but an individual site can be more restrictive. To change one site's external sharing permission level, follow these steps:

1. Go to the SharePoint admin center, then select **Sites** | **Active sites** to find the site that should have different external sharing permissions.
2. Select the site you wish to modify, then select **Settings** | **More external sharing settings**, as previously shown in *Figure 6.7*.
3. As shown in *Figure 6.8*, you can choose a new external sharing level for this site and select **Save** when finished.

Sharing

The sharing settings available for this site depend on your organization-level settings.

[Learn more about the external sharing settings](#)

External sharing

Site content can be shared with:

- ☐ **Anyone**
Users can share files and folders using links that don't require sign-in.
- ☒ **New and existing guests**
Guests must sign in or provide a verification code.
- ☐ **Existing guests only**
Only guests already in your organization's directory.
- ☐ **Only people in your organization**
No external sharing allowed.

Figure 6.8 – Default share link settings for a specific site

See also

- *Manage sharing settings for SharePoint and OneDrive in Microsoft 365*: <https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>

- *Change the sharing settings for a site:* <https://learn.microsoft.com/en-us/sharepoint/change-external-sharing-site>

Restricting sharing to specific domains

Restricting sharing to specific domains in SharePoint and OneDrive for Business is a security measure used to control external sharing by limiting interactions to approved or blocked domains. This setup helps organizations protect sensitive information while still enabling necessary external collaboration.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Policies | Sharing** from the left navigation menu.
3. Under **More external sharing settings**, check the box for **Limit external sharing by domain**, then select the **Add domains** button that appears as shown in *Figure 6.9*.

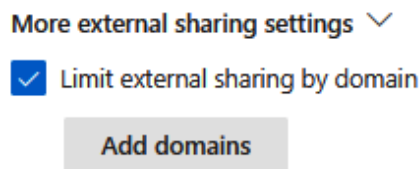


Figure 6.9 – Option to limit external sharing by domain


4. You must choose to either **Allow only specific domains** or **Block specific domains**. Essentially, you're deciding whether your organization will *only* permit sharing with specified domains or whether you'll allow sharing with all domains *except* specified domains.

Tip

Blocking specific domains may require less maintenance than allowing only specific domains since you won't have to add additional domains to include over time. If you choose to allow only specific domains, but continually expand partners, customers, and so on, you may end up frequently visiting this setting for updates.

5. Enter the domains in the provided box, as shown in *Figure 6.10*, using the *domain.com* format. For multiple domains, enter each on a new line.

Add domains

 These limitations will not apply when users share files and folders using Anyone links.

☐ Allow only specific domains

☒ Block specific domains

contoso.com
tailspintoys.com

Figure 6.10 – Adding domains for sharing restriction

6. After entering the domains, select **Save** and then **Save** again to enforce the restriction.

How it works...

Restricting sharing to specific domains is a security measure that allows organizations to control which external domains users can collaborate with. This setup is particularly useful for preventing accidental or unauthorized sharing of sensitive information with competitors or untrusted entities. Administrators can allow approved domains or block unwanted ones, thereby directly controlling the external collaboration landscape. This restriction is critical for maintaining secure business operations and protecting intellectual property by ensuring that collaborations occur only within a trusted network.

There's more...

You can also use the `Set-SPOTenant` PowerShell command to manage this setting. Here are the specific steps to do so:

1. Open **SharePoint Online Management Shell** from your start menu as an administrator (right-click | **Run as administrator**).
2. Run the following to sign in to the administrator account you wish to use, being sure to replace the tenant URL with your own:

```
Connect-SPOService -Url https://natechamberlain-admin.  
sharepoint.com
```

3. Set domain restrictions:

- A. To allow only specific domains, use the `Set-SPOTenant` cmdlet with the `-SharingDomainRestrictionMode "AllowList"` parameter and value. Replace *domain1.com* and *domain2.com* with the domains you want to allow, each delimited by a space:

```
Set-SPOTenant -SharingDomainRestrictionMode "AllowList"  
-SharingAllowedDomainList "domain1.com domain2.com"
```

- B. To block specific domains, use the `-SharingDomainRestrictionMode "BlockList"` parameter and value instead:

```
Set-SPOTenant -SharingDomainRestrictionMode "BlockList"  
-SharingBlockedDomainList "domain1.com domain2.com"
```

See also

- *Manage sharing settings for SharePoint and OneDrive in Microsoft 365*: <https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>

Enabling local sync of files

Enabling local synchronization of files with OneDrive for Business allows users to access their files on their local computer even when they're offline. This two-way synchronization ensures that any changes made to files locally are updated in the cloud once the connection is restored. It's particularly useful for users who travel often or have intermittent internet access, providing seamless access to their documents without relying on continuous connectivity.

Since it is a two-way sync, any changes made in the cloud are also reflected on the local device. This means that if a file is deleted or modified in the cloud, those changes will be mirrored locally, and vice versa. This feature can significantly enhance productivity but requires careful user awareness to avoid confusion.

Important note

When users delete local copies of their synced OneDrive or SharePoint files, these deletions are mirrored in the cloud. Users should be aware that this synchronization means files deleted locally will also be deleted from the cloud storage, potentially leading to problems if they unintentionally remove important files. Admins should provide guidance on using the OneDrive recycle bin and version history features to recover any accidentally deleted files, helping to prevent data loss and ensuring users can work confidently with local sync enabled.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Settings** from the left navigation menu.
3. Find the **OneDrive** options and select the row with **Sync** in the name column, as shown in *Figure 6.11*.

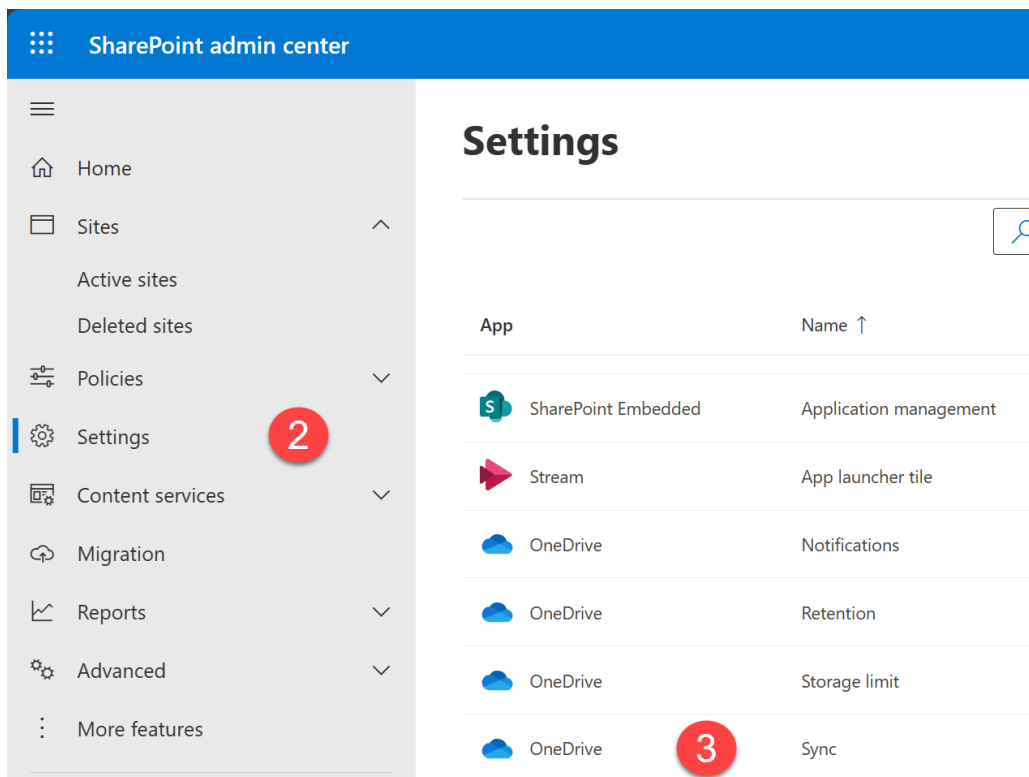


Figure 6.11 – Path to OneDrive sync settings via the SharePoint admin center

4. A side panel appears with the sync options available to administrators. These are shown in *Figure 6.12* and include the ability to hide the **Sync** option from each user's OneDrive. Note that this won't stop syncing for users who have already done so, but it will prevent new syncs from beginning. To hide the option, deselect **Show the Sync button on the OneDrive website**. Otherwise, check the box to enable sync, as shown in the following screenshot.

Sync

Use these settings to control syncing of files in OneDrive and SharePoint.

- ☒ Show the Sync button on the OneDrive website
- ☐ Allow syncing only on computers joined to specific domains
- ☐ Block upload of specific file types

Figure 6.12 – Sync options for OneDrive for Business

How it works...

When you enable local sync, the OneDrive sync app can mirror user OneDrives from the cloud to their local Windows PC, Mac, or mobile device (Linux is not supported). Any changes made to the synced files on your device are automatically uploaded to OneDrive once you reconnect to the internet. Similarly, any changes made to the files in OneDrive online are downloaded to the local device during the next sync session. This ensures that users can access and work on their documents even when they are offline.

Setting up local sync is straightforward: users simply open and sign in to the preinstalled OneDrive app using their work account on their Windows machine. Alternatively, they can open their OneDrive for Business in their browser and select **Sync this OneDrive** from their settings wheel, as shown in *Figure 6.13*.

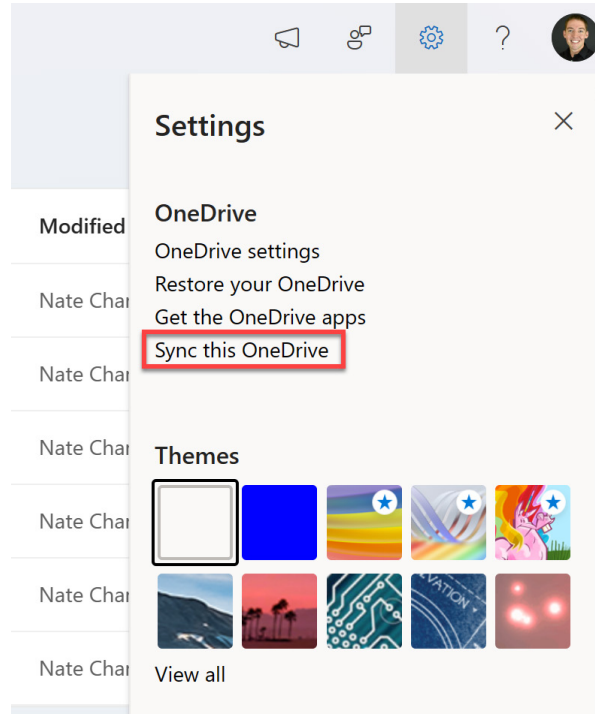


Figure 6.13 – The Sync this OneDrive option

This feature is particularly beneficial for those who travel often, work in remote environments, or have unreliable internet connections. It enhances user productivity by providing continuous access to important files, regardless of network connectivity. Sync activity for any file changes will take place when the device next connects to a network.

In addition to a user's OneDrive for Business files, users can opt to **Add shortcut to OneDrive** for any Teams or SharePoint library. This provides convenient access within their already-synced OneDrive directory to other frequently used files across their collaborative teams and sites.

There's more...

Users can choose which folders in their OneDrive they wish to sync in the event that there are some they'd prefer to have online only. This can be accomplished by following these steps:

1. Select the OneDrive icon in the system tray or notification area.
2. Select the settings wheel in the upper-right corner of the window that appears.
3. Select **Settings**, as shown in Figure 6.14.

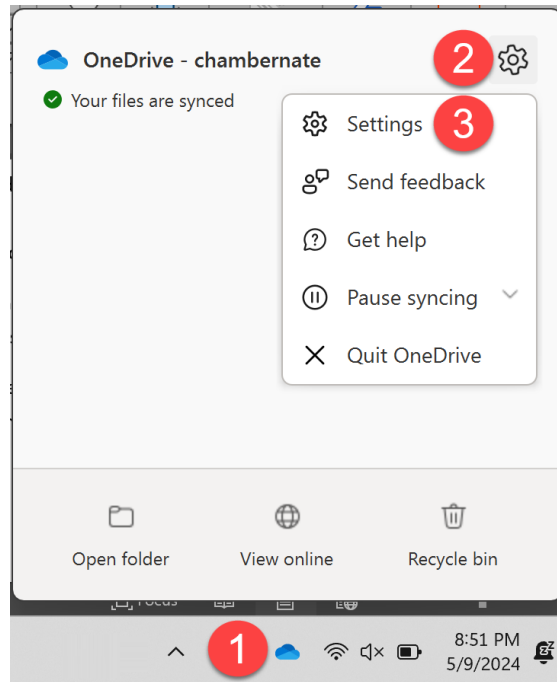


Figure 6.14 – Steps to access OneDrive settings

4. Select **Account | Choose folders** and deselect any folders that should not sync locally.
5. Select **OK** to save.

If you choose to *disable* sync organization-wide, you may wish to pair this recipe's actions with adjusting machine images or group policies so that the OneDrive client application is not installed or accessible on user machines. If users can access the app (preinstalled on Windows machines), they can still initiate a sync directly via the app. To learn more about administering OneDrive via group policy, check out <https://learn.microsoft.com/en-us/sharepoint/use-group-policy>.

See also

- *Sync SharePoint and Teams files with your computer:* <https://support.microsoft.com/en-us/office/sync-sharepoint-and-teams-files-with-your-computer-6de9ede8-5b6e-4503-80b2-6190f3354a88>
- *Prevent users from installing the OneDrive sync app:* <https://learn.microsoft.com/en-us/sharepoint/prevent-installation>

Restricting local syncing to PCs on specific domains

Restricting local syncing to PCs on specific domains is a security measure used in environments where you want to ensure that only authorized devices can sync company data via OneDrive for Business. This is particularly important in regulated industries or scenarios where data leakage could pose significant risks.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. In the SharePoint admin center, select **Settings** from the left navigation menu.
3. Find the rows with **OneDrive** listed in the **App** column and select the row with **Sync** in the **Name** column.
4. Check the box for **Allow syncing only on computers joined to specific domains**. This option was previously shown in *Figure 6.12*.
5. Enter the GUID for each domain you want to allow on a separate line, as shown in *Figure 6.15*. See the *How it works* section of this recipe if you are unsure of where you can find your domain's GUID.

Sync

Use these settings to control syncing of files in OneDrive and SharePoint.

- ☒ Show the Sync button on the OneDrive website
- ☒ Allow syncing only on computers joined to specific domains

Enter each Active Directory domain as a GUID on a new line.

```
3fa85f64-5717-4562-b3fc-2c963f66afa6  
5a105e8b-9d34-4cd7-bca0-5bd1eaf7b721
```

- ☐ Block upload of specific file types

Figure 6.15 – Specific domains for which syncing will be supported

6. Make sure to save your configuration by selecting **Save** to apply the settings.

How it works...

Restricting local syncing to PCs on specific domains enhances security by ensuring that only company-managed devices can sync and access OneDrive for Business files. This setting is imperative for organizations that handle sensitive or regulated data and need to enforce strict data security policies. By configuring domain restrictions, IT Administrators prevent data from being synced to personal or unsecured devices, which could potentially lead to data breaches.

To find your tenant's GUID, go to Microsoft Entra (<https://entra.microsoft.com>), then navigate to **Identity** | **Overview**. Your tenant's GUID will be visible in the **Basic information** section, as shown in *Figure 6.16*.

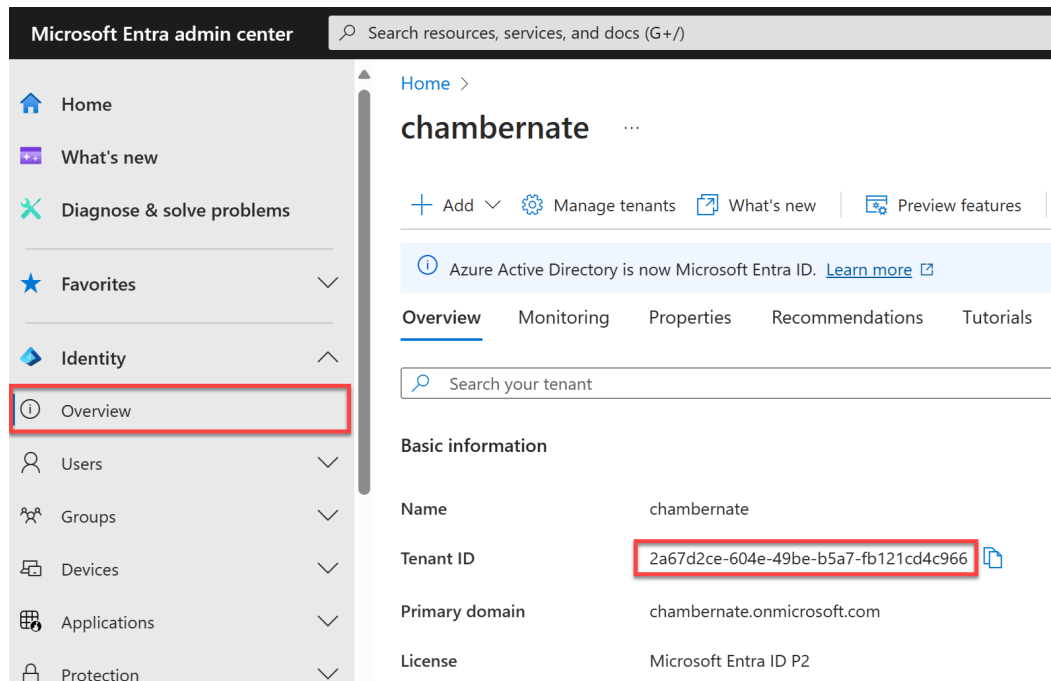


Figure 6.16 – Location of your tenant ID in Microsoft Entra

There's more...

This setting does not apply to non-Windows devices such as those running macOS or Linux. For these, alternative measures such as Conditional Access policies via Microsoft Entra are recommended.

If syncing stops working for a domain without any changes to the policy, a common fix is to temporarily disable domain restrictions using PowerShell with the `Set-SPOTenantSyncClientRestriction` command, then re-enable it.

For environments with mixed domain types or complex network configurations, ensure that all domain GUIDs are correctly added and that there are no conflicts with other sync settings.

See also

- *Allow syncing only on computers joined to specific domains:* <https://learn.microsoft.com/en-us/sharepoint/allow-syncing-only-on-specific-domains>

Setting up compliance safeguards

Setting up compliance safeguards in OneDrive for Business and SharePoint is imperative for organizations that need to manage and protect sensitive information. This involves implementing policies and configurations that help comply with legal and industry standards, ensuring that data handling within Microsoft 365 adheres to required security measures.

Tip

This topic is expansive and goes well beyond the scope of a single recipe. So, this recipe will guide you through getting started with multiple compliance considerations related to OneDrive for Business (and, by extension, SharePoint). Check *Chapters 12 and 13* for a deeper dive into security and compliance throughout Microsoft 365.

Getting ready

Configuring compliance safeguards requires the role of a Global, SharePoint, or Compliance Administrator depending on which topics you're configuring.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. In the SharePoint admin center, select **Settings** from the left navigation menu.
3. In the table on the **Settings** page, find the rows with **OneDrive** listed in the **App** column and select the row with **Retention** in the **Name** column.
4. Enter the number of days you wish to keep a user's OneDrive after their account has been deleted, as shown in *Figure 6.17*. The default is 30 days.

Retention

Specify the default retention period for a user's OneDrive when the user is deleted. Changing this setting also affects OneDrive accounts already within the retention period.

[Learn more about setting OneDrive retention](#)

Days to retain a deleted user's OneDrive

Enter a value from 30 through 3650 days.

Figure 6.17 – Retention period for delete users' OneDrives

5. Explore other compliance safeguards and topics throughout the Microsoft 365 ecosystem that affect OneDrive for Business, including the following:
 - **Information barriers:** Set up information barrier policies in **Microsoft Purview** (<https://purview.microsoft.com/informationbarrier>) to restrict communication and collaboration based on group memberships or business units. This helps prevent potential conflicts of interest and unauthorized access to sensitive information. We will cover Microsoft Purview more in *Chapter 13, Understanding the Microsoft Purview Compliance Portal*.
 - **Sensitivity labels:** Use Microsoft Purview to create and manage sensitivity labels (<https://purview.microsoft.com/informationprotection>). Apply these labels to content across SharePoint, OneDrive, and Teams to control access based on the sensitivity of the information.
 - **Data Loss Prevention (DLP):** Set up DLP policies in Microsoft Purview (<https://purview.microsoft.com/datalossprevention>) to identify, monitor, and protect sensitive information. Ensure policies are in place to prevent the accidental sharing of sensitive data both inside and outside the organization. We will cover DLP more in *Chapter 13, Understanding the Microsoft Purview Compliance Portal*.
 - **Audit and Activity logs:** Utilize Microsoft Purview's **audit logs** (<https://purview.microsoft.com/audit>) and Microsoft Defender's **Activity log** (<https://security.microsoft.com/cloudapps/activity-log>) to track and analyze activities around sensitive data. Regular review and usage of these tools can help detect and respond to potential compliance issues. We will cover auditing more in *Chapter 12, Understanding Microsoft 365 Defender*.

- **Data retention policies:** Define data retention policies in Microsoft Purview (<https://purview.microsoft.com/data/lifecyclemanagement>) to control how long information is kept and when it is disposed of, ensuring compliance with data retention regulations. We will cover retention policies more in *Chapter 13, Understanding the Microsoft Purview Compliance Portal*.

How it works...

Setting up compliance safeguards in OneDrive for Business involves configuring various settings that ensure your organization's data is handled according to legal and regulatory requirements. This recipe provides a starting point for managing compliance within OneDrive for Business, focusing on key areas such as retention policies, information barriers, sensitivity labels, and DLP.

When you follow this recipe, you'll begin by configuring the retention period for deleted users' OneDrives, ensuring that data remains available for a set time before being permanently deleted. This step is important for compliance, as it allows organizations to manage data life cycles effectively, ensuring that data is retained for only as long as necessary and in accordance with legal requirements.

Then, the recipe shares several other foundational areas for implementing essential compliance measures such as information barriers, which restrict communication and collaboration based on organizational policies, and sensitivity labels that classify and protect sensitive information across SharePoint, OneDrive, and Teams. By setting up DLP policies, you can further safeguard against the accidental sharing of sensitive information, both internally and externally.

Each of these safeguards helps maintain the integrity of your organization's data, but this recipe is just the beginning. The full process involves deeper configuration and ongoing management, which we'll explore further in *Chapters 12 and 13*, where we cover more advanced security and compliance topics within Microsoft 365. Implementing these initial steps will help ensure your OneDrive for Business environment is aligned with your organization's compliance requirements, reducing the risk of data breaches and ensuring adherence to regulations.

There's more...

We only covered a few solutions in this recipe, but there are more that may be available depending on your subscriptions and licenses. For example, **Advanced Threat Protection (ATP)** provides enhanced security for your SharePoint and OneDrive environments by protecting against sophisticated threats such as phishing and zero-day malware. **Information Rights Management (IRM)** can encrypt files and set usage restrictions to enhance security for sensitive documents.

You can also access some additional, general OneDrive for Business activity information via the Microsoft 365 admin center (<https://admin.microsoft.com>) by navigating to **Reports | Usage | OneDrive | Activity** (or by directly visiting <https://admin.microsoft.com/Adminportal/Home?#/reportsUsage/OneDriveActivity>). This will display recent activity by individual users such as the number of files viewed, shared internally and externally, and synced.

See also

- *Set the OneDrive retention for deleted users:* <https://learn.microsoft.com/en-us/sharepoint/set-retention>
- *User information barriers with OneDrive:* <https://learn.microsoft.com/en-us/purview/information-barriers-onedrive>
- *Enable sensitivity labels for files in SharePoint and OneDrive:* <https://learn.microsoft.com/en-us/purview/sensitivity-labels-sharepoint-onedrive-files>
- *Learn about data loss prevention:* <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>
- *Audit log activities:* <https://learn.microsoft.com/en-us/purview/audit-log-activities>
- *Learn about retention for SharePoint and OneDrive:* <https://learn.microsoft.com/en-us/purview/retention-policies-sharepoint>

Providing individuals access to another user's OneDrive content

In many business scenarios, such as when an employee moves roles, is on extended leave, or departs the company, it may be necessary to grant someone access to another user's OneDrive for Business content. This is important for ensuring continuity, as it allows team members or managers to access, collaborate on, or transfer critical files that are essential for ongoing projects or organizational operations. While granting this access is vital for maintaining business continuity and preventing data loss, it's equally important to handle it with respect for the user's privacy and in compliance with organizational policies.

To responsibly manage access, consider first moving or copying necessary files to a SharePoint library or a team in Microsoft Teams, which provides a more collaborative and secure environment for shared documents. This approach not only ensures that files are accessible to the relevant team members but also mitigates the risk of accidental deletion or loss of important data associated with one individual. Keep in mind that simply sharing access to OneDrive doesn't prevent files from being deleted by those with access, so it's important to have a clear plan for managing and safeguarding the content.

Getting ready

To provide an individual access to another user's OneDrive content, you should be a Global Administrator or a User Administrator.

How to do it...

1. Access the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, select **Users | Active users**.
2. Locate and select the user whose OneDrive content you want to grant access to. If the user was already deleted, restore the user from **Users | Deleted users** first, then select them from **Users | Active users**.
3. Within the panel that appears for the user, select **OneDrive**, then **Create link to files**, as shown in *Figure 6.18*. This sets the admin as a site admin for the user's OneDrive.

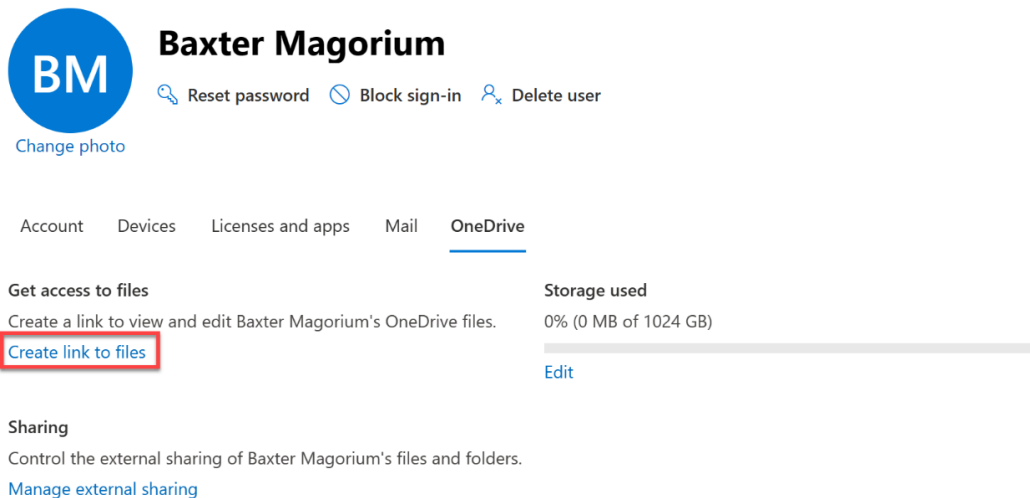


Figure 6.18 – Location of OneDrive create link to files option

4. In the same place where you selected **Create link to files**, the share link will appear for you, as the administrator, to use. Select the link.
5. From here, you can move, copy, or share individual (or multi-select) folders and files with whomever you wish as if they were your own files.

How it works...

When you provide an individual access to another user's OneDrive for Business content, the process begins by identifying the specific user whose files need to be accessed in the Microsoft 365 admin center. After selecting the user, the administrator goes to the OneDrive settings for that user to create a shareable link to the user's OneDrive files directly from the admin center. The administrator then has the ability to copy, move, or share the files as needed, essentially managing the files with the same level of access as the original user. This method ensures that important files are not lost and can be effectively transferred or overseen by someone else in the organization, all while maintaining strict adherence to security and privacy standards.

There's more...

Keep in mind that by default, when a user's account is deleted following their departure, their manager automatically receives a notification and is granted access for 30 days (unless the default retention period has been changed as described in the previous recipe, *Setting up compliance safeguards*). This automatic delegation is enabled by default to ensure continuity, but it can be manually disabled if it is not needed. Additionally, you can enhance this setup by assigning a secondary owner who will also have access to a deleted user's OneDrive in the event that a manager cannot be determined for the deleted user. Here's how to configure this automatic delegation for a secondary owner:

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at `https://admin.microsoft.com`. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **More features** from the left navigation menu, then open **User profiles**.
3. Select **Setup My Sites**.
4. Scroll to the **My Site Cleanup** section shown in *Figure 6.19*, ensure that **Enable access delegation** is checked, and enter a **Secondary Owner** who should be given access when a manager for the deleted user cannot be determined.

My Site Cleanup

When a user's profile has been deleted, that user's My Site will be flagged for deletion after thirty days. To prevent data loss, access to the former user's My Site can be granted to the user's manager or, in the absence of a manager, a secondary My Site owner. This gives the manager or the secondary owner an opportunity to retrieve content from the My Site before it is deleted. Select whether or not ownership of the Site should be transferred to a manager or secondary owner before the site is deleted.

Set a secondary owner to receive access in situations in which a user's manager cannot be determined.

☒ Enable access delegation

Secondary Owner:

Nathan Chamberlain



Figure 6.19 – My Site Cleanup settings

These steps will ensure that valuable information can be retrieved within the 30-day grace period or the custom retention period defined in the previous recipe. Even if a retention period of less than 93 days is set, a SharePoint admin can still restore a deleted OneDrive site within 93 days of the user's deletion by using PowerShell (`Restore-SPODeletedSite -Identity "<OneDrive URL>"`). After 93 days, the site is permanently deleted and cannot be recovered.

Also note that when you delete a user from the Microsoft 365 admin center, you're able to grant access to the user's entire OneDrive to anyone, not just a manager, by checking the **Give another user access to [User's] OneDrive files for 30 days after the user is deleted** box, as shown in *Figure 6.20*.

Delete Baxter Magorium

You can restore deleted users and their data, for up to 30 days after you delete them. Data on their connected devices will be removed, as well as the following:

Microsoft 365 E5 Developer (without Windows and Audio Conferencing) will be unassigned and available for other users

☐ Email aliases will be removed ⓘ
No email aliases

☐ Mailbox delegate permissions will be removed ⓘ
No mailbox delegate permissions

☒ Give another user access to Baxter Magorium's OneDrive files for 30 days after the user is deleted

MB

Megan Bowen

×

☐ Give another user access to Baxter Magorium's email ⓘ

Figure 6.20 – Option to share a user's entire OneDrive upon user deletion

See also

- *OneDrive retention and deletion*: <https://learn.microsoft.com/en-us/sharepoint/retention-and-deletion>

Setting the default share link type

Configuring the default share link type for OneDrive for Business and SharePoint is an important measure to prevent potential data loss or unauthorized access when sharing documents and files both inside and outside your organization. This setting aligns sharing practices with your organization's security policies by defaulting to a more secure link type. This helps ensure that even when users need to share files quickly, the default option is safer and less likely to expose sensitive information to unintended recipients.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at `https://admin.microsoft.com`. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Policies | Sharing** from the left navigation menu; then specify the default link type settings under **File and folder links**, as shown in *Figure 6.21*.

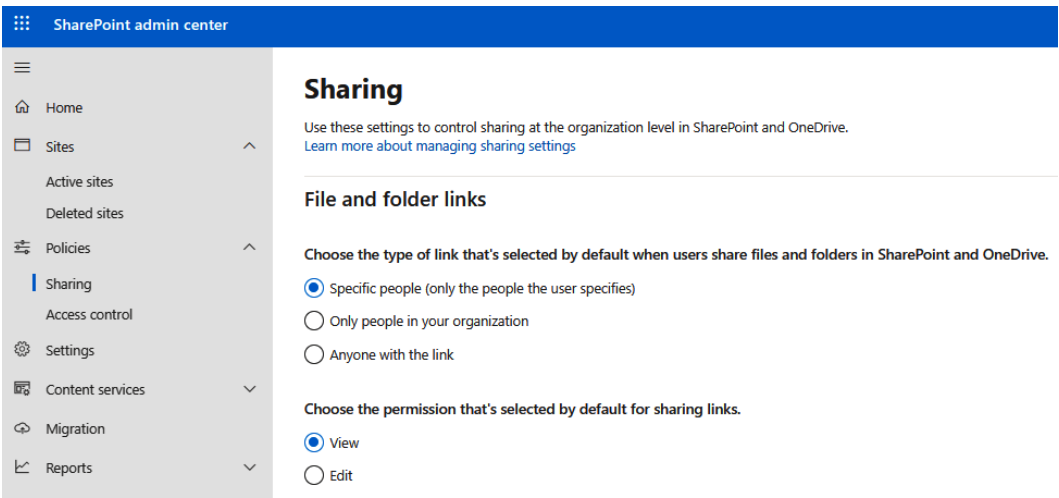


Figure 6.21 – Default share link type settings in the SharePoint admin center

These settings allow administrators to define the level of access for shared links—publicly accessible, restricted to organization members, or limited to designated individuals.

How it works...

Configuring the default share link type for OneDrive for Business helps organizations establish uniform sharing settings, ensuring consistency in how files are shared by default. It plays an important role in safeguarding sensitive data and preventing unauthorized information dissemination. By setting a restrictive default, the organization can reduce the risk of accidental data exposure while maintaining the ability to adapt the settings for specific needs when necessary.

There’s more...

Below the default link type and permission settings, you can specify additional settings, including the number of days after which an **Anyone** link will expire (if allowed and applicable), and which abilities **Anyone** links can provide such as view and edit/upload.

Individual sites can also have their own default share link setting, which may be helpful when a particular team shares in a specific manner (e.g., **Anyone with the link**) most often. To change one site’s default share link type, follow these steps:

1. Go to the SharePoint admin center, then select **Sites | Active sites** to find the team that should have a unique default share link type.
2. Select the team you wish to modify, then select **Settings | More sharing settings**, as shown in *Figure 6.22*.

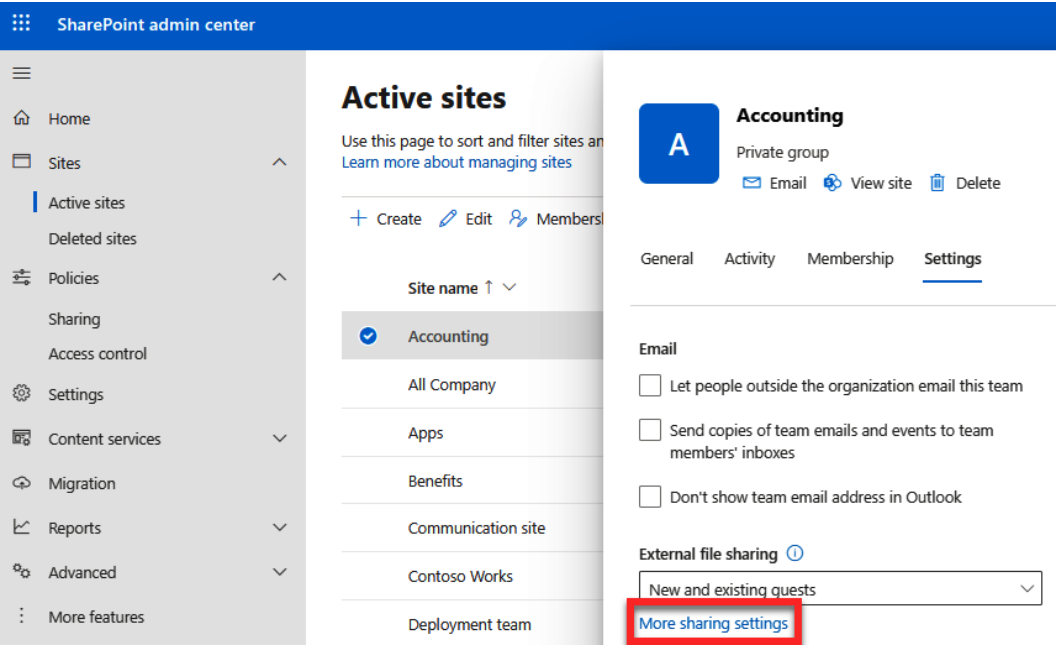


Figure 6.22 – More sharing settings for a specific site

3. Scroll down to the **Advanced settings for external sharing** section and uncheck **Same as organization-level setting** to specify something different for this site.

4. As shown in *Figure 6.23*, you can choose a new default share link type and permission for this site, then select **Save** when finished.

Sharing

Advanced settings for external sharing ▾

Default sharing link type

Choose the type of link that's selected by default when users share files and folders on this site. [Learn more about the default link types](#)

- ☒ Same as organization-level setting (Anyone with the link)
- ☐ People with existing access
- ☐ Specific people (only the people the user specifies)
- ☐ Only people in your organization
- ☒ Anyone with the link

Advanced settings for Anyone links ▾

Default link permission

- ☒ Same as organization-level setting (Edit)
- ☐ View
- ☒ Edit

Save [Reset to organization-level settings](#)

Figure 6.23 – Default share link settings for a specific site

Important note

If you've implemented sensitivity labels (covered more in *Chapter 13*), your sites' sensitivity labels will determine the sites' default sharing settings.

See also

- *Manage sharing settings for SharePoint and OneDrive in Microsoft 365*: <https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>

Adjusting all users' default storage allocation and retention periods

Adjusting the default storage allocation and retention periods for all users in OneDrive for Business is critical for managing your organization's data effectively. This helps to ensure that your organization's storage resources are optimized and that data retention complies with your internal policies and any relevant regulations.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Settings** and identify the **OneDrive** settings for **Retention** and **Storage limit**, as shown in *Figure 6.24*.

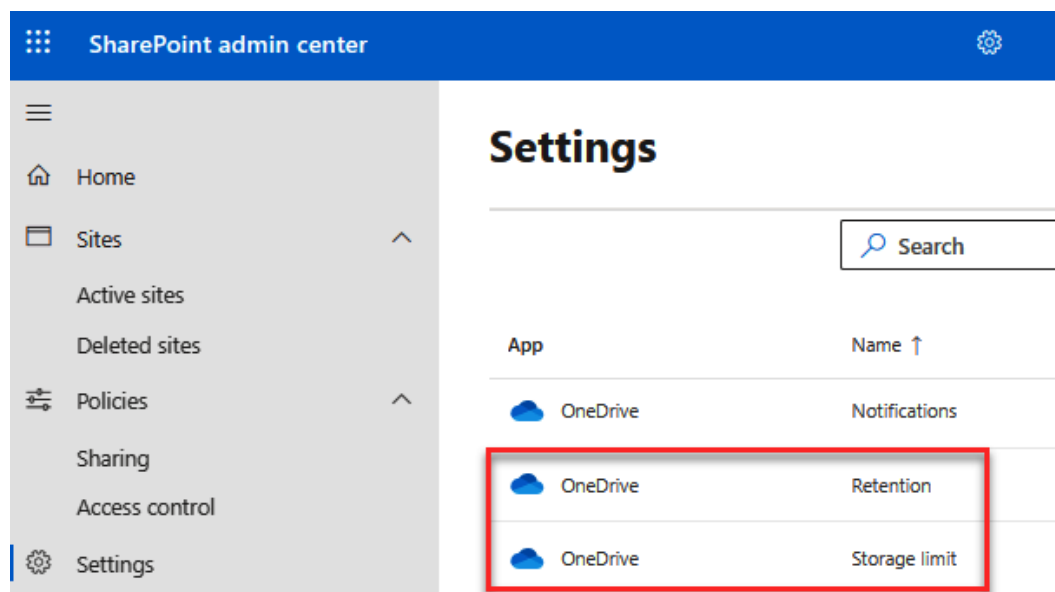


Figure 6.24 – Settings for OneDrive retention and storage

3. First, select **Retention**.

4. Enter the number of days you wish to retain a deleted user's OneDrive. The default is 30 days, but you can choose a number of days up to 10 years, as shown in *Figure 6.25*.

Retention

Specify the default retention period for a user's OneDrive when the user is deleted. Changing this setting also affects OneDrive accounts already within the retention period.

[Learn more about setting OneDrive retention](#)

Days to retain a deleted user's OneDrive
Enter a value from 30 through 3650 days.

Figure 6.25 – OneDrive retention settings

5. Select **Save**.
6. Now, select OneDrive's **Storage limit** setting.
7. In the **Default storage limit** box, input the desired default storage amount for each user in gigabytes. The system supports setting a default from 1 GB to a maximum of 5 TB, as shown in *Figure 6.26*.

Default storage limit

Set the OneDrive storage limit for all new and existing users who are assigned a qualifying license. If you've set specific storage limits for certain users, changing this setting won't affect their storage.

[Learn more about setting OneDrive storage limits](#)

Default storage limit
Enter a value of at least 1. For 1 TB of storage, enter 1024. If you have a subscription that provides more than 1 TB of storage, you can enter a value up to 5120 (5 TB).

Figure 6.26 – Default storage limit setting for OneDrive

How it works...

Adjusting default storage allocations and establishing retention policies for OneDrive for Business users are critical components of efficient data management within an organization. Administrators have the flexibility to set specific storage limits for users, which helps in effectively budgeting and allocating the organization's storage resources. This is particularly important not just for controlling costs but also for preventing data sprawl, whereby users might consume excessive storage if no limits are imposed.

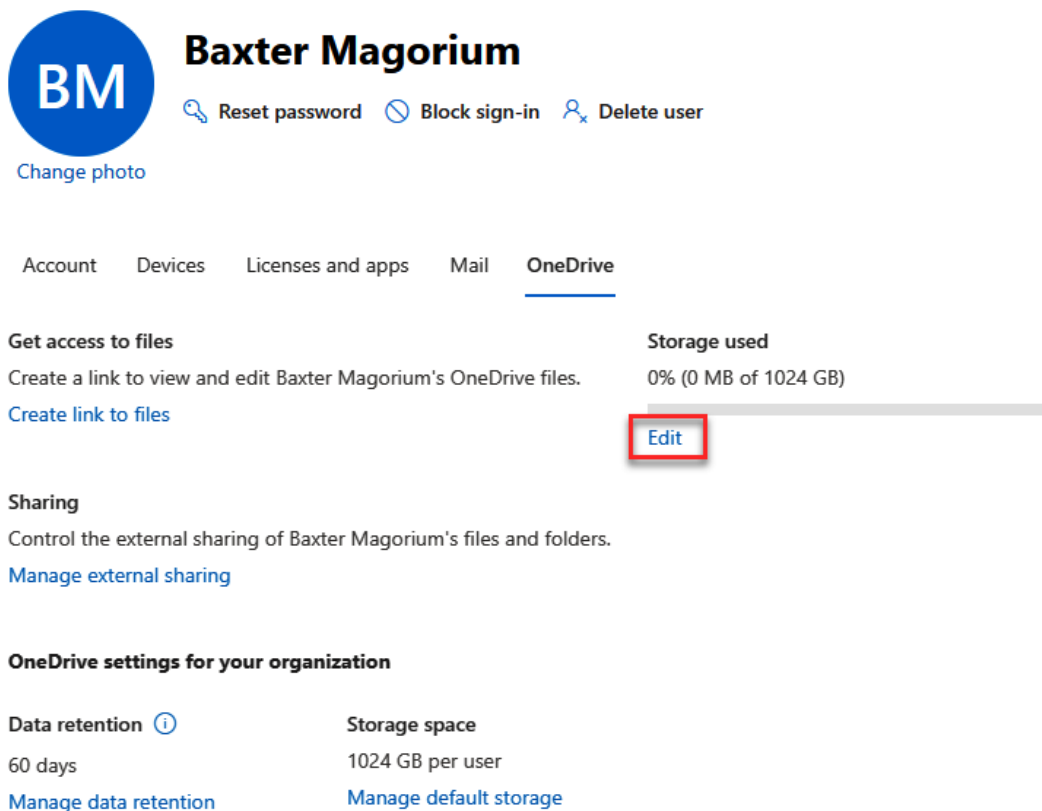
Furthermore, setting retention policies ensures that data is kept only as long as necessary, which supports compliance with legal and regulatory frameworks and maximizes storage efficiency. This practice is essential for managing the life cycle of data, reducing clutter, and improving the overall data retrieval and management processes. Such policies are especially useful in scenarios where access to information from deleted users' OneDrives needs to be extended beyond the typical retention period, which is often required for legal, audit, or business reasons.

There's more...

Beyond setting default storage settings for all users, administrators may need to adjust storage limits for individual users based on specific requirements or exceptions. This can be done directly through the Microsoft 365 admin center, allowing for granular control over each user's storage capacity in OneDrive for Business.

To change the storage settings for a specific user, follow these steps:

1. Navigate to the Microsoft 365 admin center at <https://admin.microsoft.com> as a Global or User Administrator.
2. Select **Active users** from the left navigation menu.
3. Find the user whose storage settings you need to modify by using the search function or browsing the user list and select their name to open a panel with their details.
4. Select **OneDrive** then select **Edit** under **Storage used**, as shown in *Figure 6.27*.



Baxter Magorium

[Reset password](#) [Block sign-in](#) [Delete user](#)

[Change photo](#)

Account Devices Licenses and apps Mail **OneDrive**

Get access to files
Create a link to view and edit Baxter Magorium's OneDrive files.
[Create link to files](#)

Storage used
0% (0 MB of 1024 GB)
[Edit](#)

Sharing
Control the external sharing of Baxter Magorium's files and folders.
[Manage external sharing](#)

OneDrive settings for your organization

Data retention ⓘ	Storage space
60 days	1024 GB per user
Manage data retention	Manage default storage

Figure 6.27 – Location of the individual storage limit for a user

- Here, you can set a specific storage limit for the user's OneDrive. Enter the desired amount of storage in gigabytes, then select **Save**.

This capability is particularly useful for accommodating users who may require more storage than the standard allocation due to their role or the nature of their work. It allows organizations to remain flexible and responsive to the varying data needs of their workforce.

See also

- Set the OneDrive retention for deleted users:* <https://learn.microsoft.com/en-us/sharepoint/set-retention>
- Set the default storage space for OneDrive users:* <https://learn.microsoft.com/en-us/sharepoint/set-default-storage-space>

Migrating data using the SPMT

Migrating data using the SPMT is a strategic process for organizations looking to move content from on-premises SharePoint 2010, 2013, or 2016 sites or file shares into Microsoft 365. This tool facilitates a secure and efficient transfer of data, ensuring that critical information is preserved and adapted to the cloud environment.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Download and install the SPMT from the official Microsoft site at <https://aka.ms/spmt-ga-page>.
2. Open the SPMT and sign in using your Global or SharePoint Administrator account.
3. Select the source data files or SharePoint content by selecting the corresponding option's **Add new migration** button, as shown in *Figure 6.28*. For this recipe, we'll choose the **Add new migration** button under **File share** to migrate a network location.

SharePoint Migration Tool

This tool helps you migrate your SharePoint and File share content to Microsoft 365.

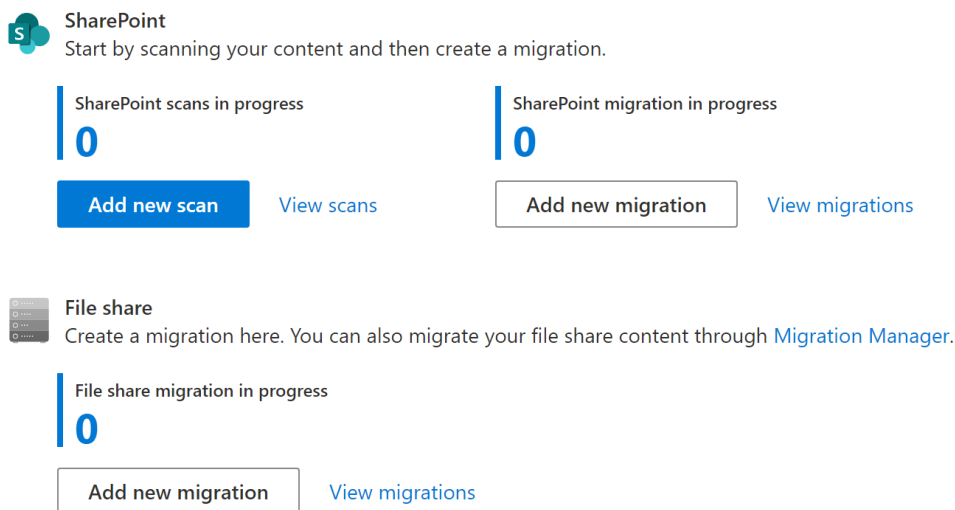


Figure 6.28 – SPMT start screen with options for SharePoint or file share migrations

4. Specify whether you're migrating a single source by selecting **Single file share source**, or whether you'll upload a JSON or CSV file with multiple locations to be migrated by selecting **Bulk migration using JSON or CSV file**. For this recipe, we'll choose **Single file share source**.
5. Specify the source and whether you want to migrate the folder and its contents, or just its contents, as shown in *Figure 6.29*.

Home > File share migrations > Add a new migration

Select a source

File share you want to migrate

C:\Temp

Choose folder

Options

- ☐ Migrate selected folder and folder contents
- ☒ Migrate only folder contents

Figure 6.29 – Source configuration in the SPMT

6. Select **Next**, then specify the destination: **Microsoft Teams**, **SharePoint**, or **OneDrive**. Since we're focused on OneDrive in this chapter, we'll choose **OneDrive**.
7. Enter the email address of the user to whose OneDrive you're migrating the specified content. Also, choose or create a folder in their OneDrive (**Documents**) to which the files should migrate, as shown in *Figure 6.30*.

Home > File share migrations > Add a new migration

Select a OneDrive destination

User email address or OneDrive URL

nate@chambernate.onmicrosoft.com

Location you want to migrate to

Documents

Documents

Apps

Attachments

Demo Finance Reports

Microsoft Teams Chat Files

Microsoft Teams Updates app Docu...

Power BI Reports

Create folder

Previous

Next

Back to list

Figure 6.30 – Destination specification screen of the SPMT




8. Select **Next**, then name the migration task. For example, you might name it Temp to ODFB Migration 10/09/2024 16:00.
9. Select **Next** to continue or choose **Add another migration**, as shown in *Figure 6.31*, to add additional migration tasks to execute.

Home > File share migrations > Add a new migration

Review migration

Name your migration

Temp to ODFB Migration 10/09/2024 16:00

Source	Destination	Migration type
✓  C:\Temp C:\Temp	 nate@chambernate.o... Documents/Migrated files	File share 

Next

Add another migration

Back to list

Figure 6.31 – The Review migration screen of the SPMT

10. Select **Next** when all desired tasks have been added to the **Review migration** screen.
11. Configure settings as desired (such as whether or not to preserve file share permissions) then select **Start** to run the tool and begin migrating data. You can monitor progress directly within the tool, as shown in *Figure 6.32*.

Home > File share migrations > View migration details

'Temp to ODFB Migration 10/09/2024...

[Migration details](#)

1%



|| ✕

0 min elapsed

Migrating C:\Temp to nate@chambernate.onmicrosoft.com

Checking environments

[View reports](#)

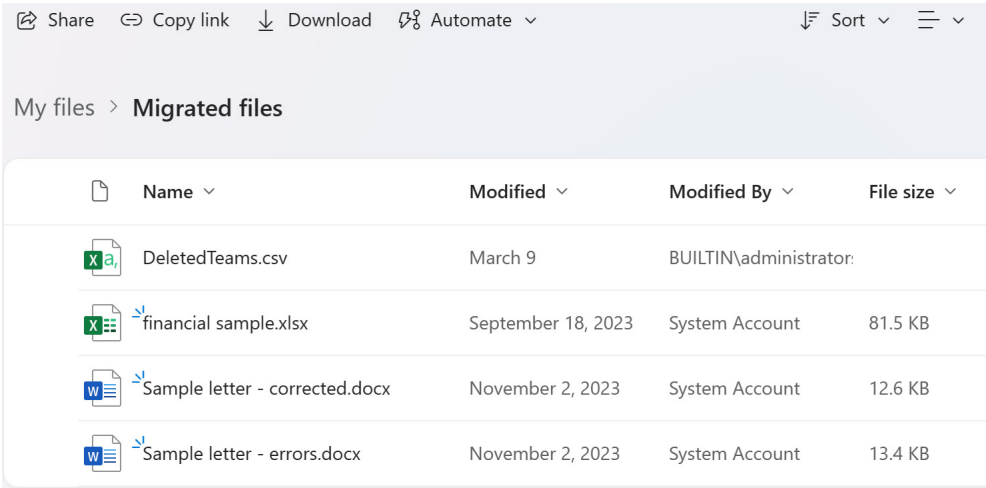
Figure 6.32 – Progress monitoring of migration in the SPMT

12. After migration, check the data integrity and permissions in the new environment to ensure that everything is functioning as expected.
13. Inform users about the new location of migrated data and provide any necessary training or resources to help them adapt.

How it works...

Using the SPMT for data migration involves transferring content from legacy systems or other digital storage solutions into Microsoft Teams, SharePoint, and OneDrive for Business. This tool simplifies the migration process, allowing organizations to streamline the movement of large volumes of data with minimal downtime. The migration not only facilitates better data management and collaboration within the new cloud environment but also supports the organization’s transition to more modern and efficient operational platforms. This tool is particularly valuable for ensuring that data integrity is maintained during the transition, providing a seamless migration experience.

Once the migration completes, files will appear in their new cloud home, as seen in *Figure 6.33*. You may also note that this is where the original **Modified** metadata is maintained.



The screenshot shows the OneDrive web interface for a user named 'My files'. The breadcrumb navigation shows 'My files > Migrated files'. The top navigation bar includes 'Share', 'Copy link', 'Download', 'Automate', 'Sort', and a menu icon. Below the navigation bar, there is a table of migrated files. The table has four columns: 'Name', 'Modified', 'Modified By', and 'File size'. The files listed are 'DeletedTeams.csv', 'financial sample.xlsx', 'Sample letter - corrected.docx', and 'Sample letter - errors.docx'. Each file has a blue arrow icon next to its name, indicating it was migrated. The 'Modified' column shows the original modification date, and the 'Modified By' column shows the original user.

Name	Modified	Modified By	File size
DeletedTeams.csv	March 9	BUILTIN\administrator	
financial sample.xlsx	September 18, 2023	System Account	81.5 KB
Sample letter - corrected.docx	November 2, 2023	System Account	12.6 KB
Sample letter - errors.docx	November 2, 2023	System Account	13.4 KB

Figure 6.33 – Migrated files in OneDrive for Business showing original Modified metadata

There’s more...

You can also sync a OneDrive and use File Explorer’s native cut/paste or copy/paste features or scripts to copy content from one synced location to another. OneDrive’s **Copy to** or **Move to** features in the OneDrive web user interface can also help move content across SharePoint sites and OneDrive.

If you use the SPMT, be sure to use the bulk migration option to save time instead of manually configuring each source and destination pairing.

Use insights from the migration process to refine future migrations. The SPMT provides various settings and options that can be tailored to improve efficiency and address specific needs.

Microsoft FastTrack and other professional services offer additional support and resources for complex migrations, which can be particularly useful for large-scale or specialized data transfers.

See also

- *Overview of the SharePoint Migration Tool (SPMT)*: <https://learn.microsoft.com/en-us/sharepointmigration/introducing-the-sharepoint-migration-tool>

Configuring Power Platform

Microsoft Power Platform is a transformative suite that combines several tools that enable businesses to create custom applications, automate workflows, analyze data through comprehensive dashboards and reports, and more. These tools are designed to work both individually and together, providing flexibility and power through integration.

In this chapter, our primary focus will be on effectively configuring and managing Power Platform services such as Power Apps, Power Automate, and Power BI. We will also explore shared resources such as Dataverse, environments, and on-premises data gateways. The aim is to enhance operational efficiency and ensure the security of business data across these platforms. By delving into these areas, we can optimize how these tools and services are utilized within your organization, ensuring they align with business needs and compliance requirements.

We will cover the following recipes in this chapter:

- Creating a new Power Platform environment
- Creating a Dataverse database
- Restricting certain connectors in Power Apps and Power Automate from accessing business data
- Using Analytics to explore usage, failures, and performance in Microsoft Power Platform
- Installing an on-premises data gateway
- Restricting users from installing on-premises data gateways
- Restricting Power BI's Publish to web (anonymous share) ability to specific security group members
- Auditing Power BI embed codes created by your organization
- Configuring a default logo, cover image, and theme for Power BI

Technical requirements

This chapter requires administrative access to Microsoft 365. Users assigned the Global Administrator role will have the capability to execute all tasks presented, and Power Platform Administrators will be able to execute most.

For your organization's users to utilize Power Platform applications, they may need licenses assigned depending on their specific app requirements. Power Platform licensing is complex, has multiple options such as pay-as-you-go or per-app, and evolves regularly. Check the latest licensing documentation at <https://learn.microsoft.com/en-us/power-platform/admin/pricing-billing-skus> for more information.

Creating a new Power Platform environment

Creating a new Power Platform environment is necessary when your organization needs a segregated space to manage and store its data, applications, and flows securely. This can be particularly useful when dealing with sensitive information that requires isolation from other projects or when a clear delineation of resources is required for organizational governance. Establishing separate environments, such as Development, Test, and Production, is a best practice even for low-code development in Power Platform. This setup helps maintain data integrity and security while facilitating effective collaboration within a controlled environment across different segments of the organization.

Getting ready

You must be a Global, Power Platform, or Dynamics 365 Administrator to follow the steps in this recipe.

Important note

Dynamics 365 and the Power Platform share a common infrastructure that includes the use of environments and Dataverse, enabling Dynamics 365 Administrators to also oversee several aspects of Power Platform environment creation and management. Since Dynamics 365 environments are integrated within the Microsoft Power Platform, they are governed through the same administrative center – the Power Platform admin center. This integrated setup allows Dynamics 365 Administrators to perform administrative duties not only specific to Dynamics 365 applications but also across the broader spectrum of Power Platform services, managing everything from environmental settings to data stored in Dataverse.

How to do it...

1. Sign in to the Power Platform admin center at <https://admin.powerplatform.microsoft.com>.
2. In the navigation pane, select **Environments**, then select **New**, as shown in *Figure 7.1*.

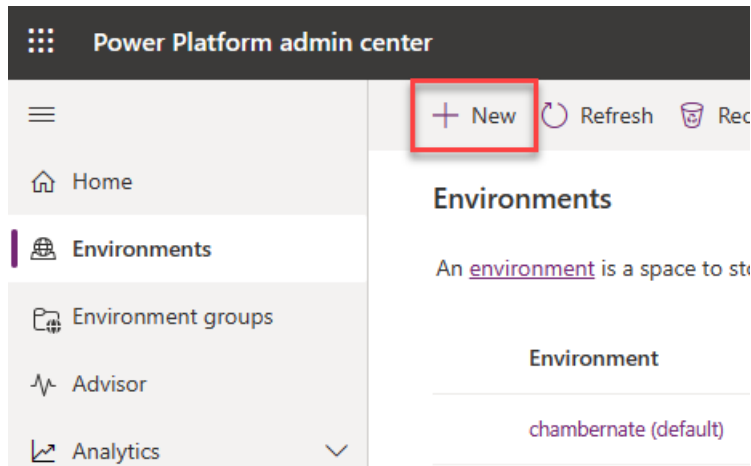


Figure 7.1 – Option to create a new environment in the Power Platform admin center

3. In the side panel that appears, provide the details for your environment, as shown in the example in *Figure 7.2*:
 - A. **Name:** Enter a name for your environment, such as Legal.
 - B. **Group:** If applicable, select an environment group to which this new environment belongs. Environment groups help organize multiple environments within a larger context, making it easier to manage and apply governance policies across similar environments.

Tip

By creating environment groups, organizations can streamline management, apply consistent security policies, and organize environments based on business units or project teams, enhancing overall governance and operational efficiency.

- C. **Region:** Select the geographic region where your environment will be hosted.
 - D. **Type:** Choose between **Production**, **Trial**, or **Sandbox**, depending on the purpose of the environment.
 - E. **Purpose:** Provide a description of the environment.

4. **Add a Dataverse data store:** Choose **Yes** to include a Dataverse database. Note that this option is only available if your subscription comes with Dataverse capacity.
- A. **Pay-as-you-go with Azure:** Choose **Yes** if you wish to link the environment to an Azure subscription for billing.

New environment ✕

i This operation is subject to [capacity constraints](#)

Name *

Group

No groups available ▼

Region *

United States - Default ▼

A local region can provide quicker data access

Type i *

Production ▼

Purpose

This is an example of a new environment created to segregate business apps and their data from non-legal apps. ▲
▼

Add a Dataverse data store? i

☒ Yes

Pay-as-you-go with Azure? i

☐ No

Next

Cancel

Figure 7.2 – New environment configuration panel

5. Select **Next**, then configure additional settings:
 - A. **Language:** Set the default language for the environment.
 - B. **Currency:** Select the base currency for financial transactions within the environment.
 - C. **Security group:** Assign a security group to restrict access to this environment or select **None** for all users to have access. Using security groups is essential for managing who has permission to access and manage resources within the environment. This step is crucial for maintaining a secure and well-governed environment.
 - D. **URL:** Specify a unique URL for the environment (optional).
 - E. **Enable Dynamics 365 apps:** Choose **Yes** if you wish to automatically deploy Dynamics 365 apps.
 - F. **Deploy sample apps and data:** Choose **Yes** for this to include sample apps and data for demonstration purposes.
6. Select **Save** to create the environment.

How it works...

When you create a new Power Platform environment, you are essentially setting up a dedicated space that segregates your organization's data, applications, chatbots, and workflows from others. This digital boundary ensures that sensitive information and critical operations can be managed and monitored independently from other projects or departments within the organization.

By establishing separate environments, such as Development, Test, and Production, you follow a basic development lifecycle that is critical for maintaining data integrity and security. In a typical development lifecycle, the following applies:

- **Development** environments are used for building and testing new applications or features
- **Test** environments allow for more rigorous testing, including user acceptance testing, without affecting live data
- **Production** environments are where finalized and approved applications are deployed for everyday use

Understanding and utilizing this lifecycle is important for ensuring that changes are thoroughly tested and approved before they reach end users. Solutions and apps can be moved between these environments to ensure a smooth transition from development to production.

The default environment is automatically created for each tenant and is often used for personal productivity. However, it is important to create separate environments for production and development purposes to maintain security and governance over business-critical data.

During the creation process, an environment is configured with specific settings such as region, type (production, trial, or sandbox), and whether to include a Dataverse database. You’ll learn more about Dataverse in the next recipe, *Creating a Dataverse database*. These choices dictate how the environment will function and what resources will be available. For instance, selecting a geographic region for the environment helps optimize the performance by reducing latency for users in that region. Adding a Dataverse database enables structured data storage and is essential for deploying certain types of applications that rely on complex data interactions.

Furthermore, specifying the environment type is critical as it influences the environment’s capabilities and limitations. Production environments are robust and suited for deploying business-critical applications, while sandbox environments are ideal for testing without affecting live data. Trial environments offer a temporary setup to explore features before full-scale implementation.

Once the environment is created, it appears on the **Environments** screen of the Power Platform admin center, as shown in *Figure 7.3*, where it can be managed and monitored.

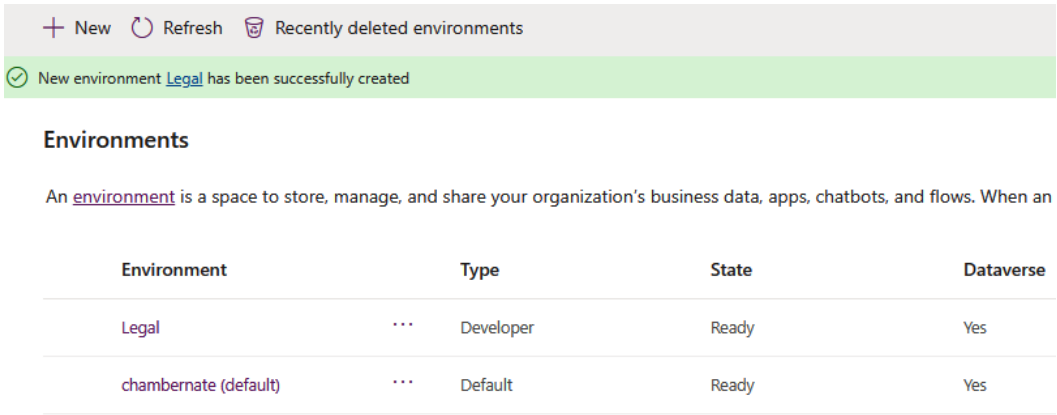


Figure 7.3 – Environments screen of the Power Platform admin center

There’s more...

When you select an existing environment from the **Environments** screen of the Power Platform admin center, you’ll be able to manage several settings and have access to features such as resetting or restoring the environment, as shown in *Figure 7.4*.

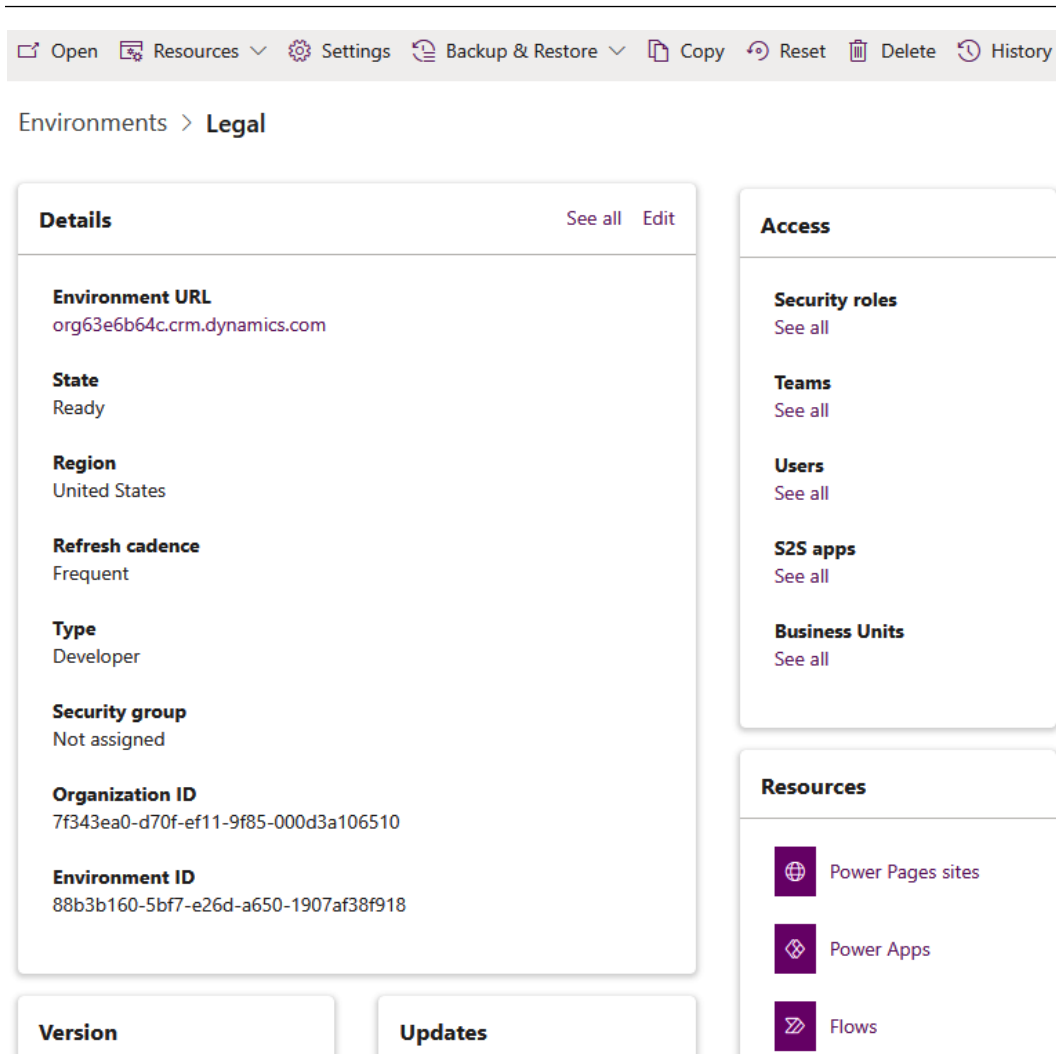


Figure 7.4 – Environment details

From this screen, it is easy to find all the associated resources (sites, apps, flows, etc.) within the environment, manage its users, and adjust its settings, such as enabling auditing of Dataverse data or allowing Teams integration.

See also

- *Create and manage environments in the Power Platform admin center:* <https://learn.microsoft.com/en-us/power-platform/admin/create-environment>

Creating a Dataverse database

Dataverse, which was previously known as **Common Data Service**, is a cloud-based platform that structures data into a usable format, supporting secure data storage and management for business applications developed on Microsoft Power Platform. Creating a Dataverse database facilitates centralized data management, allowing businesses to maintain information in a scalable and secure setting. While creating a database is optional during the initial environment setup, this recipe assumes no database was established initially.

For organizations with distinct business units or projects that necessitate separate governance, security, or compliance measures, setting up multiple Dataverse databases can be highly beneficial. However, each environment can only host one database. Therefore, if data segregation is required, it is advisable to first create a new environment following the procedure outlined in this chapter's *Creating a new Power Platform environment* recipe. After or while establishing this new environment, you can create a database within it. This strategy ensures configurations are tailored to meet specific data privacy standards and operational needs, supporting the unique requirements of different organizational segments. The steps to add a Dataverse database to an existing environment are detailed in this recipe.

Getting ready

You must be a Global or Power Platform Administrator, and an administrator of the environment to which you're adding a database, to follow the steps in this recipe.

How to do it...

1. Sign in to the Power Platform admin center at <https://admin.powerplatform.microsoft.com>.
2. Select **Environments** from the left navigation menu and choose the environment in which you want to create the database.
3. Select **Add database**.
4. Configure the database settings:
 - A. **Language**: Set the default language for the environment.
 - B. **Currency**: Select the base currency for reporting.
 - C. **Enable Dynamics 365 apps**: Choose **Yes** if you wish to automatically deploy Dynamics 365 apps.
 - D. **Deploy sample apps and data**: Choose **Yes** for this to include sample apps and data for demonstration purposes.
 - E. **Security group**: Assign a security group to restrict access to this environment or select **None** for all users to have access.

5. Confirm the settings and select **Add** to complete the database setup.

How it works...

In this recipe, you added a database to an existing environment. This enables your environment to host data supporting the apps within the environment such as Power BI reports, apps built in Power Apps, and flows built in Power Automate.

There's more...

When configuring a new database for an existing environment, you can add a security group for the database specifically. The existing roles assigned to its parent environment remain unchanged, however. Specifically, users holding the Environment Admin role automatically receive the System Administrator privileges in the new database. Similarly, those designated as Environment Makers retain their roles, ensuring continuity in their ability to create and manage resources within the environment. This structure helps maintain a consistent level of access and control as new databases are integrated into the environment.

See also

- *Add a Microsoft Dataverse database:* <https://learn.microsoft.com/en-us/power-platform/admin/create-database>

Restricting certain connectors in Power Apps and Power Automate from accessing business data

Connectors in Power Apps and Power Automate provide essential links to data sources and services, enabling automation and data interaction within your applications. However, not all connectors should have access to all types of business data due to security or compliance reasons. This recipe guides you through setting up restrictions on specific connectors to prevent unauthorized access to sensitive data, thus enhancing the security posture of your business solutions.

Getting ready

You must be a Global or Power Platform Administrator to follow the steps in this recipe. It's important to ensure that users involved in this process have the correct security roles:

- **Solution Users:** Should have appropriate access to the connectors they need
- **Makers:** Typically need permissions to create and manage apps and flows within environments
- **Admins:** Require the necessary roles to manage and enforce **Data Loss Prevention (DLP)** policies.

How to do it...

1. Sign in to the Power Platform admin center at <https://admin.powerplatform.microsoft.com>.
2. From the left navigation menu, select **Policies | Data Policies**.
3. Select **New Policy** to start creating a new data policy.
4. Enter a name for your policy and then select **Next**.
5. Select the connectors that should be restricted. You can choose connectors and classify them as either **Business** or **Non-business** based on the data they can access or block them if they shouldn't be used at all. For this recipe, we'll select **SharePoint** and **OneDrive for Business** and move them to **Business** as shown in *Figure 7.5*.

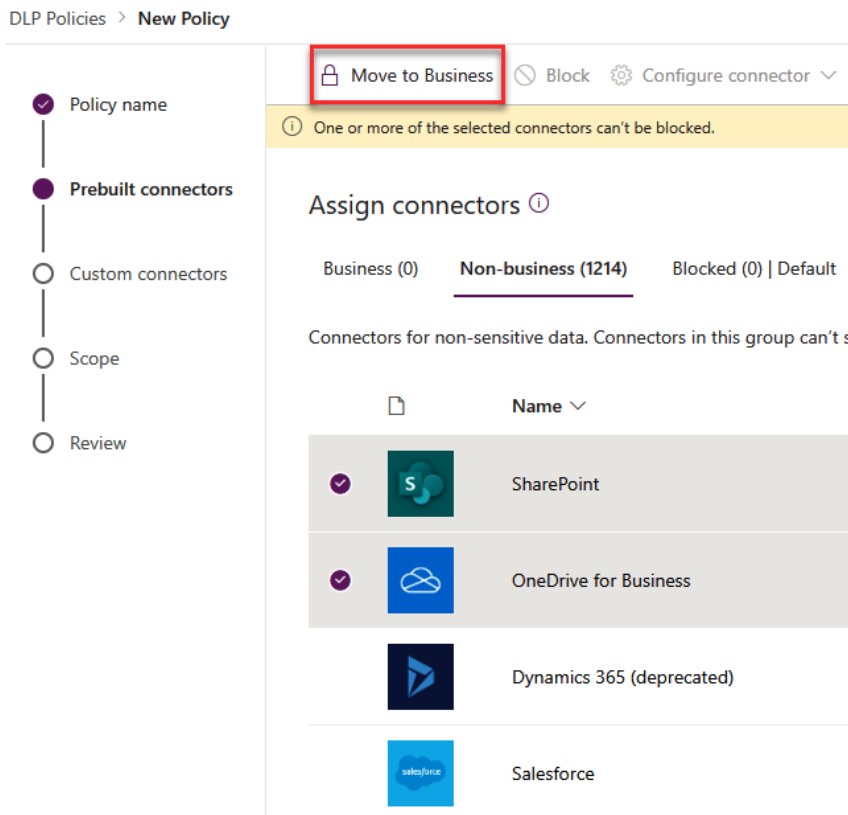


Figure 7.5 – Connectors being moved to Business

6. Select **Next** to skip custom connector patterns, then define the scope for this policy by selecting the environments to which the policy applies.

Tip

Custom connector patterns are used to specify URL patterns that should be allowed, blocked, or ignored. For instance, in a financial institution, a custom connector might be created to integrate its internal financial system with the Power Platform. The custom connector pattern defines the rules for how this connector can communicate with various endpoints. Learn more about this at <https://learn.microsoft.com/en-us/power-platform/admin/dlp-custom-connector-parity>.

7. Select **Next** to review your settings, as shown in *Figure 7.6*, and, if everything is correct, select **Create policy** to enforce the restrictions.

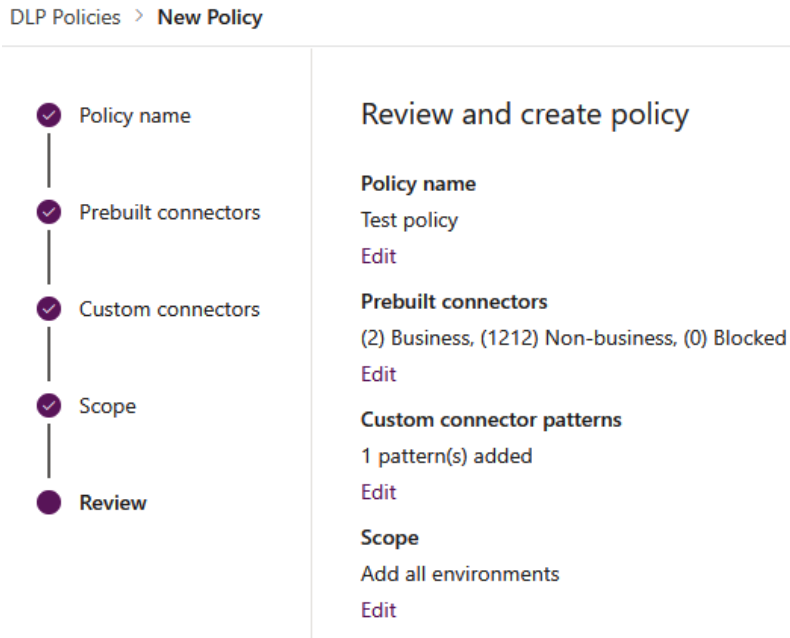


Figure 7.6 – Data Loss Prevention policy review screen

How it works...

When you restrict certain connectors in Power Apps and Power Automate from accessing business data, you are implementing what are known as **Data Loss Prevention (DLP)** policies. These policies play a fundamental role in safeguarding sensitive information and ensuring that data flows within your organization comply with internal and external regulatory requirements.

Additionally, using **Service Principals (S2S)** in environments can further enhance security by allowing apps and flows to connect securely to other services without relying on user credentials. This setup is particularly useful in scenarios where automation needs to be consistent and unaffected by changes in user roles or access rights.

The process of restricting connectors involves classifying them into different groups based on their trust level or the sensitivity of the data they handle. For instance, connectors such as **SharePoint** and **OneDrive for Business** might be categorized under **Business** because they are used for internal operations and handle sensitive corporate data. On the other hand, connectors that are less secure or that typically interact with external data, such as social media platforms, might be classified as **Non-business**.

Once these classifications are in place, the DLP policies enforce rules that prevent data exchange between the groups. This means that if a connector is classified as **Business**, it cannot interact with connectors classified as **Non-business**. This segregation helps prevent potential data breaches and leaks by controlling which data can be accessed and shared through apps and workflows.

In practice, this setup not only enhances security but also aids in compliance with data governance policies. By monitoring and controlling how data is accessed and shared across different connectors, organizations can mitigate risks associated with data handling and ensure compliance with legal and regulatory standards.

There’s more...

Once your policy is created, it will appear on the **Policies | Data policies** screen of the Power Platform admin center, as shown in *Figure 7.7*.

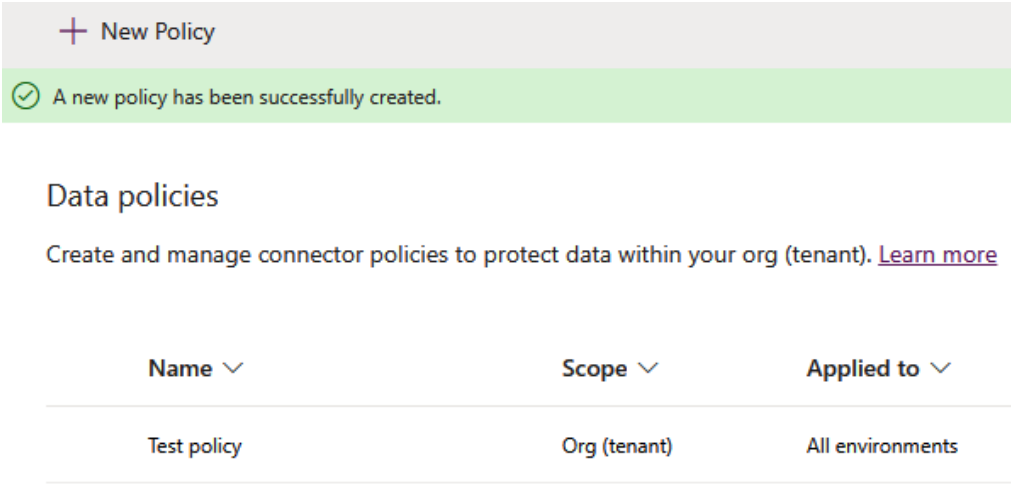


Figure 7.7 – Data policies screen of the Power Platform admin center

From here, you can select a policy to edit or delete at any time.

By establishing separate DLP policies for each environment, rather than creating one policy for all environments, you can effectively manage and control data flows specific to different groups or applications within the organization. For example, you might configure the DLP settings to restrict the Legal department from using apps and flows that transmit data to third-party applications. Conversely, the Marketing or Public Relations departments could be permitted to integrate business connectors such as SharePoint with third-party non-business connectors. This flexibility allows for tailored data governance strategies that align with the specific needs and security requirements of each department.

See also

- *Data policies*: <https://learn.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention>

Using Analytics to explore usage, failures, and performance in Microsoft Power Platform

Understanding the usage, failures, and performance of applications within the Power Platform, including Microsoft Dataverse, Power Apps, and Power Automate, is helpful for maintaining efficient operations. This recipe will guide you through discovering the analytics available in the Power Platform admin center, helping you leverage data to monitor system health and optimize processes.

Getting ready

You must be a Global or Power Platform Administrator to follow the steps in this recipe.

How to do it...

1. Sign in to the Power Platform admin center at <https://admin.powerplatform.microsoft.com>.
2. From the left navigation menu, select **Analytics | Dataverse**, as shown in *Figure 7.8*.

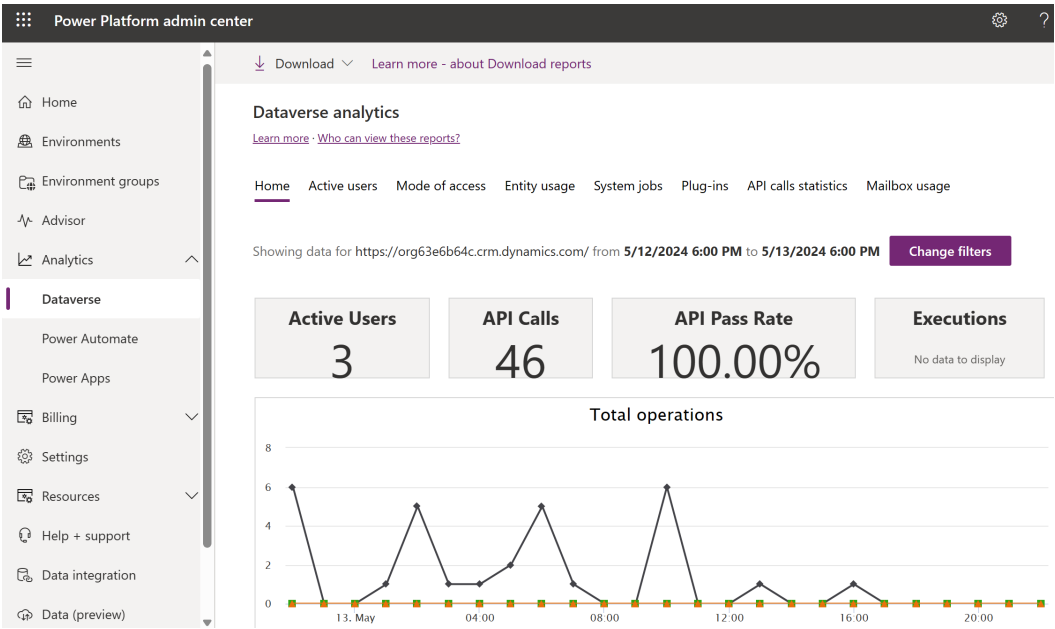


Figure 7.8 – Datarverse analytics

- Here, you can view various reports, such as active users and operations performed, which show user engagement and operational metrics across your Datarverse environment.
- Next, from the left navigation menu, select **Analytics | Power Automate**, as shown in *Figure 7.9*.

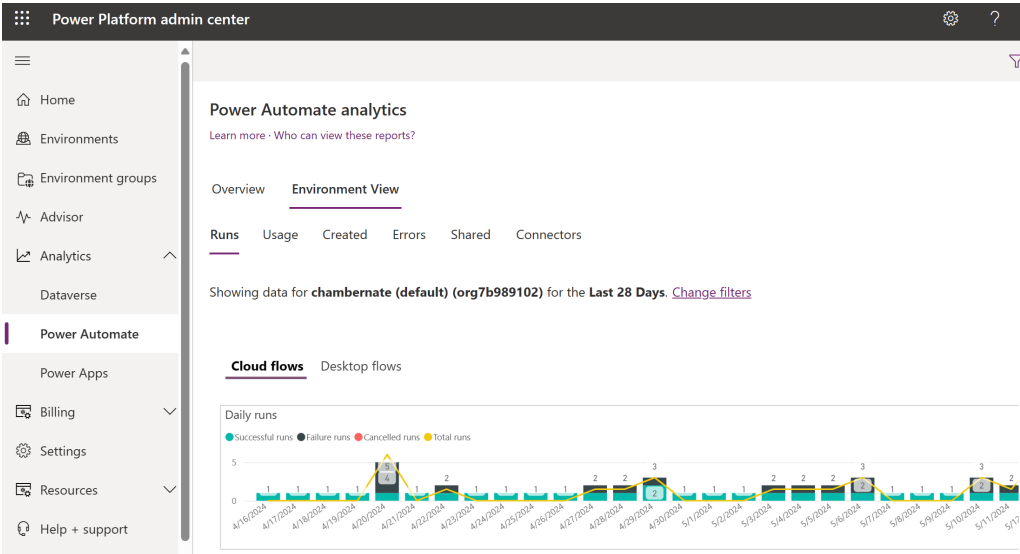


Figure 7.9 – Power Automate analytics

5. Examine detailed reports on your cloud flows, including usage, connector utilization, successful runs, failures, and performance issues. This helps in identifying trends and potential bottlenecks in your automated workflows.
6. Lastly, from the left navigation menu, select **Analytics | Power Apps**. This section provides insights into app usage patterns such as the number of active users, and session details such as where users access your apps geographically, helping you understand how frequently and effectively your applications are being used. You'll also find performance metrics and toast errors.

How it works...

Using these analytics, administrators can gain a comprehensive view of the system's performance and user interaction across the Power Platform. Each analytics section provides specific metrics related to the components of the platform:

- Dataverse analytics offers a deep dive into database operations and user activity
- Power Automate analytics focuses on the efficiency and reliability of automated workflows
- Power Apps analytics reveals the engagement levels and usage statistics of your apps

Analytics are not just about monitoring; they provide critical insights that drive business decisions. By analyzing usage patterns and identifying failures or performance bottlenecks, organizations can optimize resources, improve operational efficiency, and ensure that their applications are meeting user needs. This data-driven approach helps businesses to allocate resources effectively, plan for future growth, and maintain a high level of service availability and performance, which is crucial for business success.

There's more...

Beyond monitoring, these analytics tools allow for proactive management of your Power Platform environments. By understanding usage patterns and operational performance, you can make informed decisions about resource allocation, potential upgrades, and workflow optimizations. Furthermore, the analytics dashboards are updated constantly, ensuring you have access to the latest data for making timely adjustments.

See also

- *Microsoft Dataverse Analytics*: <https://learn.microsoft.com/en-us/power-platform/admin/analytics-common-data-service>
- *Admin Analytics for Power Apps*: <https://learn.microsoft.com/en-us/power-platform/admin/analytics-powerapps>
- *View analytics for cloud flows*: <https://learn.microsoft.com/en-us/power-platform/admin/analytics-flow>

Installing an on-premises data gateway

For organizations that use both on-premises and cloud services, installing an on-premises data gateway facilitates secure data integration across environments. This recipe is relevant when you need to ensure that cloud-based apps in Power Apps, Power Automate, and Power BI can access and interact with data stored on local servers. The gateway acts as a bridge, providing a continuous flow of data while maintaining the necessary security controls.

Getting ready

For this recipe, you only need administrative rights to a machine (virtual or physical) to install software.

How to do it...

1. Navigate to the Power BI service at <https://app.powerbi.com>.
2. Download the gateway installer by selecting the download icon, then **Data Gateway**, as shown in *Figure 7.10*.

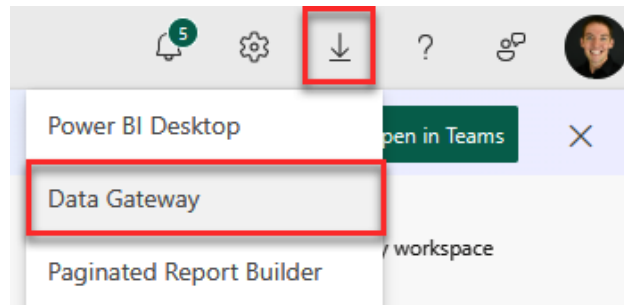


Figure 7.10 – Location of gateway installer in the Power BI service

3. Select **Download standard mode**, then run the downloaded installer on a server that meets the recommended configuration (see <https://learn.microsoft.com/en-us/data-integration/gateway/service-gateway-install>) and is always on.

Important note

You can install gateways on individual/personal laptops using personal mode, but if the machine is not powered on, any flow depending on the gateway will fail. Personal mode also only supports one user, whereas standard supports multiple. This is why this recipe recommends installation on an always-on machine.

4. Follow the installation prompts, accepting the default settings unless specific changes are required for your environment.
5. Sign in with your work or school account when prompted, as shown in *Figure 7.11*.

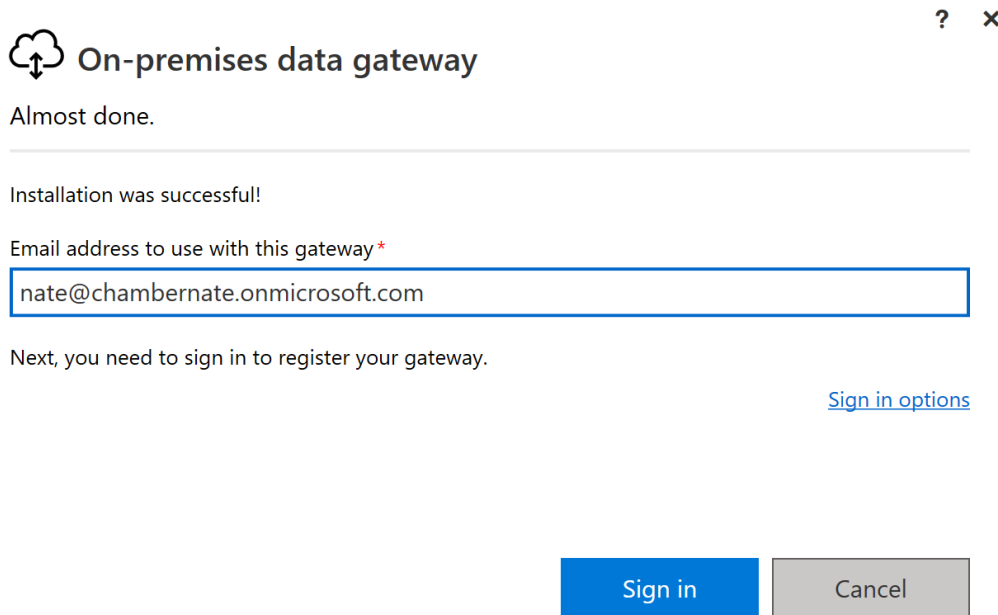


Figure 7.11 – On-premises data gateway installer

6. Select **Sign in**, then choose **Register a new gateway on this computer**, as shown in *Figure 7.12*.

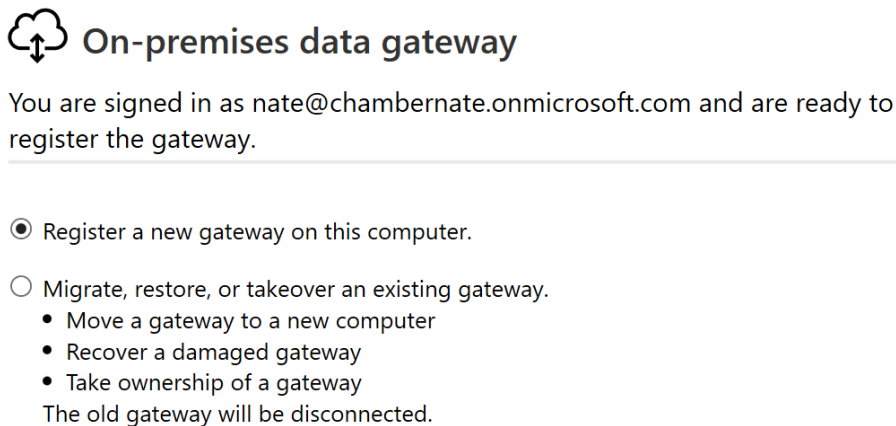



Figure 7.12 – Register or change gateway option

7. Name the gateway and create a recovery key, as shown in *Figure 7.13*. You can also change the data gateway's region if you wish.


 **On-premises data gateway** ? ×

You are signed in as nate@chambernate.onmicrosoft.com and are ready to register the gateway.

New on-premises data gateway name *

☐ Add to an existing gateway cluster [Learn more](#)

Recovery key (8 character minimum) *

 This key is needed to restore the gateway and can't be changed. Record it in a safe place.

Confirm recovery key *

We'll use this region to connect the gateway to cloud services: East US [Change Region](#)
[Provide relay details \(optional\)](#) By default, Azure Relays are automatically provisioned

Figure 7.13 – Gateway name and recovery key entry

8. Select **Configure** to complete the process.

How it works...

Installing a gateway on a machine allows you to connect to data on that machine for use in cloud apps and flows. After you've installed and configured the gateway, it'll be ready for use, as shown in *Figure 7.14*.

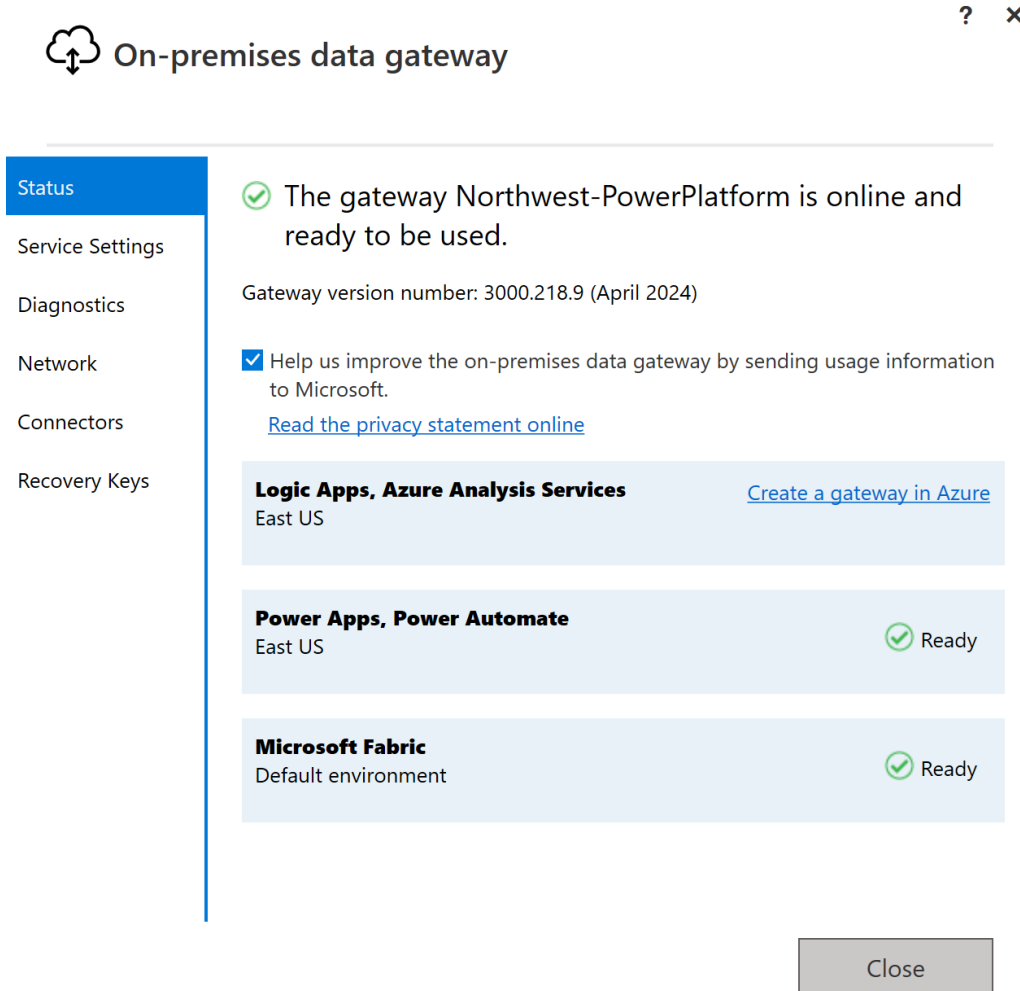


Figure 7.14 – Status screen of an on-premises data gateway

Now, when you create apps or flows that need to connect to on-premises data, you'll be able to select this gateway in your actions, as shown in *Figure 7.15*.

Create Connection



List files in folder

Create a new connection

Connection Name *	<input type="text" value="Network Drive H"/>
Root Folder *	<input type="text" value="H:\"/>
Authentication Type	<input type="text" value="Windows"/> ▾
Username *	<input type="text" value="CHAMBERNATE\nate"/>
Password *	<input type="password" value="....."/>
Gateway	
	<input type="text" value="Northwest-PowerPlatform"/> ▾

Create New

Figure 7.15 – Gateway connection dialog for a “List files in folder” action in Power Automate

There’s more...

Manage gateway user access and permissions through the admin portal (<https://admin.powerplatform.microsoft.com>), ensuring only authorized users can access or configure the gateway.

To find your gateways in the admin portal and adjust their settings or permissions, navigate to **Data** on the left navigation menu, then find your gateways under **On-premises data gateways**, as shown in *Figure 7.16*.

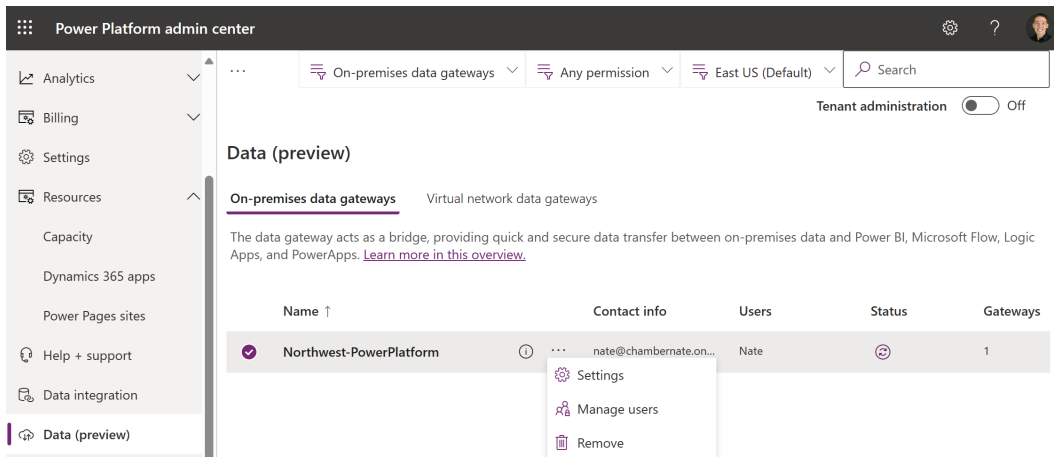


Figure 7.16 – On-premises data gateways shown in the admin center

When considering your management strategy for gateways, apps, and flows, it's important to have a process in place for transferring ownership of these resources when team members change roles or leave the organization. Transferring ownership ensures that critical workflows and applications continue to function without disruption and remain under the control of authorized personnel. This process is essential for maintaining business continuity and should be part of your organization's governance strategy.

See also

- *What is an on-premises data gateway?:* <https://learn.microsoft.com/en-us/power-bi/connect-data/service-gateway-onprem>
- *Install an on-premises data gateway:* <https://learn.microsoft.com/en-us/data-integration/gateway/service-gateway-install>

Restricting users from installing on-premises data gateways

Restricting the installation of on-premises data gateways helps maintain control over how data is accessed and shared within the organization. This recipe is important for enforcing governance and compliance policies by limiting who can set up new gateways, thereby ensuring that only authorized gateways are used for data access and transfer. It helps prevent data leaks and ensures that all data flows are monitored and secure.

Getting ready

You must be a Global or Power BI Administrator to follow the steps in this recipe.

How to do it...

1. Sign in to the Power Platform admin center at `https://admin.powerplatform.microsoft.com`.
2. Navigate to **Data (preview)** in the left navigation menu.
3. Toggle **Tenant administration** to the **On** position.
4. Select the ellipsis (...) that appears in the upper-left corner, then choose **Manage gateway installers**, as shown in *Figure 7.17*, to access the configuration options for gateway installations.

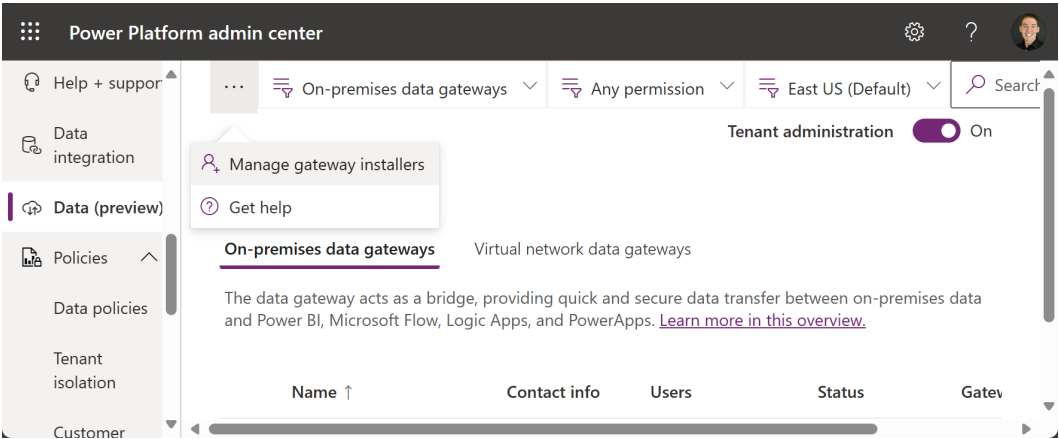


Figure 7.17 – Option to manage gateway installers

5. Enable the **Restrict users in your organization from installing gateways** option by toggling it to the **On** position.
6. Specify which users are authorized to install gateways by adding them as shown in *Figure 7.18*. Select **Add** when you’ve finished entering users.

Manage gateway installers



Manage who can install gateway in your organization. This does not impact gateway administration capabilities. [Learn more.](#)

Restrict users in your organization from installing gateways



On

Users who can install gateways

BM

Baxter Magorium

×

Search by name or email

Add

Current gateway installers



Figure 7.18 – Panel for managing gateway installers

How it works...

By restricting the installation of on-premises data gateways to specific individuals, you ensure that only authorized personnel can set up and configure these critical data access points. This prevents unauthorized users from installing a gateway, which could otherwise allow them to access sensitive organizational data through their personal setups. Typically, it is advisable to centralize the installation and management of these gateways, allowing only designated administrators to handle their configuration. This strategy not only secures data access points but also standardizes data management practices across the organization, ensuring that all data transfers through these gateways are monitored and regulated under strict administrative oversight.

There's more...

To remove an individual's permission to install on-premises data gateways, repeat *Steps 1–4* in this recipe then, under **Current gateway installers**, select the **X** next to the installer's name, as shown in *Figure 7.19*.

Current gateway installers

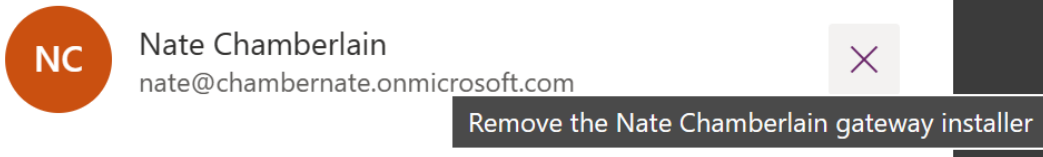


Figure 7.19 – Option to remove a current gateway installer

See also

- *On-premises data gateway management (preview)*: <https://learn.microsoft.com/en-us/power-platform/admin/onpremises-data-gateway-management>

Restricting Power BI's Publish to web (anonymous share) ability to specific security group members

The ability to publish Power BI reports to the web can lead to wide-reaching data exposure if not properly controlled. This recipe helps tighten security by limiting this capability to designated security group members who understand the implications of sharing data publicly. It's a vital step for organizations that require strict control over how their data is distributed and consumed publicly.

Getting ready

You must be a Global or Power BI Administrator to follow the steps in this recipe.

How to do it...

1. Navigate to the Power BI admin portal at <https://app.powerbi.com/admin-portal> or by selecting the settings wheel from Power BI (<https://app.powerbi.com>), then selecting **Admin portal**.
2. In **Tenant settings** (the default tab), scroll to the **Export and sharing settings** section and expand **Publish to web**.

3. Under **Apply to**, select **Specific security groups** to restrict anonymous sharing to specified user groups. Enter the names of the security groups that should have this permission, as shown in *Figure 7.20*.

Admin portal

Tenant settings **New**

Usage metrics

Users

Premium Per User

Audit logs

Domains **New**

Capacity settings

Refresh summary

Embed Codes

Organizational visuals

Azure connections

Workspaces

Custom branding

Protection metrics

Featured content

Help + support

Publish to web

Unapplied changes

People in your org can publish public reports on the web. Publicly published reports don't require authentication to view them.

Go to [Embed Codes](#) in the admin portal to review and manage public embed codes. If any of the codes contain private or confidential content remove them.

Review embed codes regularly to make sure no confidential information is live on the web. [Learn more about Publish to web](#)

☒ Enabled

When publish to web is enabled, existing embed codes work. Choose if users can create new codes

☒ Allow users to create new embed codes

⚠ To enable Publish to Web, you need to disable Block Public Internet Access first.

Apply to:

☐ The entire organization

☒ Specific security groups

MG M365 Group Creators

☐ Except specific security groups

Apply Cancel

Figure 7.20 – Publish to web settings

4. Select **Apply** to enforce this new setting.

How it works...

By specifying security groups in the **Publish to web** settings, you're creating a controlled environment where only designated individuals or groups can share reports publicly. This functionality is important for managing how data is disseminated beyond the organization, ensuring that only those with the correct training and authorization can distribute sensitive or critical business information. This strategic restriction acts as a safeguard against data leaks, as it minimizes the risk of exposing proprietary or confidential data to unauthorized external parties.

For example, it might be suitable for senior analysts or specific departments such as Market Research to share insights publicly, while restricting this ability for others who may not be aware of the broader implications of public data sharing.

Effectively, this setup not only protects sensitive data but also supports compliance with data governance policies and regulatory requirements, which might dictate stringent controls over who can disseminate data and how. It's an essential feature for organizations that operate under strict privacy laws or where data security is paramount.

There's more...

In addition to restricting the **Publish to web** option in Power BI, you can further refine the settings to maintain existing public accessibility while halting the creation of new embed codes. By leaving the main toggle for **Publish to web** enabled but disabling the toggle next to **Allow users to create new embed codes**, you ensure that any previously generated embed codes remain active, allowing continued access to the shared reports. However, this setting prevents the creation of new embed codes, effectively stopping the dissemination of new public links and enhancing control over how data is shared externally.

This approach is particularly useful in scenarios where you need to phase out the sharing of new data publicly while maintaining access to existing published content for continuity or compliance reasons. It allows for a more gradual transition in data sharing policies and can help mitigate potential disruptions in external communications or reporting that rely on already published Power BI reports.

See also

- *Publish to web from Power BI:* <https://learn.microsoft.com/en-us/power-bi/collaborate-share/service-publish-to-web>

Auditing Power BI embed codes created by your organization

Auditing Power BI embed codes is an essential practice for overseeing how reports and dashboards are shared externally. This recipe is important for organizations that need to control and review external access to their data visualizations, ensuring that sensitive information is not inadvertently exposed outside the organization. By auditing these codes, you can manage and revoke access when necessary, maintaining control over your data dissemination.

Getting ready

You must be a Global or Power BI Administrator to follow the steps in this recipe.

How to do it...

1. Navigate to the Power BI admin portal at `https://app.powerbi.com/admin-portal` or by selecting the settings wheel from Power BI (`https://app.powerbi.com`), then selecting **Admin portal**.
2. Navigate to the **Embed Codes** screen, as shown in *Figure 7.21*.

Admin portal

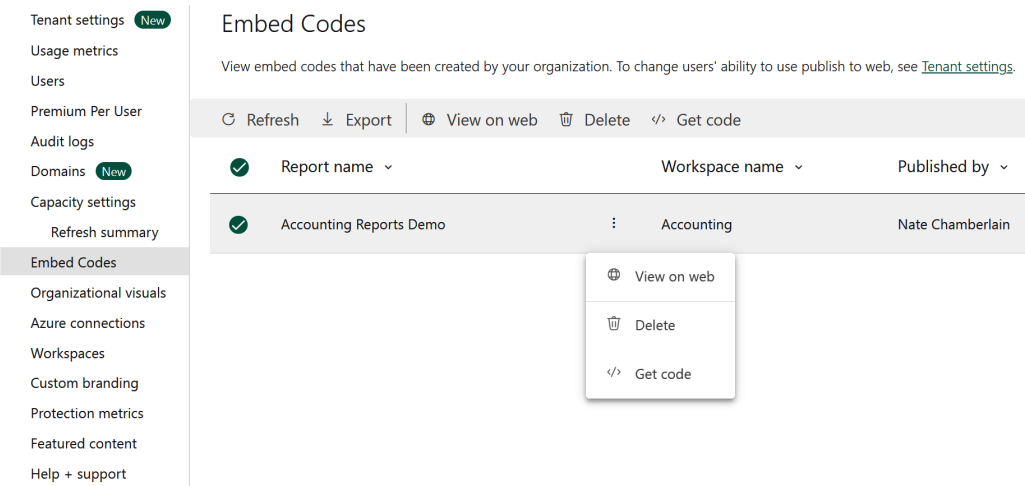


Figure 7.21 – Embed Codes screen of the Power BI admin portal

3. Select the ellipsis (...) next to a specific embed code to do the following:
 - A. **View on web:** View the content of the published report
 - B. **Delete:** Permanently delete the code, effectively stopping its use globally
 - C. **Get code:** Get the embed code for use in communications or to embed on a page yourself
4. Choose the **Export** option in the ribbon menu of **Embed Codes** to export a CSV list of all embed codes, as well as the specific reports and workspaces involved.

How it works...

In this recipe, you learned about the process of managing embed codes within your organization using the Power BI admin portal. As an administrator, you have the capability to oversee all embed codes that have been generated. This oversight includes the ability to view all active embed codes, examine the content they link to, and ensure compliance with organizational best practices and policies. If, during your review, you discover any embed codes that expose private or confidential information, you have the authority to delete these codes immediately, thus terminating any unauthorized sharing or publishing of sensitive data.

There’s more...

Individual users can find embed codes they’ve generated by visiting the workspace in which the published report lives, selecting the settings wheel, and then selecting **Manage embed codes**, as shown in *Figure 7.22*.

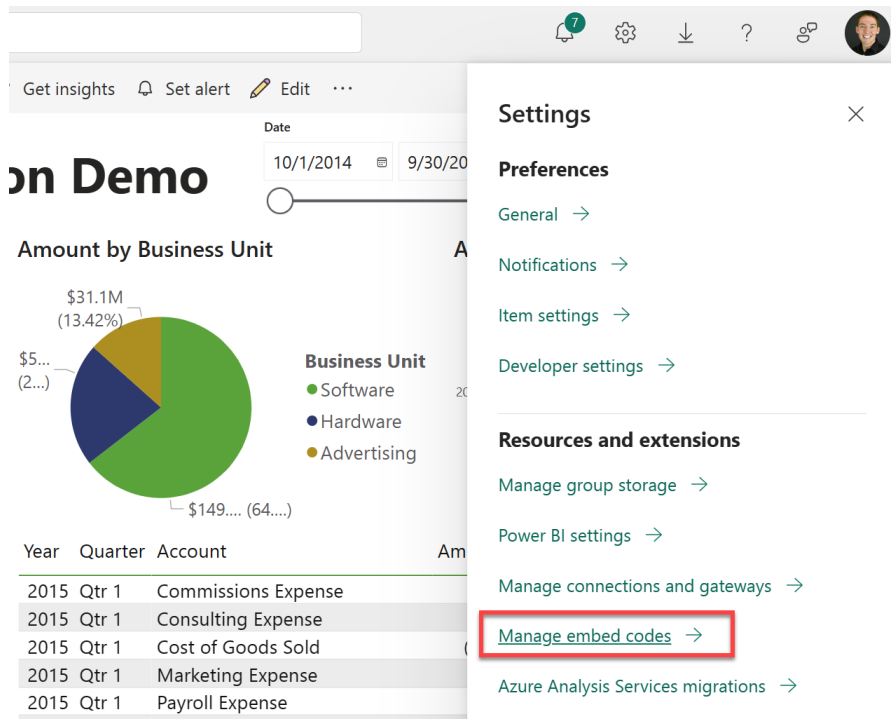


Figure 7.22 – Manage embed codes option in Settings for a workspace

From here, users can get the code for the published report(s) again or delete the codes from one centralized location.

To enhance control over how data is shared publicly throughout your organization, you can adjust settings in the Power BI admin portal to disable all embed codes or prevent the creation of new embed codes. By disabling the **Publish to web** option in the admin portal, you can ensure that no new public links or embed codes can be generated and any existing ones will no longer function. For more detailed steps on how to restrict the **Publish to web** feature to specific security group members, refer to the previous recipe, *Restricting Power BI’s Publish to web (anonymous share) ability to specific security group members*.

See also

- *Publish to web from Power BI:* <https://learn.microsoft.com/en-us/power-bi/collaborate-share/service-publish-to-web>

Configuring a default logo, cover image, and theme for Power BI

Setting a default logo, cover image, and theme for Power BI helps maintain brand consistency and enhances the visual appeal of your reports and dashboards. This recipe is beneficial for organizations looking to standardize the appearance of their business intelligence tools across departments, reinforcing brand identity and providing a cohesive user experience to report viewers.

Getting ready

You must be a Global or Fabric Administrator to follow the steps in this recipe.

How to do it...

1. Navigate to the Power BI admin portal at <https://app.powerbi.com/admin-portal> or by selecting the settings wheel from Power BI (<https://app.powerbi.com>), then selecting **Admin portal**.
2. Select **Custom branding** from the left navigation menu, as shown in *Figure 7.23*.

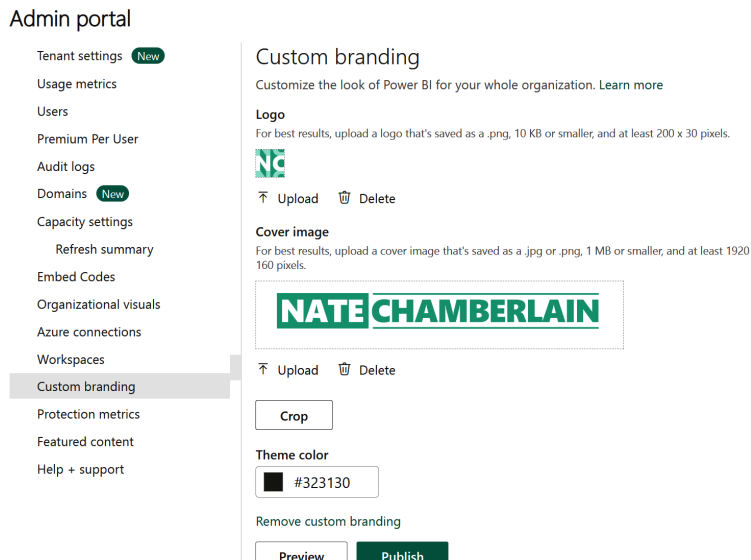


Figure 7.23 – Custom branding in the Power BI admin portal

3. Upload your organization's logo and select a cover image that aligns with your branding guidelines.
4. Choose a theme color that represents your corporate identity.
5. Select **Publish** to apply and save these settings to update the look and feel of Power BI reports across your organization.

How it works...

In this recipe, you implemented custom branding for your organization's Power BI service. After configuring the logo, cover image, and theme color (as outlined in *Steps 4–5*), you will have successfully tailored the Power BI user interface to reflect your organization's branding. This customization enhances the user experience by integrating familiar visual elements into the online platform. An example of implemented branding is shown in *Figure 7.24*.

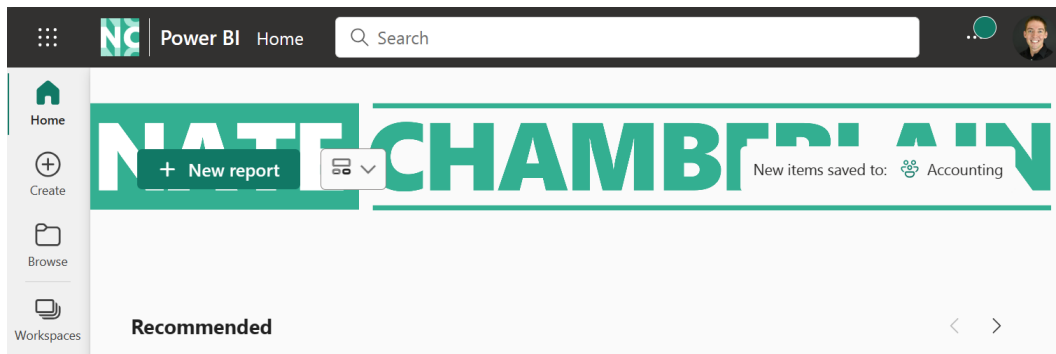


Figure 7.24 – An example of custom branding implemented in the Power BI service

As you can see in *Figure 7.24*, color contrast is an important consideration for your cover image. And because the image is responsive in size, having text in a cover image can be problematic as it will be partially obscured and potentially cropped on the sides depending on screen size.

There's more...

To remove custom branding, repeat *Steps 1–2* then select **Remove custom branding** and **Publish**.

See also

- *Add custom branding to the Power BI service:* <https://learn.microsoft.com/en-us/fabric/admin/service-admin-custom-branding>

8

Administering SharePoint Online

In this chapter, we delve into the fundamental aspects of managing and customizing SharePoint Online environments to align with your organization's needs. SharePoint serves as a robust platform for collaboration and information management and is often the backbone of organizational intranets. It also supports many other Microsoft 365 apps and services, including Microsoft Teams, OneDrive, and Planner. Mastering its configuration is essential for effective digital workspace management.

We will explore a variety of practical recipes designed to equip you with the skills to create and delete sites, tailor site settings for enhanced security, and manage site collections efficiently.

We will cover the following recipes in this chapter:

- Creating a new site
- Deleting a site
- Limiting external sharing abilities
- Setting stricter external sharing settings for a specific site
- Setting the default share link type
- Configuring site collection storage
- Importing data from network locations using the Migration Manager or SPMT
- Hiding the subsite creation button
- Designating a site as a hub site and associating other sites with it
- Restricting access by IP address

Technical requirements

This chapter requires administrative access within Microsoft 365. Users assigned the Global or SharePoint Administrator role will have the capability to execute all tasks presented.

Creating a new site

In this recipe, you will learn how to create a new SharePoint site. This is typically done when a new project team is formed, or when a new department needs its own dedicated space for collaboration and information sharing. Creating a SharePoint site provides a centralized platform for team members to share documents, track tasks, and collaborate effectively.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**, as shown in *Figure 8.1*.

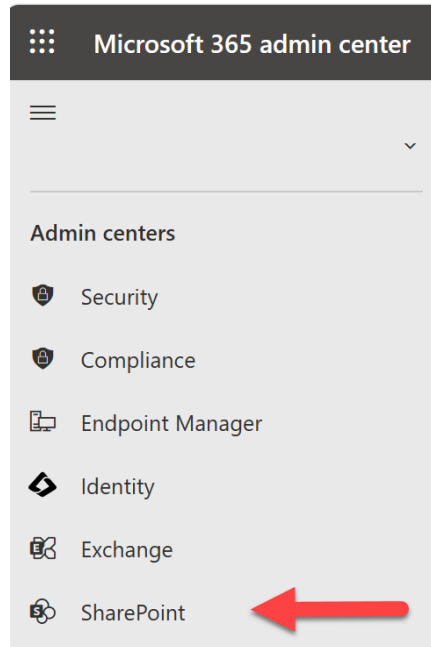


Figure 8.1 – SharePoint admin center location in Microsoft 365 admin center

2. Select **Sites** | **Active sites** from the left navigation menu, then click **Create**.
3. In the dialog that appears, which is shown in *Figure 8.2*, choose either **Team site** or **Communication site**. Since Team sites come with every team in Microsoft Teams, we'll choose **Communication site** in this recipe to showcase something unique from what you'll learn about in *Chapter 9, Managing Microsoft Teams*.

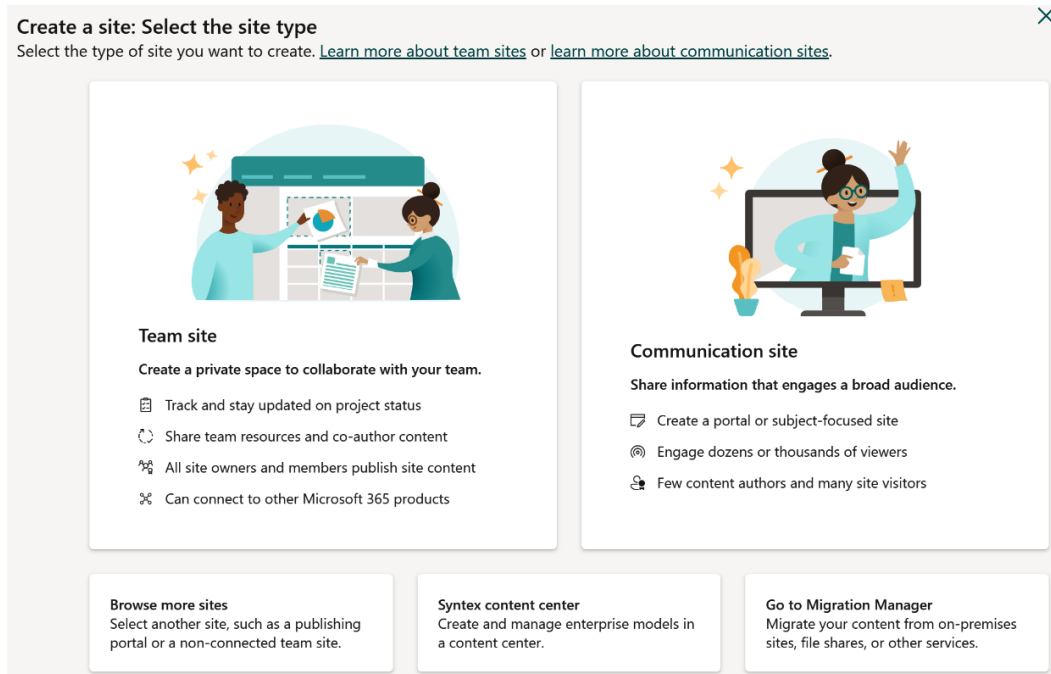


Figure 8.2 – Dialog for choosing site type in SharePoint Online

Tip

Use SharePoint Team sites for collaboration within a specific group, enabling document sharing, task management, and real-time communication, while Communication sites are best for broadcasting information broadly across the organization, offering a visually rich layout to engage a wider audience.

4. Choose the **Standard communication** site template, or another template if it better suits your new site's purpose, such as **Department** to share your department's news and resources org-wide.

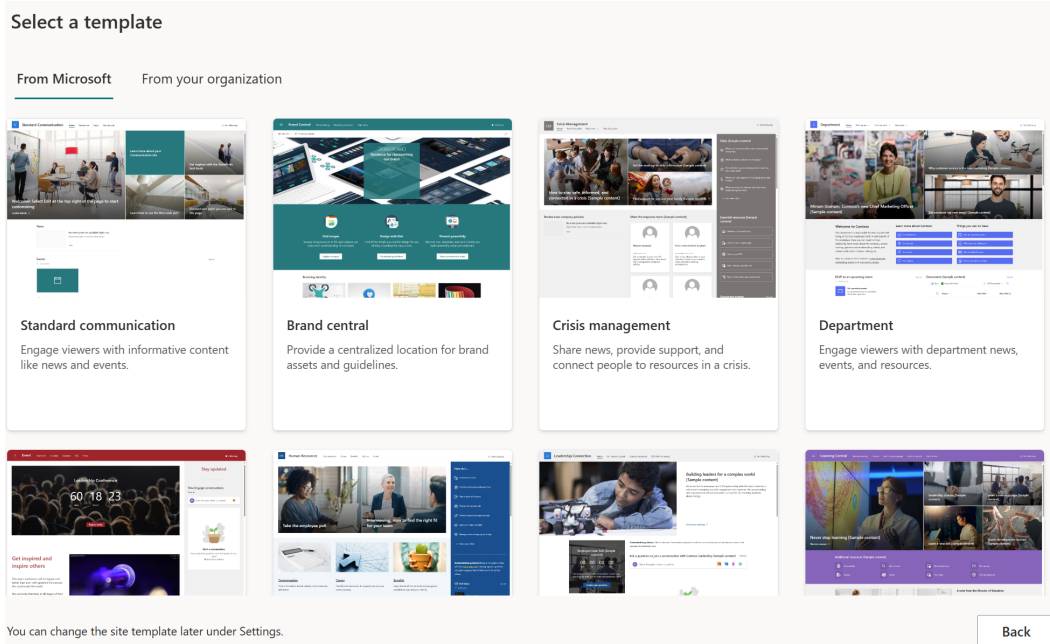


Figure 8.3 – Communication site template options for a new SharePoint site

5. Select **Use template** to confirm your template choice after reviewing its features.
6. Specify the site's main details, including the following:
 - A. **Site name**
 - B. **Site description**
 - C. **Site address**
 - D. **Site owner** (limited to one at present, but you can add more later)
7. Select **Next**, then select the new site's **Language** and **Time zone**.
8. Select **Create site** when finished.

How it works...

When you provision a new site using the SharePoint admin center, it immediately becomes available to the site owner, who can then manage access and permissions, tailoring the site to meet specific needs or organizational policies. This recipe's new Communication site would be best utilized for org-wide communications and resource sharing. In contrast, a Team site, which is more collaboration-oriented, can be created either as a standalone site or in tandem with a Microsoft Teams team. These Team sites are better suited for internal team or group collaboration, facilitating real-time communication and resource-sharing.

There's more...

When managing a new SharePoint site designed for organizational communication, it's essential to effectively handle access permissions. This site management involves specifying permissions for different users to view, edit, upload, and delete content. Carefully configuring these permissions ensures that sensitive information is protected yet accessible to those who need it. Moreover, well-structured permission settings help organize the site's content and prevent unintended data exposure, allowing team members access only to the resources pertinent to their roles.

Note

The default user group named **Everyone Except External Users** can be used to assign read (**Visitors**) permissions to your entire organization, automatically including all internal users without needing manual updates as your organization's users change. This group is ideal for scenarios where you want all users to have read-only access to your site, such as for publishing policies, procedures, news, images, and other content that should be accessible to everyone within the organization. However, use this option with caution, as it grants access to all content on the site, and should only be used when your intention is to share everything on the site with the entire organization.

Each new site is configured with three default SharePoint permission groups:

- **Owners:** They possess comprehensive control over the site, including its settings and permissions
- **Members:** They have the ability to edit, add, and remove site content – ranging from pages and list items to documents, lists, and libraries
- **Visitors:** They, on the other hand, have read-only access

For a Communication site, as illustrated in this recipe, it's advisable to appoint an additional site owner for backup purposes and several site members for content creation and management. Typically, a broad range of organization members (if not everyone) will be included as visitors to access, read, and engage with the content.

See also

- *Create a site:* <https://learn.microsoft.com/en-us/sharepoint/create-site-collection>

Deleting a site

In this recipe, you will learn how to delete a SharePoint site. This task is often necessary when a project concludes, a department restructures, or when you simply want to remove unused sites to maintain a streamlined organizational SharePoint environment. Deleting a SharePoint site helps manage the digital workspace efficiently by removing outdated or unnecessary content.

Important note

To follow the steps in this recipe, the SharePoint site must not have a Purview retention policy applied. If a retention policy is in place, the site must be added to the exemptions within that policy before it can be deleted.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Sites | Active sites** from the left navigation menu, then select the site you wish to delete.
3. Within the site's information panel, select **Delete**, as shown in *Figure 8.4*.

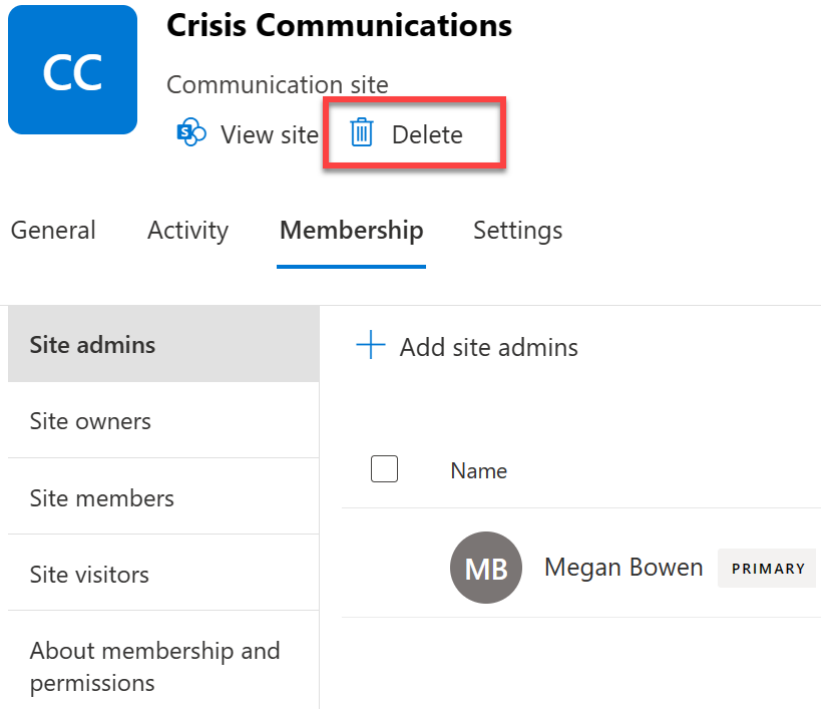


Figure 8.4 – Option to delete a site within the SharePoint admin center

4. Confirm the deletion when prompted by selecting **Delete** again, acknowledging that you'll have 93 days during which you can restore the site before it's permanently deleted.

How it works...

When you delete a site using the SharePoint admin center, the site is immediately removed from active sites but remains recoverable from **Deleted sites** for a period of 93 days. This allows administrators to recover the site if the deletion was a mistake or if circumstances change.

There’s more...

You can restore a deleted site by visiting the SharePoint admin center and selecting **Sites | Deleted sites**. From here, select the deleted site, then click **Restore**, as shown in *Figure 8.5*.

Deleted sites

Sites are retained for 93 days and then permanently deleted.
[Learn more about restoring deleted sites](#)

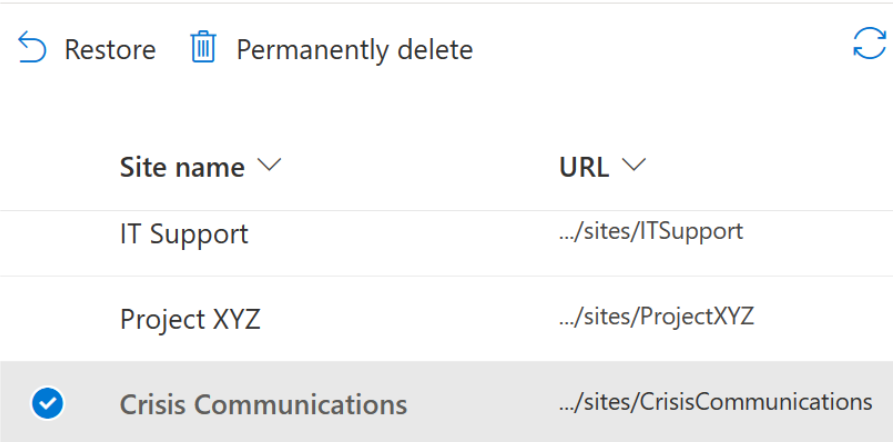


Figure 8.5 – A selected site ready to be restored in the SharePoint admin center

See also

- *Delete a site:* <https://learn.microsoft.com/en-us/sharepoint/delete-site-collection>
- *Restore deleted sites:* <https://learn.microsoft.com/en-us/sharepoint/restore-deleted-site-collection>

Limiting external sharing abilities

In this recipe, you will configure the settings to limit external sharing abilities in SharePoint. This is important for enhancing data security by controlling how data is shared with external users and ensuring that sensitive information does not leave the organizational boundaries without proper authorization.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Policies | Sharing** from the left navigation menu.

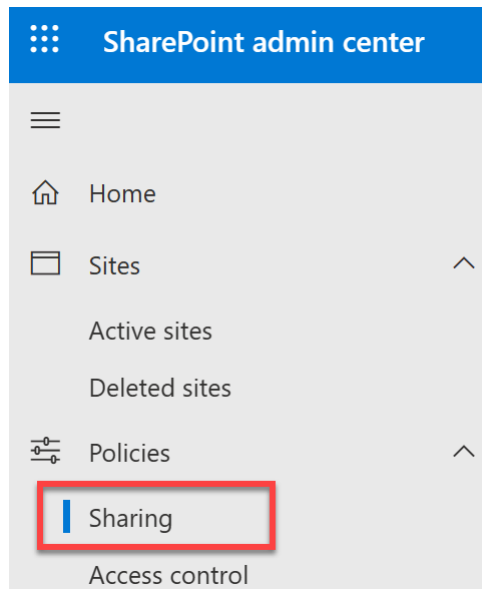


Figure 8.6 – External sharing settings location in the SharePoint admin center

3. In the **External sharing** section, you can define the permitted scope of sharing throughout your organization. These settings apply to both SharePoint and OneDrive for Business. The sharing options are shown in *Figure 8.7* and described here:
 - **Anyone:** This allows users to share files and folders using links that do not require sign-in. It's best used for non-sensitive information.
 - **New and existing guests:** This setting supports sharing with guests who are either new to your directory or already exist within it. They must sign in to access the shared item(s).
 - **Existing guests:** This only supports guests already within your directory but will not support new guests.

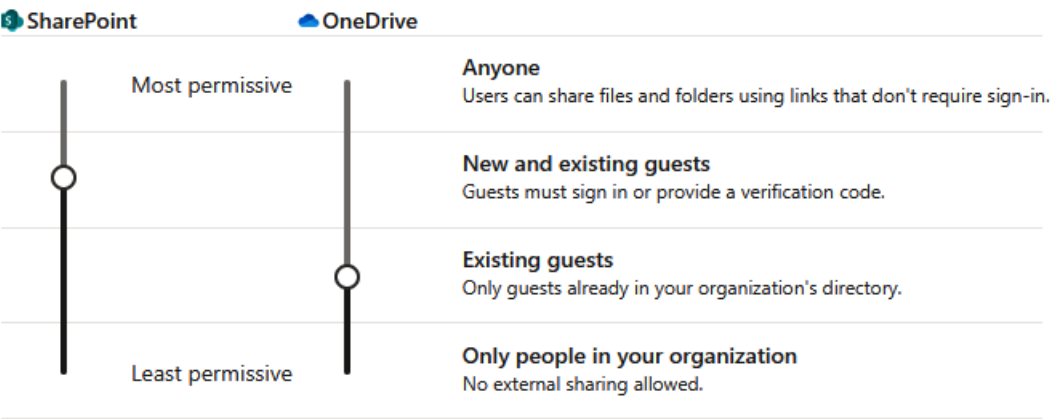
- **Only people in your organization:** This disables external sharing throughout your organization.

Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive.
[Learn more about managing sharing settings](#)

External sharing

Content can be shared with:



You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

More external sharing settings ✓

Figure 8.7 – External sharing settings for SharePoint and OneDrive

4. Expand **More external sharing settings** to adjust a number of settings, shown in *Figure 8.8*, that further protect your SharePoint and OneDrive (and, by extension, Teams) content. These settings are as follows:
 - **Limit external sharing by domain:** This lets you specify which domains your organization can share with by specifying allowed or blocked domains.

- **Allow only users in specific security groups to share externally:** You can limit external sharing capabilities to specified security groups, ensuring only authorized individuals are able to share content outside the organization. This does not affect sharing through Microsoft 365 Groups or Teams.
- **Guests must sign in using the same account to which sharing invitations are sent:** This option ensures that guests sign in with the account to which an invitation was sent, adding an extra layer of security.
- **Allow guests to share items they don't own:** Determine whether guests can share resources of which they are not owners.
- **Guest access to a site or OneDrive will expire automatically after this many days:** Specify how many days a guest will have access to resources shared with them.
- **People who use a verification code must reauthenticate after this many days:** Specify after how many days a guest using an authentication code to access shared resources must reauthenticate to continue accessing them.

More external sharing settings ✓

- ☐ Limit external sharing by domain
- ☒ Allow only users in specific security groups to share externally

1 security group: Marketing Members

Manage security groups

- ☒ Guests must sign in using the same account to which sharing invitations are sent
- ☒ Allow guests to share items they don't own
- ☒ Guest access to a site or OneDrive will expire automatically after this many days
- ☒ People who use a verification code must reauthenticate after this many days [Learn more](#) ⓘ

Figure 8.8 – More external sharing settings for SharePoint and OneDrive

5. Scroll down and configure the rest of the settings on the page shown in *Figure 8.9*. Note that when configuring the default link types (anyone, people in your org, etc.) and permissions (**Edit** versus **View**), your options are limited to those specified at the top for SharePoint and OneDrive permission settings.

File and folder links

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

- ☐ Specific people (only the people the user specifies)
- ☒ Only people in your organization
- ☐ Anyone with the link

Choose the permission that's selected by default for sharing links.

- ☐ View
- ☒ Edit

Other settings

- ☒ Show owners the names of people who viewed their files in OneDrive
- ☒ Let site owners choose to display the names of people who viewed files or pages in SharePoint
- ☒ Use short links for sharing files and folders

Figure 8.9 – File and folder link and other settings for SharePoint and OneDrive

The **Specific people** option for link type is most appropriate and secure if you anticipate the need to share files and folders with guests on a regular basis.

6. Select **Save**.

Important note

It's important to remember these settings apply at an organizational level for SharePoint, and they determine the settings available at the individual site level. The individual site settings cannot be more permissive than the organization-wide settings.

How it works...

Enabling external sharing for SharePoint allows users to share content with individuals outside the organization. This feature is especially beneficial for collaborating on projects with external partners, clients, or contractors. Administrators can customize the sharing options, such as permitting sharing with anyone who has the link or restricting it to guests who must either sign in or are explicitly granted access. External sharing can greatly enhance productivity and enable smooth collaboration across organizational boundaries. However, administrators must configure these settings carefully to balance the need for collaboration with the need to protect sensitive information.

There's more...

Educating users on secure sharing practices is essential. Regular training sessions can significantly reduce risks by informing users about the dangers of careless sharing and teaching them to use secure methods, such as sharing links with specific individuals. Implementing **Data Loss Prevention (DLP)** policies adds an extra layer of security by automatically detecting and preventing the improper sharing of sensitive information. Together, these measures create a robust strategy to manage and secure external sharing within SharePoint and OneDrive.

See also

- *Manage sharing settings for SharePoint and OneDrive in Microsoft 365*: <https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>

Setting stricter external sharing settings for a specific site

This recipe focuses on applying external sharing settings to a specific site that are more restrictive than the org-wide external sharing settings specified in the previous recipe, *Limiting external sharing abilities*. It's particularly useful for sites containing sensitive or confidential information, where tighter control over who can view and share content is necessary to comply with internal policies or regulatory requirements.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Sites** | **Active sites** from the left navigation menu.

3. Select the site for which you wish to configure more restrictive external sharing settings, then select **Settings** from its panel's top menu, as shown in *Figure 8.10*.

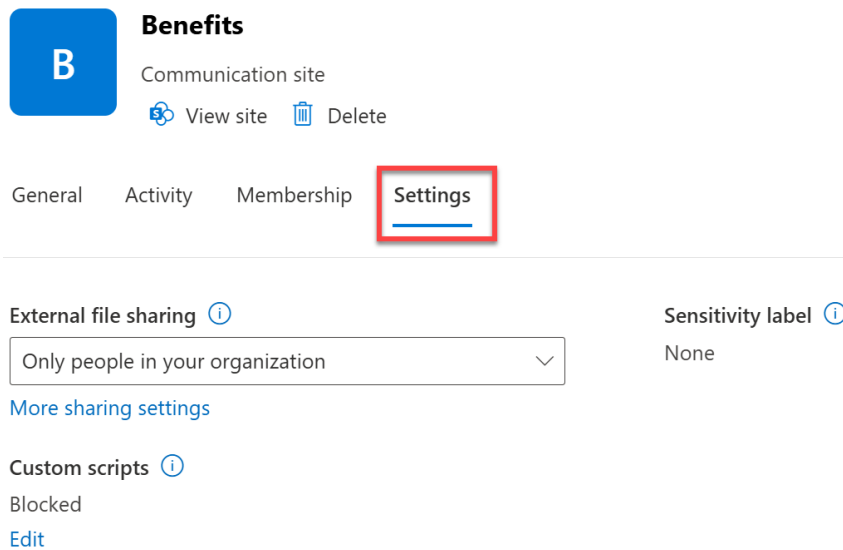


Figure 8.10 – Location of external sharing settings for a site in the SharePoint admin center

4. Choose the specific **External file sharing** setting you'd like to enforce for the selected site:

- **Anyone**
- **New and existing guests**
- **Existing guests**
- **Only people in your organization** (most secure; disables external sharing)

For this recipe, ensure that you've chosen **Only people in your organization** to disable external sharing for this site.

5. Select **Save**.

How it works...

When you apply stricter external sharing settings to a specific site, you enhance the security and control over who can access and share content within that site. By setting the external sharing permissions to **Only people in your organization**, you effectively disable any external sharing for the selected site. This means that only users within your organization will be able to access and share the site's contents, significantly reducing the risk of data breaches or unauthorized access. This granular level of control allows administrators to tailor security settings to the sensitivity of the content housed within each site, providing a robust defense against potential information leaks.

There's more...

Besides modifying the overall external sharing settings for a specific site, you can also adjust the default share link type that is used when a user selects **Copy link** or **Share**. This adjustment helps reduce the risk of users sharing content with unintended recipients or broader audiences than necessary. To do so, follow these steps:

1. In the SharePoint admin center, select **Sites | Active sites** from the left navigation menu.
2. Select the site for which you wish to configure a new default share link type and permissions, then select **Settings** from its panel's top menu, as previously shown in *Figure 8.10*.
3. Under the **External file sharing** dropdown, select the **More sharing settings** link shown in *Figure 8.11*.

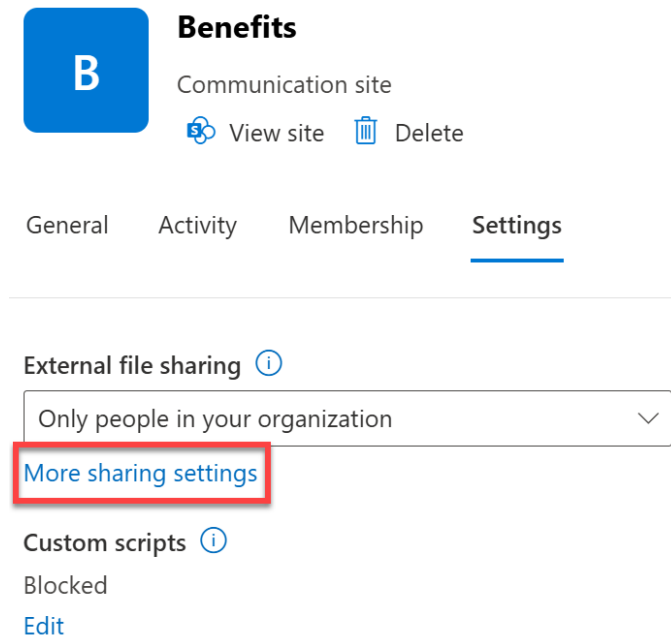


Figure 8.11 – Location of more sharing settings for a specific site

4. Scroll to the bottom of the screen and uncheck both boxes for **Same as organization-level setting** to separate this site from the org-wide default setting specified in the previous recipe, *Limiting external sharing abilities*.
5. Now that you can adjust this site's settings, choose the new default share link settings for this site. For example, you may wish for the default share link settings to be set to **Only people in your organization** and **View**, as shown in the configuration in *Figure 8.12*.

Advanced settings for external sharing ▾

Default sharing link type

Choose the type of link that's selected by default when users share files and folders on this site.

- ☐ Same as organization-level setting (Specific people)
- ☐ People with existing access
- ☐ Specific people (only the people the user specifies)
- ☒ Only people in your organization
- ☐ Anyone with the link

Advanced settings for Anyone links ▾

Default link permission

- ☐ Same as organization-level setting (View)
- ☒ View
- ☐ Edit

Save[Reset to organization-level settings](#)

Figure 8.12 – A site's unique default share link settings

6. Select **Save**.

See also

- *Change the sharing settings for a site:* <https://learn.microsoft.com/en-us/sharepoint/change-external-sharing-site>

Setting the default share link type

In this recipe, you will set the default share link type for SharePoint sites within your organization. This setting helps streamline how documents are shared by default, promoting a consistent sharing practice across the organization, whether to enhance security or simplify user interactions.

Important note

This recipe applies universally across your organization as a baseline. See the *There's more...* section of the previous recipe, *Settings stricter external sharing settings for a specific site*, to learn how to change the default share link type for one specific site rather than all sites.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at `https://admin.microsoft.com`. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Policies | Sharing** from the left navigation menu, then specify the default link type settings under **File and folder links**, as shown in *Figure 8.13*.

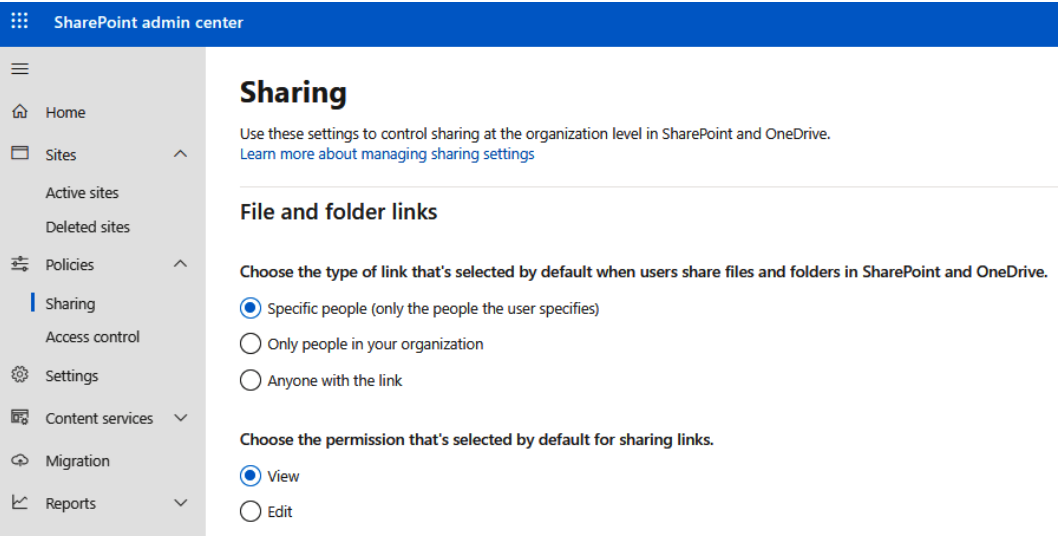


Figure 8.13 – Default share link type settings in the SharePoint admin center

How it works...

Configuring the default share link type for SharePoint helps organizations standardize their sharing settings, ensuring consistency in how files are shared by default. This setting allows administrators to define the access level for shared links, choosing whether they are publicly accessible, restricted to organization members, or limited to specific individuals. It plays an important role in safeguarding sensitive data and preventing unauthorized information dissemination. By setting a more restrictive default, the organization can minimize the risk of accidental data exposure while still having the flexibility to adjust settings for specific needs when necessary.

There's more...

Below the default link type and permission settings, you can specify additional settings including the number of days after which an **Anyone** link will expire (if allowed and applicable), and which abilities **Anyone** links can provide, such as view and edit/upload.

Individual sites can also have their own default share link setting, which may be helpful when a particular team shares in a specific manner (e.g., **Anyone with the link**) most often. To change one site's default share link type, follow these steps:

1. Go to the SharePoint admin center, then select **Sites | Active sites** to find the team that should have a unique default share link type.
2. Select the team you wish to modify, then select **Settings | More sharing settings**, as shown in *Figure 8.14*.

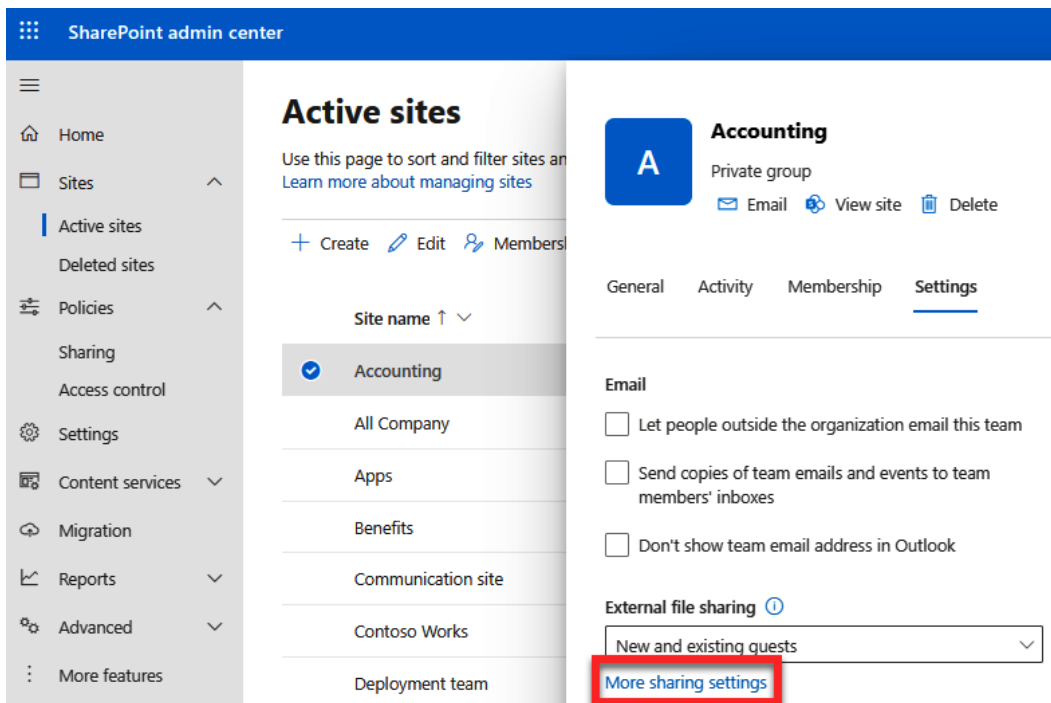


Figure 8.14 – More sharing settings for a specific site

3. Scroll down to the **Advanced settings for external sharing** section and uncheck **Same as organization-level setting** to specify something different for this site.
4. As shown in *Figure 8.15*, you can choose a new default share link type and permission for this site and select **Save** when finished.

Sharing

Advanced settings for external sharing 

Default sharing link type

Choose the type of link that's selected by default when users share files and folders on this site. [Learn more about the default link types](#)

- ☐ Same as organization-level setting (Specific people)
- ☐ People with existing access
- ☐ Specific people (only the people the user specifies)
- ☒ Only people in your organization
- ☐ Anyone with the link

Advanced settings for Anyone links 

Default link permission

- ☐ Same as organization-level setting (View)
- ☐ View
- ☒ Edit

Save

[Reset to organization-level settings](#)

Figure 8.15 – Default share link settings for a specific site

Important note

If you've implemented sensitivity labels, your sites' sensitivity labels will determine the sites' default sharing settings.

See also

- *Manage sharing settings for SharePoint and OneDrive in Microsoft 365*: <https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>
- *Change the sharing settings for a site*: <https://learn.microsoft.com/en-us/sharepoint/change-external-sharing-site>

Configuring site collection storage

This recipe will show you how to configure storage limits for a site in SharePoint. Proper management of storage limits is essential to prevent the overuse of resources, maintain site performance, and ensure that storage space is utilized efficiently across multiple sites.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at `https://admin.microsoft.com`. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Settings** from the left-hand navigation menu. Then, select **Site storage limits**, as shown in *Figure 8.16*.

Settings






App	Name ↑	Description
 SharePoint	Home sites	Set up home sites that link to Viva Connections experiences
 SharePoint	Notifications	Allow mobile app notifications about site activity
 SharePoint	Pages	Allow users to create and comment on modern pages
 SharePoint	Site creation	Set default settings for new sites
 SharePoint	Site storage limits	Use automatic or manual site storage limits

Figure 8.16 – Site storage limits setting location in the SharePoint admin center

3. Select **Manual**. Then, select **Save**. This enables you to specify different site storage limits per site, rather than allowing all sites to use as much storage as they need.
4. Now select **Sites | Active sites** from the left navigation menu.
5. Find the specific site for which you wish to configure a new storage limit and select it. Then select **Storage** from the ribbon menu, as shown in *Figure 8.17* (note that it may be on an ellipsis menu depending on your screen size).

Active sites

Use this page to sort and filter sites and change site settings.

[Learn more about managing sites](#)

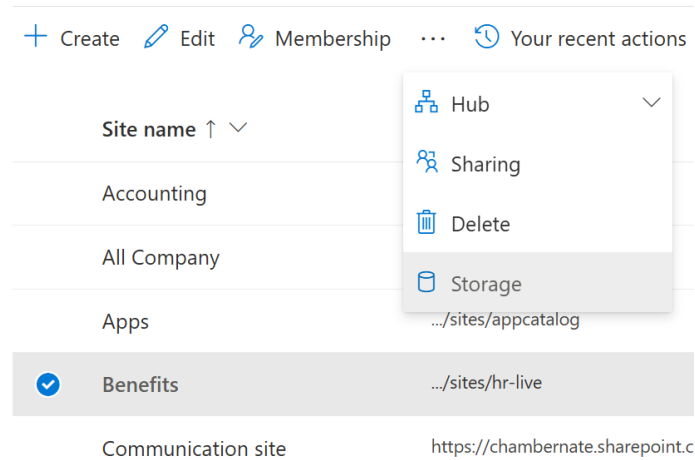


Figure 8.17 – Location of storage settings for a site in the SharePoint admin center

6. Change the site's storage limit in **Gigabytes (GBs)** and set a threshold at which to notify site owners of storage usage, as shown in *Figure 8.18*.

Edit storage limit

The actual storage available for this site depends on the available storage for your organization.

[Learn more about managing site storage limits](#)

Maximum storage for this site *

 GB

Enter a value from 1 through 25600.

☒ Allow notifications

Email owners when this much of the storage limit is used: *

 %

Figure 8.18 – Storage limit settings for a specific site

7. Select **Save**.

How it works...

Configuring site storage limits in SharePoint is helpful for maintaining control over content sprawl and ensuring organizational governance. While SharePoint allows sites to grow indefinitely by default (up to your organization's shared storage limit across all sites), setting specific storage limits helps manage and prioritize the allocation of storage resources based on the site's importance and usage patterns.

For example, consider a scenario where a project Team site is created for a short-term initiative. Without storage limits, the site could accumulate excessive files and data, potentially cluttering the storage and making it difficult to manage. By setting a storage limit, you can encourage the team to regularly review and clean up unnecessary files, keeping the site organized and relevant.

In addition to basic storage management, it's important to consider how site storage interacts with version history and file types. Each version of a document stored in SharePoint consumes additional storage space, so sites with extensive versioning settings may require more storage than anticipated. Setting storage limits can help enforce regular reviews of version history to ensure that only necessary versions are retained, optimizing storage usage.

Additionally, different file types can vary significantly in size. For instance, multimedia files such as videos and high-resolution images consume far more storage than standard documents. By setting storage limits, you can encourage users to be mindful of the types of files they upload, helping to prevent sites from becoming overloaded with large, non-essential files.

Another scenario involves compliance and regulatory requirements. Certain departments, such as legal or finance, might need to retain documents for a specific period, but not indefinitely. By setting storage limits, you can ensure that these sites do not hold onto data longer than necessary, helping to enforce data retention policies and reduce the risk of non-compliance.

Setting storage limits can also help with budget management. If your organization has a limited budget for additional storage, enforcing storage quotas on sites ensures that high-priority projects or departments get the necessary resources without unexpected added costs from overuse by lower-priority sites.

There's more...

You can monitor your organization's overall storage usage on the **Active sites** screen of the SharePoint admin center. You'll see a usage bar in the upper-right corner illustrating how much storage remains for your subscription.

If you need to purchase additional storage, review the latest guidance at <https://learn.microsoft.com/en-us/microsoft-365/commerce/add-storage-space>.

See also

- *Manage site storage limits in SharePoint in Microsoft 365*: <https://learn.microsoft.com/en-us/sharepoint/manage-site-collection-storage-limits>

Importing data from network locations using the Migration Manager or SPMT

This recipe details how to find the best methods to import data into SharePoint Online from network and other cloud locations using the **Migration Manager** or **SharePoint Migration Tool (SPMT)**. Such migrations are typically required when consolidating digital assets into SharePoint Online to centralize content management and facilitate easier access and collaboration.

Getting ready

You must be a Global Administrator to complete this recipe. You will also need access to the source files being brought into Microsoft 365. For example, if you're migrating on-premises content, you will need administrative permissions for any on-premises machines, as well as access to their specific file share locations being migrated. Or, if you're migrating a cloud location's files, you must be an administrator of third-party cloud locations such as Dropbox.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Migration** from the left navigation menu.
3. In the **Migration Manager** section shown in *Figure 8.19*, note that you can use **Migration Manager** to begin migrations of content from **File shares**, **Box**, **Google Workspace**, **Dropbox**, and **Egnyte**.

Migration

Migration Manager

[Learn what's new](#)



File shares

Copy your on-premises file shares to Microsoft 365. [Learn more](#)

Get started



Stream

Migrate your Stream (Classic) content to Microsoft 365 to use Stream (on SharePoint). [Learn more](#)

Get started



Dropbox

Copy your Dropbox content to Microsoft 365. [Learn more](#)

Get started



Box

Copy your Box content to Microsoft 365. [Learn more](#)

Get started



Google Workspace

Copy your Google Workspace content to Microsoft 365. [Learn more](#)

Get started



Egnyte

Copy your Egnyte content to Microsoft 365. [Learn more](#)

Get started

Figure 8.19 – Migration Manager options

4. Scroll down to the **Other migration solutions** section shown in *Figure 8.20* to find a link to **Download SharePoint Migration Tool** for any SharePoint Server migrations to SharePoint Online. This supports migrating content from SharePoint 2010, 2013, and 2016.

Other migration solutions



For SharePoint Server 2010, 2013 and 2016

Use the SharePoint Migration Tool to copy content from SharePoint Server to Microsoft 365.

Download SharePoint Migration Tool

Figure 8.20 – Other migration solutions for SharePoint Server content

How it works...

Migration Manager is a versatile tool integrated into the SharePoint admin center. It supports migrations from a variety of sources, including file shares, Box, Google Workspace, Dropbox, Stream, and Egnyte. The tool allows you to install agents on multiple machines to help distribute and manage the migration tasks, ensuring efficient and organized data transfer. Migration Manager provides a centralized interface, shown in *Figure 8.21*, where you can monitor the progress of each migration task, troubleshoot issues, and ensure data is transferred securely and accurately.

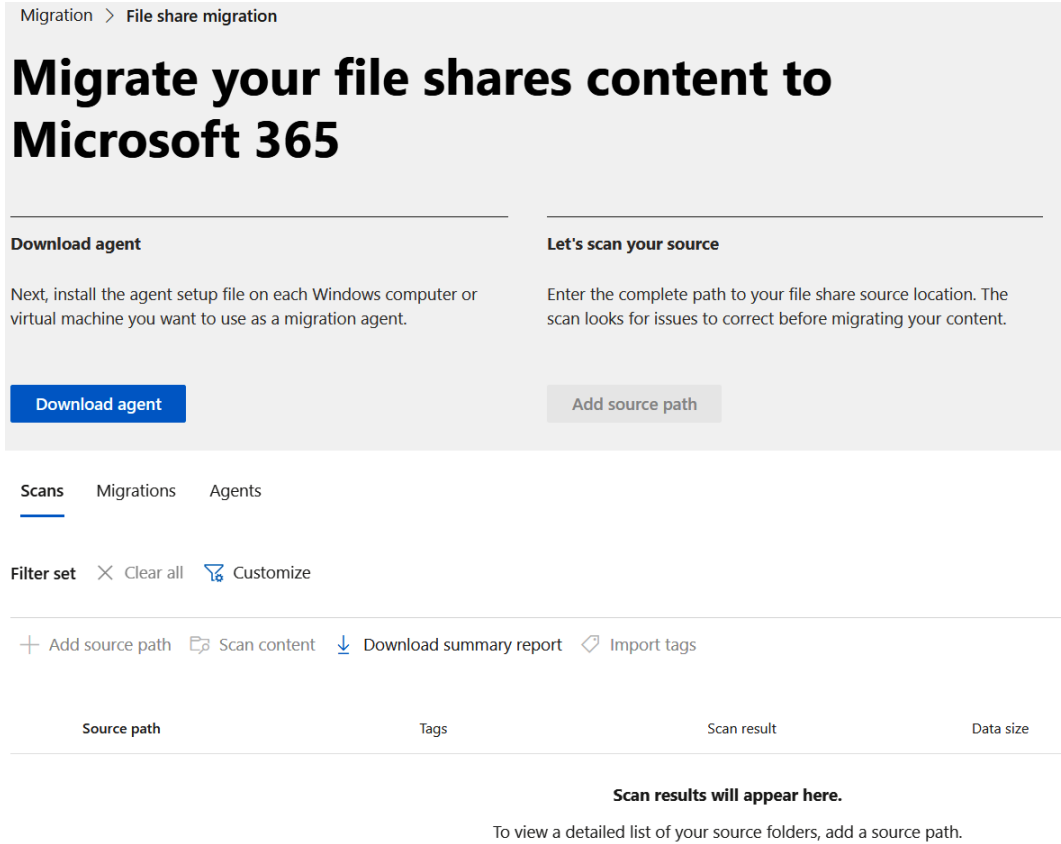


Figure 8.21 – Migration Manager screen when beginning a file share migration

The SPMT is designed for migrating content from on-premises SharePoint servers (versions 2010, 2013, and 2016) to SharePoint Online. SPMT supports a wide range of migration scenarios, from simple document libraries to complex site collections, preserving metadata, version history, and permissions during the migration process. The tool is particularly useful for organizations transitioning from older SharePoint environments to the modern SharePoint Online platform, helping them leverage the latest features and integrations available in Microsoft 365.

Both Migration Manager and SPMT offer robust options for managing large-scale migrations, ensuring that data integrity and security are maintained throughout the process. By centralizing content in SharePoint Online, organizations can enhance collaboration, improve content management, and provide users with seamless access to critical information from anywhere.

Important note

Mover, previously covered in the first edition of this book, has been retired. Migration Manager and SPMT can cover most migration needs, and third-party vendors are also available to assist with specific migration requirements.

There's more...

Cross-tenant migration (SharePoint Online to another SharePoint Online tenant) is in development and in private preview as of the writing of this book. Learn more about this upcoming migration ability at <https://learn.microsoft.com/en-us/microsoft-365/enterprise/cross-tenant-sharepoint-migration>.

See also

- *Migrate your content to Microsoft 365*: <https://learn.microsoft.com/en-us/sharepointmigration/migrate-to-sharepoint-online>

Hiding the subsite creation button

This recipe guides you through hiding the subsite creation button in SharePoint. This can be useful in organizations aiming to simplify their SharePoint architecture or to discourage the creation of unnecessary subsites that could lead to governance issues.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Settings** and then scroll down to select the link to the classic settings page at the bottom of the screen.

3. Scroll down to **Subsite Creation** and select the **Disable subsite creation for all sites** command radio button shown in *Figure 8.22*.

Subsite Creation

Control subsite creation for people who have permission to create sites. This controls visibility of the Subsite option on the Site contents page and enables new subsite creation. Use hub sites to connect related sites instead of using subsites.

- ☒ Disable subsite creation for all sites
- ☐ Enable sub site creation for classic sites only
- ☐ Enable subsite creation for all sites

[Learn about hub sites](#)

Figure 8.22 – Subsite creation settings in the SharePoint admin center

4. Scroll to the bottom of the screen and select **OK** to save.

How it works...

Without disabling subsite creation, site owners can provision subsites by visiting their site's **Site contents** and selecting **New | Subsite**. After this recipe's steps are followed, however, this option is removed, as shown in *Figure 8.23*.

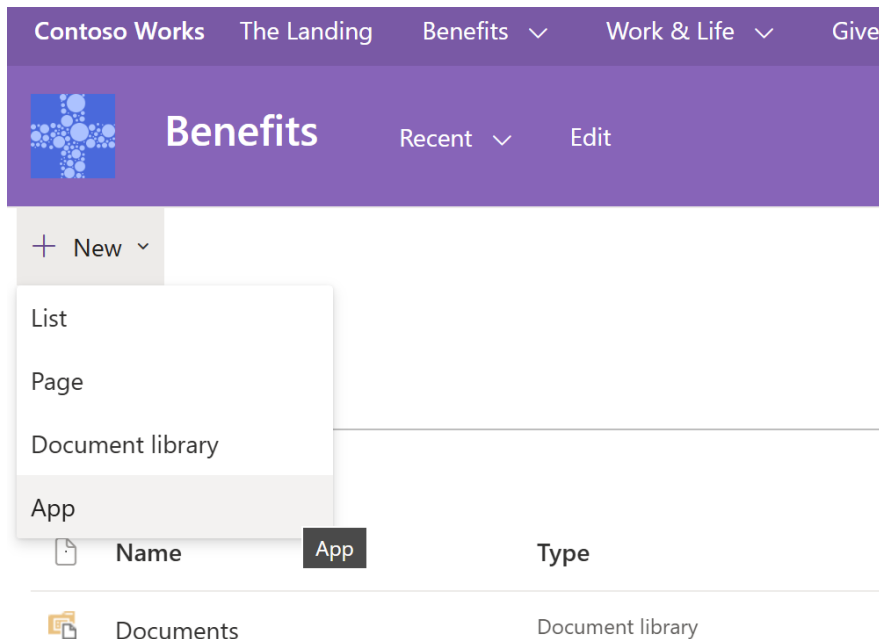


Figure 8.23 – New button dropdown showing options with subsite excluded

Modern best practices for SharePoint site architecture recommend using a flat structure instead of a hierarchical one. This approach means not creating subsites and it offers several advantages, particularly in terms of flexibility, manageability, and user experience.

A flat structure allows organizations to easily adapt to changes without disrupting the entire site architecture. Each site operates as a standalone entity, making it simpler to reassign or reorganize departments and functions without affecting other areas of the organization. Permissions, navigation, and site settings are also easier to control and customize because they are not inherited from a parent site. This flexibility is integral in dynamic business environments where organizational changes are frequent.

There's more...

In modern SharePoint architecture, **hubs** are used to structure flat site collections by linking them into a cohesive network. Hubs facilitate features such as content aggregation, unified navigation, and consistent branding across independent sites. This approach allows for rolling up news and events from different sites into a central hub, inheriting navigation elements, and applying a consistent look and feel throughout the connected sites. By grouping related sites based on projects or departments, hubs enhance content discoverability, governance, and overall user experience, aligning with the needs of dynamic and responsive digital workplaces. We'll cover hub sites more in the next recipe, *Designating a site as a hub site and associating other sites with it*.

See also

- *Manage site creation in SharePoint:* <https://learn.microsoft.com/en-us/sharepoint/manage-site-creation#manage-detailed-site-and-subsite-creation-settings-in-the-classic-sharepoint-admin-center>

Designating a site as a hub site and associating other sites with it

In this recipe, you will designate a site as a **hub site** and associate other sites with it. Hub sites are used to organize related sites into a unified interface with shared navigation and branding, enhancing discoverability and cohesion across projects or departmental sites.

Tip

Implementing hub site structures is recommended in place of former subsite structures.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Sites | Active sites** from the left navigation menu.
3. Find the site you want to designate as a hub site and select it. Then, select **Hub** from the top menu (it may be under the ellipsis menu depending on your screen size), and choose **Register as hub site**, as shown in *Figure 8.24*.

Active sites

Use this page to sort and filter sites and change site settings

[Learn more about managing sites](#)

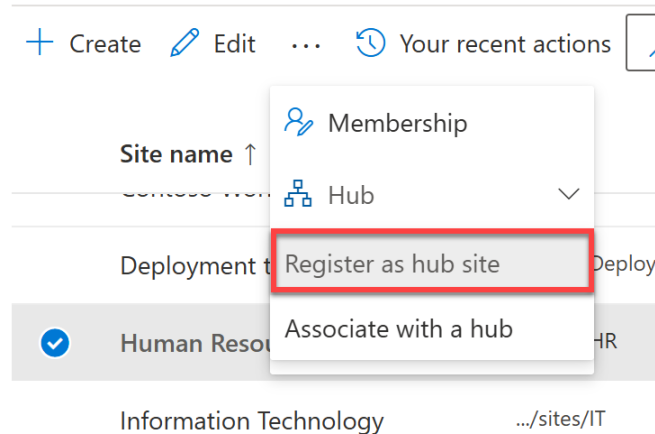


Figure 8.24 – Register as hub site option for a selected site

4. In the **Register as hub site** pane, enter a display name for the hub site. By default, this will be the same as the site's name. Optionally, you can also specify individuals who are allowed to associate sites with this hub. This enables site owners to easily connect their sites to the hub site, allowing them to inherit the hub's branding and navigation, and display their site's content in the hub site's supported web parts.
5. Select **Save**. The site is now designated as a hub site.
6. To associate other sites with the new hub site, go back to the **Sites | Active sites** list.

7. Select the site(s) you want to associate with the hub site. Then do the following:
- A. For a single selected site, select **Hub** from the top menu, and choose **Associate with a hub**.
 - B. For multiple selected sites, select **Bulk edit**, then **Hub association**, as shown in *Figure 8.25*.

Active sites

Use this page to sort and filter sites and change site settings.
[Learn more about managing sites](#)

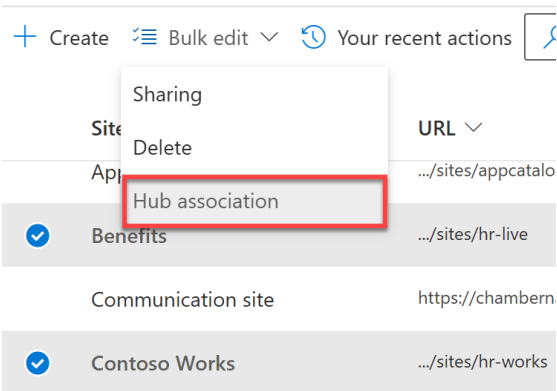


Figure 8.25 – Bulk site association with a hub

8. In the **Edit hub association** pane, select the hub site you created earlier in this recipe from the drop-down list.
9. Select **Save**. The selected sites are now associated with the hub site, inheriting its navigation and branding, and contributing their content to any web parts funneling connected sites' contents.

How it works...

Hub sites play a critical role in organizing and managing site collections by linking them into a cohesive network. Unlike traditional hierarchical subsites, hubs facilitate a flat structure, allowing for more flexibility and scalability. Hub sites offer several key benefits that enhance the overall SharePoint experience, particularly in areas such as navigation, search, security, and branding:

- **Navigation:** When you register a site as a hub site, it becomes the central point for organizing and managing related sites. Associating other sites with this hub site allows them to inherit the hub site's navigation, making it easier for users to navigate between related sites. This approach is particularly useful for departments or project teams that need a centralized way to manage and access their sites. You could consider using the hub navigation menu to list all sites connected within the hub so that no matter which site a user finds themselves on, they can move throughout the hub seamlessly with the consistent navigation menu.

- **Search:** One of the most significant advantages of using hub sites is the ability to roll up search results across all associated sites. When users search within a hub site, the results include relevant content from all sites connected to that hub. This improves content discoverability and allows users to find the information they need more quickly and efficiently, without having to navigate through multiple sites individually or change the search scope.
- **Security:** Hub sites also contribute to more streamlined security management. While each site associated with a hub maintains its own unique permissions, hub sites allow for centralized management of site settings and policies. This means that administrators can enforce consistent security practices across all associated sites, reducing the risk of security gaps and ensuring compliance with organizational standards. Additionally, when a site is associated with a hub, it can inherit classification labels, which further align with the organization's security and compliance policies.
- **Branding:** Consistent branding across SharePoint sites is essential for reinforcing the organization's identity and ensuring a unified user experience. Hub sites enable administrators to apply a consistent look and feel across all associated sites. This includes shared themes, logos, and navigation elements. Changes made to the branding of the hub site are automatically propagated to all associated sites, ensuring uniformity without the need for manual updates on each individual site. This not only saves time but also ensures that all sites reflect the organization's current branding guidelines.

By grouping related sites based on projects, departments, or other organizational units, hubs enhance content discoverability, governance, and overall user experience. This modern approach aligns with the needs of dynamic and responsive digital workplaces, supporting efficient collaboration and communication across the organization.

There's more...

To edit your hub site's navigation (the menu that is inherited by associated sites), you must go to the hub site (not an associated site). If no links have yet been added to the hub navigation, you'll see a link in the hub navigation menu to **Add link**. Otherwise, once a link has been added, you'll see an **Edit** link, as shown in *Figure 8.26*.

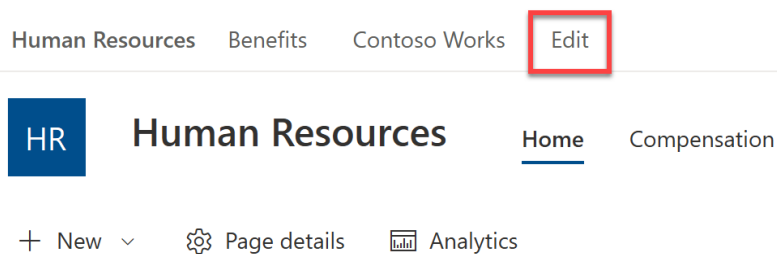


Figure 8.26 – Hub navigation Edit option

Any changes made at the top (hub) level's hub navigation menu will be reflected on all associated sites. The individual site navigation menus, however, remain unique to each site.

To edit the hub's (and associated sites') branding, choose the settings wheel from the hub's upper-right corner, then **Change the look**. Any changes saved here will appear on all associated sites as well.

See also

- *Planning your SharePoint hub sites*: <https://learn.microsoft.com/en-us/sharepoint/planning-hub-sites>

Restricting access by IP address

In this recipe, you will learn how to set up IP address restrictions to ensure that only specified IP addresses can access your organization's SharePoint and OneDrive content. This security measure is important for organizations that want to limit access to their intranet or user content to employees from specific locations, thereby protecting sensitive corporate data from unauthorized external access.


Getting ready

In order to follow the steps in this recipe, you must be either a Global or SharePoint Administrator.

How to do it...

1. Access the SharePoint admin center by logging in to the Microsoft 365 admin center at <https://admin.microsoft.com>. On the left navigation menu, under **Admin centers**, find and select **SharePoint**.
2. Select **Policies | Access control** on the left navigation menu.
3. Select **Network location**.
4. Enable the **Allow access only from specific IP address ranges** setting, then enter the desired IP addresses and ranges separated by commas, as shown in *Figure 8.27*.

Network location

 Make sure your IP address is included in the ranges you enter so you don't lock yourself out.

Use this setting to allow access only from IP addresses that your organization owns.

[Learn more about controlling access based on network location](#)

Allow access only from specific IP address ranges

 On

Enter IP addresses or ranges

Examples: 172.16.0.0, 192.168.1.0/27, 2001:4898:80e8::0/48

172.16.0.0, 192.168.1.0/27, 2001:4898:80e8::0/48

Figure 8.27 – Network location setting

Important note

Be sure to include your own IP address to prevent locking yourself out.

5. Select **Save**.

How it works...

Restricting access to SharePoint and OneDrive for Business to specific IP addresses enhances security by ensuring that users can only access corporate data from secure, approved locations, such as physical office premises. If a user tries to access SharePoint or OneDrive for Business from an unauthorized IP address, they will receive an **Access restricted** error message, indicating that their current network location is not permitted due to organizational policy.

This setting is important for organizations that need to protect sensitive data from unauthorized access, particularly when employees might connect from insecure networks. By configuring IP-based access restrictions, organizations can prevent potential cyber threats from untrusted or unknown networks, thereby strengthening their overall data security framework.

There's more...

To configure IP address restrictions via PowerShell, follow these steps:

1. Open **SharePoint Online Management Shell** from your start menu as an administrator.
2. Run the following to sign in to the administrator account you wish to use, being sure to replace the tenant URL with your own:

```
Connect-SPOService -Url https://natechamberlain-admin.  
sharepoint.com
```

3. Run the `Set-SPOTenant` command with the `-IPAddressAllowList` parameter as follows, replacing the fictional IP addresses with your actual IP addresses:

```
Set-SPOTenant -IPAddressAllowList "192.168.1.1, 10.0.0.2,  
172.16.0.3" -IPAddressEnforcement $true
```

See also

- *Control access to SharePoint and OneDrive data based on network location:* <https://learn.microsoft.com/en-us/sharepoint/control-access-based-on-network-location>

Managing Microsoft Teams

Managing Microsoft Teams effectively ensures seamless and secure collaboration and communication within your organization. This chapter provides guidance on how to manage various aspects of Microsoft Teams, from creating teams and policies to configuring settings for meetings, town halls, and messaging. We will also cover how to apply these policies to specific users, manage external and guest access, and review the ownership of teams. By the end of this chapter, you will have the knowledge to optimize your Teams environment to suit your organization's needs.

We will cover the following recipes in this chapter:

- Creating a team
- Creating a Team policy
- Configuring meeting settings
- Creating a Meeting policy
- Creating an Events policy
- Creating a Messaging policy
- Applying a policy (Team/Meeting/Messaging) to specific users
- Configuring Teams setup policies
- Configuring external access
- Configuring guest access
- Reviewing all teams and their owners

Technical requirements

To create and manage teams, policies, and settings, you must have the Global Administrator or Teams Administrator role. Ensure your organization’s Microsoft 365 subscription includes Teams services, as this is crucial for accessing the necessary functionalities. Note that some features you may find throughout the Microsoft Teams admin center may be disabled if they require Teams Premium licensing and you are not currently assigned a Teams Premium license.

Creating a team

Creating a team in Microsoft Teams is fundamental to organizing and facilitating collaboration within your organization. Teams provide a centralized space where groups can communicate in real time, share files, and work together on projects.

Getting ready

In order to follow the steps in this recipe, you must be either a Global Administrator or Teams Administrator.

How to do it...

1. From the Microsoft Teams admin center (<https://admin.teams.microsoft.com>), select **Teams** | **Manage teams** from the left navigation menu. Once there, select **Add**, as shown in *Figure 9.1*.

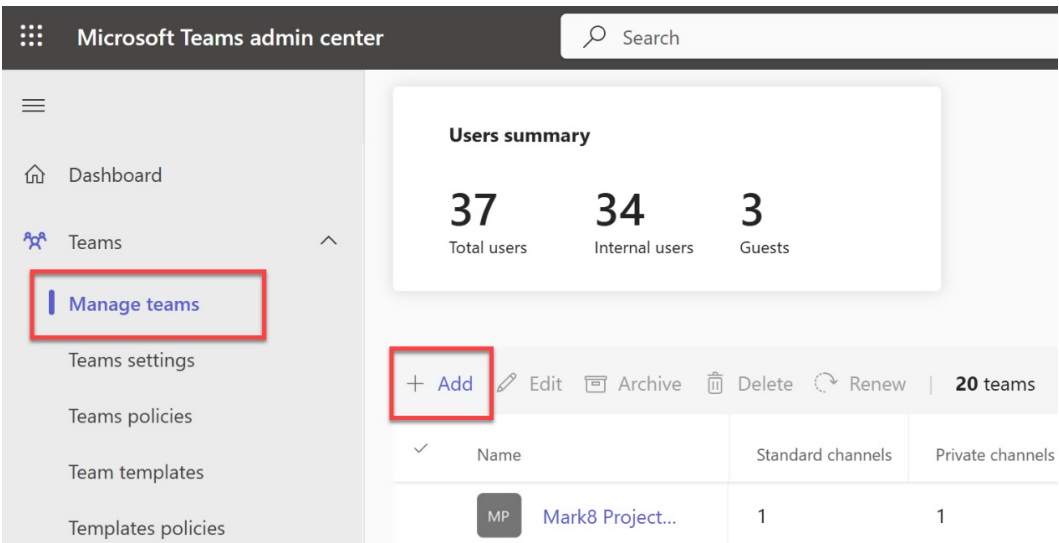


Figure 9.1 – Steps to add a new team via the Microsoft Teams admin center

2. In the side panel that floats in from the right, enter the new team's **Name**, **Description**, **Team owners**, **Sensitivity** (if you've implemented sensitivity labels in your organization), and **Privacy** level details.
3. Once you've configured the new team's details, select **Apply**.

How it works...

Creating a team in Microsoft Teams involves setting up a dedicated workspace where team members can collaborate, share files, and communicate in real time. When you create a team, you also create an associated Microsoft 365 group, which provides the underlying permissions and shared resources, such as a group mailbox and calendar in Exchange, a site in SharePoint, and a notebook in OneNote.

Tip

The terms *team* and *group* are sometimes used interchangeably, but *team* always refers to the Microsoft Teams-oriented usage of the group, whereas a *group* doesn't necessarily have an associated team (such as security groups).

When creating the team, you specify the team's **Name** and **Description** details, and the **Privacy** level (**Public** or **Private**). It's important to understand the implications of these **Privacy** settings:

- **Public:** Anyone in your organization can join the team. This setting will automatically add all users except guests to the associated SharePoint site's Members group, which exposes all content saved on the site in search results by default.
- **Private:** Only team owners can add members to the team, which helps prevent accidental oversharing of sensitive content.

Teams are divided into *channels*, which can be **Standard** (accessible to all team members), **Private** (restricted to a subset of team members), or **Shared** (an individual channel that can be shared across teams inside and outside your organization without sharing the team's other resources). Channels organize conversations and files around specific topics or projects, enhancing collaboration and focus.

Important note

When a team is created, a SharePoint site is automatically created to store the team's files. The SharePoint site is secured by the Microsoft 365 group associated with the team.

After creating a team, you can customize settings such as member permissions and roles, team pictures, and tabs within the channels. Tabs allow you to integrate first- and third-party services and custom applications directly into the team interface, providing quick access to essential tools and information.

Team owners can manage membership, settings, and permissions independently (without IT support) and continuously adapt to changing team dynamics and requirements. This flexibility ensures that teams remain effective and aligned with organizational goals, while not adding additional administrative burdens on IT staff.

There's more...

Once you've created a team, you can still change its name, privacy level, and even the Microsoft 365 group name later without using PowerShell. However, to change the Microsoft 365 group email address, you'll need to use PowerShell. To do so, first install the ExchangeOnline PowerShell module if you haven't already by running `Install-Module -Name ExchangeOnlineManagement`.

After installing the module, connect to Exchange Online using the following command, replacing `user@domain.com` with your actual **User Principal Name (UPN)**:

```
Connect-ExchangeOnline -UserPrincipalName user@domain.com.
```

To add an email alias for the team that is different from the original email address, run the following command, updating the parameters with your specific email addresses:

```
Set-UnifiedGroup -Identity "old@mydomain.com" -EmailAddresses @  
{remove="SMTP:old@mydomain.com";add="SMTP:new@mydomain.com","smtp:old@  
mydomain.com"}
```

Tip

After running this command, the change will be reflected when viewing the Microsoft 365 group details in the admin center. However, if you check the team itself, only the original email address will be visible. This might be confusing because the alias isn't shown directly in the Teams interface. To verify that the alias has been successfully added, you need to check the email addresses associated with the Microsoft 365 group directly in the admin center or by using a PowerShell command such as `Get-UnifiedGroup` to view all associated email addresses.

See also

- *Introduction to Microsoft Teams for admins*: <https://learn.microsoft.com/en-us/microsoftteams/teams-overview>
- *Manage teams in the Microsoft Teams admin center*: <https://learn.microsoft.com/en-us/microsoftteams/manage-teams-in-modern-portal>

Creating a Team policy

Creating a Team policy in Microsoft Teams allows administrators to customize and manage how teams and channels are used within an organization. This is essential for maintaining security, compliance, and governance. With team policies, you can control the creation of private channels, restrict who can discover teams, and set other permissions to align with organizational standards.

Getting ready

In order to follow the steps in this recipe, you must be either a Global Administrator or Teams Administrator.

How to do it...

1. From the Microsoft Teams admin center (<https://admin.teams.microsoft.com>), select **Teams** | **Teams policies** from the left navigation menu, as shown in *Figure 9.2*.

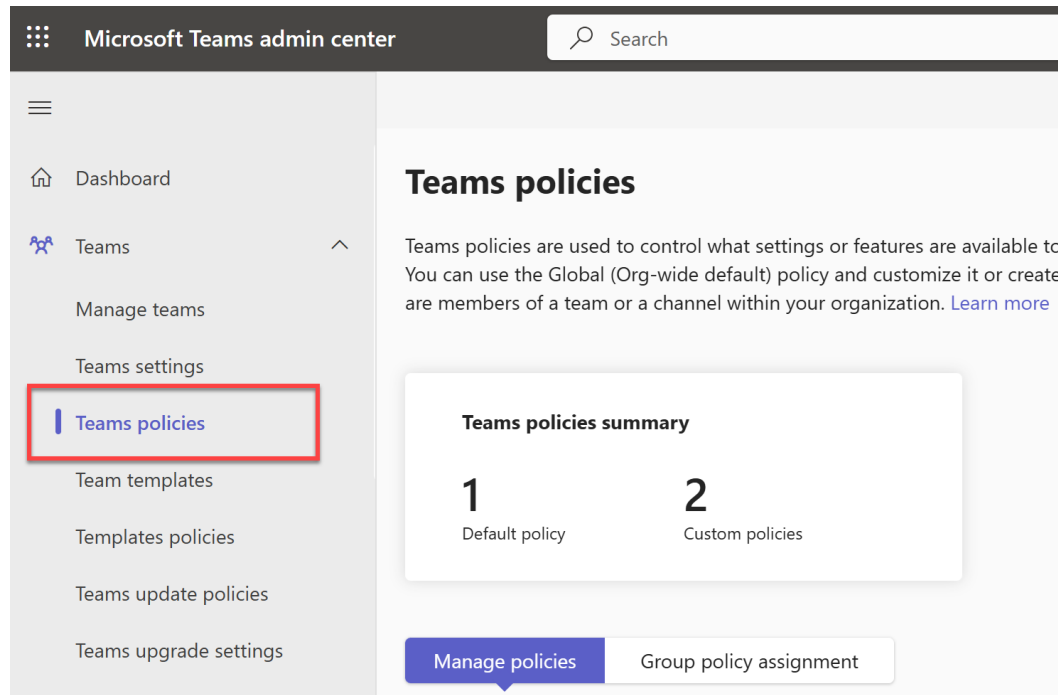
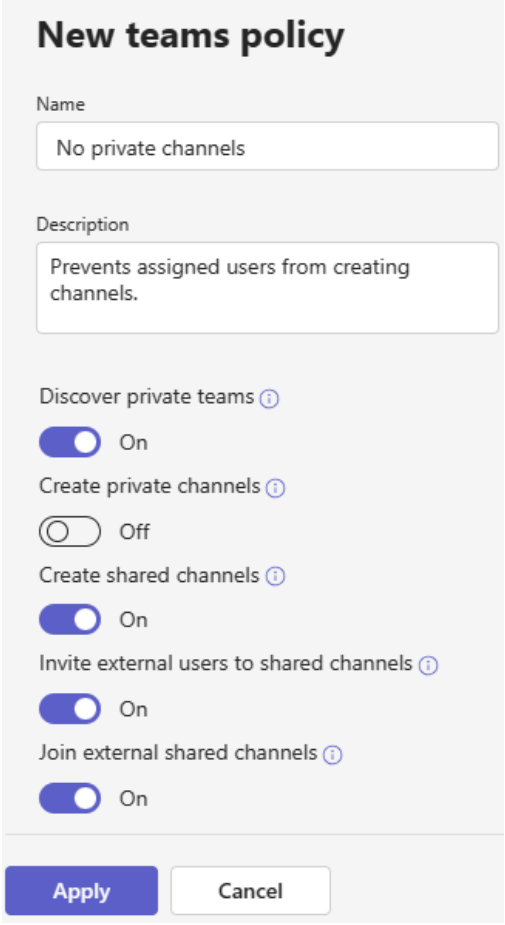


Figure 9.2 – Location of Teams policies in the Microsoft Teams admin center

2. Select the **Add** button to create a new policy.
3. Provide a clear name and description for the policy such as *No private channels*.

4. Configure the settings to specify whether users can create private or shared channels, discover private teams, invite external users to shared channels, or join external shared channels, as shown in *Figure 9.3*.



New teams policy

Name

No private channels

Description

Prevents assigned users from creating channels.

Discover private teams ⓘ

☒ On

Create private channels ⓘ

☐ Off

Create shared channels ⓘ

☒ On

Invite external users to shared channels ⓘ

☒ On

Join external shared channels ⓘ

☒ On

Apply Cancel

Figure 9.3 – Options for a new Teams policy

5. Select **Apply** to save the policy.

How it works...

Team policies in Microsoft Teams allow administrators to enforce rules and settings that manage how teams and channels operate. By creating custom policies, you can ensure that only authorized users have access to specific features, such as creating private channels or discovering teams. These policies help maintain security and governance within your organization. Changes to policies can take up to 24 hours to take effect, and users will receive notifications if they attempt to perform restricted actions.

There's more...

In addition to managing private channels and team discovery, team policies can also be configured using PowerShell. To manage team policies using PowerShell, you'll first need to ensure that you have the required Teams PowerShell module installed. Here's how you can install it: `Install-Module -Name MicrosoftTeams`.

Once installed, connect by running `Connect-MicrosoftTeams`.

Once connected, you can use the `New-CsTeamsChannelsPolicy` command to create a new Teams channels policy. For example, to create a policy that restricts the creation of private channels, you would use the following:

```
New-CsTeamsChannelsPolicy -Identity RestrictPrivateChannels  
-AllowPrivateChannelCreation $false
```

This command prevents users assigned to the policy from creating private channels within Teams, making it useful for organizations that want to control how private channels are used.

See also

- *Manage channel policies in Microsoft Teams*: <https://learn.microsoft.com/en-US/microsoftteams/teams-policies>

Configuring meeting settings

Configuring meeting settings in Microsoft Teams involves setting up options that dictate the behavior and functionality of meetings for all users in your organization. This includes settings for audio, video, content sharing, and participant management.

Important note

In the Teams admin center, settings apply to all users and cannot be customized for individual users or groups. After configuring these baseline settings, you can use policies such as those described in the previous recipe to further modify abilities and experiences for specific users or groups, allowing for more tailored control within the organization.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or Teams Administrator.

How to do it...

1. From the Microsoft Teams admin center (<https://admin.teams.microsoft.com>), select **Meetings | Meeting settings** from the left navigation menu.
2. Specify your preferences for each of the following settings, some of which are shown in *Figure 9.4*:

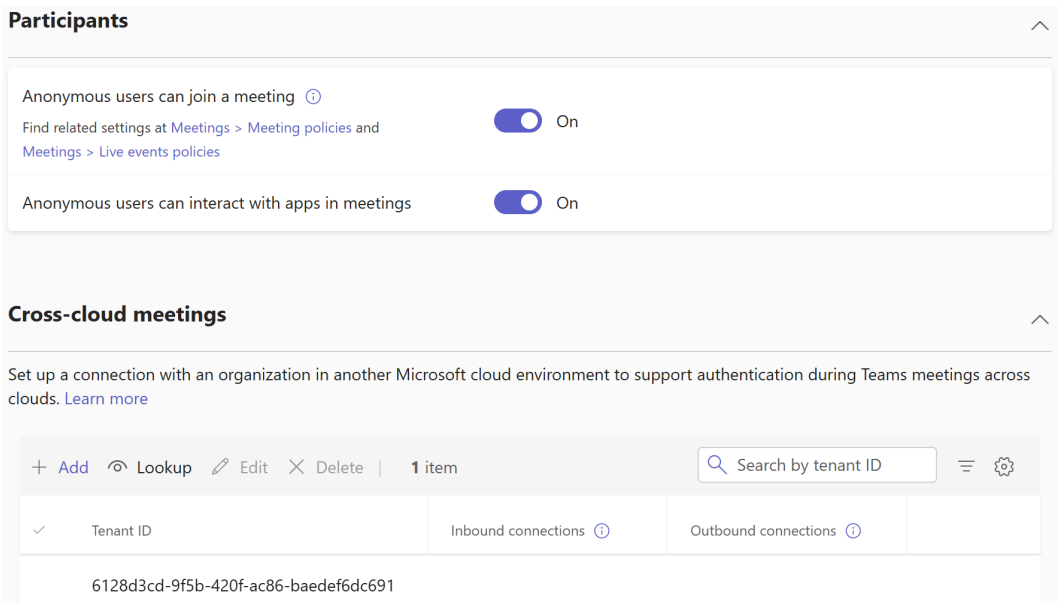


Figure 9.4 – Meeting settings

- **Anonymous users can join a meeting:** Toggle **On** or **Off** to allow or disallow anonymous users from joining your meetings
- **Anonymous users can interact with apps in meetings:** Toggle **On** or **Off** to permit anonymous users to interact with apps during meetings
- **Cross-cloud meetings:** Configure connections with another Microsoft cloud environment to support authentication during Teams meetings across clouds
- **Logo URL:** Enter a hyperlink to a logo that will appear in meeting invitations
- **Privacy and security URL:** Enter a hyperlink to a legal disclaimer or policy
- **Help URL:** Enter a hyperlink to a help or support page that will appear in meeting invitations
- **Footer:** Add custom text to the footer of meeting invitations
- **Insert Quality of Service (QoS) markers for real-time media traffic:** Toggle **On** or **Off** to enable or disable QoS markers

- **Select a port range for each type of real-time media traffic:** You can select **Specify port ranges** to set the port ranges or select **Automatically use any available ports** for different types of real-time media traffic including audio, video, and screen sharing

3. Select **Save** to save your changes to the settings.

How it works...

Most of these settings are straightforward, but **Cross-cloud meetings** is a newer section. With **Cross-cloud meetings** settings, administrators can set up a connection with another Microsoft cloud environment to support authentication during Teams meetings across clouds. For example, you can manage inbound and outbound connections and configure settings for specific environments such as Microsoft Azure Government and Microsoft Azure China. Changing these settings affects all collaboration with organizations from this cloud, including guest user access and authentication.

In the **Email invitation** section, select **Preview invite** to see how recipients will view the invitation, including any changes you've made to URLs and footer content. This preview helps ensure that your customizations appear correctly in the actual email invitations.

By configuring these meeting settings, you can ensure that your organization's Teams meetings are tailored to meet specific needs and compliance requirements. These settings help manage participant access, customize meeting invitations, and optimize network performance for real-time media traffic.

There's more...

For further customization and control over meeting experiences, explore the use of meeting policies in the Teams admin center to customize abilities on a user or group basis.

See also

- *Teams settings and policies reference:* <https://learn.microsoft.com/en-us/microsoftteams/settings-policies-reference#meetings>

Creating a Meeting policy

Configuring meeting settings in Microsoft Teams involves setting up options that dictate the behavior and functionality of meetings. This includes settings for audio, video, content sharing, and participant management.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or Teams Administrator.

How to do it...

1. From the Microsoft Teams admin center (<https://admin.teams.microsoft.com>), select **Meetings | Meeting policies** from the left navigation menu.
2. Select **Add** to create a new policy.
3. Enter a name and description for the policy.
4. Configure the settings based on your requirements. These settings include the following:
 - **Meeting scheduling:** Control options such as **Meet now**, **Outlook add-in**, and permissions for scheduling private and channel meetings, as shown in *Figure 9.5*

Meeting scheduling

Meeting scheduling settings let you control how users can set up and attend meetings. [Learn more about meeting scheduling settings](#)

Private meeting scheduling	<input checked="" type="checkbox"/> On
Find related settings at Voice > Calling policies	
Meet now in private meetings	<input checked="" type="checkbox"/> On
Channel meeting scheduling	<input checked="" type="checkbox"/> On
Meet now in channel meetings	<input checked="" type="checkbox"/> On
Outlook add-in	<input checked="" type="checkbox"/> On
Meeting registration ⓘ	<input checked="" type="checkbox"/> On
Who can register ⓘ	<div>Everyone</div>
Attendance and engagement report ⓘ	<div>On, but organizers can turn it off</div>
Include attendees in the report ⓘ	<div>Yes, but attendees can opt out</div>
Attendee information ⓘ	<div>Show everything</div>

Figure 9.5 – Meeting scheduling section of a Meeting policy

- **Meeting join & lobby:** Manage who can join meetings directly, who must wait in the lobby, and settings for anonymous users
- **Meeting engagement:** Configure features to enhance participant interaction, such as in-meeting chat, reactions, and Q&A
- **Content sharing:** Specify what content can be shared during meetings, including screen sharing, PowerPoint, Whiteboard, and collaborative annotations

- **Content protection** (Teams Premium only): Protect shared content with options such as watermarking videos and shared content
- **Recording & transcription**: Control settings for recording and transcribing meetings, including storage and expiration options
- **Audio & video**: Determine the audio and video capabilities of users, including IP audio/video modes and media bit rate

5. Select **Save** to apply the policy.

How it works...

Meeting policies help manage meeting join and engagement experiences including the features available during meetings, such as who can share their screen, use video, or access meeting notes. By configuring these settings, you can tailor the meeting experience to suit your organization's needs. The policy applied to a meeting will depend on both the organizer's and the participants' policies, with the most restrictive settings taking precedence.

There's more...

You can also manage these policies using PowerShell. First, you'll need to ensure that you have the required Teams PowerShell module installed by running the following:

```
Install-Module -Name MicrosoftTeams
```

Once installed, connect by running `Connect-MicrosoftTeams`.

Then, you can manage meeting policies with commands such as `Set-CsTeamsMeetingPolicy` to configure settings such as `AllowPrivateMeetNow`, `ScreenSharingMode`, and `AllowWhiteboard`. Additionally, reviewing the global (org-wide default) policy ensures it covers the majority of users, reducing the need for individual assignments.

See also

- *Teams settings and policies reference*: <https://learn.microsoft.com/en-us/microsoftteams/settings-policies-reference#meetings>
- *Manage Teams with policies*: <https://learn.microsoft.com/en-us/microsoftteams/manage-teams-with-policies>
- *Set-CsTeamsMeetingPolicy*: <https://learn.microsoft.com/en-us/powershell/module/teams/set-csteamsmeetingpolicy>

Creating an Events policy

Events policies in Microsoft Teams control the features that users can utilize during webinars and town hall events. Each user can have only one policy per policy type at any time. If a user belongs to multiple groups with different policies, the policy ranking determines which one applies.

Getting ready

In order to follow the steps in this recipe, you must be either a Global Administrator or Teams Administrator.

How to do it...

1. From the Microsoft Teams admin center (<https://admin.teams.microsoft.com>), select **Meetings | Events policies** from the left navigation menu.
2. Select **Add** to create a new Events policy.
3. Enter a name and description for the policy.
4. Configure the following settings shown in *Figure 9.6*:
 - **Webinars**: Toggle to enable or disable webinars
 - **Who can attend webinars**: Choose who can attend (e.g., everyone or only internal users)
 - **Town halls**: Toggle to enable or disable town halls
 - **Customize event emails**: Allow or disallow the customization of event emails
 - **Webinar registration form questions**: Select the type of questions (required only, standard and required, or custom)
 - **Allowed webinar types for recordings**: Set allowed recording types (not allowed, invite only, organization-wide, or public)
 - **Allowed town hall types for recordings**: Set allowed recording types (not allowed, invite only, organization-wide, or public)
 - **Use Microsoft ECDN**: Enable or disable Microsoft ECDN to optimize bandwidth usage
 - **Townhall Chat Experience**: Choose the chat experience (none or optimized)

Webinars	<input checked="" type="checkbox"/> On
Who can attend webinars	Everyone ▼
Town halls	<input checked="" type="checkbox"/> On
Customize event emails	<input checked="" type="checkbox"/> On
Webinar registration form questions	Custom, standard, and required ▼
Allowed webinar types for recordings	Public ▼
Allowed town hall types for recordings	Public ▼
Use Microsoft ECDN	<input checked="" type="checkbox"/> On
Townhall Chat Experience	Optimized ▼

Figure 9.6 – Events policy settings

5. Select **Save** to create the policy.

How it works...

By default, a global Events policy is applied to all users in your tenant. Creating additional policies allows you to tailor event experiences for different users or groups. Users without a custom policy assigned remain under the global policy.

Events policies help manage the following:

- The availability and features of webinars and town halls
- Attendee permissions and registration form requirements
- Customization of event-related emails
- Rules for event recordings
- Network optimization during events

Important note

Some advanced event features in Microsoft Teams, such as increased attendee limits, increased concurrent events, and live translation options, are only available with a **Teams Premium** license. Without Teams Premium, town halls are limited to 10,000 attendees, 15 concurrent events, and live translation in 6 languages. With Teams Premium, these limits increase to 20,000 attendees, 50 concurrent events, and live translation in 10 languages. Teams Premium is an add-on license that enhances the capabilities of Teams by offering features such as advanced meeting customization, enhanced security options, and rich analytics.

There's more...

You can also use `MicrosoftTeams` PowerShell module cmdlets to create and manage Events policies. For example, use the following to create a new Events policy:

```
New-CsTeamsEventsPolicy -Identity "NewEventsPolicy" -AllowWebinars  
Enabled -AllowTownHalls Enabled
```

To assign a policy to a user (replace `user@domain.com` with a valid address), use this one:

```
Grant-CsTeamsEventsPolicy -Identity user@domain.com -PolicyName  
"NewEventsPolicy"
```

See also

- *Manage who can schedule webinars in Microsoft Teams:* <https://learn.microsoft.com/en-US/microsoftteams/set-up-webinars>

Creating a Messaging policy

Messaging policies allow Teams Administrators to indicate which messaging features team owners and members are allowed to use. For example, you may wish to prevent the deletion of sent messages for a specific group of users. As with other Teams policies, there's a default/global policy that applies to all users. You can create a custom Messaging policy that applies to specific users, while the remaining (unassigned) users adhere to the default policy. This recipe guides you through creating a custom Messaging policy to apply to specific users, restricting their abilities when it comes to messaging in channels and chats.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or Teams Administrator.

How to do it...

1. From the Microsoft Teams admin center (<https://admin.teams.microsoft.com>), select **Messaging | Messaging policies** from the left navigation menu.
2. Select **Add** at the top of the **Messaging policies** list.
3. Go through the list of settings and configure them according to the type of users this policy will apply to. For example, you might disallow the deletion of messages, restrict Giphy GIFs to strict content ratings, or toggle them off altogether. *Table 9.1* shows all the configuration possibilities for a Messaging policy.

Setting	Options
Owners can delete sent messages	On or Off
Delete sent messages	On or Off
Delete chat	On or Off
Edit sent messages	On or Off
Read receipts	User controlled, Turned off for everyone, or Turned on for everyone
Upload custom emojis	On or Off
Delete custom emojis	On or Off
Chat	On or Off
Chat with groups	On or Off
Giphy in conversations	On or Off
Giphy content rating	Strict, Moderate, or No restriction
Memes in conversations	On or Off
Stickers in conversations	On or Off
URL previews	On or Off
Report inappropriate content	On or Off
Report a security concern	On or Off
Translate messages	On or Off
Immersive reader for messages	On or Off
Send urgent messages using priority notifications	On or Off
Create voice messages	Allowed in chats and channels, Allowed in chats only, or Not enabled
On mobile devices, display favorite channels above recent chats	Enabled or Not enabled
Remove users from group chats	On or Off

Setting	Options
Text predictions	On or Off
Suggested replies	On or Off
Chat permission role	Restricted permissions, Limited permissions, or Full permissions
Users with full chat permissions can delete any message	On or Off
Video messages	On or Off
Use Designer to create backgrounds and images	Enabled or Not enabled

Table 9.1 – Configurable options for each Messaging policy

4. After configuring the settings, select **Save**.

Note

To delete a Messaging policy, you must first reassign all users currently assigned to it to a different policy.

How it works...

In this recipe, you created a custom Messaging policy that restricts assigned users from utilizing certain features in Teams chat messages and channel conversations. Any user not assigned one of your custom policies will default to the global policy.

There’s more...

For administrators who prefer automation or need to manage a large number of policies and users, PowerShell can be a powerful tool. The Microsoft Teams PowerShell module allows you to create and manage Messaging policies programmatically. To install the module and connect to Microsoft Teams, run the following:

```
Install-Module -Name MicrosoftTeams -Force -AllowClobber
$credential = Get-Credential
Connect-MicrosoftTeams -Credential $credential
```

Then, to create a new Messaging policy, run something like the following:

```
New-CsTeamsMessagingPolicy -Identity "CustomPolicy" -AllowUserChat
$true -AllowOwnerDeleteMessage $false -GiphyRatingType STRICT
```

See also

- *Manage Messaging policies in Teams*: <https://learn.microsoft.com/en-US/microsoftteams/messaging-policies-in-teams>

Applying a policy (Team/Meeting/Messaging) to specific users

Once a policy is created in Microsoft Teams, it must be applied to specific users to ensure the policy takes effect. This recipe guides you through the process of assigning a Teams, Meeting, or Messaging policy to specific users in your organization.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or Teams Administrator.

How to do it...

1. Access the Microsoft Teams admin center at <https://admin.teams.microsoft.com>.
2. Depending on the type of policy you wish to assign, select its screen from the left-hand navigation menu:
 - **Teams** | **Teams Policies** for channel-related policies
 - **Meetings** | **Meeting Policies** for meeting-related policies
 - **Messaging** | **Messaging Policies** for messaging-related policies
3. In the policy list, select the bubble next to the policy you want to assign to users, as shown in *Figure 9.7*. This will highlight the policy and display its details.

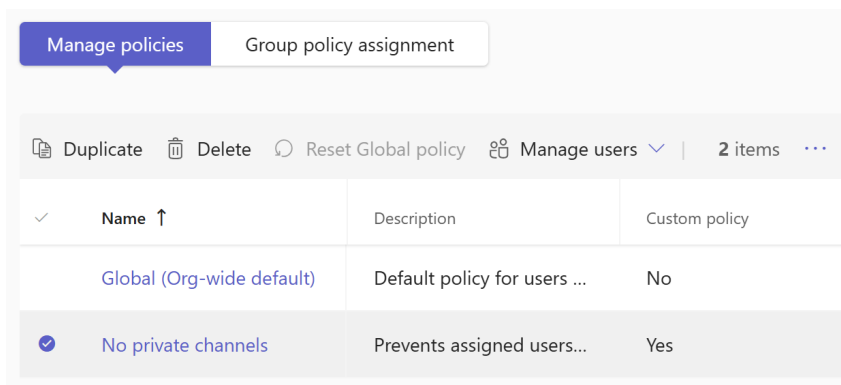


Figure 9.7 – A policy selected by selecting the bubble to the left of its name

4. With the policy selected, select **Manage users** and then **Assign users**.
5. In the search dialog, enter the names or email addresses of the users or groups to whom you want to apply the policy. You can add multiple users or groups at once.
6. Select the users or groups from the search results and select **Add**.
7. After adding the users or groups, select **Apply** to assign the policy to the selected users or groups.

How it works...

By following these steps, you assign a specific Teams, Meeting, or Messaging policy to selected users or groups. This ensures that the settings defined in the policy are enforced for those users or groups, providing a customized experience based on their roles or needs. Users or groups not assigned a custom policy will fall back on the global/default policy.

There's more...

To assign multiple policies to larger batches of users, you can navigate to the Microsoft Teams admin center, then select **Users | Manage users** from the left navigation menu. Here, you can use the checkmark above the selection column to select all users or you can filter/search as needed to select a larger group of users for whom you'll be adjusting policy settings. When you're ready to bulk-assign policies, select **Edit settings**, as shown in *Figure 9.8*:

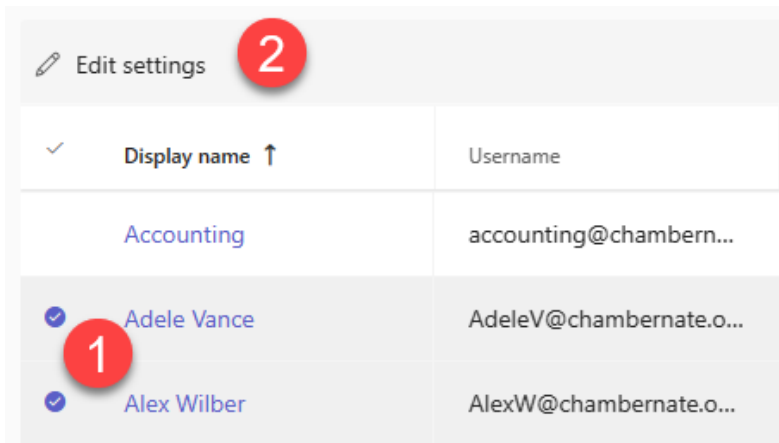


Figure 9.8 – Initial steps to multi-select and assign multiple policies to selected users

If you're not changing a specific policy type for the selected users, leave it as **Keep existing policy**. Otherwise, choose the policy to overwrite the currently effective policy for the effective users. When finished, select **Apply**. These steps are illustrated in *Figure 9.9*.

The screenshot shows a web interface titled "Edit settings". Below the title is a descriptive sentence: "You can assign these policies to one or more people in your organization at the same time." followed by a blue link "Learn more". A section header "Policies" is followed by a list of policy types, each with a dropdown menu. The policies and their current selections are: Call hold policy (Global (Org-wide default)), Voicemail policy (Keep existing policy), Meeting policy (RestrictedAnonymousAccess), Audio Conferencing policy (Global (Org-wide default)), Messaging policy (Demo messaging policy), Events policy (Keep existing policy), and Live events policy (empty). At the bottom are two buttons: "Apply" (blue) and "Cancel" (white).

Edit settings

You can assign these policies to one or more people in your organization at the same time.
[Learn more](#)

Policies

- Call hold policy
Global (Org-wide default)
- Voicemail policy
Keep existing policy
- Meeting policy
RestrictedAnonymousAccess
- Audio Conferencing policy
Global (Org-wide default)
- Messaging policy
Demo messaging policy
- Events policy
Keep existing policy
- Live events policy

Apply Cancel

Figure 9.9 – Bulk policy assignment for selected users

In the event that a user is part of multiple groups that each have policies assigned to them, you can configure the rank for policies under **Group Policy Assignment** on the **Messaging policies** page of the Microsoft Teams admin center. As seen in the following screenshot, you'd select a group, enter a numeric rank, and select the policy assigned to that group:

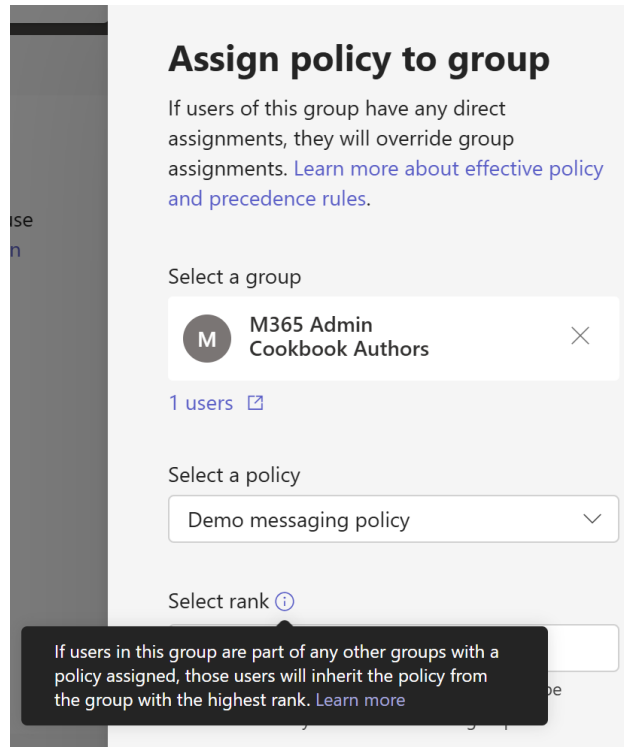


Figure 9.10 – Side panel for assigning a policy and its rank to members of a specific group

In some cases, the Microsoft Teams admin center may prove too hands-on for large-scale operations. In those circumstances, we turn to PowerShell.

Using the `MicrosoftTeams` PowerShell module, you can assign Messaging policies to one or more users using the `Grant-CsTeamsMessagingPolicy` PowerShell cmdlet rather than the Microsoft Teams admin center. In many cases, this would be much more efficient. First, connect using `Connect-MicrosoftTeams`. Then, use the following:

- If assigning a Messaging policy to one user, you would use something like this (update the `Identity` and `PolicyName` values):

```
Grant-CsTeamsMessagingPolicy -Identity "Nate Chamberlain"
-PolicyName "IT Admin Policy"
```

- And if assigning a Messaging policy to many users, you might filter all users by department or another attribute. That PowerShell command would look like this (update values with your own):

```
Get-CsOnlineUser -Filter {Department -eq 'IT Administration'} |  
Grant-CsTeamsMessagingPolicy -PolicyName "IT Admin Policy"
```

You can also use the `MicrosoftTeams` PowerShell module's `New-CsBatchPolicyAssignmentOperation` cmdlet with the `-PolicyType TeamsMessagingPolicy` parameter and value to assign a Messaging policy to users in bulk. A batch can contain up to 5,000 users. The following example demonstrates how this might look, whereby users are referenced using **Session Initiation Protocol (SIP)** in an array (though it could also be a reference to a text file of SIPs or otherwise):

```
$users_ids = @("nate@natechamberlain.com","harry@natechamberlain.  
com","bertha@natechamberlain.com")  
New-CsBatchPolicyAssignmentOperation -PolicyType TeamsMessagingPolicy  
-PolicyName "IT Admin Policy" -Identity $users_ids -OperationName  
"Batch assign ITAdminPolicy"
```

Tip

Replace the `-PolicyName` parameter's value with `$null` to unassign a specified policy type for specified users. The affected users would then fall back to the global (org-wide default) policy.

Also in the `MicrosoftTeams` PowerShell module is the `New-CsGroupPolicyAssignment` cmdlet. This allows a policy to be assigned to a security group or members of a distribution list. Note that group policy assignment is only recommended for groups with no more than 50,000 users. In the following example, using the **human resources (HR)** department group's SIP, we use this cmdlet to assign an `AllOn` policy to its members:

```
New-CsGroupPolicyAssignment -GroupId hr@natechamberlain.com  
-PolicyType TeamsMeetingPolicy -PolicyName AllOn
```

Policy propagation isn't an instant process, and the higher the number of users that are being updated, the longer it will take. A best practice is to update policies during off-peak hours to speed up propagation.

See also

- *Manage Teams with policies*: <https://learn.microsoft.com/en-us/microsoftteams/manage-teams-with-policies>
- *Grant-CsTeamsMessagingPolicy*: <https://learn.microsoft.com/en-us/powershell/module/teams/grant-csteamsmessagingpolicy>
- *New-CsBatchPolicyAssignmentOperation*: <https://learn.microsoft.com/en-us/powershell/module/teams/new-csbatchpolicyassignmentoperation>

Configuring Teams setup policies

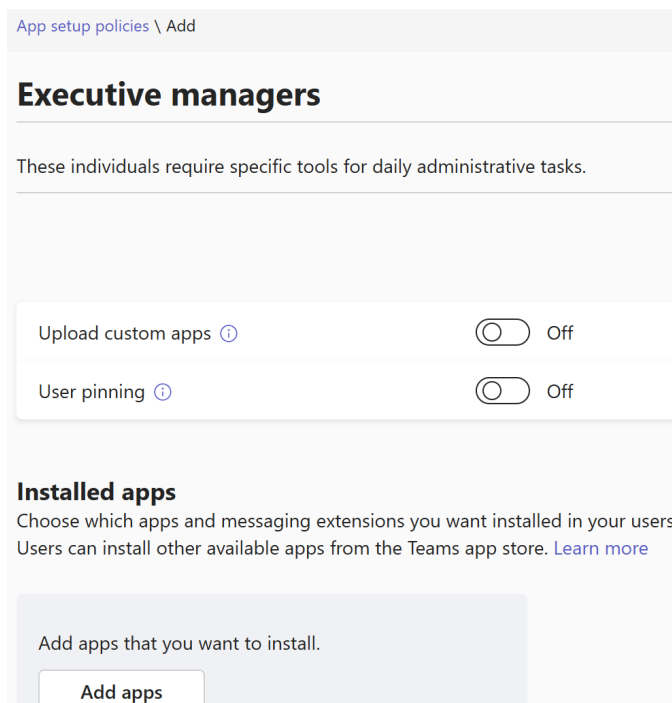
Microsoft Teams setup policies help ensure a consistent user experience and allow administrators to control how Teams apps are deployed, appear for users, and are used within the organization. This recipe will guide you through configuring Teams setup policies, enabling you to manage app availability and pinning for specific user groups.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or Teams Administrator.

How to do it...

1. From the Microsoft Teams admin center (<https://admin.teams.microsoft.com>), select **Teams apps** | **Setup policies** from the left navigation menu.
2. Select **Add** at the top of the policy list.
3. Provide a name and description for the new policy.
4. Toggle **Upload custom apps** and **User pinning** to **On** or **Off** according to your preferences for the target users and/or groups to be assigned this policy, as shown in *Figure 9.11*.



The screenshot displays the 'App setup policies \ Add' interface in the Microsoft Teams admin center. At the top, the breadcrumb 'App setup policies \ Add' is visible. Below it, the section 'Executive managers' is highlighted, with a subtitle stating 'These individuals require specific tools for daily administrative tasks.' Underneath this, there are two toggle switches: 'Upload custom apps' and 'User pinning', both currently set to 'Off'. Below these toggles, the 'Installed apps' section is visible, with a subtitle 'Choose which apps and messaging extensions you want installed in your users' and a link to 'Learn more'. At the bottom, there is a text input field with the placeholder 'Add apps that you want to install.' and a button labeled 'Add apps'.

Figure 9.11 – A new app setup policy

5. Under the **Installed apps** section, select **Add apps**. Then, search for the apps you want to include and select **Add**.
6. Under **Pinned apps**, arrange the apps in the order you want them to appear in the Teams client for the assigned users, as shown in *Figure 9.12*.

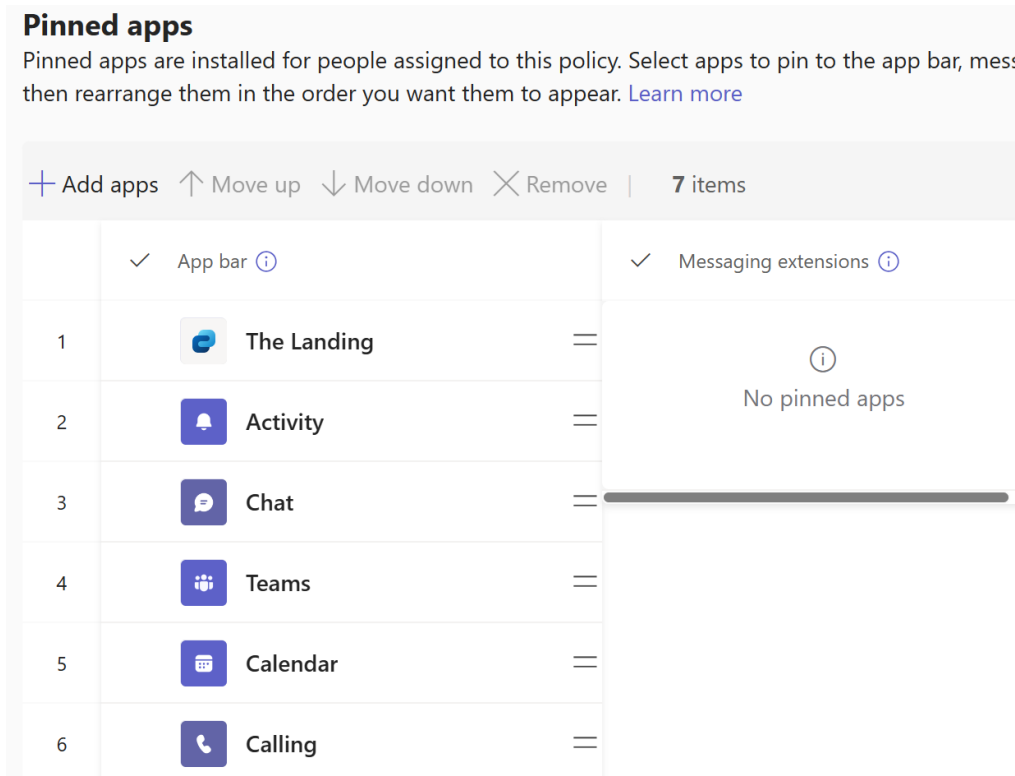


Figure 9.12 – The Pinned apps section of a new app setup policy

7. Once you have configured the settings, select **Save**.

How it works...

By creating and assigning app setup policies, administrators can control which apps are pinned and the order of their appearance in the Teams client. This helps drive the adoption of critical tools and ensures that users have quick access to the apps they need. For example, you may wish to pin project management apps for those who heavily rely on task and project management capabilities but may choose to only pin general resources such as Viva Connections and Shifts for other users.

There's more...

Administrators can use PowerShell to create and manage app setup policies programmatically, providing a more automated approach to policy management. First, you'll need to ensure that you have the required Teams PowerShell module installed by running the following:

```
Install-Module -Name MicrosoftTeams
```

Once installed, connect by running `Connect-MicrosoftTeams`.

An example of creating a new app setup policy uses the `New-CsTeamsAppSetupPolicy` cmdlet and is used as seen in the following:

```
New-CsTeamsAppSetupPolicy -Identity "CustomPolicy" -Description  
"Custom policy for specific users" -PinnedAppIds @("AppID1", "AppID2",  
"AppID3")
```

See also

- *Manage Teams with policies:* <https://learn.microsoft.com/en-us/microsoftteams/manage-teams-with-policies>
- *Use app setup policies to pin and auto install apps for users:* <https://learn.microsoft.com/en-us/microsoftteams/teams-app-setup-policies>
- *New-CsTeamsAppSetupPolicy:* <https://learn.microsoft.com/en-us/powershell/module/teams/new-csteamsappsetuppolicy>

Configuring external access

External access in Microsoft Teams allows users in your organization to communicate with users outside your organization using Teams. This feature is essential for facilitating collaboration with partners, clients, and other stakeholders who are not part of your internal teams. This recipe will guide you through setting up external collaboration settings for your organization.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or Teams Administrator.

How to do it...

1. Navigate to the Microsoft Teams admin center at <https://admin.teams.microsoft.com> and select **Users | External access**.

2. As seen in *Figure 9.13*, you must specify an allowed setting for **Teams and Skype for Business users in external organizations**:

- **Allow all external domains:** This setting enables unrestricted communication with users outside your organization, facilitating open collaboration with any external Teams users
- **Allow only specific external domains:** Tailor your external communications by permitting interactions exclusively with selected domains, such as those of partners, affiliates, or recently acquired companies
- **Block only specific external domains:** Implement this setting to specifically prohibit communications with certain domains, which could include competitors or entities posing a risk of data leakage
- **Block all external domains:** Opt for this setting to restrict your Teams users to communicating solely within your organization, effectively isolating your Teams environment from external entities

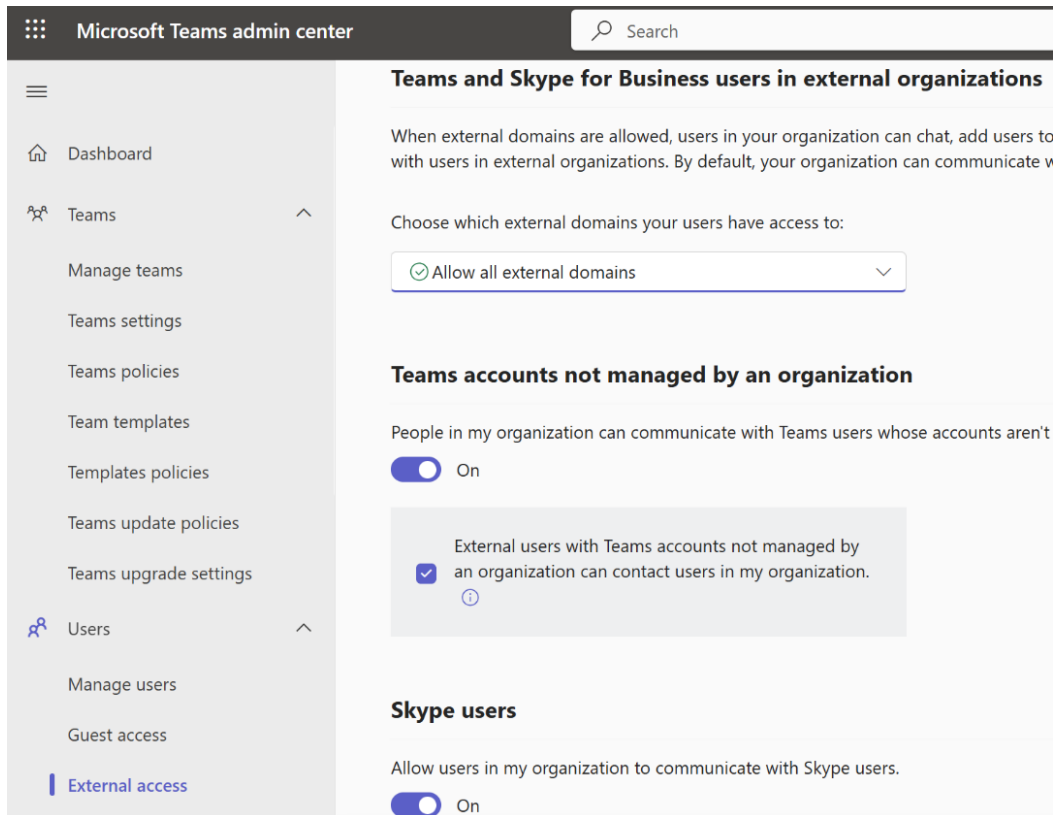


Figure 9.13 – External access settings in the Microsoft Teams admin center

3. For **Teams accounts not managed by an organization**, decide whether to allow your organization's users to find, call, chat, and arrange meetings with Teams users from unmanaged domains, and vice versa.
4. You can use **Skype users** to enable your users to connect with individuals using Skype, expanding the scope of your external communications to include Skype for Business and personal Skype accounts.
5. Select **Save**.

How it works...

When you allow communication with external domains, your users can engage in chat, include external users in meetings, and utilize audio-video conferencing with Teams and Skype for Business users from these permitted external organizations. External users will have the *[External]* tag on their profile indicating their external domain user status.

Your users can enhance meetings or chats with external participants by adding apps. Likewise, they can interact with apps shared by external hosts in their meetings or chats. It's important to note that the data policies of the host's organization and any third-party apps shared apply in these scenarios.

Important note

If anonymous access is enabled in **Meeting settings** in the Microsoft Teams admin center, people from blocked domains will be able to join meetings anonymously.

By carefully configuring these external access settings in Teams, your organization can balance the need for open collaboration with external parties against the requirements for security and data protection. These settings not only dictate the potential for interaction with a wide range of external users but also ensure that your organization retains control over its communication boundaries.

There's more...

Microsoft Entra ID plays a crucial role in how your organization collaborates with external entities such as partners, vendors, or suppliers by managing access and sharing across Teams, Microsoft 365 groups, SharePoint, and OneDrive.

To start fine-tuning your external collaboration settings, navigate to the Microsoft Entra admin center at <https://entra.microsoft.com/>, then select **External Identities** | **External collaboration settings**, as shown in *Figure 9.14*.

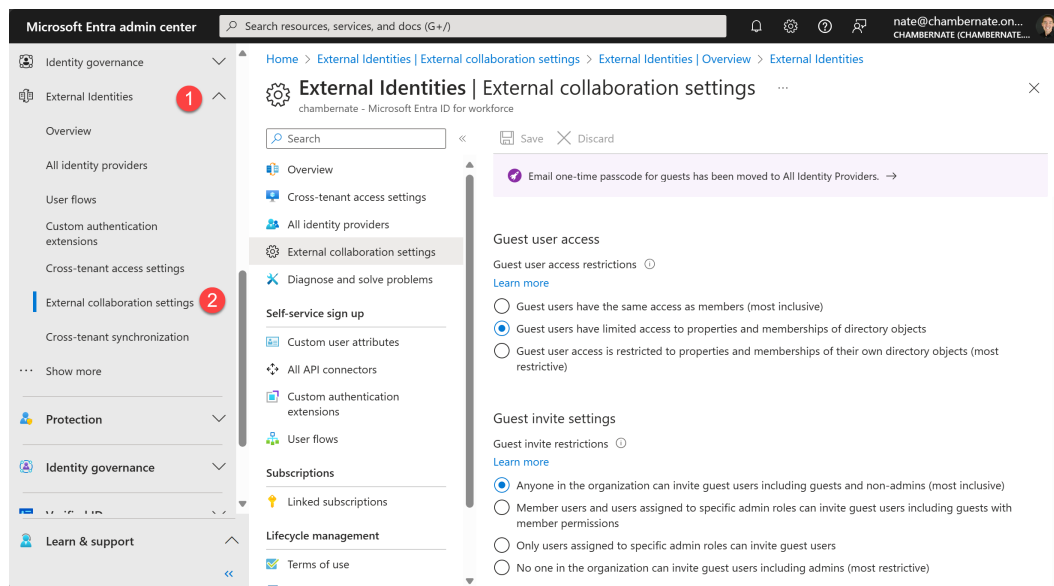


Figure 9.14 – External collaboration settings in Microsoft Entra

Here are some default settings to be aware of that you may wish to adjust:

- **Guest user access:** By default, guests have restricted access to directory object properties and memberships. This setting ensures that guests can participate in Teams and SharePoint without full directory visibility.
- **Guest invite settings:** Initially set to allow anyone within the organization to invite guests, including non-admins, facilitating broader collaboration opportunities.
- **Enable guest self-service sign up via user flows:** This option is turned off by default. Activating it enables external users to self-register for applications you offer, creating guest accounts in the process.
- **External user leave settings:** By default, and by recommendation of Microsoft, external users can choose to remove themselves from your organization. You may turn off this ability, however, which would prompt a user attempting to leave your org to review the privacy statement and/or contact someone in your org for approval.
- **Collaboration restrictions:** The default setting permits invitations to any domain. For enhanced security or compliance, you can specify allowed or blocked domains, tailoring which external entities can collaborate with your organization.

See also

- *Overview of external sharing in SharePoint and OneDrive in Microsoft 365*: <https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview>

Configuring guest access

Guest access in Microsoft Teams allows you to add individuals from outside your organization as guests. This provides them with almost the same capabilities as native team members, enabling collaboration through chats, calls, meetings, and document sharing. This differs from external access in that guests are part of your organization's directory and have broader access to the resources within teams of which they're members, such as associated SharePoint sites.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or Teams Administrator.

How to do it...

1. Log in to the Teams admin center at <https://admin.teams.microsoft.com> and navigate to **Users | Guest access**, as shown in *Figure 9.15*:

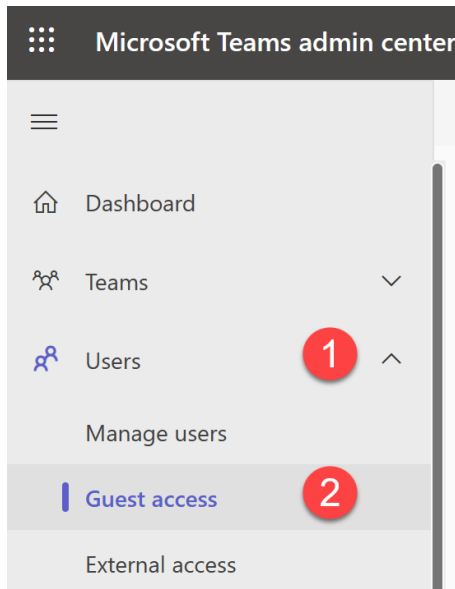


Figure 9.15 – Teams Guest access

2. Figure 9.16 shows the options for allowing guest access in Microsoft Teams, with the **Service default** setting set to **On**:

Guest access

Guest access lets you control how guests collaborate with people in your organization. You can invite people outside of your organization to have access to selected teams and allow them to join meetings and chat with your users. Learn more about guest access. [Learn more](#)

The screenshot shows the 'Guest access' settings in Microsoft Teams. At the top, there's a section titled 'Guest access' with a description: 'Guest access lets you control how guests collaborate with people in your organization. You can invite people outside of your organization to have access to selected teams and allow them to join meetings and chat with your users. Learn more about guest access. [Learn more](#)'. Below this is a dropdown menu labeled 'Guest access' with a help icon. The dropdown is open, showing 'On' as the selected option, 'Off' as an alternative, and 'Service default: On' at the bottom. Below the dropdown is a section titled 'Calling' with the text 'Manage calling settings for guests.' and a blue banner with a help icon and the text 'To manage calling settings for people in your organization, go to Voice > Calling policies'. At the bottom, there's a toggle switch for 'Make private calls' which is currently turned 'On'.

Figure 9.16 – Allowing guest access in Teams

How it works...

Enabling guest access and configuring the necessary permissions allows for secure collaboration with external users within your Teams environment. Guests can participate in teams and channels, access shared resources, and engage in chats and meetings.

There's more...

It's important to understand the distinction between guest users and external users. Guest users are added to and managed within your organization's directory, whereas external users are invited to use their own existing credentials from a different organization to access your teams and/or chats and meetings.

See also

- *Guest access in Microsoft Teams*: <https://docs.microsoft.com/en-us/microsoftteams/guest-access>

Reviewing all teams and their owners

Regularly reviewing the ownership and membership of Microsoft Teams is important for maintaining accurate access controls, ensuring compliance with organizational policies, and optimizing team management. This recipe illustrates how to review all teams and their owners using the Microsoft Teams admin center.

Getting ready

In order to follow the steps in this recipe, you must be either a Global or Teams Administrator.

How to do it...

1. From the Microsoft Teams admin center (<https://admin.teams.microsoft.com>), select **Teams** | **Manage teams** from the left navigation menu.
2. You will see a list of all teams in your organization, as shown in *Figure 9.17*. Select a team name to view details, including the team owners and members.

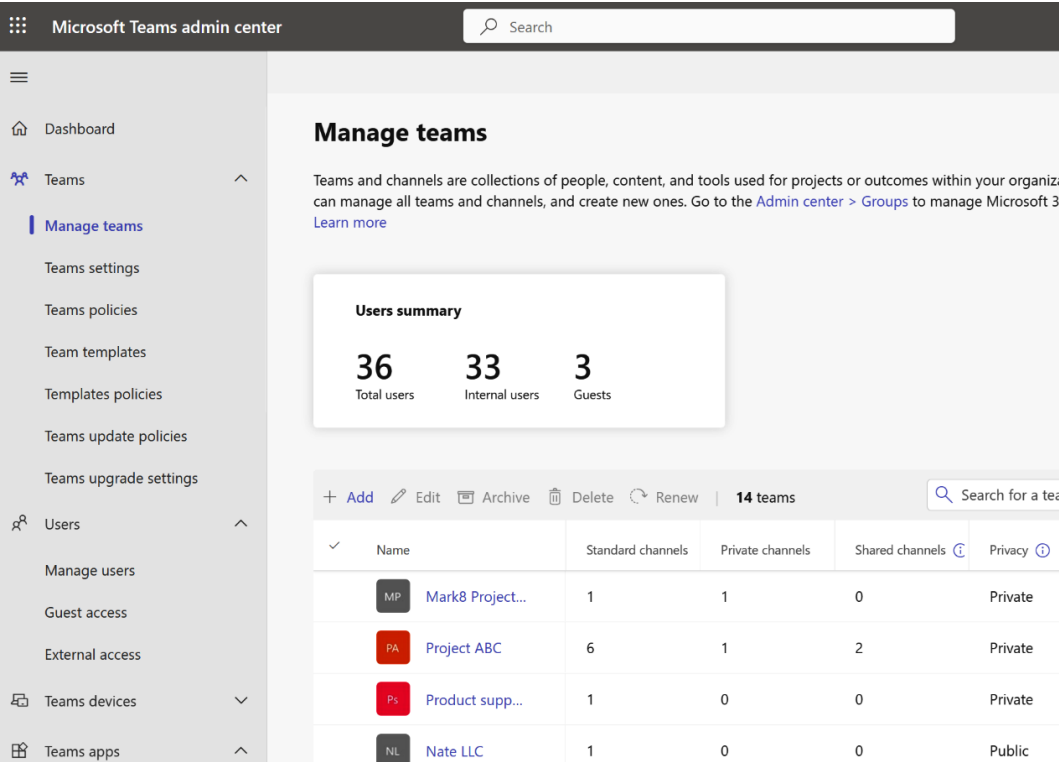


Figure 9.17 – The Manage teams screen of the Microsoft Teams admin center

How it works...

By following these simple steps, administrators can efficiently manage and audit the teams within their organization. Regular reviews help maintain proper access controls, ensuring that only authorized users have access to sensitive information and resources. You'll also be able to see the last activity date and team owners for every team, making it easy to audit teams and know which teams might be able to be deleted or archived to maintain a clean Teams environment.

There's more...

For administrators who prefer using PowerShell, you can retrieve a list of all teams and their owners and export this data to a CSV file. First, you'll need to ensure that you have the required `MicrosoftTeams` PowerShell module installed by running the following:

```
Install-Module -Name MicrosoftTeams
```

Once installed, connect by running `Connect-MicrosoftTeams`. Then, to get the list of all teams, use PowerShell to execute the following:

```
$teams = Get-Team
```

To get team owners as a CSV file, you can execute the following (update the `Path` value to your desired destination):

```
$teamOwners = @()
foreach ($team in $teams) {
    $owners = Get-TeamUser -GroupId $team.GroupId -Role Owner |
    Select-Object User, Role, Email
    foreach ($owner in $owners) {
        $teamOwners += [PSCustomObject]@{
            TeamName = $team.DisplayName
            OwnerName = $owner.User
            OwnerEmail = $owner.Email
        }
    }
}
$teamOwners | Export-Csv -Path "C:\Temp\TeamsAndOwners.csv"
-NoTypeInfo
```

By using these PowerShell scripts, you can automate the process of gathering team and owner information, making it easier to manage and audit your Teams environment regularly.

See also

- *Introduction to Microsoft Teams for admins*: <https://learn.microsoft.com/en-us/microsoftteams/teams-overview>

Managing Viva Engage

Viva Engage (formerly **Yammer**) is a dynamic platform designed to enhance communication, collaboration, and community building within an organization. As a part of Microsoft Viva, it integrates seamlessly with Microsoft Teams, providing a rich environment where employees can connect, share ideas, and build a vibrant corporate culture. Managing Viva Engage effectively ensures that the platform meets the organizational goals, fosters engagement, and maintains a healthy community environment.

Effective management of Viva Engage involves understanding the various roles and permissions, customizing the platform's look and feel to align with corporate branding, and leveraging its features to create dynamic communities. By doing so, administrators can promote meaningful interactions, facilitate the sharing of knowledge, and drive employee engagement across the organization.

We will cover the following recipes in this chapter:

- Understanding admin roles for Viva Engage
- Pinning Viva Engage in Teams
- Assigning the Corporate Communicator role to a user
- Customizing the look of your Viva Engage network
- Creating a Viva Engage community
- Creating a dynamic Viva Engage community
- Restricting posts in the All Company community

Technical requirements

This chapter requires administrative access within Microsoft 365. Users assigned the Global Administrator role or Engage Administrator (currently referred to as Yammer Administrator in Entra ID) will have the capability to execute most tasks presented. Where other roles are required, it will be noted in the recipe's *Getting ready* section. Administrators do not need Engage licenses to administer the platform but Engage users will require Viva Engage Core or premium licenses to use Viva Engage.

Understanding admin roles for Viva Engage

Managing Viva Engage requires a clear understanding of the various administrative roles and permissions available to each. These roles determine what actions users can perform and how they can manage different aspects of the platform. By assigning appropriate roles, administrators can ensure that Viva Engage operates smoothly, remains secure, and fosters a collaborative environment.

In this recipe, we'll assign a user the Network Administrator role via the Viva Engage admin center.

Tip

To see how to apply the Global or Engage Administrator role, see *Chapter 2's* recipe titled *Managing admin roles in the Microsoft 365 admin center*.

Later in this chapter, we'll cover how to assign the Corporate Communicator role to a user in the recipe titled *Assigning the Corporate Communicator role to a user*.

Getting ready

To follow the steps in this recipe, you must be either a Global Administrator or Engage Administrator.

How to do it...

1. Navigate to the Viva Engage admin center at <https://engage.cloud.microsoft/main/admin>.
2. Select the settings wheel in the upper-right corner and then select **Edit network admin settings**, as shown in *Figure 10.1*:

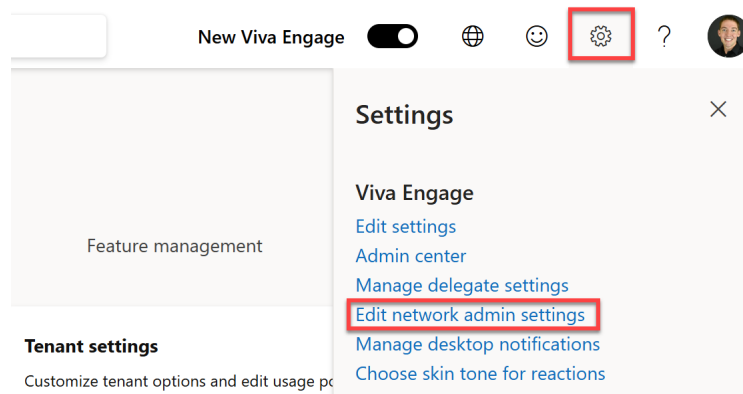


Figure 10.1 – Location of network admin settings in the Viva Engage admin center

3. Select **Admins** from the left navigation menu.

4. Enter the user's name and select them from the **Enter name** text box.
5. Select **Make this user an admin**, as shown in *Figure 10.2*:

The screenshot displays the 'Admins' management page in Viva Engage. On the left, a sidebar lists various settings categories: Network (Success, Configuration, Design, Admins, Usage Policy, External Networks, Network Migration, New Yammer), Users (Remove Users, Export Users, Profile Fields), and Content and Security (Monitor Keywords, Report Conversations, Security Settings, Export Network Data, Export User Data, Data Retention, Content Mode). The main content area is titled 'Admins' and is divided into two sections. The 'Current Admins' section lists two users: Megan Bowen and Nate Chamberlain, each with a 'Grant Verified Admin' and 'Remove' button. The 'Appoint Additional Admins' section features an 'Enter name:' text box. Below this, a user card for Miriam Graham is displayed, showing her profile picture, name, email (miriamg@chambernate.onmicrosoft.com), and join/post dates (Joined on June 15, 2023, Posted 0 messages). Below the card, there is a radio button labeled 'Make this user an admin' and a 'Submit' button.

Figure 10.2 – Adding a new admin in Viva Engage

6. Select **Submit** to confirm the role assignment.

How it works...

We just assigned the Network Administrator role to a user, but there are several others that may play a part in your Viva Engage administration strategy. Admin roles in Viva Engage are designed to provide varying levels of access and control to different users based on their responsibilities. The roles are listed and described from the most permissive to the least permissive as follows:

- **Global Administrator:** This administrator has full control over all settings and features within Viva Engage. This role can manage everything, including user permissions, settings, and overall network configurations.

- **Engage Administrator:** This tenant-level role provides comprehensive management capabilities over the entire Viva Engage network. Engage Administrators can manage settings, user roles, and configurations but might have slightly fewer permissions than Global Admins.
- **Verified Administrator:** Verified administrators have permission to manage sensitive information and security settings. They ensure that the network complies with organizational policies and security standards.
- **Network Administrator:** Network Administrators manage network settings and configurations. They handle the technical aspects of the network, such as integrations and connectivity settings.
- **Community Administrator:** Community Administrators can manage specific communities within Viva Engage. They are responsible for community-level settings, membership, and content moderation.
- **Corporate Communicator:** This role is designated for users who need to disseminate important company-wide communications. Corporate Communicators can create and manage announcements and other critical communications.
- **Answers Administrator:** Answers Administrators manage the Q&A and knowledge-sharing aspects of Viva Engage. They can moderate and organize answers to ensure that information is accurate and relevant.

Assigning roles ensures that the right individuals have the appropriate level of access to perform their duties effectively without compromising security or overloading any single admin with all responsibilities. This hierarchical structure allows for efficient management of the platform, tailored to the specific needs and expertise of the administrators.

Important note

Users assigned the Network Admin role in Viva Engage do not need to hold the Tenant-level Group Administrator role unless their responsibilities include creating and managing specific groups. While Network Admins oversee network-wide settings and configurations, Microsoft 365 group administrators focus on managing groups within the network. If a Network Admin also needs to manage group settings, they should be granted the Tenant-level Group Administrator role as well.

There's more...

After making a user a Network admin, you can also select **Grant Verified Admin** next to their name on the **Admins** screen, as previously seen in *Figure 10.2*, to allow them to assign other admins (including Verified), manage content policies, data retention, security settings, and more beyond general Network admin responsibilities.

See also

- *Manage administrator roles in Viva Engage:* <https://learn.microsoft.com/en-us/viva/engage/eac-key-admin-roles-permissions>
- *Overview of the Viva Engage admin center:* <https://learn.microsoft.com/en-us/viva/engage/eac-overview>

Pinning Viva Engage in Teams

Pinning Viva Engage in Microsoft Teams ensures that users have easy and quick access to the platform, fostering better engagement and seamless communication. This recipe will guide you through the steps to pin Viva Engage for all users in your organization.

Getting ready

To follow the steps in this recipe, you must be either a Global Administrator or Teams Administrator.

How to do it...

1. Navigate to the Microsoft Teams admin center at <https://admin.teams.microsoft.com>.
2. Select **Teams apps** | **Setup policies** from the left navigation menu, as shown in *Figure 10.3*:

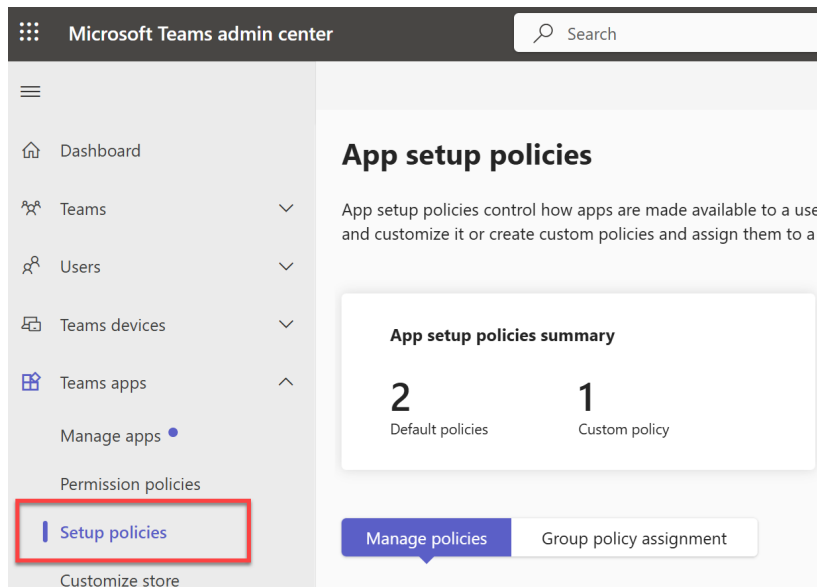


Figure 10.3 – Location of Setup policies in the Teams admin center

3. Either create a new policy by selecting **Add** or select an existing policy, such as **Global (Org-wide default)**, to modify.

Tip

Modifying the global policy applies the changes to all users across the organization. This is ideal when you want every user to have easy access to Viva Engage, ensuring consistent access to key apps organization-wide.

Creating a new app policy allows you to target specific groups or departments, tailoring the Teams experience to their specific needs. For example, you might prioritize Viva Engage for teams focused on internal communications while emphasizing different tools for other departments.

4. Enter a name and description for the policy if you are creating a new one.
5. Under the **Pinned apps** section, select **Add apps**.
6. Search for Viva Engage in the search bar.
7. Select **Viva Engage** from the search results and then select **Add** so it appears as shown in *Figure 10.4*.

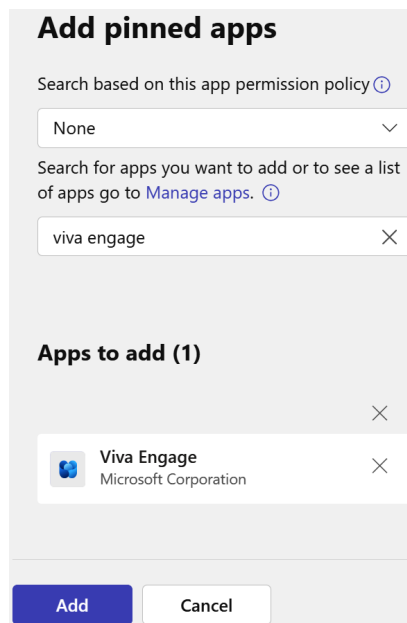


Figure 10.4 – Adding Viva Engage to pinned apps in a setup policy

8. Arrange Viva Engage in the list to determine its order in the app bar.
9. Select **Save** to apply the changes.

How it works...

By pinning Viva Engage in Teams, you make it easily accessible from the Teams app bar, as shown in *Figure 10.5*, ensuring users can quickly navigate to it without searching. This improves visibility and usage of Viva Engage, promoting better communication and collaboration within your organization.

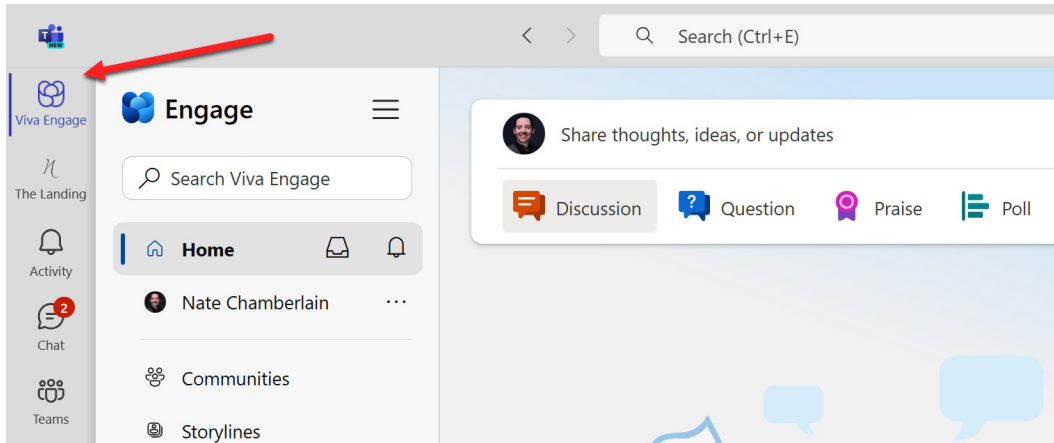


Figure 10.5 – Viva Engage pinned to the Teams app bar for a user

There's more...

Customizing your app setup policies in Teams allows you to strategically position key tools such as Viva Engage, Viva Connections, or Approvals within the app bar. This approach ensures that essential apps are not only readily available but also prioritized according to their relevance to your organization's workflows.

By thoughtfully arranging these apps, you can enhance user engagement, drive the adoption of critical tools, and streamline daily operations. Prioritizing apps in the app bar based on their importance helps users access the tools they need most efficiently, ultimately boosting productivity and fostering a more focused work environment.

See also

- *Use app setup policies to pin and auto install apps for users:* <https://learn.microsoft.com/en-us/microsoftteams/teams-app-setup-policies>
- *Overview of app management and governance in Teams admin center:* <https://learn.microsoft.com/en-us/microsoftteams/manage-apps>

Assigning the Corporate Communicator role to a user

The **Corporate Communicator role** in Viva Engage is essential for managing and disseminating important company-wide communications. Assigning this role ensures that specific users have the necessary permissions to create and manage announcements and other critical communications effectively.

Getting ready

To follow the steps in this recipe, you must be either a Global or Engage Administrator.

How to do it...

1. Navigate to the Viva Engage admin center at `https://engage.cloud.microsoft/main/admin`.
2. Select **Corporate communicators** from the **Setup and configuration** section, as shown in *Figure 10.6*:

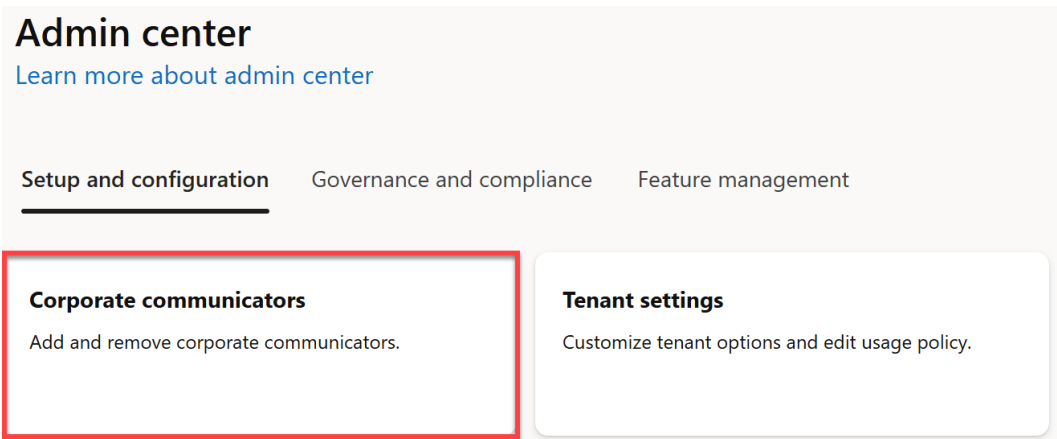


Figure 10.6 – Location of Corporate communicators in the Viva Engage admin center

3. Select **Add User**.
4. Enter the name or email address of the user you want to assign the role to and then select them from the suggested results.
5. Select **Save** to confirm the role assignment.
6. Verify that the user has been added to the Corporate Communicator role by checking the list of assigned users, as shown in *Figure 10.7*:

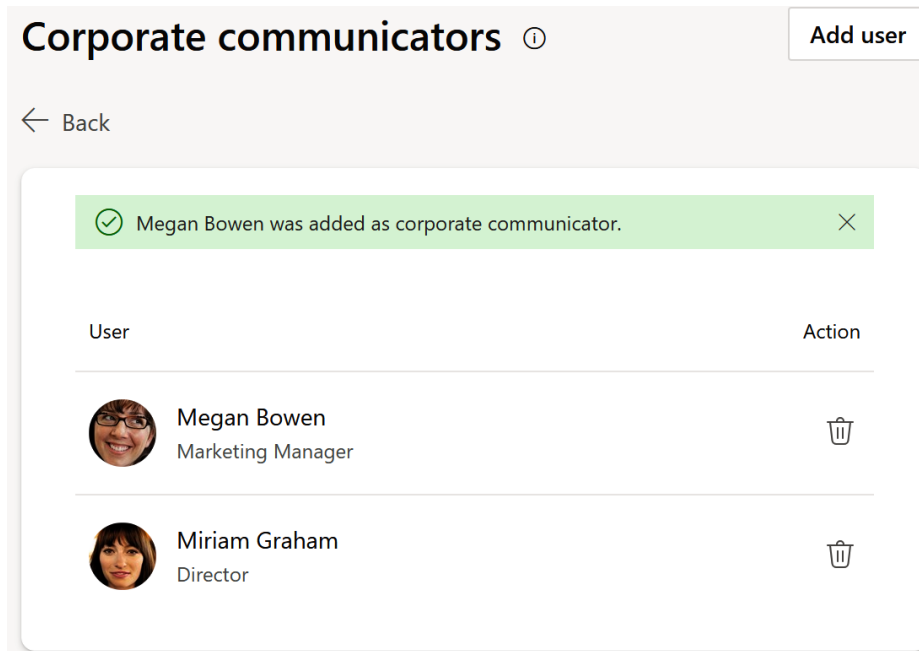


Figure 10.7 – Corporate communicators list in the Viva Engage admin center

How it works...

Assigning the Corporate Communicator role grants the user permissions to create and manage corporate communication campaigns, such as announcements and important updates, driving engagement, and identifying leaders and their audiences across the Viva Engage network. This role is important for maintaining effective internal communications and ensuring that key messages reach all employees.

There's more...

In addition to assigning the Corporate Communicator role, consider providing training and resources to the designated users to help them understand their responsibilities and use the platform effectively.

See also

- *Manage administrator roles in Viva Engage*: <https://learn.microsoft.com/en-us/viva/engage/eac-key-admin-roles-permissions>
- *Overview of the Viva Engage admin center*: <https://learn.microsoft.com/en-us/viva/engage/eac-overview>

Customizing the look of your Viva Engage network

Customizing the look of your Viva Engage network is essential for creating a cohesive and engaging user experience that aligns with your organization’s branding. By tailoring the visual aspects of Viva Engage, you can enhance user adoption and foster a stronger sense of community.

Getting ready

To follow the steps in this recipe, you must be either a Global or Engage Administrator. You will also want to have your organization’s branding assets (logo, a 56 px by 1200 px banner image, and a 50 px by 160 px logo for emails) ready.

How to do it...

- 1. Navigate to the Viva Engage admin center at `https://engage.cloud.microsoft/main/admin`.
- 2. Select **Tenant settings** from the **Setup and configuration** section, as shown in *Figure 10.8*:

Admin center

[Learn more about admin center](#)

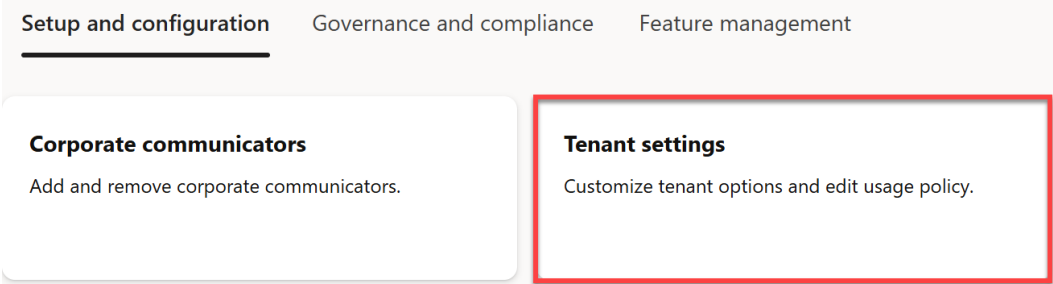


Figure 10.8 – Location of Tenant settings in the Viva Engage admin center

- 3. To upload your organization’s logo, select **Add** in the **Tenant logo** section, and then select **Choose file** to find and upload your organization’s logo.
- 4. Under the **Other** header, select **Manage other tenant configurations through the Yammer admin center**.
- 5. Select **Design** from the left navigation menu and then you can choose image files from your computer for the header image and logo for emails, as shown in *Figure 10.9*.

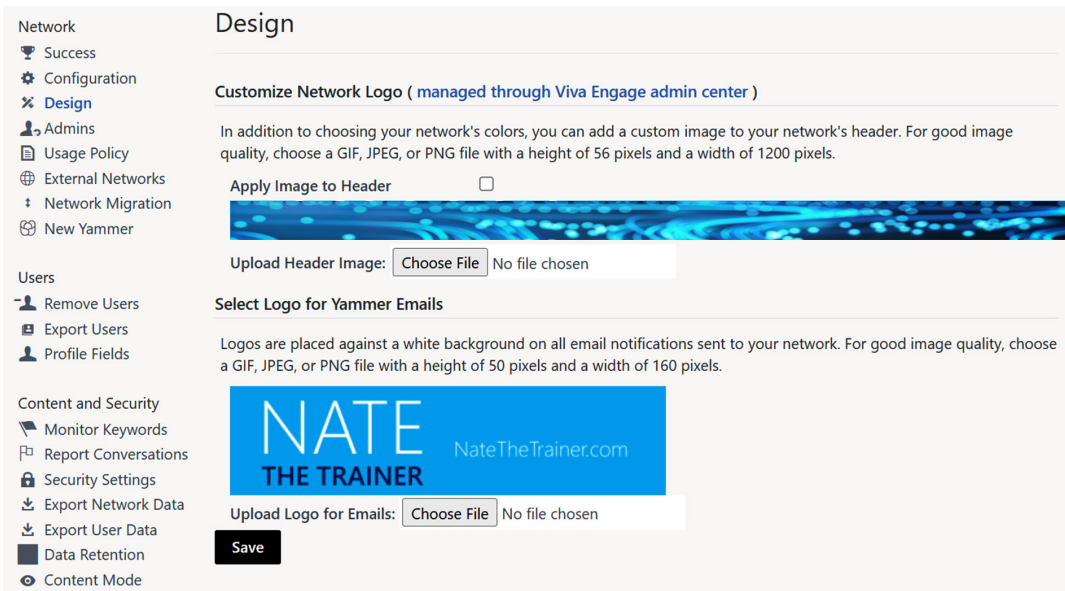


Figure 10.9 – Network header and email logo configuration

6. Review the preview of your customizations to ensure they appear as desired.
7. Select **Save** to apply the changes.

How it works...

Customizing the look of your Viva Engage network involves updating the logo, header, and email images to reflect your organization's branding. This not only creates a visually appealing environment but also helps in promoting a consistent brand identity across the platform. Customizations are applied instantly, enhancing the user experience and making the platform more engaging.

There's more...

Consider periodically updating the visuals to keep the network fresh and aligned with any changes in your organization's branding. Additionally, gather feedback from users to ensure the customizations enhance their experience and engagement.

Each community within Viva Engage can further customize and personalize its individual community by setting a cover photo and community icon, as shown in *Figure 10.10*:

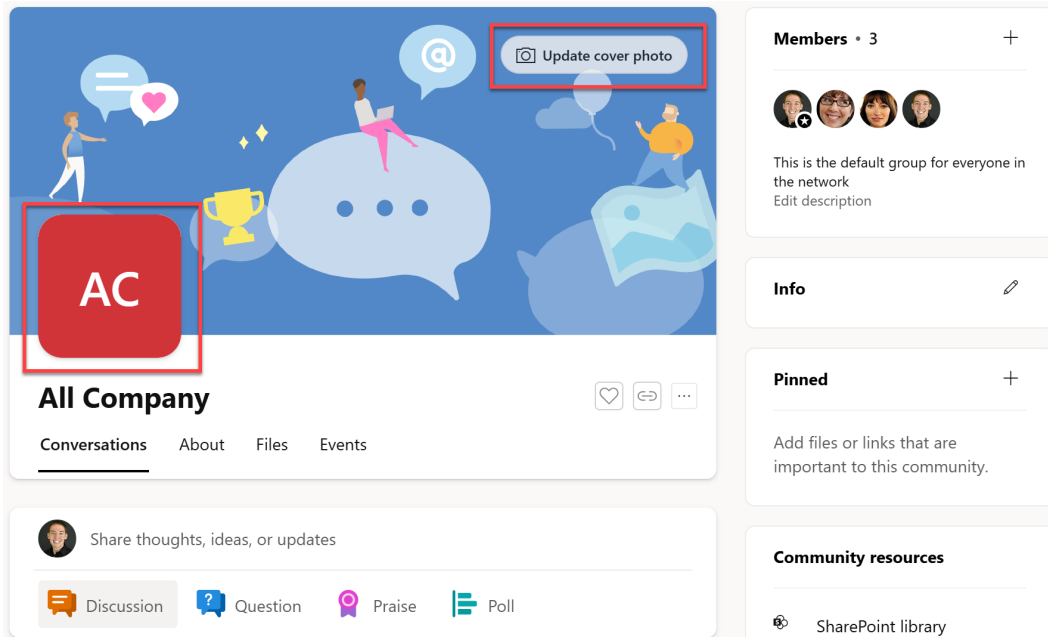


Figure 10.10 – Locations of individual community branding assets

See also

- *Customize your network*: <https://learn.microsoft.com/en-us/viva/engage/manage-viva-engage-groups/customize-your-network>
- *Overview of the Viva Engage admin center*: <https://learn.microsoft.com/en-us/viva/engage/eac-overview>

Creating a Viva Engage community

Creating a Viva Engage community allows users within your organization to connect, share information, and collaborate on specific topics or projects. Communities are vital for fostering engagement, facilitating communication, and building a sense of belonging among members.

Getting ready

To follow the steps in this recipe, you must be either a Global or Engage Administrator or a Microsoft 365 user with permission to create Microsoft 365 groups (determined by your administrators).

How to do it...

1. Navigate to the Viva Engage home page at <https://engage.cloud.microsoft/> or by navigating to <https://microsoft365.com> and selecting **Viva Engage** from your app launcher (nine-dot grid icon in the upper-left corner).
2. Select **Communities** from the left navigation menu and then scroll to the bottom and select **Create a community**, as shown in *Figure 10.11*:

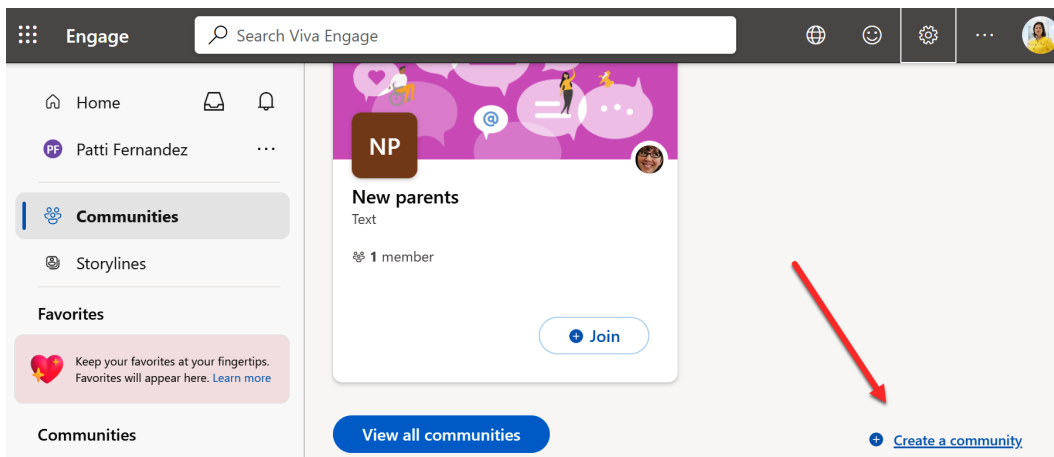


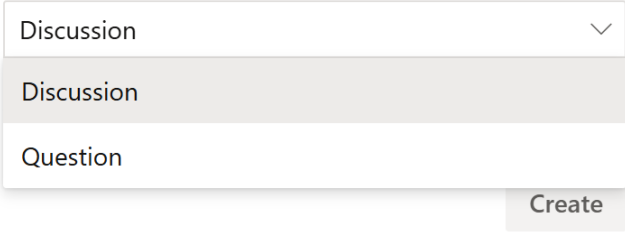
Figure 10.11 – Location of option to create a new community in Viva Engage

3. Enter a name for your community in the **Name** field, such as **Book Club**.
4. Add a **Description** for your community to inform potential members about its purpose.
5. Add **Members** by name or email address. You can also manage membership after creation.
6. Under **Settings**, choose whether the community will be **Public** or **Private**. Public communities are open to anyone in the organization, while private communities require approval to join.

7. Under **Default publisher**, choose whether users will primarily create discussions or questions by selecting **Discussion** or **Question**, as shown in *Figure 10.12*.

Communication configurations

Default publisher



Discussion

Discussion

Question

Create

Figure 10.12 – Option to set a community’s default publisher to Discussion or Question

8. Select **Create**.
9. Once the community is created, you can further customize it by uploading a community image and cover photo, which can be done by selecting **Edit Community Settings**.
10. Invite members to join the community by selecting **Invite Members** and entering their email addresses or selecting them from the user list.

How it works...

Creating a Viva Engage community establishes a dedicated space for users to engage in discussions, share resources, and collaborate on projects or topics of interest. *Figure 10.13* shows a *New parents* community created to encourage discussions and facilitate employee connections around something they have in common. Parenthood, pets, vacations, photography, book clubs, and sports are all examples of social topics that could facilitate similar togetherness across department lines.

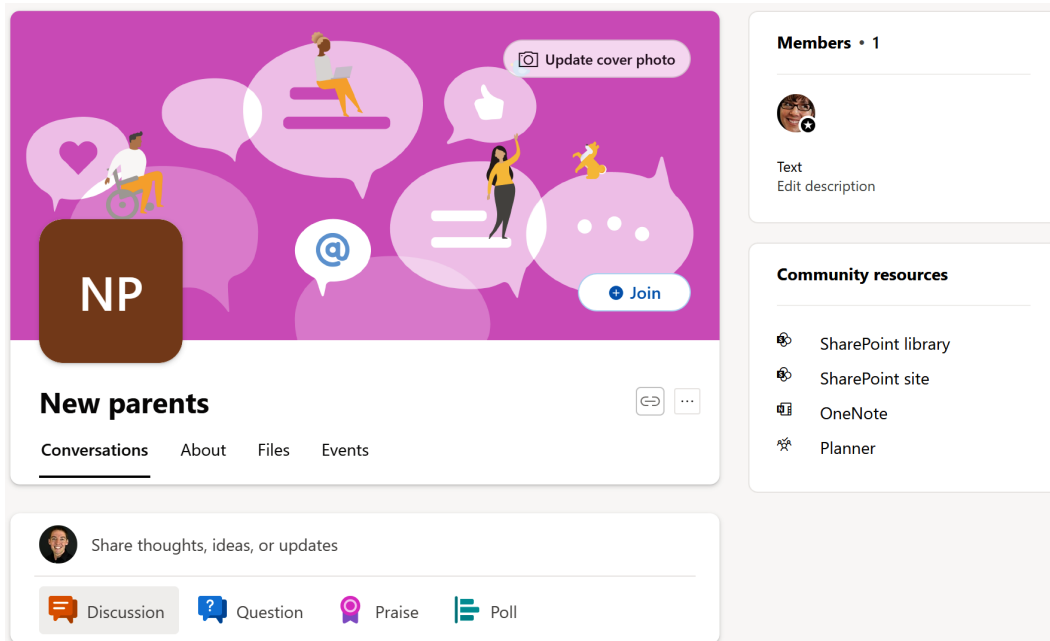


Figure 10.13 – New parents community example with publisher ready for a new discussion

By setting up a community, you enable focused interactions and provide a platform for employees to connect over common interests or goals. Customizing the community with images and inviting members helps in creating an inviting and active environment.

There's more...

To keep the community active and engaging, regularly post updates, share relevant content, and encourage members to participate in discussions. Appointing community managers or moderators can also help in maintaining the community and fostering engagement. If these appointed individuals notice an unanswered question or a post without engagement, they can help encourage engagement from other community members to help them get in the habit of visiting and engaging regularly, adding value and improving employee experiences for all members.

See also

- *Create a community in Viva Engage:* <https://support.microsoft.com/en-gb/office/create-a-community-in-viva-engage-56aaf591-1fbc-4160-ba26-0c4723c23fd6>

Creating a dynamic Viva Engage community

Creating a dynamic Viva Engage community is essential for large organizations where employees frequently change roles, teams, or locations. Dynamic communities automatically update their membership based on specific criteria, ensuring that the right people are always included. This guide will help you set up a dynamic Viva Engage community using Microsoft Entra ID attributes.

Getting ready

To follow the steps in this recipe, you must be either a Global or Entra Administrator. You must also have Microsoft Entra ID P1 or P2 licenses assigned to any user you intend to add to the dynamic community.

The steps in this recipe also should take place once your community is already created. Follow the steps in this chapter's recipe titled *Creating a Viva Engage Community* if you don't already have a community that you wish to make dynamic.

How to do it...

1. Navigate to the Microsoft Entra admin center at `https://entra.microsoft.com`.
2. Select **Identity | Groups | All groups** from the left navigation menu.
3. Find and select the name of your existing community's group, as shown in *Figure 10.14*:

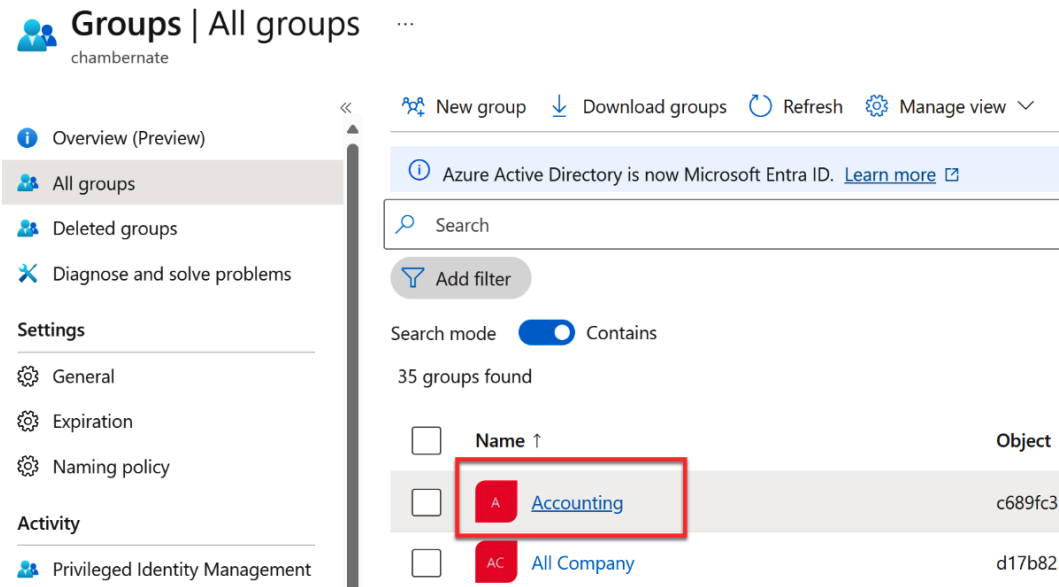


Figure 10.14 – All groups screen of Entra ID

4. Under **Properties**, set **Membership type** to **Dynamic User**, as shown in *Figure 10.15*:

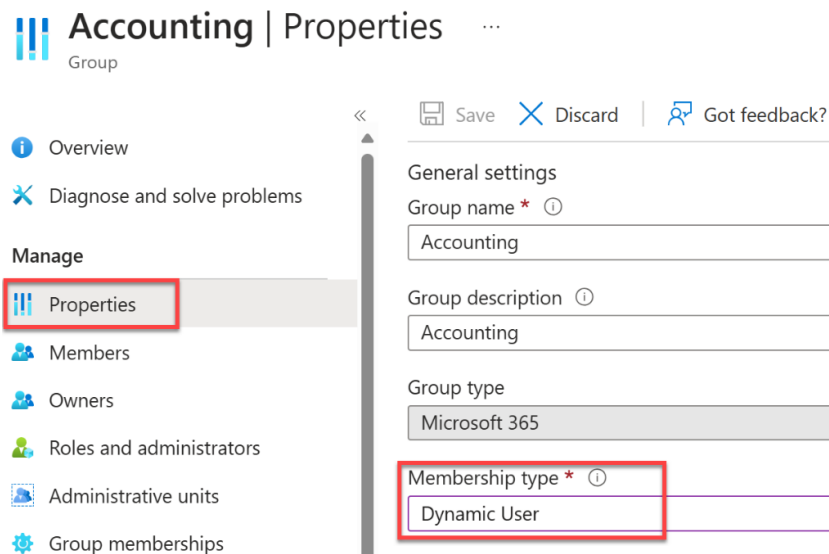


Figure 10.15 – Group properties screen

- 5. Select **Add dynamic query** under **Dynamic user members**.
- 6. Configure the membership rules by selecting a **Property**, **Operator**, and **Value** setting. For example, to add all members of the *Human Resources* department, you would select **department** for **Property**, **Equals** for **Operator**, and enter *Human Resources* for **Value**.
- 7. Review the dynamic query syntax generated below the expression. It should look similar to `(user.department -eq "Human Resources")`, as shown in *Figure 10.16*:

Configure Rules

Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
<div></div>	<div>department</div>	<div>Equals</div>	<div>Human Resources</div>

+ Add expression

+ Get custom extension properties

Rule syntax

Edit

(user.department -eq "Human Resources")

Figure 10.16 – Dynamic user query

8. Select **Save** to commit your membership rules, then **Save** again to save changes to the group's properties.

How it works...

Dynamic Viva Engage communities leverage Microsoft Entra ID attributes to automatically manage group membership. When specified user attributes, such as department, role, or location change, the dynamic group updates its membership accordingly. This ensures that the community always includes the relevant members without manual intervention.

Dynamic groups operate on a scheduled synchronization process that typically runs every few minutes but may take up to an hour to fully update. This interval ensures that changes in user attributes are reflected in the group membership in a timely manner, keeping the community up to date.

There's more...

Dynamic groups support various attributes and complex rules, allowing for sophisticated membership management. You can also accomplish this using PowerShell with Microsoft Graph. Here's how you can change a group to dynamic membership using Microsoft Graph PowerShell:

```
# Install and connect to Microsoft Graph PowerShell
Install-Module Microsoft.Graph -Scope CurrentUser -Force -AllowClobber
Connect-MgGraph -Scopes "Group.ReadWrite.All"

# Define the group you want to modify
$GroupId = "<Your-Group-Object-ID-From-Entra-Here>"

# Update the group properties
$GroupUpdateBody = @{
    GroupTypes = @("DynamicMembership", "Unified")
    MembershipRule = '(user.department -eq "Marketing")'
    MembershipRuleProcessingState = 'On'
}
Update-MgGroup -GroupId $GroupId -BodyParameter $GroupUpdateBody
```

See also

- *Create or update a dynamic group in Microsoft Entra ID:* <https://learn.microsoft.com/en-us/entra/identity/users/groups-create-rule>
- *Create a dynamic group in Viva Engage:* <https://learn.microsoft.com/en-us/viva/engage/manage-viva-engage-groups/create-a-dynamic-group>

Restricting posts in the All Company community

The All Company community in Viva Engage is a default community where important announcements and updates can be shared with the entire organization. Restricting posts in this community ensures that only authorized users can post messages, maintaining the quality and relevance of the content shared.

Getting ready

To follow the steps in this recipe, you must be an admin of the All Company community. See this recipe's *There's more...* section to learn how to promote a community member to an admin.

How to do it...

1. Navigate to the Viva Engage home page at <https://engage.cloud.microsoft/> or by navigating to <https://microsoft365.com> and selecting **Viva Engage** from your app launcher (nine-dot grid icon in the upper-left corner).
2. Select **Communities** from the left navigation menu and then select **All Company** from the list of communities.
3. Select the three dots (...) in the top-right corner of the main feed area and then select **Settings**, as shown in *Figure 10.17*:

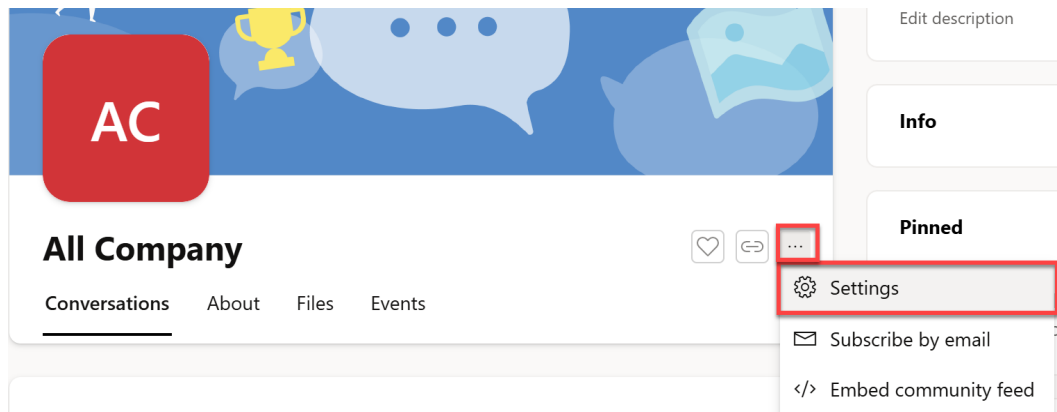
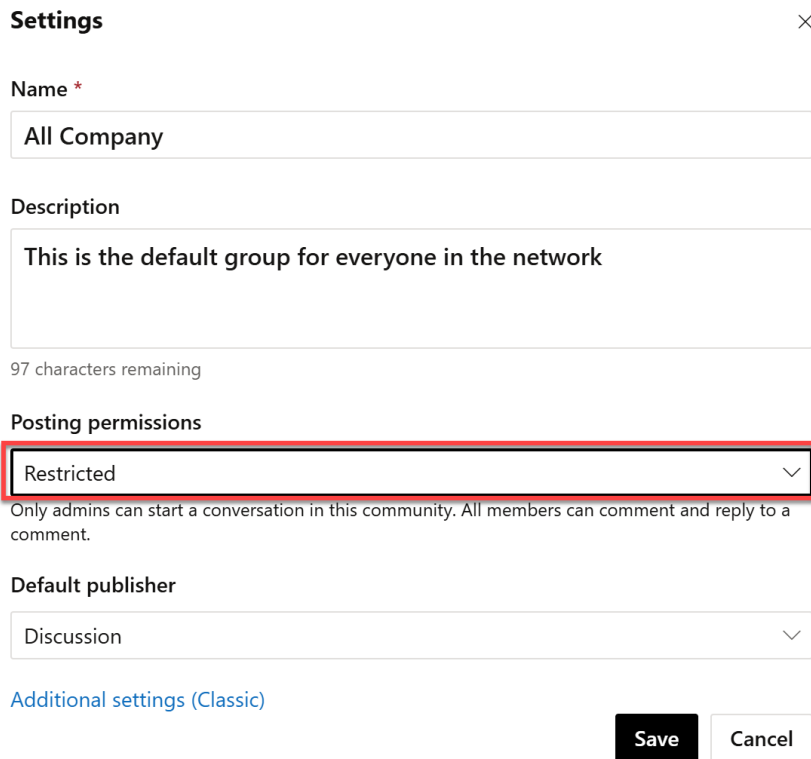


Figure 10.17 – Location of community settings

4. In the **Settings** menu, find the **Posting permissions** section and change it from **Open** to **Restricted**, as shown in *Figure 10.18*:



The screenshot shows a 'Settings' dialog box with a close button (X) in the top right corner. It contains several sections: 'Name' with a red asterisk and a text input field containing 'All Company'; 'Description' with a text area containing 'This is the default group for everyone in the network' and a character count of '97 characters remaining'; 'Posting permissions' with a dropdown menu set to 'Restricted' (highlighted with a red border) and a description 'Only admins can start a conversation in this community. All members can comment and reply to a comment.'; and 'Default publisher' with a dropdown menu set to 'Discussion'. At the bottom, there is a link for 'Additional settings (Classic)' and two buttons: 'Save' and 'Cancel'.

Figure 10.18 – Posting permissions setting

5. Select **Save** to apply the changes.

How it works...

By restricting posts in the All Company community, you ensure that only designated admins can share content. This helps maintain the focus of the community on important organizational updates and announcements, preventing irrelevant or off-topic posts from cluttering the community feed.

There's more...

If you want to promote an employee from a community member to an admin, select the plus icon in the **Members** section of the **All Company** community, as shown in *Figure 10.19*.

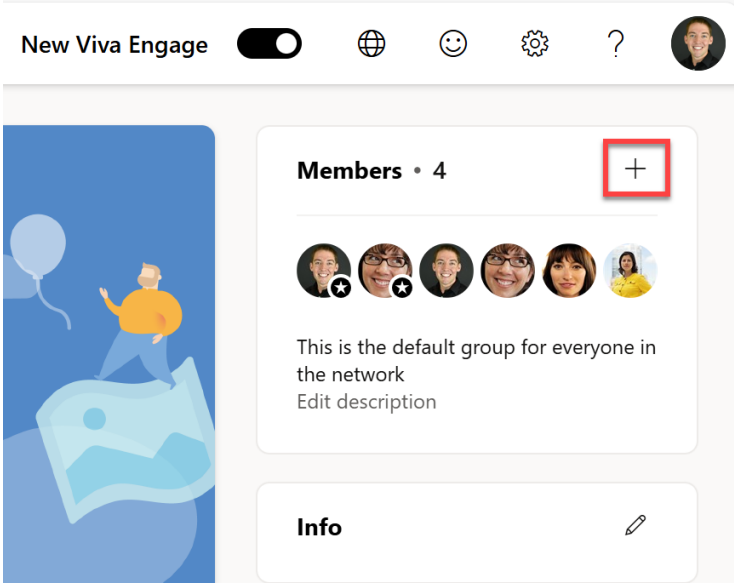


Figure 10.19 – Member management section of a community

Search for a user, select the three dots (...), and choose **Make admin**, as shown in *Figure 10.20*.

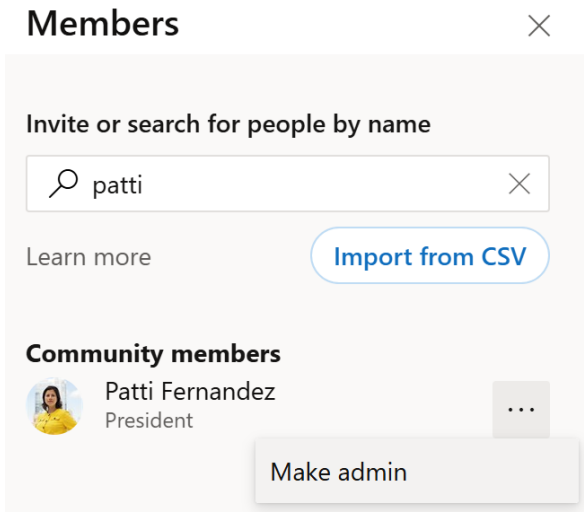


Figure 10.20 – Option to make a community member an admin

Consider regularly reviewing the list of community admins to ensure that only the appropriate users have posting permissions. Additionally, communicate the purpose of the All Company community to all members so they understand where to find important updates and where to post their own messages.

See also

- *Restrict All Company posts in Viva Engage*: <https://support.microsoft.com/en-us/office/restrict-all-company-posts-in-viva-engage-3219d2ae-db15-4c9f-9dd2-28559ae39a97>

Configuring and Managing Users in Microsoft Entra ID

Configuring and managing users in **Microsoft Entra ID** (formerly known as Azure Active Directory) is a critical aspect of IT administration for organizations using Microsoft 365 and related services on which all other apps and services rely. Entra ID provides a centralized platform for managing user identities, controlling access to resources, and ensuring security compliance across the enterprise. Effective management of user accounts, including creating, updating, and removing users, is essential for maintaining operational efficiency and security. Additionally, customizing the user experience through branding, setting up automated provisioning and de-provisioning of accounts, and implementing **single sign-on (SSO)** can enhance user satisfaction and streamline access to organizational resources.

We will cover the following recipes in this chapter:

- Creating and populating Microsoft Entra ID
- Adding branding to the Entra ID sign-in page
- Adding a privacy statement to the Entra ID sign-in page
- Adding SSO for an application
- Getting direct sign-on links for organizational apps
- Installing and connecting to the Microsoft Graph SDK via PowerShell
- Adding/removing users via PowerShell in Microsoft Graph
- Creating an Access review report in Entra ID
- Reviewing and completing an Access review report in Entra ID
- Enabling self-service password reset

Technical requirements

This chapter will often require that you're a Global Administrator in your tenant although, in certain cases, a User Administrator role will suffice. You'll also need to be able to run PowerShell and may need rights to install software on a machine in order to complete all the recipes. Additionally, having familiarity with Microsoft Entra ID and related concepts will be beneficial for understanding and efficiently executing the tasks described.

Creating and populating Microsoft Entra ID

In this recipe, we will walk through the steps to create and populate a new Microsoft Entra ID directory. This process is fundamental for administrators as it allows for the management of user identities and access to resources within an organization. Entra ID serves as the backbone for managing access to Microsoft 365 services and other integrated applications, ensuring that the right users have the appropriate access to necessary resources.

Getting ready

To complete the steps in this recipe, you must be a Global Administrator.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Navigate to **Identity** from the left navigation pane under **Admin centers**.
3. On the Entra ID **Overview** page, select **Manage tenants**, as shown in *Figure 11.1*:

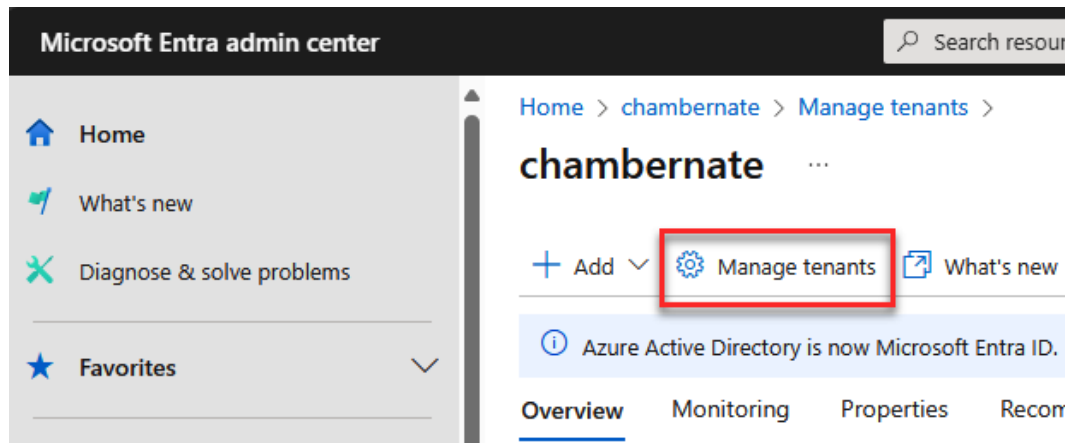


Figure 11.1 – The Manage tenants option in Entra ID

- 4. Select **Create**.
- 5. Choose **Workforce** for configuration to allow for the management of employees, internal resources, and external collaborators, then select **Continue**.
- 6. Enter the appropriate options shown in *Figure 11.2* for your new directory, such as the organization name, initial domain name, and region, then select **Create**.

[Home](#) > [Nate LLC](#) > [Manage tenants](#) > [Choose a configuration for your tenant](#) >

Create a tenant ...

A Microsoft Entra tenant contains a directory for managing users and provides identity and access management (IAM) capab

Tenant Name * ⓘ

Tailspin Customers ✓

Domain Name * ⓘ

tailspincustomers ✓ .onmicrosoft.com

ⓘ

This domain <domainname>.onmicrosoft.com cannot be edited or deleted.

Location ⓘ

United States ▼

✓

Geographic location - United States

ⓘ

Location selected above determines the datacenter of your tenant. This must be your data is located

Figure 11.2 – Details screen for a new tenant

- 7. After the directory is created, you can toggle between multiple directories by choosing your identity in the upper-right corner and then selecting **Switch directory**, as shown in *Figure 11.3*:

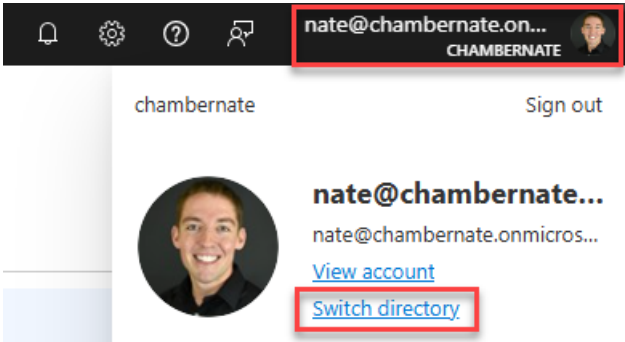


Figure 11.3 – Steps to switch directories


8. To populate the directory, we need to add users. Go to **Users | All users** and select **New user | Create new user**.
9. Enter the required information for the new user, such as name, username, and profile details, as shown in *Figure 11.4*. Note the options tabs across the top to add **Properties** information (such as job title, manager, and department), and any role or group assignments under **Assignments**.

[Home](#) > [chambernate](#) > [Manage tenants](#) > [Choose a configuration for your tenant](#) > [chambernate](#) > [Users](#) >

Create new user ...

Create a new internal user in your organization

Basics Properties Assignments Review + create


Create a new user in your organization. This user will have a user name like `alice@contoso.com`. [Learn more](#) 

Identity

User principal name *

Gerald.Jones

@

chambernate.onmicros... 



Domain not listed? [Learn more](#) 

Mail nickname *

Gerald.Jones



Derive from user principal name

Display name *

Gerald Jones

Password *

.....



Auto-generate password


Account enabled 



Figure 11.4 – New user screen in Entra ID

10. Set the user's password options. You can either auto-generate a password or create one manually, as seen previously in *Figure 11.4*.
11. When you've entered all the necessary details across the various tabs for the new user, select **Review + create**.
12. Select **Create** to add the user to the directory.

How it works...

Creating and populating a Microsoft Entra ID involves setting up a new directory to manage organizational resources and identities. When you create a new directory, you establish a separate instance of Entra ID, which can be used to isolate resources and user accounts. Adding users either individually or in bulk populates the directory with the necessary identities that can be assigned roles, access permissions, and licenses as required.

There's more...

Bulk uploading users can be much more efficient for large organizations. To bulk upload users, follow these steps:

1. Select **Users** | **All users** and then **Bulk operations** | **Bulk create**.
2. Download the CSV template provided in the panel that appears in *Figure 11.5*:

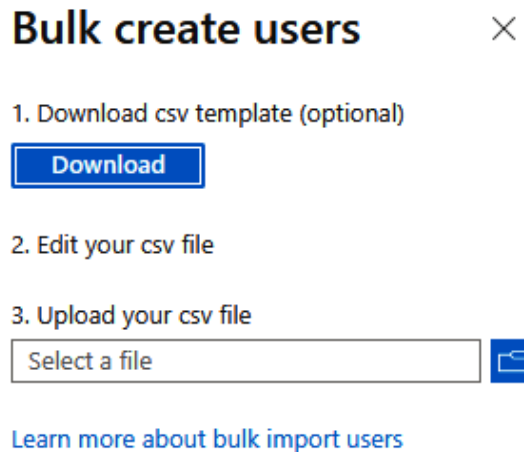


Figure 11.5 – The Bulk create users panel

3. Fill in the CSV's required user details and any additional that you wish to populate. These properties can include the following:
 - **Name** [**displayName**] (Required)
 - **User name** [**userPrincipalName**] (Required)
 - **Initial password** [**passwordProfile**] (Required)
 - **Block sign in (Yes/No)** [**accountEnabled**] (Required)
 - **First name** [**givenName**]

- **Last name** [surname]
 - **Job title** [jobTitle]
 - **Department** [department]
 - **Usage location** [usageLocation]
 - **Street address** [streetAddress]
 - **State or province** [state]
 - **Country or region** [country]
 - **Office** [physicalDeliveryOfficeName]
 - **City** [city]
 - **ZIP or postal code** [postalCode]
 - **Office phone** [telephoneNumber]
 - **Mobile phone** [mobilePhone]
4. Upload the completed CSV file in the same panel previously shown in *Figure 11.5*.
 5. Review the upload details and select **Submit** to create users in bulk.
 6. Verify that users are created by checking the **Users** | **All users** section in your directory.

For more advanced configurations, such as setting up dynamic groups, Conditional Access policies, or integrating with on-premises directories, you can explore additional features in the Azure portal as long as your subscription supports it (typically an Entra ID P1 or P2 license required). These configurations could further help in automating user management tasks and enhancing security.

See also

- *Quickstart: Create a new tenant in Microsoft Entra ID:* <https://learn.microsoft.com/en-us/entra/fundamentals/create-new-tenant>
- *How to create, invite, and delete users:* <https://learn.microsoft.com/en-us/entra/fundamentals/how-to-create-delete-users>
- *Bulk create users in Microsoft Entra ID:* <https://learn.microsoft.com/en-us/entra/identity/users/users-bulk-add>

Adding branding to the Entra ID sign-in page

Branding the Entra ID sign-in page helps users recognize and trust the login process by displaying familiar graphics and information. This enhances the professional appearance of your organization to both internal and external users. In this recipe, we will add branding elements to the Entra ID sign-in page.

Getting ready

You must have the Global Administrator role and a Microsoft Entra ID P1 or P2, Business Standard, or SharePoint (Plan 1) license to complete these steps. Prepare the following images, ensuring they meet the specified criteria:

- Favicon: 32 x 32 px | <5 KB | PNG (preferred), JPG, or JPEG

Note

A favicon is a small icon displayed in the browser tab alongside the page name, representing the site.

- Background: 1920 x 1080 px | <300 KB | PNG, JPG, or JPEG
- Header logo: 245 x 36 px | <10 KB | PNG, JPG, or JPEG
- Banner logo: 245 x 36 px | <50 KB | PNG, JPG, or JPEG
- Square logo: 240 x 240 px | <50 KB | PNG (preferred), JPG, or JPEG

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Navigate to **Identity** from the left navigation menu under **Admin centers**.
3. Choose **User experiences** | **Company branding** from the left navigation menu options. Note that you may first have to click **Show more** to find this option.
4. Select **Customize**.

5. On the **Basics** tab, upload your images for the favicon, background image and background color (shown in *Figure 11.6*), header, layout, and logos. Ensure they meet the specifications mentioned earlier.

Background image ⓘ

Select file(s)

Browse

Image will appear darkened to improve contrast and legibility.




Image size: 1920x1080px

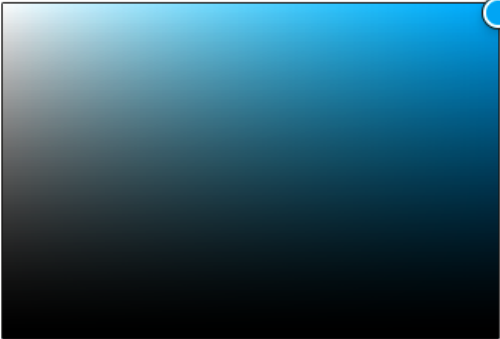
Max file size: 300KB


File Type: PNG, JPG, or JPEG

Remove

Page background color ⓘ

#00bff8 Remove





Hex

00bff8

Red

0

Green

191

Blue

248

Review + save

< Previous

Next: Layout >

Figure 11.6 – Some of the company branding options on the Basics tab

6. Optionally, configure additional text for the username entry box and the footer of the sign-in page by selecting the **Sign-in form** tab and entering those details.

7. Select **Review + create** and then **Create** to save and implement your changes.

How it works...

When branding the Entra ID sign-in page, you provide a custom look and feel that users will recognize it to be like that, as shown in *Figure 11.7*:

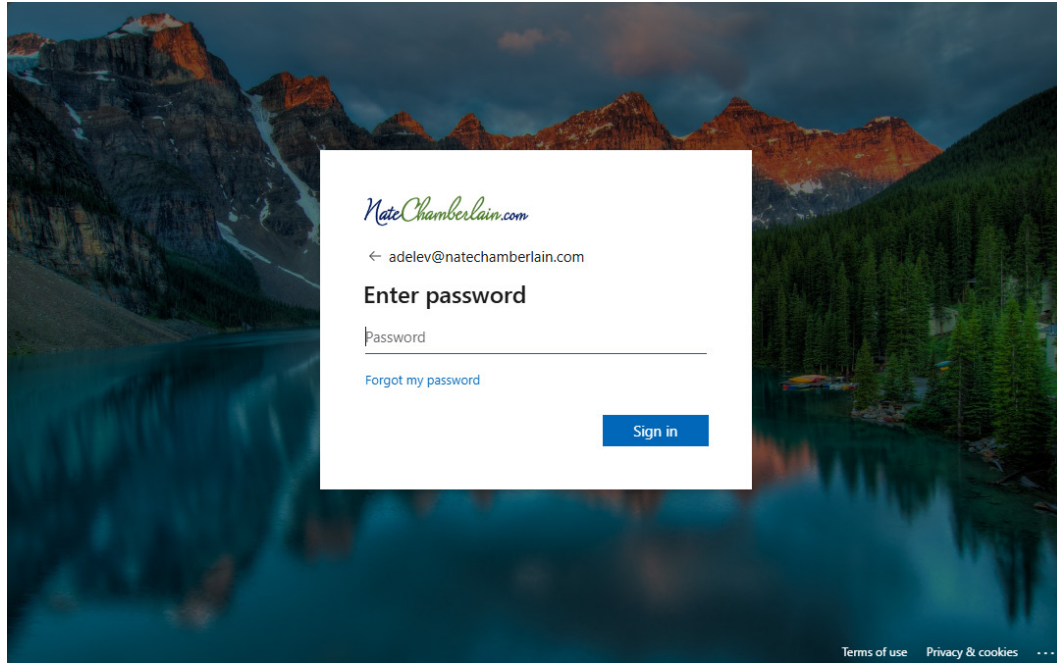


Figure 11.7 – A custom sign-in screen configured via Entra ID

This can help in reducing phishing risks by making it clear when users are on the correct sign-in page. Initially, users will see a generic login screen until Entra ID identifies the tenant they are trying to authenticate. After entering their username, the custom branding will be applied, guiding users through the familiar, branded sign-in process. Once the user enters their password correctly, they'll be asked whether they want to remain signed in. If they choose **Yes**, the custom branding will be shown immediately upon their next sign-in since Entra ID remembers them.

There's more...

To further enhance security, consider configuring Conditional Access policies that provide additional layers of authentication and control based on user location, device, and other factors.

See also

- *Configure your company branding*: <https://learn.microsoft.com/en-us/entra/fundamentals/how-to-customize-branding>

Adding a privacy statement to the Entra ID sign-in page

In this recipe, we will add a privacy statement to the Entra ID sign-in page. Including a privacy statement helps ensure that users are aware of your organization’s data handling practices and privacy policies. This transparency is important for compliance with legal and regulatory requirements.

Getting ready

You must have the Global Administrator role to complete these steps.

How to do it...

1. Sign in to the Microsoft 365 admin center at `https://admin.microsoft.com`.
2. Navigate to **Identity** from the left navigation menu under **Admin centers**.
3. Choose **User experiences | Company branding** from the left navigation menu options.
4. Select **Customize**.
5. Select the **Footer** tab at the top.
6. Locate the section for **Privacy & Cookies** and enter the **Display text** and **URL** details of your organization’s privacy statement, as shown in *Figure 11.8*:

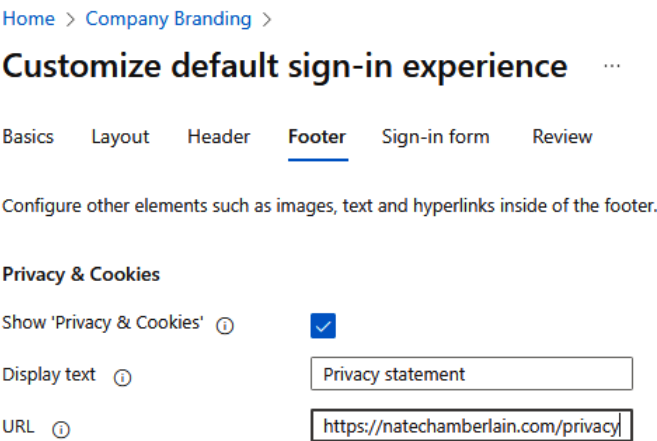


Figure 11.8 – The Privacy & Cookies section of the Footer customization

7. Select **Review + create** and then **Create** to save and implement your changes.

How it works...

When you add a privacy statement URL, it will appear on the sign-in page of your organization’s Entra ID, as shown in *Figure 11.9*:

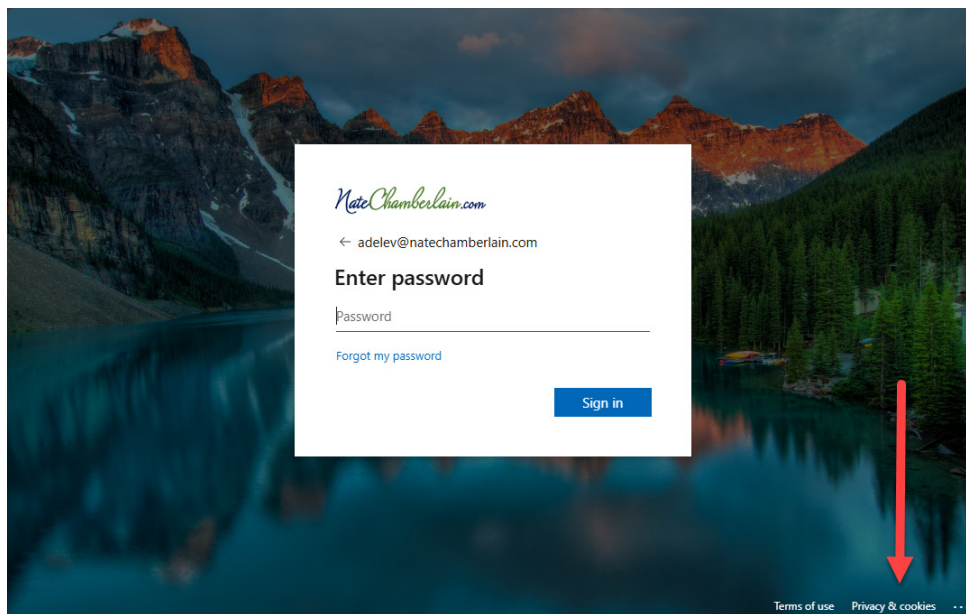


Figure 11.9 – Location of the Privacy & cookies URL you can customize

This ensures that all users and external guests are informed about your organization's privacy policies before they sign in. The privacy statement provides transparency on how user data is managed and protected, which is essential for maintaining trust and meeting regulatory requirements.

There's more...

Always consult your legal department or legal counsel when dealing with privacy or legal topics to ensure compliance with local laws and regulations. You'll also want to periodically review your privacy statement's relevance and compliance with new or changing international requirements such as the **General Data Protection Regulation (GDPR)**.

See also

- *Configure your company branding:* <https://learn.microsoft.com/en-us/entra/fundamentals/how-to-customize-branding>

Adding SSO for an application

SSO simplifies the authentication process by allowing users to access multiple third-party applications with one set of login credentials. Choosing the right SSO method is essential for ensuring security, compliance, and ease of use. This recipe will guide you through the process of selecting the appropriate SSO method for your organization based on your specific requirements and infrastructure.

Getting ready

You must have the Global or Cloud Application Administrator role to complete these steps.

How to do it...

1. Determine the applications and services that will use SSO.
2. Identify the authentication protocols supported by these applications (e.g., SAML, OpenID Connect, and OAuth).
3. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
4. Navigate to **Identity** from the left navigation menu under **Admin centers**.
5. In the left navigation menu, select **Applications | Enterprise applications**.
6. Select an application for which you wish to enable SSO.
7. Select **Single sign-on** from the application's left navigation menu, as shown in *Figure 11.10*:

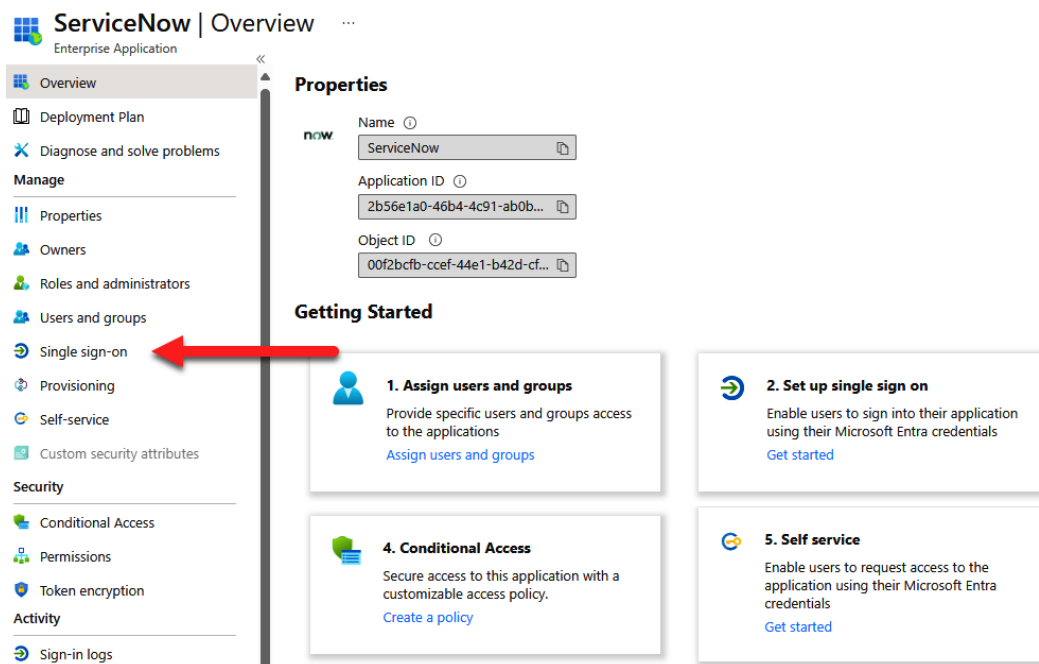


Figure 11.10 – The Single sign-on location for an application

8. Use the flowchart at **Select a single sign-on method** to help determine the best SSO method for your scenario. Different apps have different options. For example, ServiceNow offers **SAML** or **Linked**, as shown in *Figure 11.11*:

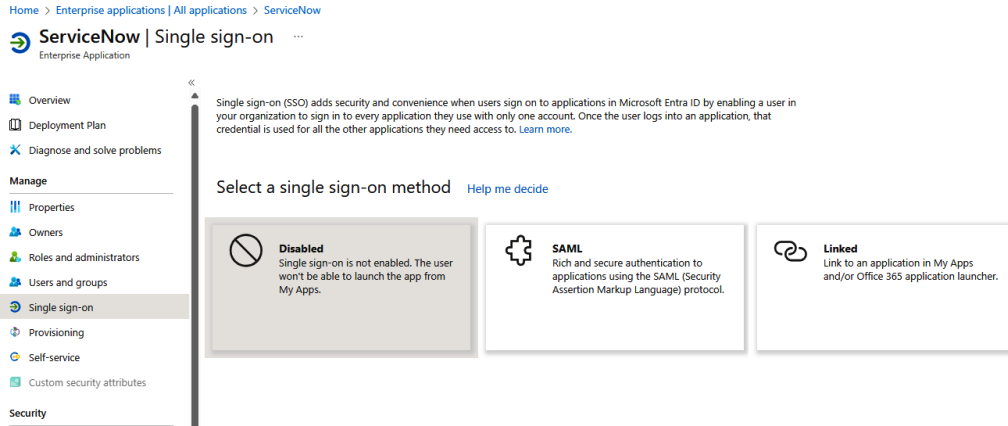


Figure 11.11 – SSO options for ServiceNow

Important note

The **Linked** option for SSO doesn't add SSO for that application. **Linked** only adds an icon to **My Apps** or the Microsoft 365 portal that can redirect users conveniently to another sign-in URL. In this case, you would likely have SSO configured through another identity service provider. If you wish to add SSO for this app, you should choose **SAML** in the ServiceNow example.

9. Enter the required details for the chosen application. Here is a breakdown of the key elements:
 - **Identifier/Entity ID:** This is a unique identifier for your application. It typically takes the form of a URL or a **Uniform Resource Identifier (URI)** that identifies the application within your identity provider (e.g., Microsoft Entra ID). The Entity ID is used to verify the authenticity of the SSO request.
 - **Reply URL/Assertion Consumer Service URL:** The Reply URL is where your identity provider sends the authentication response after the user successfully signs in. This URL must match the configuration within the application's settings. It's important to ensure that this URL is correctly entered to avoid authentication errors.
 - **Sign on URL:** The Sign-on URL is the endpoint where users will be redirected to sign in when accessing the application. This URL directs users to the SSO service where they authenticate using their Microsoft Entra ID credentials. In some cases, this URL may also be referred to as the "Login URL."
10. After configuring SSO for the chosen app, ensure that you test the setup with a small group of users to validate the integration.
11. Monitor user feedback and address any issues that arise during the testing phase.
12. Once validated, roll out the SSO configuration to the entire organization.

How it works...

Selecting the correct SSO method involves evaluating your organization's needs, understanding the supported authentication protocols, and configuring the chosen method in the Microsoft Entra admin center. This can vary greatly from one application to the next. SSO ensures that users can seamlessly access multiple applications using a single set of credentials, enhancing security and user experience. By integrating applications with Microsoft Entra ID, you centralize authentication and improve compliance with organizational policies.

There's more...

Explore advanced features such as Conditional Access policies to enhance security further. Conditional Access allows you to enforce policies based on user location, device compliance, and other factors, ensuring that only authorized users can access sensitive resources.

See also

- *What is single sign-on in Microsoft Entra ID?:* <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-single-sign-on>
- *Tutorials for integrating applications with Microsoft Entra ID:* <https://learn.microsoft.com/en-us/entra/identity/saas-apps/tutorial-list>
- *Add linked single sign-on to an application:* <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-linked-sign-on>

Getting direct sign-on links for organizational apps

Direct sign-on links allow users to access specific organizational applications directly without navigating through multiple pages. This enhances user experience by reducing the steps required to access commonly used applications, leading to increased productivity and user satisfaction.

Getting ready

You must have the Global Administrator or Application Administrator role to complete these steps. You'll also need to have completed the steps in the previous recipe, *Adding SSO for an application*, for the application(s) for which you want direct sign-on links, assuming you want the convenience of bypassing any “front door” experience to the app and utilizing your configured SSO for that app.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Navigate to **Identity** from the left navigation menu under **Admin centers**.

3. In the left navigation menu, select **Applications | Enterprise applications**.
4. Select the application for which you want to get a direct sign-on link.
5. Select **Single sign-on** from the application's left navigation menu, as previously shown in *Figure 11.10*.
6. Ensure that SSO is configured for the application. If not, follow the SSO configuration steps specific to the application. Start with this chapter's *Adding SSO for an application* recipe for guidance.
7. Once SSO is configured, select **Properties** under the **Manage** section in the application's left navigation menu, as shown in *Figure 11.12*:

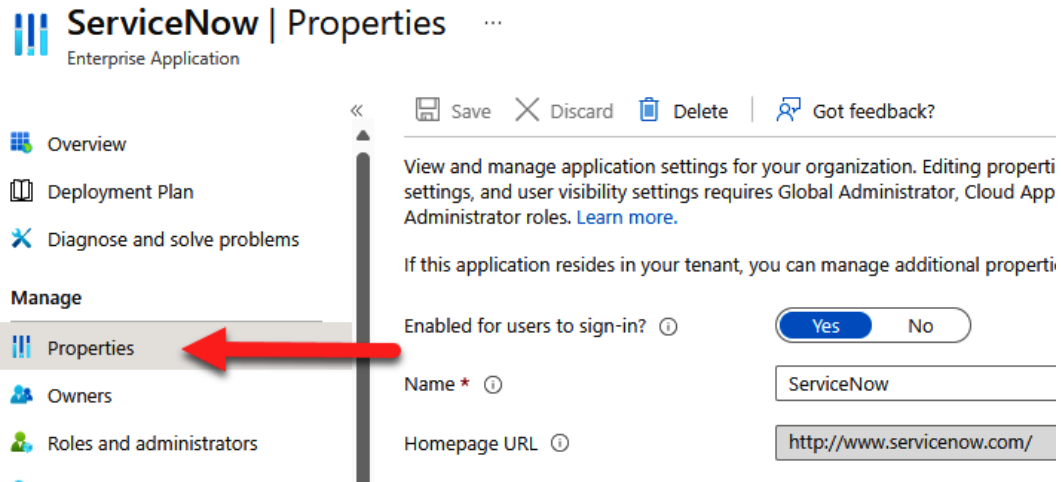


Figure 11.12 – Properties for an application in Entra ID

8. Locate **Homepage URL** and ensure it is set to the direct sign-on URL of the application. This URL should take users directly to the application after authentication.
9. Copy the **Homepage URL** details.
10. Communicate this URL to your users through email, your company's intranet, or any other communication channels.

How it works...

Getting direct sign-on links involves setting up SSO and sharing the application's homepage URL to ensure users are taken directly to the application after signing in. This bypasses intermediate navigation steps, making the login process more efficient. When users select the direct sign-on link, they are authenticated via Microsoft Entra ID and then immediately redirected to the specified application, provided SSO is properly configured.

There's more...

Direct sign-on links can be best utilized by being integrated into various organizational tools and portals. Embedding these links in your company's intranet homepage can centralize access points, making navigation straightforward for employees. Integrating these links into the **My Apps** section in Microsoft 365 (<https://myapps.microsoft.com/>) and the Microsoft 365 app launcher provides familiar locations for users to find and launch their essential applications with SSO enabled. Sharing direct sign-on links via email communications, especially during onboarding or when introducing new applications, also ensures that users have immediate access without needing to search for the links themselves.

See also

- *Five steps to integrate your apps with Microsoft Entra ID:* <https://learn.microsoft.com/en-us/entra/fundamentals/five-steps-to-full-application-integration>
- *What is single sign-on in Microsoft Entra ID?:* <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-single-sign-on>
- *What is application management in Microsoft Entra ID?:* <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>

Installing and connecting to the Microsoft Graph SDK via PowerShell

The Microsoft Graph SDK for PowerShell allows administrators to automate tasks and manage Microsoft 365 services efficiently. By using this SDK, you can access a wide range of Microsoft Graph APIs through PowerShell cmdlets, streamlining the management of Entra ID, Microsoft 365 apps, and other Microsoft services.

Getting ready

Ensure you have PowerShell 7.0 or later, administrative rights on your machine, and administrative rights to the service(s) you wish to administer via PowerShell (Entra ID for the recipes in this chapter, as a Global or User Administrator).

How to do it...

1. Open PowerShell as an administrator by searching for **PowerShell** in your **Start** menu, right-clicking it, and selecting **Run as administrator**.

2. Install the Microsoft Graph SDK module by executing the following command:

```
Install-Module Microsoft.Graph -Scope AllUsers
```

3. If prompted to install the NuGet provider, type *Y* and press *Enter*. If prompted to install from an untrusted repository, type *Y* and press *Enter*.
4. Authenticate to Microsoft Graph by running the following command:

```
Connect-MgGraph
```

5. In the dialog box that appears, enter your Microsoft 365 Administrator credentials to sign in (whichever account/role you have that is needed to execute the PowerShell tasks you wish to execute).
6. Grant the required permissions for the Graph API when prompted, as shown in *Figure 11.13*. Review and consent to the permissions.

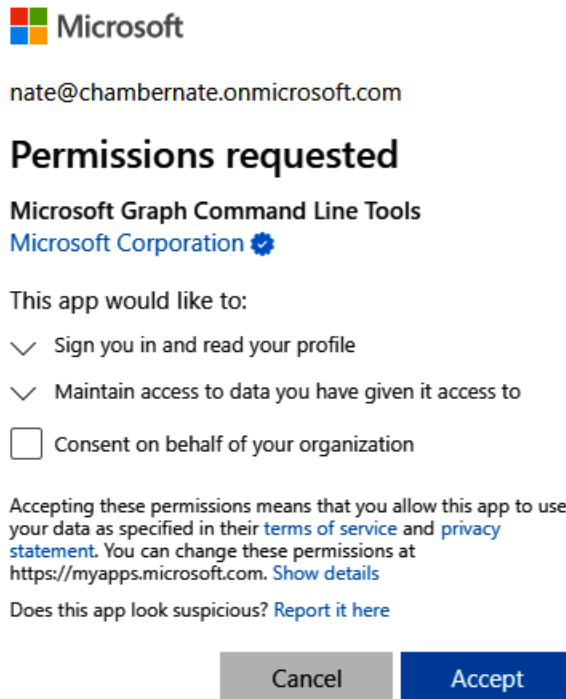


Figure 11.13 – Permissions consent for Microsoft Graph Command Line Tools

7. Verify the connection by replacing `your-user-id` with an actual user ID or email address in your tenant and running a simple command, such as the following:

```
Get-MgUser -UserId your-user-id
```

8. If successful, you'll be provided that user's display name and ID, as shown in *Figure 11.14*:

```
PS C:\Users\ndcha> Get-MgUser -UserId nate@chambernate.onmicrosoft.com
DisplayName      Id                                     Mail                                     UserPrincipalName
-----
Nate Chamberlain b97a8a47-d2c6-4874-a7c4-23c8c16779ca nate@chambernate.onmicrosoft.com nate@chambernate.onmicrosoft.com
```

Figure 11.14 – PowerShell output of the `Get-MgUser` cmdlet

How it works...

Installing and connecting to the Microsoft Graph SDK via PowerShell allows administrators to leverage the comprehensive capabilities of the Microsoft Graph API through a familiar scripting environment. The SDK translates API calls into easy-to-use PowerShell cmdlets, enabling efficient automation and management of Microsoft 365 services. The initial setup involves installing the module, authenticating it with the necessary permissions, and verifying the connection to ensure that the environment is configured correctly.

There's more...

For Microsoft 365 Administrators, especially those managing identities and groups, several cmdlets are frequently used to streamline administrative tasks. These cmdlets allow you to manage users, groups, and licenses efficiently. The following are some of the most commonly needed cmdlets along with brief explanations of what they do:

- `Get-MgUser`: Retrieves information about a specific user or a list of users in your organization. This is essential for auditing and managing user accounts.
- `New-MgUser`: Creates a new user in Microsoft 365. This cmdlet is used during the onboarding process to add new employees to the organization.
- `Update-MgUser`: Updates the properties of an existing user. This is useful for changing user details such as job titles, departments, or contact information.
- `Remove-MgUser`: Deletes a user from Microsoft 365. This cmdlet is used when offboarding employees to ensure they no longer have access to company resources.
- `Get-MgGroup`: Retrieves information about a specific group or a list of groups in your organization. This is used for managing and auditing group memberships.
- `New-MgGroup`: Creates a new group in Microsoft 365. This is useful for setting up new collaboration spaces or security groups.

- `Add-MgGroupMember`: Adds a member to a specified group. This cmdlet helps in managing group memberships effectively.
- `Remove-MgGroupMember`: Removes a member from a specified group. This is used to update group memberships when roles change.
- `Get-MgUserLicenseDetail`: Retrieves details about the licenses assigned to a user. This cmdlet is crucial for managing and auditing license assignments.
- `Update-MgUserLicenseDetail`: Assigns or removes licenses for a user. This is used to ensure that users have the necessary licenses for their roles.

By understanding what these common cmdlets can do, administrators can significantly enhance their efficiency and effectiveness in managing Microsoft 365 environments, ensuring that user and group management tasks are performed accurately and swiftly.

In the next recipe, *Adding/removing users via PowerShell in Microsoft Graph*, we'll take a closer look at using PowerShell to create and remove users.

See also

- *Get started with the Microsoft Graph PowerShell SDK*: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/get-started>
- *Install the Microsoft Graph PowerShell SDK*: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/installation>
- *Update-MgUser*: <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/update-mguser>
- *Update-MgUserLicenseDetail*: <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/update-mguserlicensedetail>

Adding/removing users via PowerShell in Microsoft Graph

Managing users through PowerShell and the Microsoft Graph SDK allows administrators to automate and streamline user account management tasks. This is particularly useful for bulk operations and can significantly reduce the time and effort required to manage user accounts.

Getting ready

Ensure you have PowerShell 7.0 or later, administrative rights on your machine, and the Global or User Administrator role in Microsoft 365.

How to do it...

1. Follow the steps in the previous recipe, *Installing and connecting to the Microsoft Graph SDK via PowerShell*, to install and connect to Microsoft Graph, if not already completed.
2. To add a new user, run the following script, replacing the placeholder values with actual user information:

```
$PasswordProfile = New-Object -TypeName Microsoft.Graph.  
PowerShell.Models.MicrosoftGraphPasswordProfile  
$PasswordProfile.Password = "aStrongP@ssw0rd"  
New-MgUser -AccountEnabled -DisplayName "John Doe"  
-PasswordProfile $PasswordProfile -MailNickName "JohnD"  
-UserPrincipalName johnd@yourdomain.com
```

3. To remove a user, run the following command, replacing the placeholder with the actual **User Principal Name (UPN)**:

```
Remove-MgUser -UserId johnd@yourdomain.com
```

4. You can double-check to ensure the user has been removed by running `Get-MgUser` with the same `-UserId` parameter value as *Step 3*.

How it works...

Adding a user involves creating a new user object and specifying necessary details such as the display name, user principal name, and password profile. The `New-MgUser` cmdlet is used to create the user in Microsoft Entra ID. Removing a user is done using the `Remove-MgUser` cmdlet, which deletes the specified user from the directory.

There's more...

The `Update-MgUser` cmdlet is a powerful tool for administrators to update user details in Microsoft 365 efficiently. This cmdlet can modify various properties of a user account, ensuring that the information remains current and accurate. Here are some examples of how you can use `Update-MgUser` to update user details.

You can update a user's display name (the `-DisplayName` parameter):

```
Update-MgUser -UserId user@example.com -DisplayName "New Display Name"
```

You can change a user's job title (the `-JobTitle` parameter):

```
Update-MgUser -UserId user@example.com -JobTitle "Senior Manager"
```

You can also combine multiple properties into one command, such as if you need to change a user's department (-Department), mobile phone number (-MobilePhone), and office location (-OfficeLocation):

```
Update-MgUser -UserId user@example.com -Department "Marketing"  
-MobilePhone "+1234567890" -OfficeLocation "Building A, Room 101"
```

By using the Update-MgUser cmdlet, administrators can swiftly ensure that user profiles are up to date with accurate information.

See also

- *Create User*: <https://learn.microsoft.com/en-us/graph/api/user-post-users>
- *Update user*: <https://learn.microsoft.com/en-us/graph/api/user-update>
- *Delete a User*: <https://learn.microsoft.com/en-us/graph/api/user-delete>

Creating an Access review report in Entra ID

Access reviews in Microsoft Entra ID allow administrators to regularly review who has access to specific applications and groups, ensuring compliance and security. This process helps manage memberships, control guest access, and enhance governance by making access privileges transparent and regularly updated.

Getting ready

To complete this recipe, you must be a Global Administrator or User Administrator. Additionally, you need a Microsoft Entra ID Premium P2 subscription.

Important note

Some access review features require an Entra ID Premium P2 subscription, while a full Microsoft Entra ID Governance subscription is needed for complete functionality. Learn more at <https://learn.microsoft.com/en-us/entra/id-governance/licensing-fundamentals>.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Navigate to **Identity** from the left navigation menu under **Admin centers**.

3. Select **Identity Governance** | **Access reviews**, as shown in *Figure 11.15*:

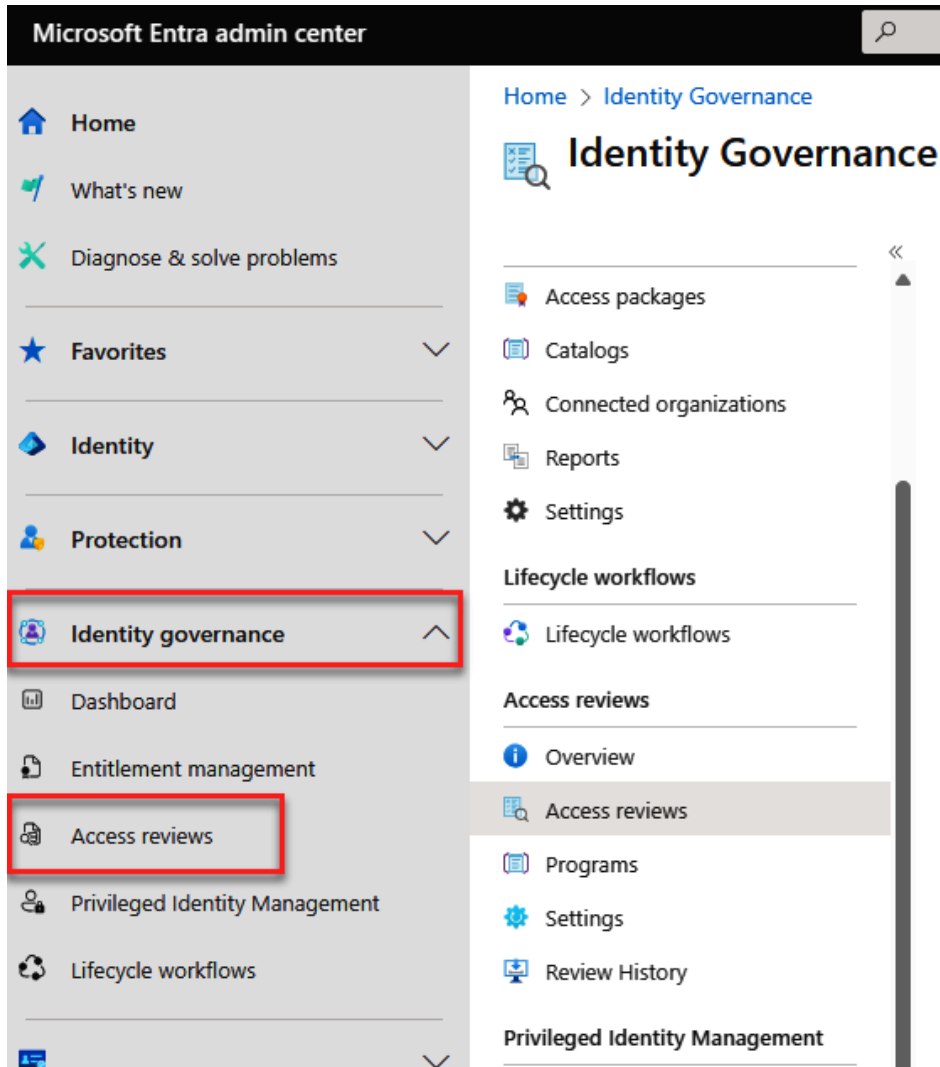


Figure 11.15 – Location of Access reviews in the Microsoft Entra admin center

4. If this is your first time creating an access review, select **Onboard** and follow the instructions. If you have already onboarded, skip to *Step 8*.
5. Review the onboarding information and select **Onboard Now**.
6. Wait for the onboarding process to complete. You will receive a notification once it's done.

7. Navigate back to **Identity Governance | Access reviews**.
8. Select **New access review**.
9. Select **Teams + Groups** for the review type.
10. Choose either **All Microsoft 365 groups with guest users** or **Select Teams + groups**.
11. Decide whether to review **Guest users only** or **All users** in the chosen group(s). *Figure 11.16* illustrates the access review setup so far, with specific groups selected and all members included:

New access review ...

*** Review type** *** Reviews** Settings *** Review + Create**

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles.
[Learn more](#)

Select what to review *

Teams + Groups

Review scope *

☐ All Microsoft 365 groups with guest users ⓘ

☒ Select Teams + groups

Group *

[Recognition Committee and 3 others](#)

Scope *

☐ Guest users only

☒ All users ⓘ

Figure 11.16 – Initial configuration screen of an Entra ID access review

12. Select **Next: Reviews**.
13. Choose between a multi-stage or single-stage review. For multi-stage reviews, you can have up to three levels of reviewers.
14. For reviewers, select from the following:
 - **Group owner(s)**
 - **Selected user(s) or group(s)**
 - **Users review their own access**
 - **Managers of users**

15. Specify the review period duration and the frequency for repeating the review. *Figure 11.17* shows a single-stage access review, assigned to group owners with **Nate Chamberlain** as a fallback reviewer, set for 7 days, and repeating semi-annually:

New access review

* Review type

* **Reviews**

Settings

* Review + Create

Determine review stages, reviewers, and timeline below.

Multi-stage review *

☐

Specify reviewers

Select reviewers *

Group owner(s)

Fallback reviewers

Nate Chamberlain

Specify recurrence of review

Duration (in days) *

7

Review recurrence *

Semi-annually

Start date *

03/17/2024

End

☒ Never

☐ End on specific date

☐ End after number of occurrences

< Previous

Next: Settings

Figure 11.17 – Reviewers and recurrence settings of an access review

16. Select **Next: Settings**.
17. Configure completion and advanced settings, such as automatic removal or retention of access after the review. *Figure 11.18* displays the settings available:

New access review ...

* Review type * Reviews **Settings** * Review + Create

Configure additional settings, including decision helpers and email notifications.

Upon completion settings

Auto apply results to resource ⓘ



If reviewers don't respond ⓘ

Take recommendations



Setting 'If reviewers don't respond' to 'Remove access' or 'Take recommendations' while 'Auto-apply results to resource' is enabled could potentially lead to all access to this resource being revoked if the reviewers fail to respond.

At end of review, send notification to

[Nate Chamberlain](#)

Enable reviewer decision helpers

No sign-in within 30 days ⓘ



User-to-Group Affiliation ⓘ



Advanced settings

Justification required ⓘ



Email notifications ⓘ



Reminders ⓘ



Additional content for reviewer email ⓘ

< Previous

Next: Review + Create

Figure 11.18 – Settings for an access review

18. Select **Next: Review + Create**, review your settings, name your review, and select **Create** to start the access review.

19. If you selected specific groups, each group will appear as a separate review in the **Access reviews** section of Microsoft Entra ID, as shown in *Figure 11.19*. This allows administrators to monitor the results and status of each group’s review independently:

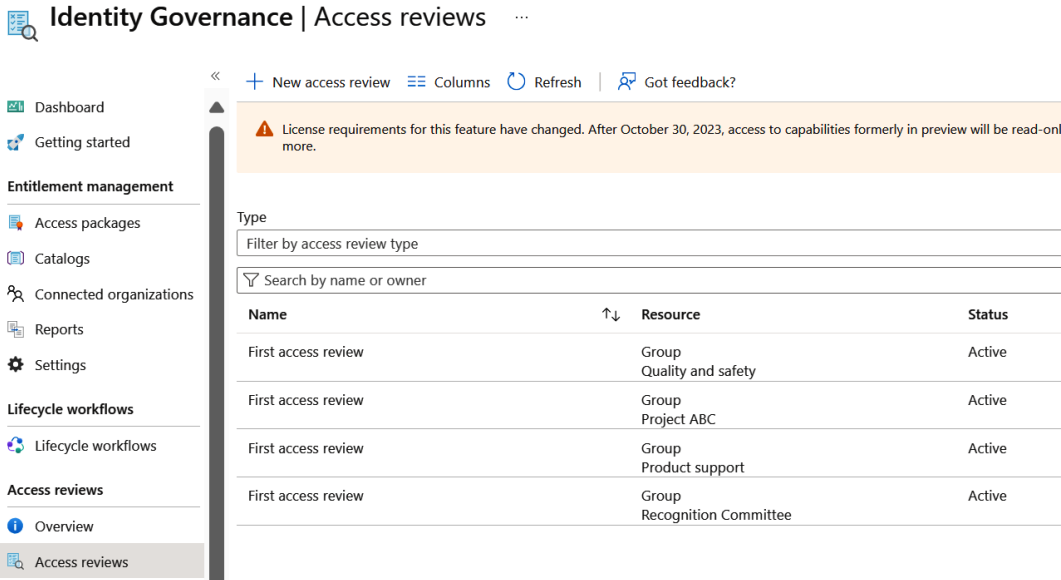


Figure 11.19 – Access reviews in Microsoft Entra ID

How it works...

Creating an access review in Entra ID enables administrators to periodically verify user access to applications and groups, ensuring only authorized users retain access. This enhances security and compliance by maintaining up-to-date access controls.

Specified reviewers will also receive email notifications, such as the one shown in *Figure 11.20*, prompting them to review and confirm or revoke access based on user activity and organizational requirements.

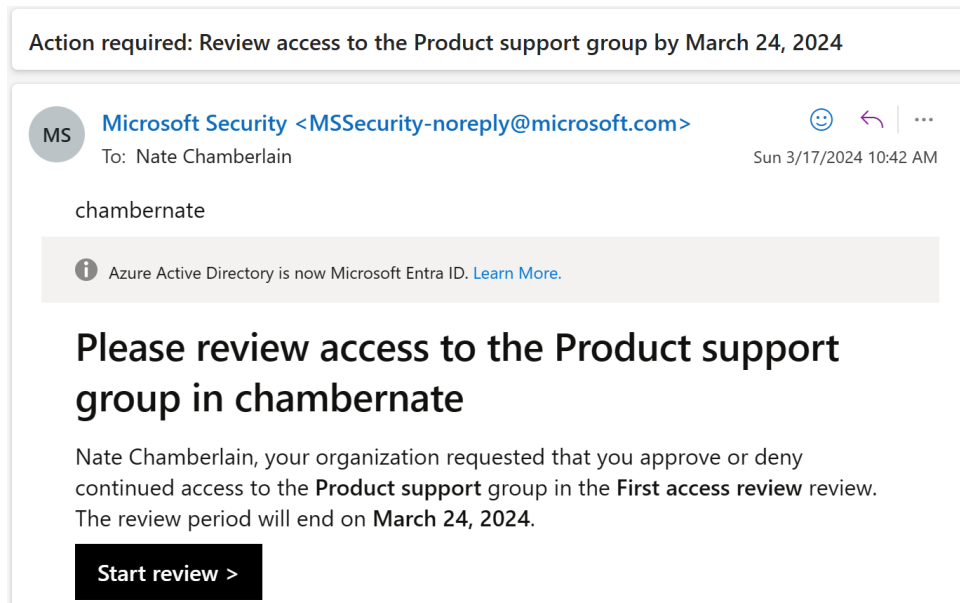


Figure 11.20 – Email requesting group member review

See the next recipe, *Reviewing and completing an Access review report in Entra ID*, to learn more about the review process.

There's more...

For more advanced capabilities, consider using automation features in Entra ID, such as dynamic groups and Conditional Access policies. These features further streamline access management and enhance security.

See also

- *What are access reviews?:* <https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview>
- *Review access for yourself to groups or applications in access reviews:* <https://learn.microsoft.com/en-us/entra/id-governance/review-your-access>
- *Create an access review of groups and applications in Microsoft Entra ID:* <https://learn.microsoft.com/en-us/entra/id-governance/create-access-review>

Reviewing and completing an Access review report in Entra ID

Reviewing and completing an access review report in Entra ID helps administrators ensure that users have appropriate access to applications and groups. This process is essential for maintaining security and compliance by regularly validating access permissions.

Getting ready

You must be a Global Administrator or User Administrator to complete these steps. Additionally, you need a Microsoft Entra ID Premium P2 subscription.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Navigate to **Identity** from the left navigation menu under **Admin centers**.
3. Select **Identity Governance | Access reviews**, as previously shown in *Figure 11.15*.
4. Select the access review you want to complete.
5. Select **Reviewers** if you want to see who needs to review access.
6. You, as an administrator, or the reviewers listed can review the access details and decide whether to approve or deny access for each user. Reviewers also receive an emailed link specifically to the access review, as shown in *Figure 11.21*:

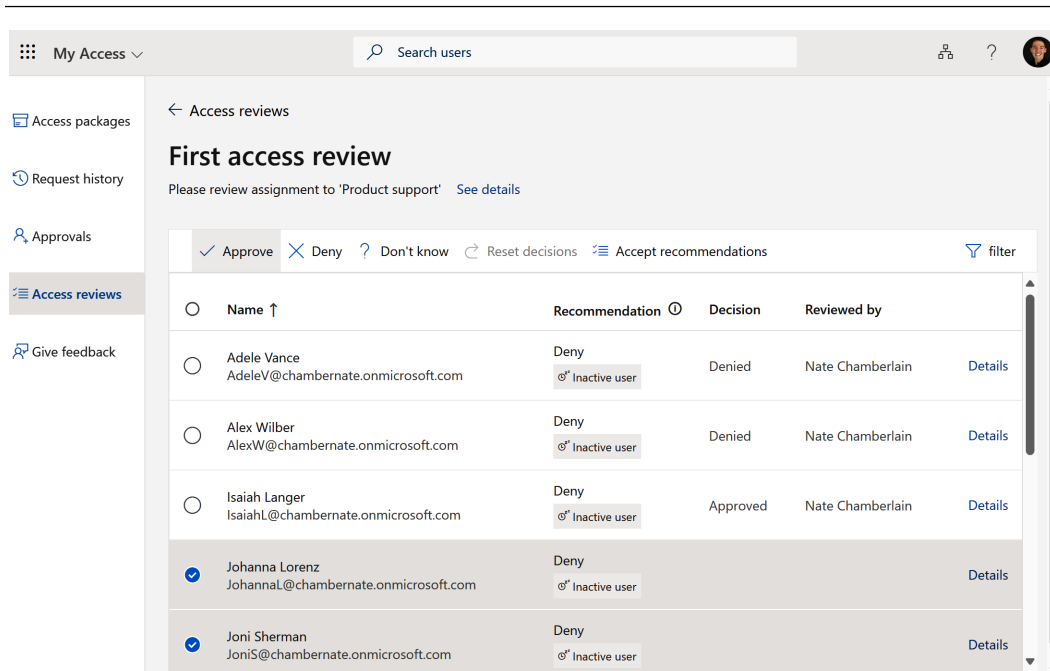


Figure 11.21 – Access review screen for a group reviewer

7. Use the **Approve** or **Deny** buttons to complete your decisions.
8. Select **Complete** to finalize the review.

How it works...

Completing an access review involves verifying user access to applications and groups. The reviewers examine the access rights of each user and decide whether to approve or revoke access. This ensures that only authorized users retain access, enhancing security and compliance.

There's more...

Rather than manually visiting the admin center, your access reviews email the reviewers and remind them, giving them a direct link to begin. Here's what their experience resembles:

1. Once the review starts, specified reviewers will receive an email similar to the one previously shown in *Figure 11.20*, with a link to the review.
2. During the review, reviewers can choose **Approve**, **Deny**, **Don't know**, or **Accept recommendations** (based on member activity), as previously shown in *Figure 11.21*.
3. Based on their selections, members will be removed, retained, or moved to the next review stage, if applicable.

Your reviewers might be group owners or even group members themselves, self-certifying the need for continued access.

See also

- *What are access reviews?:* <https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview>
- *Review access for yourself to groups or applications in access reviews:* <https://learn.microsoft.com/en-us/entra/id-governance/review-your-access>
- *Create an access review of groups and applications in Microsoft Entra ID:* <https://learn.microsoft.com/en-us/entra/id-governance/create-access-review>

Enabling self-service password reset

Self-service password reset (SSPR) allows users to reset their passwords without administrator intervention. This feature enhances user productivity and reduces the administrative burden by enabling users to manage their own passwords securely.

Getting ready

You must be a Global Administrator to complete these steps. Additionally, you need a Microsoft Entra ID Premium P1 or P2 subscription.

How to do it...

1. Sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Navigate to **Identity** from the left navigation menu under **Admin centers**.
3. In the left navigation menu, select **Protection | Password reset**.
4. By default, you will be on the **Properties** screen shown in *Figure 11.22*:

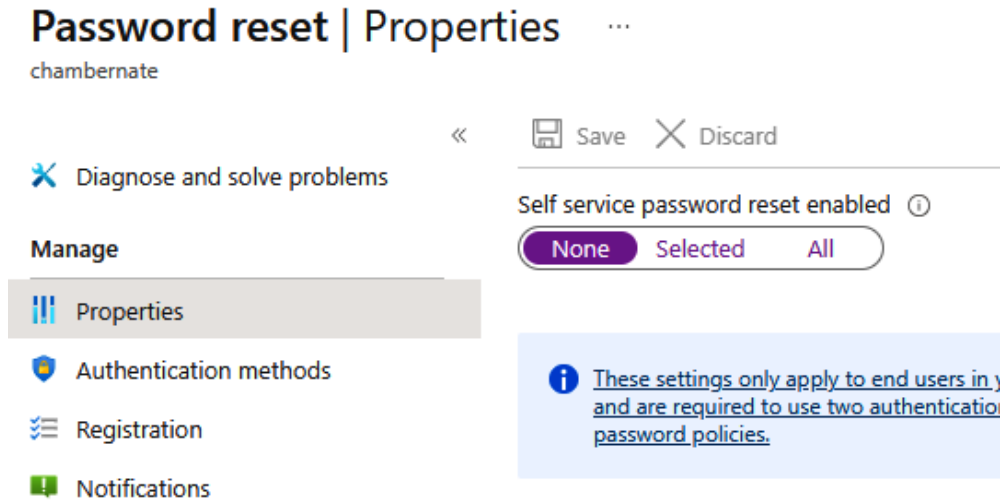


Figure 11.22 – The Self service password reset setting

5. Set **Self service password reset enabled** to **Selected** (some users) or **All**.
6. If you chose **Selected**, select the users or groups for whom you want to enable SSPR.
7. Select **Save**.

How it works...

Enabling SSPR allows users to reset their passwords using preconfigured authentication methods. When a user forgets their password, they can verify their identity using these methods and reset their password without needing to contact the help desk. This improves user satisfaction and reduces support costs.

There's more...

Once you've enabled SSPR, you can further configure the authentication methods users are allowed to use to reset their passwords. Here's how:

1. On the **Password reset** screen, go to **Authentication methods**.
2. Configure the methods users can use to reset their passwords (e.g., email, mobile phone, etc.) as well as the **Number of methods required to reset** value (1 or 2). These options are shown in *Figure 11.23*:

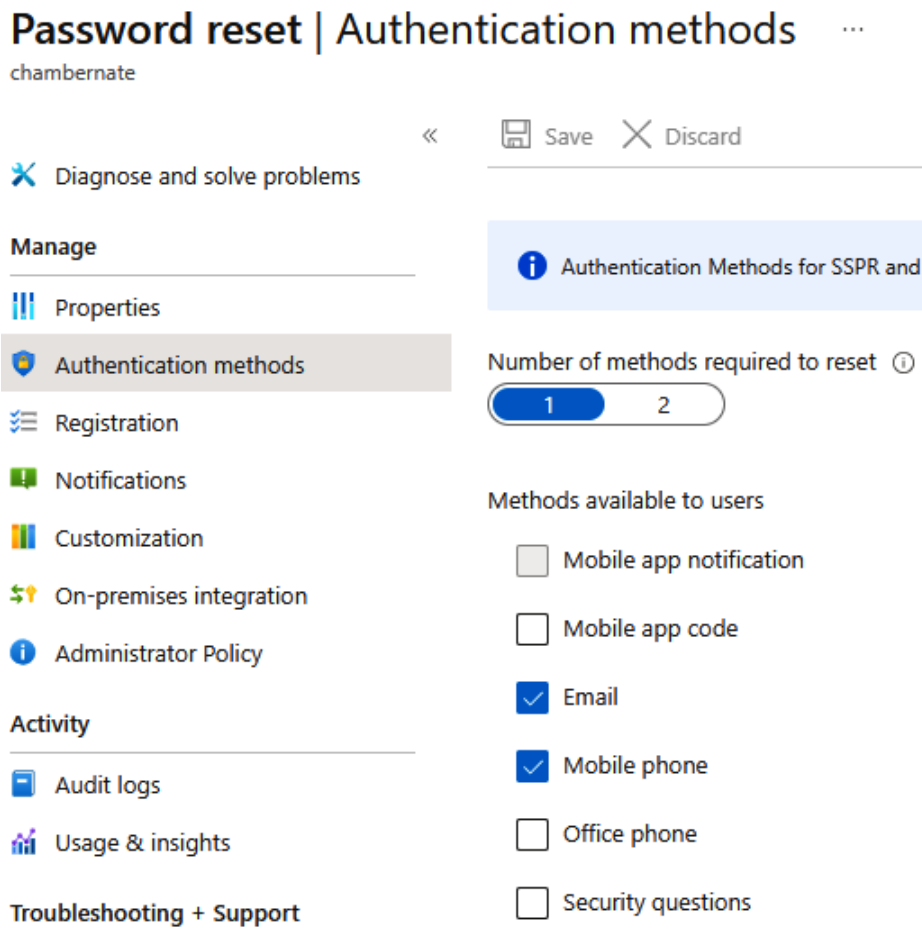


Figure 11.23 – Authentication methods for password reset

3. Select **Save** to apply the settings.

You should also consider enabling additional security features such as **multi-factor authentication (MFA)** to further secure the password reset process. MFA ensures that only verified users can reset their passwords.

See also

- *Tutorial: Enable users to unlock their account or reset passwords using Microsoft Entra self-service password reset:* <https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr>
- *How it works: Microsoft Entra self-service password reset:* <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks>
- *Self-service password reset FAQ:* <https://learn.microsoft.com/en-us/entra/identity/authentication/passwords-faq>

Understanding Microsoft Defender

Microsoft Defender provides a comprehensive suite of security tools designed to protect your Microsoft 365 environment from various threats. This chapter covers essential recipes for utilizing Microsoft Defender to enhance your organization's security posture. You'll learn how to set up policies, monitor reports, and use advanced security features to ensure your data and users are protected.

We will cover the following recipes in this chapter:

- Creating a threat protection policy
- Setting up a Safe Links policy
- Setting up a Safe Attachments policy
- Accessing and reviewing an organization's Secure Score
- Complying with Secure Score security configuration recommendations
- Assigning permissions for non-IT users to Microsoft Defender
- Monitoring Microsoft Defender reports
- Utilizing threat investigation and response capabilities
- Utilizing automated investigation and response capabilities

Technical requirements

To complete the recipes in this chapter, you need a Microsoft 365 E5, A5, or Microsoft 365 Business Premium subscription, or add-on licensing, for most security features as well as the Global or Security Administrator role in your Microsoft 365 tenant.

Several actions will require that audit logging is enabled in your tenant. You can check to see if it is by visiting the Microsoft Purview portal's **Audit** feature at <https://purview.microsoft.com/audit>. If logging is not currently enabled, select **Start recording user and admin activity** at the top of the page to enable it.

Creating a threat protection policy

Threat protection policies in Microsoft Defender for Office 365 are essential for safeguarding your organization from various types of threats, such as phishing, spam, and malware. This recipe will help you set up a comprehensive threat protection policy.

Getting ready

To create a threat protection policy, you must have Global or Security Administrator privileges. Ensure audit logging is enabled for your organization via the Microsoft Purview portal at <https://purview.microsoft.com/audit>. Additionally, verify that your Microsoft 365 licensing includes E5, A5, or Business Premium.

How to do it...

1. Navigate to the Microsoft Defender portal at <https://security.microsoft.com/> and select **Email & Collaboration | Policies & Rules**.
2. Select **Threat policies** and then choose **Create policy**.
3. Select the type of threat protection policy you want to create, such as **Anti-malware**, **Anti-spam**, or **Anti-phishing**. These, and more, are shown in *Figure 12.1*:

Threat policies

Templated policies



Preset Security Policies



Configuration analyzer

Policies



Anti-phishing



Anti-spam



Anti-malware



Safe Attachments



Safe Links

Figure 12.1 – Threat policy options

4. Provide a unique and descriptive name for your policy, then select **Next**.
5. Add the users and/or groups to whom this policy should apply, then select **Next**.
6. Configure protection settings:
 - **For anti-phishing policies:** Add users and domains to protect against impersonation and specify actions for detected phishing attempts, such as moving to junk or quarantining.
 - **For anti-spam policies:** Create an inbound or outbound policy that specifies criteria for determining spam scores and thresholds. If a message scores high enough, you can prepend the subject line with text such as [SPAM], move a message to the Spam folder, forward to additional recipients, or prevent it from being sent in the first place (if it's outbound).
 - **For anti-malware policies:** Specify the action to take when malware is detected, such as block, quarantine, or monitor.
7. Set up admin notifications for detected threats, specifying email addresses for alerts.
8. Define specific actions for detected threats, such as blocking, replacing, or monitoring emails and attachments.
9. Carefully review all configured settings.
10. Select **Submit** to apply the policy.

How it works...

Threat protection policies in Microsoft Defender for Office 365 scan emails, attachments, and links for malicious content. They use advanced threat intelligence and machine learning to detect and block threats before they reach end users. These policies ensure that the organization remains protected against evolving cyber threats by providing real-time protection and alerts to administrators.

While we covered three specific policy types in this recipe, there are more to be found under **Threat policies**:

- **Templated policies:**
 - **Preset Security Policies**
 - **Configuration analyzer**
- **Policies:**
 - **Anti-phishing**
 - **Anti-spam**
 - **Anti-malware**
 - **Safe Attachments** (see this chapter's *Setting up Safe Attachments policy* recipe)
 - **Safe Links** (see this chapter's *Setting up Safe Links policy* recipe)
- **Rules:**
 - **Tenant Allow/Block Lists**
 - **Email authentication settings**
 - **Advanced delivery**
 - **Enhanced filtering**
 - **Quarantine policies**
- **Others:**
 - **Evaluation mode**

There's more...

Microsoft Defender for Office 365 includes advanced features such as Threat Explorer, Threat Trackers, and Attack Simulation Training to enhance your threat protection strategy. These tools provide detailed insights and training capabilities to help your organization stay ahead of potential threats.

See also

- *Anti-malware protection in EOP*: <https://learn.microsoft.com/en-us/defender-office-365/anti-malware-protection-about>
- *MS-102 Implement threat protection by using Microsoft Defender XDR*: <https://learn.microsoft.com/en-us/training/paths/implement-threat-protection-use-microsoft-365-defender/>

Setting up a Safe Links policy

Safe Links in Microsoft Defender helps protect your organization by providing time-of-click verification of URLs, preventing users from accessing malicious links in emails, Teams, and Office documents. This recipe guides you through the process of setting up a Safe Links policy.

Getting ready

To complete these steps, you must have either Global or Security Administrator privileges. Additionally, verify that your Microsoft 365 licensing includes E5, A5, or Business Premium or that you have licensing for Microsoft Defender for Office Plan 1 or 2. Plan 1 is included in Business Premium and E3 (and equivalent) licensing. Plan 2 is included in E5 (and equivalent) licensing.

How to do it...

1. Navigate to Microsoft Defender at <https://security.microsoft.com/> and go to **Email & collaboration | Policies & rules**.
2. Select **Threat policies**, as shown in *Figure 12.2*:

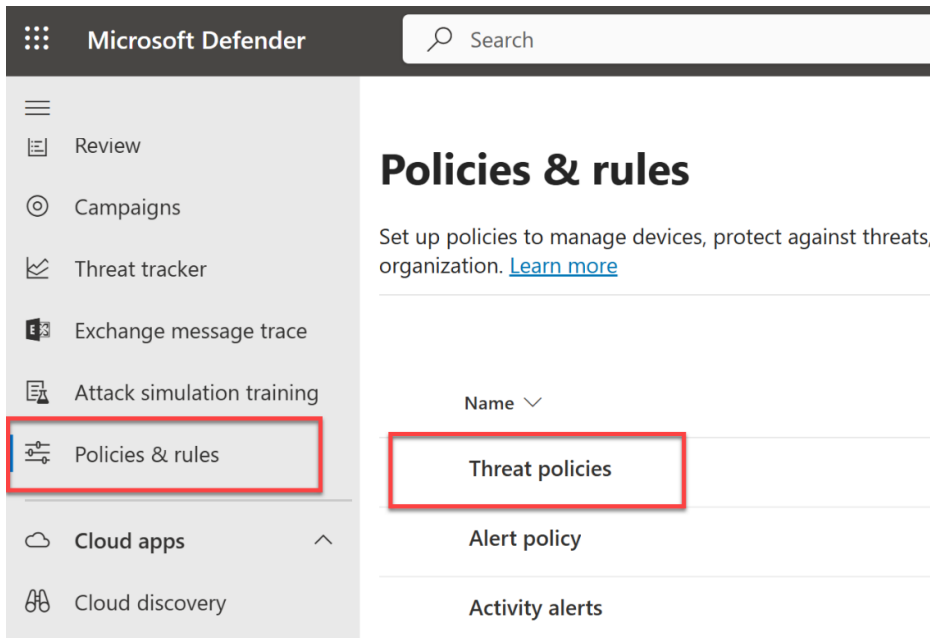
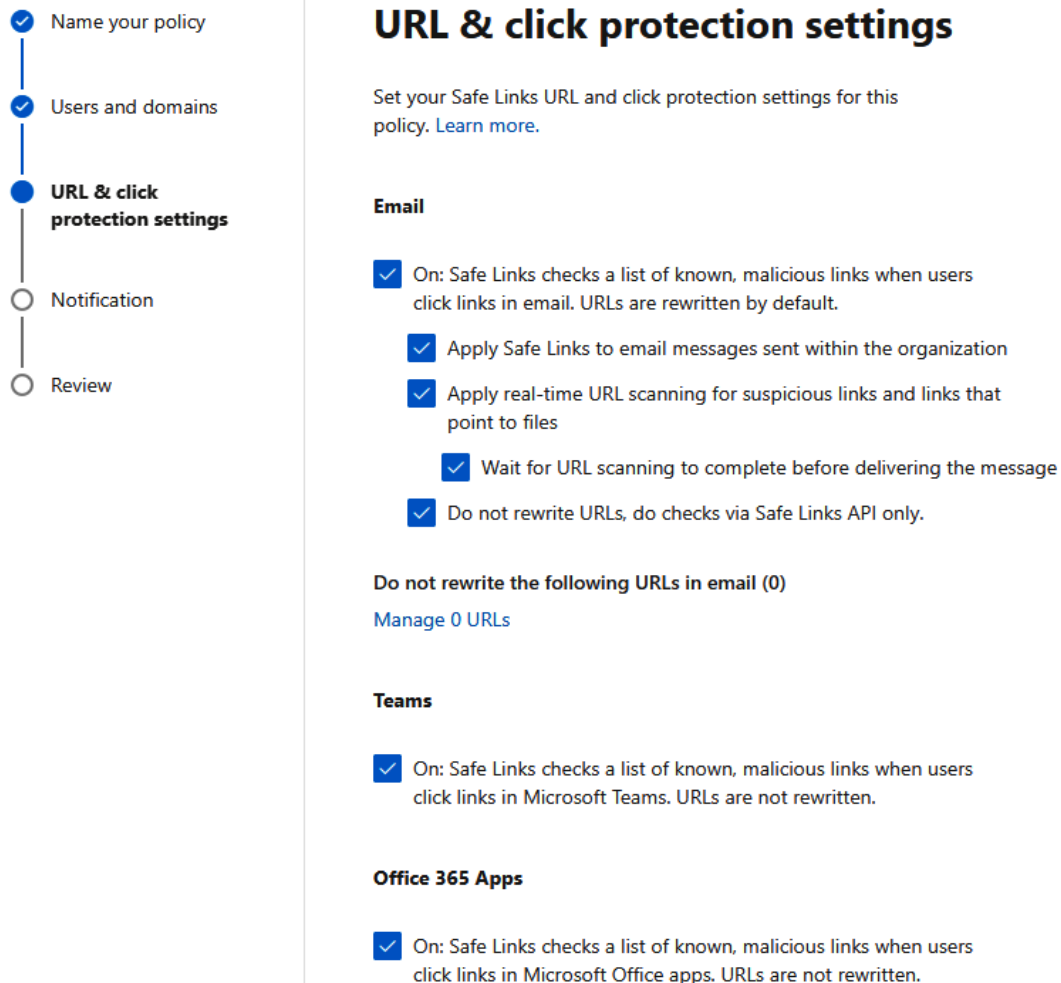


Figure 12.2 – Location of Threat policies in Microsoft Defender

3. In the **Policies** section, select **Safe Links**.
4. Select **Create** to set up a new policy.
5. Name and describe the new **Safe Links** policy and select **Next**.
6. Specify the users and/or groups the new policy will apply to.
7. Select **Next** and define the scenarios to enable **Safe Links**, such as URL rewriting, applying the policy to internal emails, and checking links shared in Teams. These settings and more are shown in *Figure 12.3*:

Policies & rules > Threat policies > Create safe links policy



URL & click protection settings

Set your Safe Links URL and click protection settings for this policy. [Learn more.](#)

Email

- ☒ On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default.
- ☒ Apply Safe Links to email messages sent within the organization
- ☒ Apply real-time URL scanning for suspicious links and links that point to files
- ☒ Wait for URL scanning to complete before delivering the message
- ☒ Do not rewrite URLs, do checks via Safe Links API only.

Do not rewrite the following URLs in email (0)
[Manage 0 URLs](#)

Teams

- ☒ On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten.

Office 365 Apps

- ☒ On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office apps. URLs are not rewritten.

Figure 12.3 – Safe Links policy settings

8. Select **Next**, then choose whether to use the default notification or create a custom notification message for users.
9. Select **Review** then **Submit** to apply the policy.

How it works...

Setting up Safe Links policies involves configuring URL scanning and rewriting settings to ensure that users are protected from malicious links. Safe Links verifies URLs at the time of click, blocking access to dangerous sites or content. This protection extends to emails, Microsoft Teams, and Office applications, ensuring comprehensive security across Microsoft 365 services.

There's more...

Microsoft automatically enables built-in protection for Safe Links and Safe Attachments for Defender for Office 365 tenants. Custom policies are only necessary if you need configurations different from the preset security policies. To review preset security options, visit <https://security.microsoft.com/presetSecurityPolicies> and select whether to add exclusions or choose **Standard protection** or **Strict protection**, as shown in *Figure 12.4*:

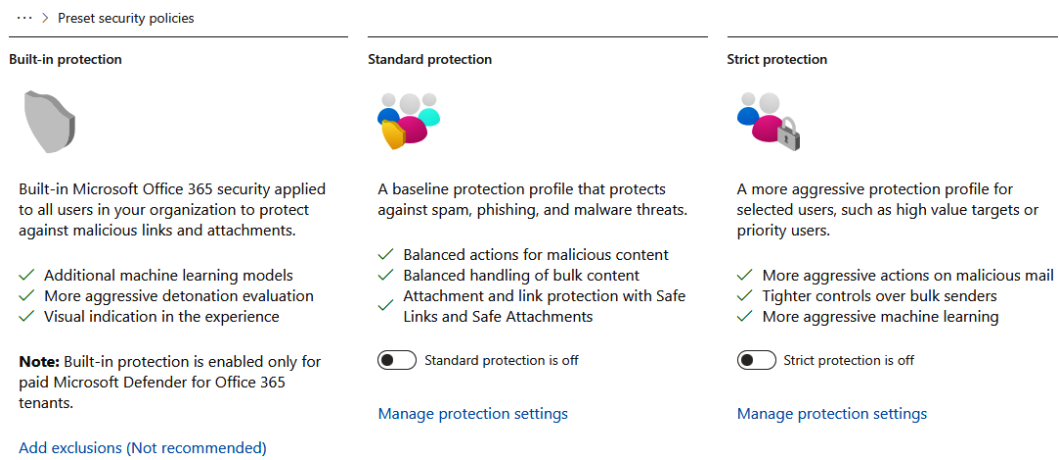


Figure 12.4 – Preset security policies in Microsoft Defender

See also

- *Safe Links in Microsoft Defender for Office 365*: <https://learn.microsoft.com/en-us/defender-office-365/safe-links-about>
- *Preset security policies in EOP and Microsoft Defender for Office 365*: <https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies>

Setting up a Safe Attachments policy

Safe Attachments in Microsoft Defender provides an extra layer of security by using a virtual environment to analyze email attachments for malicious content before they are delivered to recipients. This guide will walk you through the process of setting up a Safe Attachments policy.

Getting ready

To set up a Safe Attachments policy, you need Global or Security Administrator privileges. Ensure that audit logging is enabled for your organization, which can be done from the Microsoft Purview portal at <https://purview.microsoft.com/audit>. Additionally, verify that your Microsoft 365 licensing includes E5, A5, or Business Premium.

How to do it...

1. Navigate to the Microsoft Defender portal at <https://security.microsoft.com/> and go to **Email & Collaboration | Policies & Rules**.
2. Select **Threat policies**, and then select **Safe Attachments**.
3. Select **Create**, as shown in *Figure 12.5*, to set up a new policy.

Policies & rules > Threat policies > Safe attachments

Safe attachments

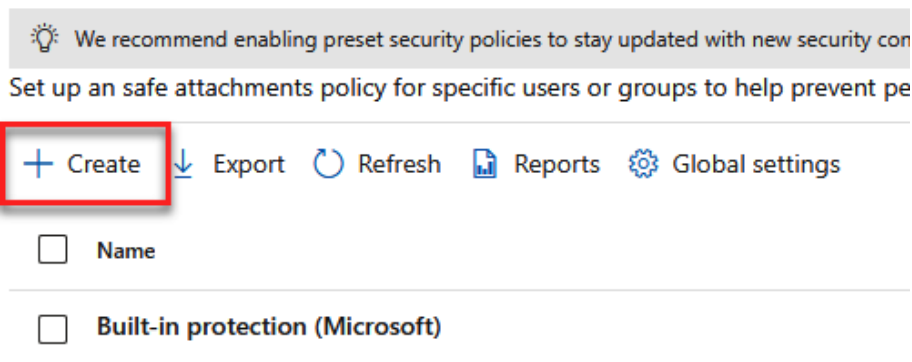


Figure 12.5 – Safe attachments policy creation button

4. Name and describe the new **Safe Attachments** policy, then select **Next**.
5. Specify the users and/or groups to whom the new policy will apply, then select **Next**.

6. Define the actions to take when an attachment is detected as malicious, such as **Off** (do nothing), **Block** (blocks current and future messages with malware), **Monitor** (deliver if malware is detected, but track results), or **Dynamic Delivery** (where emails are delivered but attachments are delayed until malware scanning is complete). Some of these options are shown in the configuration screen in *Figure 12.6*:

Safe Attachments unknown malware response

Select the action for unknown malware in attachments. [Learn more](#)

Warning

- **Monitor** and **Block** actions might cause a significant delay in message delivery. [Learn more](#)
- **Dynamic Delivery** is only available for recipients with hosted mailboxes.
- For **Block** or **Dynamic Delivery**, messages with detected attachments are quarantined and can be released only by an admin.

- ☐ Off - Attachments will not be scanned by Safe Attachments.
- ☐ Monitor - Deliver the message if malware is detected and track scanning results.
- ☐ Block - Block current and future messages and attachments with detected malware.
- ☒ Dynamic Delivery (Preview messages) - Immediately deliver the message without attachments. Reattach files after scanning is complete.


Quarantine policy

AdminOnlyAccessPolicy

Permission to release quarantined messages will be ignored for messages with malware detected and we will fall back to release request instead

Redirect messages with detected attachments

Enable redirect only supports the Monitor action. [Learn more](#)

☐ Enable redirect 

Send messages that contain monitored attachments to the specified email address.

Figure 12.6 – Safe attachments policy configuration options

7. Select **Next**, verify your settings, and then select **Submit** to apply the policy.

How it works...

Safe Attachments uses a virtual environment to analyze attachments in emails and documents for malicious content. When an attachment is detected as malicious, the policy you configure determines the action taken:

- **Off:** No action is taken, and the attachment is delivered without scanning
- **Block:** Blocks the attachment and any future messages containing the same malware
- **Monitor:** Delivers the attachment but logs and monitors it for any malicious activity
- **Dynamic Delivery:** Delivers the email immediately, but delays the attachment until it has been scanned and confirmed safe

With the **Dynamic Delivery** option, the delay for attachments typically ranges from a few seconds to several minutes, depending on the size of the attachment and the current system load. This delay ensures that the attachment is thoroughly scanned in a virtual environment, providing an extra layer of protection without significantly impacting the user experience.

There's more...

As with Safe Links, Microsoft automatically enables built-in protection for Safe Attachments for Defender for Office 365 tenants. Custom policies are only necessary if you need configurations different from the preset security policies.

For comprehensive protection, Microsoft Defender for Office 365 also includes features like Safe Links covered in the previous recipe as well as integration with SharePoint, OneDrive, and Teams. Safe Attachments can be extended to protect files stored and shared within these services, providing a robust defense against malware across all Microsoft 365 platforms.

See also

- *Safe Attachments in Microsoft Defender for Office 365:* <https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-about>
- *Safe Attachments for SharePoint, OneDrive, and Microsoft Teams:* <https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-for-spo-odfb-teams-about>

Accessing and reviewing an organization's Secure Score

Your organization's **Secure Score** provides an assessment of your security posture based on your configuration settings, security policies, and user activity. This score helps you understand how well protected your organization is and provides recommendations to improve security. This recipe will guide you through accessing and reviewing your Secure Score in Microsoft 365.

Getting ready

You need to be a Global Administrator, Security Administrator, Compliance Administrator, Global Reader, or Security Reader to access Secure Score.

How to do it...

1. Navigate to Microsoft Secure Score at <https://security.microsoft.com/securescore>. Alternatively, go to Microsoft Defender at <https://security.microsoft.com> and select **Exposure management | Secure Score** from the left navigation menu.
2. On the Secure Score **Overview** page, review the breakdown of your score in the leftmost column, which includes categories such as **Identity** (accounts and roles in Entra ID), **Data** (Microsoft Information Protection), and **Apps** (email and cloud apps, including Microsoft 365 and Cloud App Security). An example of this is shown in *Figure 12.7*:

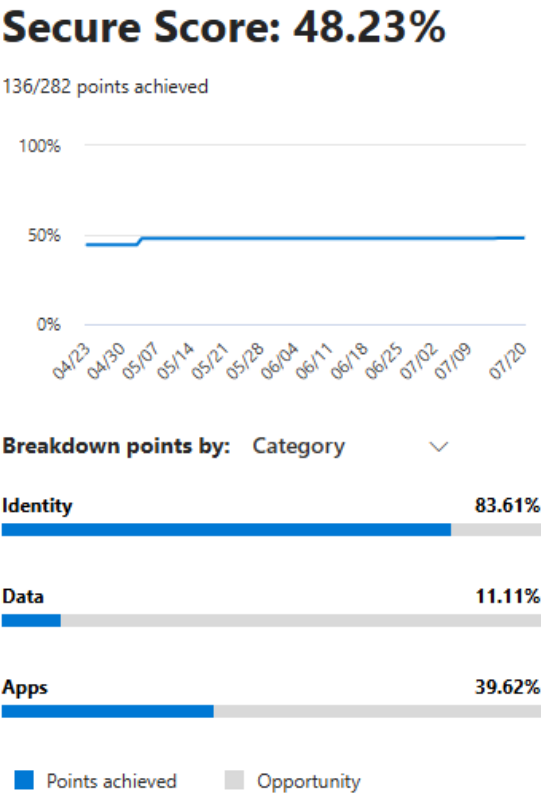
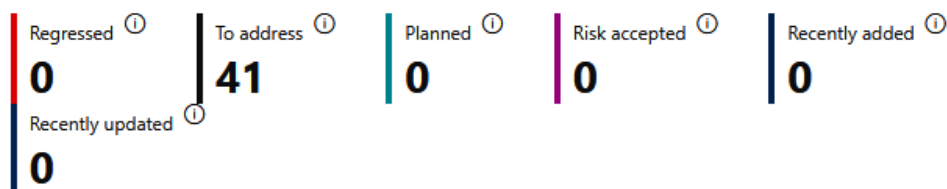


Figure 12.7 – Secure score breakdown by category

3. You'll also find **Comparison** on the **Overview** page, showing how your organization's Secure Score compares to organizations of a similar size.
4. Analyze the improvement actions listed in the middle column (or scroll down if necessary) titled **Actions to review**. The changes that would have the greatest impact on your score are shown at the top, as reflected in the example shown in *Figure 12.8*, where enabling impersonation protection could increase the Secure Score by 2.84%.

Actions to review



Top recommended actions

Recommended action	Score impact	Status	Category
Ensure that intelligence for impersonation protection i...	+2.84%	<input type="radio"/> To address	Apps
Move messages that are detected as impersonated us...	+2.84%	<input type="radio"/> To address	Apps
Enable impersonated domain protection	+2.84%	<input type="radio"/> To address	Apps
Set the phishing email level threshold at 2 or higher	+2.84%	<input type="radio"/> To address	Apps
Enable impersonated user protection	+2.84%	<input type="radio"/> To address	Apps
Quarantine messages that are detected from imperso...	+2.13%	<input type="radio"/> To address	Apps
Quarantine messages that are detected from imperso...	+2.13%	<input type="radio"/> To address	Apps
Start your Defender for Identity deployment, installin...	+1.77%	<input type="radio"/> To address	Identity

Figure 12.8 – Actions to review for Secure Score improvements

5. Under **History**, you can see recent changes related to **Secure Score** actions, as shown in *Figure 12.9*, where an activity update is visible alongside previous points improvements.

History

Date/Time	Activity
Jul 21, 2024 12:53 PM	nate@chambernate.onmicrosoft.com marked Ensure that intelligence for imper...
Jul 15, 2024 7:00 PM	0.94 points gained by completing Ensure 'Self service password reset enabled' i...
May 8, 2024 7:00 PM	0.03 points gained for Ensure 'Self service password reset enabled' is set to 'All' ...
May 4, 2024 7:00 PM	▲ 5.00 points gained by completing Turn on Microsoft Defender for Office 365 ...
May 4, 2024 7:00 PM	▲ 5.00 points gained by completing Turn on Safe Documents for Office Clients...

Figure 12.9 – History of Secure Score changes

6. Other than **Overview**, you’ll find three other tabs on your **Secure Score** page. **Recommended actions** expands the **Actions to review** section and shows all recommended actions.
7. **History** expands upon the **History** section of **Overview** to allow more visible history.
8. Under **Metrics & trends**, view changes over time in your score as well as your organization’s comparison to similar organizations over time.

How it works...

In this recipe, you accessed your organization’s Secure Score dashboard to review and analyze your security posture. The Secure Score provides a breakdown of your security configuration across categories such as identity, data, and apps. By analyzing the improvement actions, you can identify specific steps to enhance your security score. Each action includes detailed instructions and indicates the potential increase in your score if resolved. Comparing your score with similar organizations helps you gauge your security effectiveness. The **Metrics & trends** section provides insights into how your score has changed over time, allowing you to track improvements and identify areas needing attention.

In the next recipe, we will take action to improve our score by complying with one of the recommended actions.

There's more...

Regularly monitoring and addressing the recommendations in your Secure Score can significantly improve your organization's security posture. By implementing the suggested actions, you reduce risks and enhance your overall security. *Figure 12.10* shows the filter pane you can use to refine **Recommended actions** to specific statuses, categories, regression status, and more. This makes it simpler to filter to related improvement actions that you can then easily delegate to relevant team members to ensure continuous progress.

The screenshot displays the Microsoft Secure Score dashboard. The 'Recommended actions' tab is selected, showing a list of actions to improve the score. On the right, a 'Filter' pane allows users to refine these actions based on Category, Status, and Regression status.

Microsoft Secure Score

Overview **Recommended actions** History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export

Rank	Recommended action	Score impact
1	Ensure that intelligence for impersonation protection is enabled	+2.84%
2	Move messages that are detected as impersonated users by mail	+2.84%
3	Enable impersonated domain protection	+2.84%
4	Set the phishing email level threshold at 2 or higher	+2.84%
5	Enable impersonated user protection	+2.84%
6	Quarantine messages that are detected from impersonated domains	+2.13%
7	Quarantine messages that are detected from impersonated users	+2.13%

Filter

Clear filters

Category

- ☐ Apps
- ☐ Data
- ☒ Identity

Status

- ☐ Alternate mitigation
- ☐ Completed
- ☐ Planned
- ☐ Risk accepted
- ☐ Third party
- ☐ To address

Regressed in last 90 days

- ☐ No

Apply Cancel

Figure 12.10 – Filter pane on Secure Score's Recommended actions tab

See also

- *Microsoft Secure Score*: <https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score>

Complying with Secure Score security configuration recommendations

In the previous recipe, you accessed and reviewed your organization's Secure Score. This recipe will guide you through the process of complying with a specific Secure Score security configuration recommendation to improve your overall security posture.

Getting ready

You need to be a Global Administrator, Security Administrator, Compliance Administrator, Global Reader, or Security Reader to access Secure Score. Depending on the selected recommended action, you may require additional permissions to resolve the action.

How to do it...

1. Navigate to Microsoft Secure Score at <https://security.microsoft.com/securescore>. Alternatively, go to Microsoft Defender at <https://security.microsoft.com> and select **Investigation & response | Secure Score** from the left navigation menu.
2. Select a top improvement action from the **Actions to review** section or **Recommended actions** tab to explore the action's suggested steps in more detail. This will provide a comprehensive description of the improvement action and allow you to tag it for better organization or update its status and action plan. When updating the status and action plan, you can provide specific details as reminders for yourself or other administrators with **Secure Score** access. *Figure 12.11* shows an example of editing a recommended action, **Ensure user consent to apps accessing company data on their behalf is not allowed**.

Ensure that intelligence for impersonation protection is enabled

☐ To address

[Edit status & action plan](#) [Manage tags](#)

General Implementation

Description

Enables enhanced impersonation results based on... allows you to define specific actions for impersonation.

This setting is available only if **Enable mailbox intelligence** is turned on.

Implementation status

100% of users are affected by policies that are configured to meet this recommendation.

- Office365 AntiPhish Default - 32 users (100%)

Status & action plan

Ensure that intelligence for impersonation protection is enabled

Update the status and action plan for this recommended action. System-generated statuses can't be updated.

Status

☐ Completed

☐ To address

☒ Planned

☐ Risk accepted

☐ Resolved through third party

☐ Resolved through alternate mitigation

Action plan

Miguel is handling this implementation prior to 10/1.

Figure 12.11 – Editing status and action plan for a recommended action

3. Select **Save and close** to update the item's status and action plan. In *Figure 12.11*, the selected action has been changed from **To address** (the default) to **Planned** and a note has been added detailing the specific plan to resolve to action item.
4. When you are ready to implement a recommended action, its **Implementation** tab provides step-by-step instructions to address the action. Select the **Implementation** tab for a recommended action.
5. *Figure 12.12* shows the prerequisites for the selected action, **Ensure user consent to apps accessing company data on their behalf is not allowed**, are met. The **Next steps** section lets the responsible administrator know what needs to happen next to comply with the recommendation and boost the Secure Score. Select **Manage** to be taken directly to the screen on which the change must be made, in most cases.

Ensure user consent to apps accessing company data on their behalf is not allowed

○ Planned

 Edit status & action plan  Manage tags

General **Implementation** History (1)

Prerequisites

✗ Microsoft Entra ID Free is needed.

Next steps

1. Go to Microsoft Entra ID > Enterprise applications > Consent and permissions. [Go to Consent and permissions](#)
2. Select "Allow user consent for apps from verified publishers, for selected permissions (Recommended)" to follow Microsoft's best practice. [Learn more](#)

Figure 12.12 – Implementation tab of a recommended action

6. Once you have made the required changes, wait 24-48 hours for the changes to update the score.
7. After the score updates, Secure Score will automatically mark the improvement action as **Completed** if all steps are complete. You can still edit the completed action to note the action you took for future reference.
8. Monitor the **Secure Score** dashboard to ensure the changes positively impact your score and continue to take action where possible to further improve your organization's score.

How it works...

In this recipe, you selected and addressed a specific improvement action from the Secure Score recommendations. By following the provided step-by-step instructions, you implemented a security measure that enhances your organization's protection. Enabling self-service password reset, for example, empowers users to manage their password issues, reducing the risk of compromised accounts and improving overall security. Once the action is complete and has been saved, Secure Score updates within 24-48 hours, reflecting the improvement in your security posture. Documenting the action taken ensures transparency and accountability in your security management process.



There's more...

Managing tags in Secure Score provides a significant advantage in organizing and prioritizing the recommended actions effectively. Tags enable administrators to categorize these actions based on various criteria such as project, team, or urgency, making the tasks more manageable and trackable. This enhanced organization aids in improving the overall security posture by ensuring that critical actions are not overlooked.

To manage tags, select a recommended action from the **Actions to review** section or the **Recommended actions** tab to delve into its details. Select **Manage tags**, as shown in *Figure 12.13*:

Ensure that intelligence for impersonation protection is enabled

○ Planned

 Edit status & action plan  **Manage tags**

General Implementation History (1)

Action plan

Miguel is handling this implementation prior to 10/1.

Description

Enables enhanced impersonation results based on each user's individual sender map and allows you to define specific actions for impersonated messages.

This setting is available only if **'Enable mailbox intelligence'** is selected.

Implementation status

100% of users are affected by policies that are configured less securely than is recommended

- Office365 AntiPhish Default - 32 users (100%)

Details

Points achieved **0 / 8**

History

[1 events](#)

Category

Apps

Product

Defender for Office

Figure 12.13 – Manage tags option for a recommended action

Tags can be anything you need them to be, and since there are no default options, you will need to create some initially. This can be done by selecting **Manage tags** in the same box where you will choose them after they have been established. Using descriptive tags, such as *High Priority*, *Compliance*, or *IT Team*, can significantly enhance the categorization and prioritization of actions. After making the necessary changes, ensure to save them by clicking **Save and close**. This updates the action with the new tags, making it easier to filter, find, and manage in future reviews, as well as to clearly identify who is accountable for specific actions.

See also

- *Assess your security posture with Microsoft Secure Score:* <https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score-improvement-actions>

Assigning permissions for non-IT users to Microsoft Defender

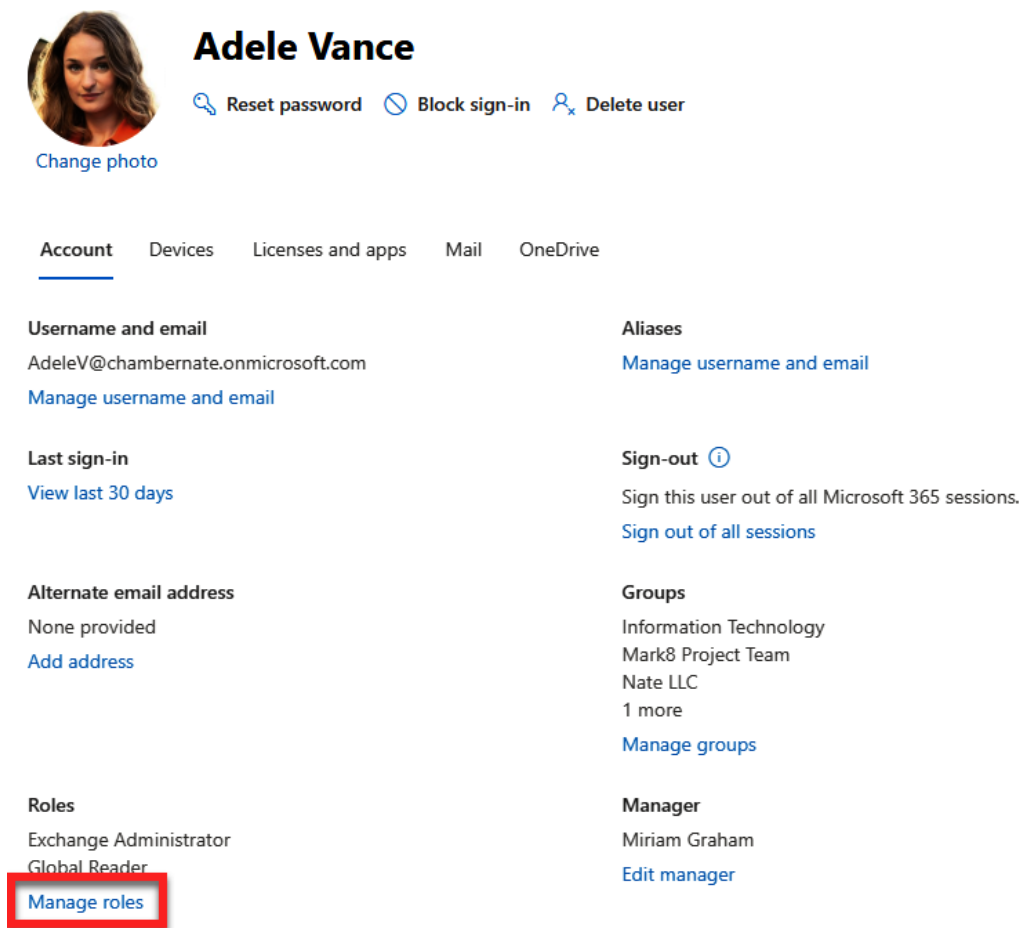
Assigning appropriate permissions to non-IT users in Microsoft Defender ensures they can access necessary features without compromising security or gaining unnecessary permissions (following the principle of least privilege). This recipe will help you assign roles and permissions in Microsoft Defender. Specifically, we'll assign a user the Security Reader role, which will allow them to read reports and logs, but not change configurations.

Getting ready

Ensure you have the Global Administrator or Security Administrator role to complete the steps in this recipe.

How to do it...

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. In the left navigation menu, select **Users | Active users**.
3. Choose the user account you want to assign permissions to by selecting the user's name to open their account details.
4. In the account details pane, go to the **Roles** section and select **Manage roles**, as shown in *Figure 12.14*.



Adele Vance

[Reset password](#) [Block sign-in](#) [Delete user](#)

[Change photo](#)

Account [Devices](#) [Licenses and apps](#) [Mail](#) [OneDrive](#)

Username and email
AdeleV@chambernate.onmicrosoft.com
[Manage username and email](#)

Aliases
[Manage username and email](#)

Last sign-in
[View last 30 days](#)

Sign-out ⓘ
Sign this user out of all Microsoft 365 sessions.
[Sign out of all sessions](#)

Alternate email address
None provided
[Add address](#)

Groups
Information Technology
Mark8 Project Team
Nate LLC
1 more
[Manage groups](#)

Roles
Exchange Administrator
Global Reader
[Manage roles](#)

Manager
Miriam Graham
[Edit manager](#)

Figure 12.14 – Location of Manage roles option for a user

5. Scroll down and expand **Show all by category**.
6. To grant full access, select **Security Administrator** under **Security & Compliance**.

7. To grant read-only access, select **Security Reader** under **Read-only**, as shown in *Figure 12.15*.

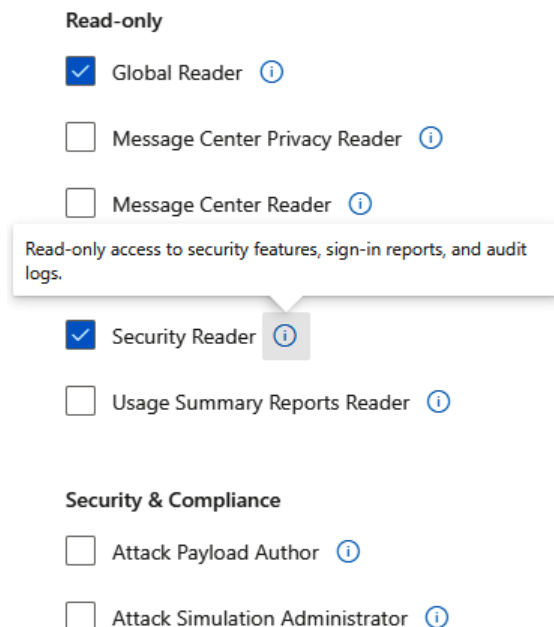


Figure 12.15 – Security Reader role selected for a user

8. Select **Save changes** to apply the new role assignments.
9. Verify that the new roles are listed under the user's account roles. This confirms that the permissions have been successfully updated.

How it works...

By assigning the Security Administrator role, the user gains full access to view all system information, manage security policies, and respond to alerts within Microsoft Defender. Assigning the Security Reader role allows the user to view security policies and alerts without making any changes, ensuring they have the necessary information while maintaining security integrity. Using the Microsoft 365 admin center simplifies the process and ensures that role assignments are easily managed and reviewed.

There's more...

For more granular control over permissions, consider using **Role-Based Access Control (RBAC)** in Microsoft Defender. RBAC allows you to define specific roles, assign user groups to these roles, and control access levels more precisely. Here's how:

1. To get started, go to Microsoft Defender at <https://security.microsoft.com> and select **Permissions** from the left navigation menu.
2. Here, you can select **Roles** from beneath **Microsoft Defender XDR**, then **Create custom role**.
3. Give the custom role a specific **Role name**, such as the job title for which you're creating the role. Add a **Description**, then select **Next**.
4. On the **Permissions** screen, you will configure the **Security operations**, **Security Posture**, and **Authorization and settings** categories for which this role will have specific access and abilities. *Figure 12.16* shows the **Authorization and settings** category, where you can choose between **All read-only permissions**, **All read and manage permissions**, and **Select custom permissions**. If you choose **Select custom permissions**, all other settings become active to be configured for this role (also shown in *Figure 12.16*).

Choose permissions

Select permissions from each permission group to

Permission group	Description
<input type="radio"/> Security operations None selected	Manages day
<input type="radio"/> Security posture None selected	Manages the
<input type="radio"/> Authorization and settings None selected	Manages the

Authorization and settings

Select the permissions for users who need to configure your security and system settings, and create and assign roles.

If you select any permissions on this page, you will also assign the security data read permission under the Security operations permission group.

Clear all permissions

☐ All read-only permissions
☐ All read and manage permissions
☒ Select custom permissions

Authorization

☐ Read-only
☐ Read and manage

Security settings

☐ Read-only
☐ Select all permissions
☐ Select custom permissions

☐ Detection tuning (manage)
☐ Core security settings (read)
☐ Core security settings (manage)

System settings

☐ Read-only (Defender for Office, Defender for Identity)
☐ Read and manage

Figure 12.16 – Authorization and settings screen for a custom role

5. Once you've configured specific permissions for **Security operations**, **Security Posture**, and **Authorization and settings** categories, select **Next**, assign the role to users and user groups, and choose the data sources these assigned users can access.
6. Select **Next**, then **Submit**.

Now you have a custom permissions role that is more specific than full control or read-only. This enables you to delegate specific tasks to users to which they're most appropriate, and ensures they have the necessary permissions without compromising security.

See also

- *Assign user access*: <https://learn.microsoft.com/en-us/defender-endpoint/assign-portal-access>
- *Microsoft Defender XDR Unified role-based access control (RBAC)*: <https://learn.microsoft.com/en-us/defender-xdr/manage-rbac>

Monitoring Microsoft Defender reports

Monitoring reports in Microsoft Defender is important for maintaining and improving your organization's security posture. These reports provide insights into various aspects of security, including threat detection, device health, and web protection.

Important note

There are numerous components to Microsoft Defender. In this recipe, we'll highlight several reports and dashboards you may find of interest. You're encouraged, however, to further explore the left navigation menu of Microsoft Defender to find all that's available to you in your specific subscription.

Getting ready

Ensure you have the Global Administrator or Security Administrator role to complete the steps in this recipe.

How to do it...

1. Navigate to the Microsoft Defender portal at <https://security.microsoft.com>.
2. Monitor **Threat analytics**:
 - I. Go to **Threat intelligence** | **Threat analytics**

- II. This report, like the one shown in *Figure 12.17*, shows the latest known vulnerabilities, phishing, ransomware, and more that Microsoft is aware of, as well as categorical data and their latest updates
- III. Select any threat to learn more about it and its impact in detail

Threat analytics

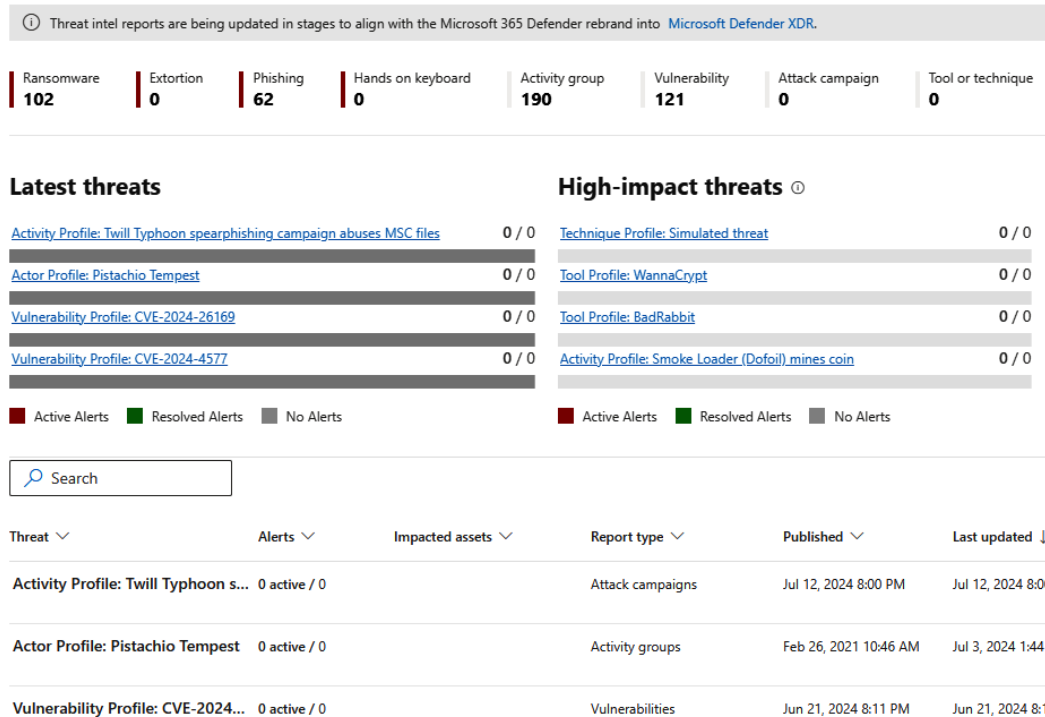


Figure 12.17 – Threat analytics in Microsoft Defender XDR

3. Monitor Incidents Queue:

- I. Go to the **Incidents** queue in the Microsoft Defender portal (**Incidents & alerts** | **Incidents**).
- II. Review and manage alerts, **indicators of compromise (IOCs)**, and **indicators of attack (IOAs)**. This helps with tracking and resolving security incidents promptly.

4. Monitor general identity and device security:

- I. Go to **Reports | Security report**.
- II. Review **Identity** metrics such as **Users at risk** and **Global admins** or **Devices** metrics such as **Threat analytics**, **Device compliance**, and **Devices with active malware**. Some of these are shown in *Figure 12.18*.

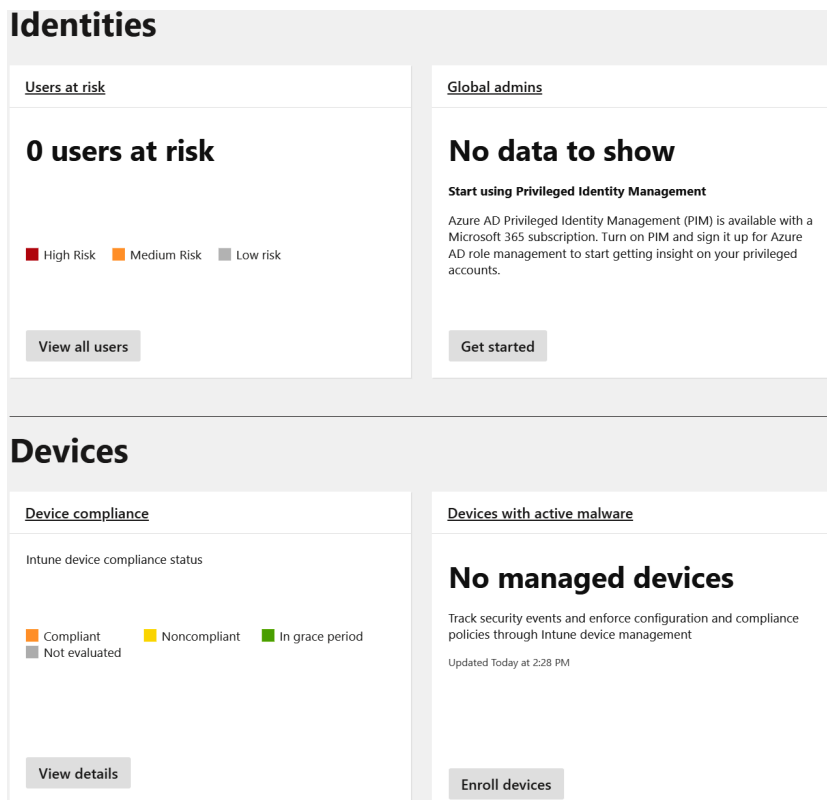


Figure 12.18 – Security report in Microsoft Defender

5. Monitor **Email & collaboration**:

- I. Go to **Reports | Email & collaboration reports**.
- II. Review topics such as **Mailflow status**, **Post-delivery activities** such as phishing and spam, **URL protection**, **Spoof detections**, and **User reported messages**. Some of these visualizations can be seen in *Figure 12.19*.

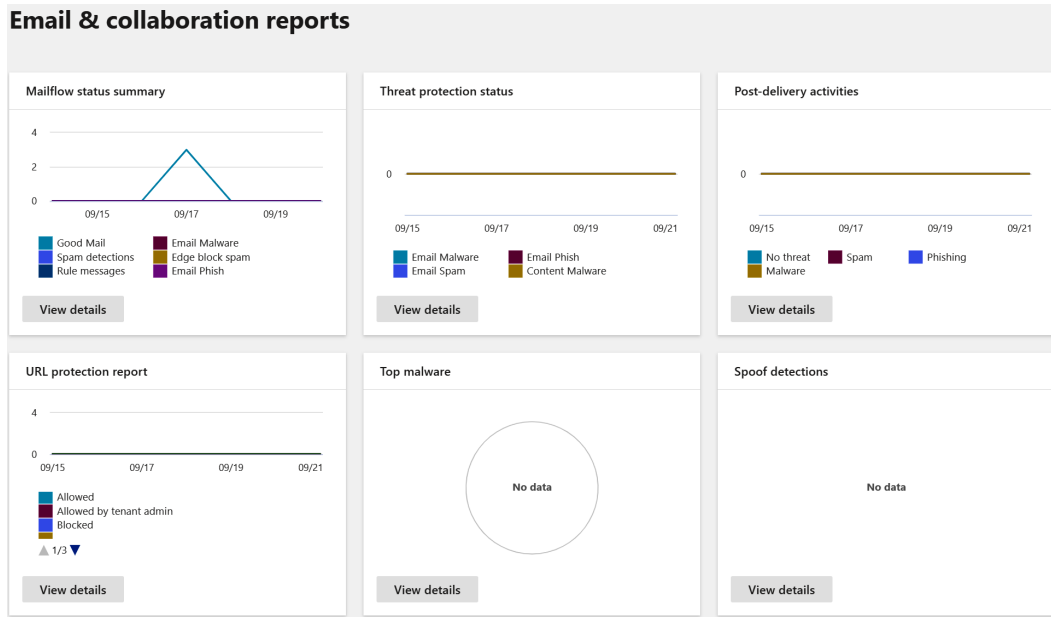


Figure 12.19 – Email & collaboration reports in Microsoft Defender

6. If you have Microsoft Defender for Endpoint, here are some other reports you may wish to review:
 - **Check the Monthly Security Summary (Reports | Endpoints | Monthly Security Summary):** The report includes sections such as **Microsoft Secure Score**, **Devices onboarded**, **Protection against threats**, **Web content monitoring and filtering**, and **Suspicious or malicious activities**. You can generate a PDF report by selecting **Generate PDF report**.
 - **Review Device Health and Compliance** (navigate to **Reports | Device health and compliance**): View the health status of your endpoints, compliance with security policies, and any devices that require attention. This report helps ensure that all devices meet your organization's security standards and are properly protected.
 - **Check Vulnerability Management** (navigate to **Threat & vulnerability management | Dashboard**): See a comprehensive view of vulnerabilities within your organization. This dashboard provides insights into the most critical vulnerabilities, affected devices, and recommended actions for remediation.
 - **Analyze Attack Surface Reduction** (navigate to **Reports | Attack surface reduction**): See how effectively your organization is minimizing the attack surface. This report includes data on the implementation of security controls, the number of threats blocked, and recommendations for further reducing the attack surface.

- **Inspect Endpoint Detection and Response (EDR) reports** (navigate to **Reports | EDR**): Review detailed logs and analytics of endpoint activities. These reports identify advanced threats and provide information on suspicious behavior patterns detected on endpoints.
- **Evaluate Web Protection** (navigate to **Reports | Web protection**): Monitor web-based threats, including blocked malicious URLs and web content filtering activities. This report helps ensure that your users are protected from web-based attacks and that your web policies are effectively enforced.

How it works...

By regularly monitoring these reports, you can gain insights into your organization's security status, identify areas for improvement, and take proactive measures to mitigate risks. The reports provide detailed information on threat detections, device health, and web security, enabling you to respond effectively to potential security issues.

There's more...

For more advanced monitoring, consider using RBAC in Microsoft Defender to assign specific permissions to different user groups. This allows for more granular control over who can view and manage security reports. See the *There's more...* section of the previous recipe, *Assigning permissions for non-IT users to Microsoft Defender*, for steps on how to set up a custom role.

Additionally, explore the various other features available in Microsoft Defender, such as the **Activity log** and **Audit** functions, to get a detailed view of your organization's activities that may be problematic to your overall security posture.

See also

- *View Defender for Office 365 reports in the Microsoft Defender portal*: <https://learn.microsoft.com/en-us/defender-office-365/reports-defender-for-office-365>
- *Microsoft 365 Reports in the admin center - Microsoft 365 groups*: <https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/office-365-groups-ww>
- *Monthly security summary report in Microsoft Defender for Endpoint*: <https://learn.microsoft.com/en-us/defender-endpoint/monthly-security-summary-report>
- *Monitor web browsing security*: <https://learn.microsoft.com/en-us/defender-endpoint/web-protection-monitoring>

Utilizing threat investigation and response capabilities

Utilizing threat investigation and response capabilities in Microsoft Defender helps your organization quickly and effectively handle security threats. This recipe will walk you through the process of investigating and responding to threats using Microsoft Defender.

Getting ready

Ensure you have the Global Administrator or Security Administrator role to complete the steps in this recipe.

How to do it...

1. Navigate to the Microsoft Defender portal at `https://security.microsoft.com`.
2. Navigate to **Incidents & alerts** | **Incidents** to view the list of current security incidents. *Figure 12.20* shows how you're able to export, search, and filter results by date, status, severity, and more.

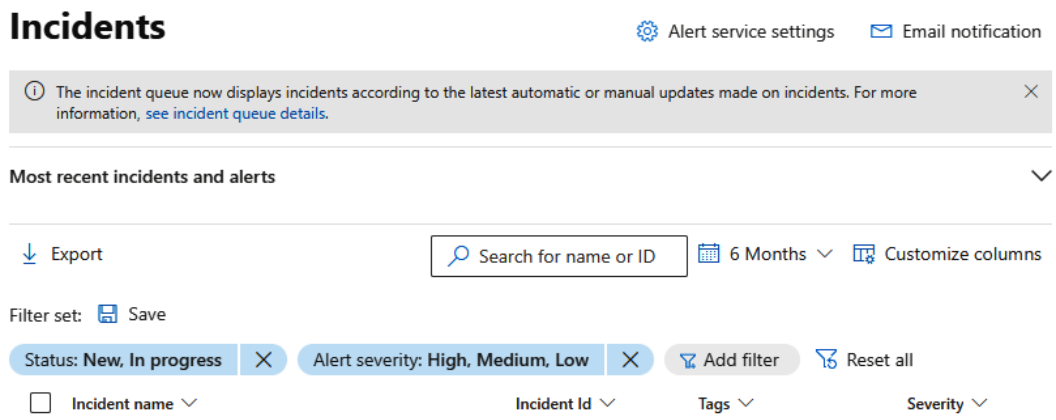


Figure 12.20 – Incidents screen of Microsoft Defender

3. Select an incident to open the incident details pane. Then select **Open incident page**. Here, you can see the alerts that triggered the incident, impacted users and devices, and evidence found.
4. Review the list of evidence to understand the scope and impact of the incident. The evidence can include files, processes, services, drivers, and network addresses.
5. Analyze the alerts and data associated with the incident to determine the nature of the threat. Look for patterns and IOCs that can help you understand the attack.
6. Perform necessary remediation actions based on your analysis. This might include isolating devices, blocking URLs, stopping processes, or quarantining files.

7. Add comments and tags to the incident to document your findings and actions taken. This helps you maintain a detailed record for future reference.
8. Once the incident is resolved, select **Manage incident** | **Resolve incident** and set the status, classification, and determination to close the incident.
9. Use Advanced Hunting to proactively search for additional threats by going to **Hunting** | **Advanced hunting** to create custom queries to search for and investigate suspicious activities.

How it works...

The process of threat investigation and response involves a deep dive into each security incident to accurately identify the nature of the threat. By thoroughly reviewing the alerts and evidence, security professionals can map out the attack sequence and understand its impact. This method allows for precise remediation actions, ensuring that threats are neutralized effectively. By documenting each step and finding, organizations build a robust knowledge base that enhances future threat response efforts.

There's more...

In addition to manual investigation, Microsoft Defender offers **Automated Investigation and Response (AIR)** capabilities. AIR leverages machine learning and automation to handle routine threat detection and remediation tasks. This reduces the burden on security teams, allowing them to focus on more complex threats. AIR continuously monitors for suspicious activities, correlates data across various sources, and provides automated responses to mitigate threats swiftly. Integrating AIR into your security strategy enhances your organization's ability to respond to threats with speed and precision. To enable AIR, you must have Microsoft Defender for Office 365 Plan 2 and must also ensure **Audit logging** is turned on for your organization (it is by default).

See also

- *Threat investigation and response*: <https://learn.microsoft.com/en-us/defender-office-365/office-365-ti>
- *Prioritize incidents in the Microsoft Defender portal*: <https://learn.microsoft.com/en-us/defender-xdr/incident-queue>
- *Manage incidents in Microsoft Defender*: <https://learn.microsoft.com/en-us/defender-xdr/manage-incidents>
- *Investigate and respond with Microsoft Defender XDR*: <https://learn.microsoft.com/en-us/defender-xdr/incident-response-overview>
- *Remediation actions in Microsoft Defender XDR*: <https://learn.microsoft.com/en-us/defender-xdr/m365d-remediation-actions>
- *Automated investigation and response (AIR) in Microsoft Defender for Office 365*: <https://learn.microsoft.com/en-us/defender-office-365/air-about>

Understanding the Microsoft Purview Portal

The **Microsoft Purview** portal is an essential tool for ensuring compliance, security, and effective data governance within your Microsoft 365 environment. As data continues to grow exponentially, managing and protecting it while adhering to regulatory requirements has become a complex yet essential task for organizations of all sizes. This chapter will guide you through several solutions within Microsoft Purview, providing practical recipes to help you navigate and utilize these powerful tools effectively.

The Microsoft Purview portal integrates various compliance and security solutions, allowing administrators to manage data protection, monitor compliance status, and respond to regulatory requirements from a single interface. Whether you're tasked with setting up **data loss prevention (DLP)** policies, managing eDiscovery cases, or configuring retention policies, this chapter offers step-by-step guidance to help you maintain a secure and compliant environment.

We will cover the following recipes in this chapter:

- Viewing a report on all users who have accessed a specific SharePoint file
- Accessing Microsoft's HIPAA business associate agreement
- Creating a DLP policy to protect content with HIPAA-protected data detected
- Using DLP to automatically report HIPAA incident reports
- Creating a custom sensitive information type based on keywords
- Creating a DLP policy for content with custom keywords in the name or subject
- Tuning a DLP policy's sensitivity
- Creating a retention policy to retain content for seven years
- Creating and using an eDiscovery case

- Assigning permissions for non-IT users to Microsoft Purview
- Using Communication Compliance to identify potential policy violations in messages

Technical requirements

To effectively follow and execute the tasks in this chapter, you need administrative access within Microsoft 365. Specifically, having Global Administrator, Compliance Administrator, or Security Administrator permissions will enable you to perform many of the recipes detailed here. Ensure you have access to the Microsoft 365 admin center to manage user roles and permissions, and that audit logging is enabled in your organization. No additional downloads or installations are required beyond these permissions and access configurations.

Viewing a report on all users who have accessed a specific SharePoint file

Monitoring access to confidential SharePoint files is critical for maintaining security and compliance. This recipe will guide you through viewing a report on all users who have accessed a specific SharePoint file using Microsoft Defender.

Getting ready

Ensure that audit logging is turned on in your organization. You can enable this from the Microsoft Purview portal at <https://purview.microsoft.com/audit>. You also need to be a Global or Security Administrator to complete this recipe.

How to do it...

1. Go to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. Select **View all solutions | Audit**.
3. In the **Activities – friendly names** dropdown, search for and select **Accessed file**, as shown in *Figure 13.1*.

Search

[Learn about audit](#)

Searches completed **0** | Active searches **0** | Active unfiltered searches **0**

Date and time range (UTC) *
 Start Jul 24 00:00
 End Jul 25 00:00

Keyword Search
 Enter the keyword to search for

Admin Units
 Choose which Admin Units to search for

Activities - friendly names
 Accessed file

File and page activities
☒ Accessed file
☐ Changed retention label for a file
☐ Deleted file marked as a record
☐ Checked in file
☐ Changed record status to locked

Users
 Add the users whose audit logs you want to search for

File, folder, or site
 Enter all or a part of the name of a file, folder, or site

Workloads
 Enter the workloads to search for

Search Clear all

Figure 13.1 – Filtering activities to Accessed file activities

- Specify the **Date and time range** values for the report.
- Enter the URL or name of the file you want to audit in the **File, folder, or site** box, such as `Benefits of indoor plants.docx`.
- Select **Search** to begin the search and await results.
- Select the **Search name** to view the report when **Job status** shows as **Completed**, as shown in *Figure 13.2*.

[Copy this search](#)
[Delete](#)
[Refresh](#)

	Search name	Job status	Prog...	Sear...	Total results
<input checked="" type="checkbox"/>	May 1 - Jul 27 fileac...	Completed	100%	2m, 38s	2
<input type="checkbox"/>	Benefits file accesse...	Completed	100%	8m, 32s	0
<input type="checkbox"/>	Mar 1 - Jul 25 fileac...	Completed	100%	3m, 56s	0

Figure 13.2 – A completed audit search

How it works...

By using this process, you can track user access to specific SharePoint files, providing valuable insights into who is viewing your sensitive documents. *Figure 13.3* shows the results which tell us the IP address, user, and location from which the document was accessed (under **Details**).

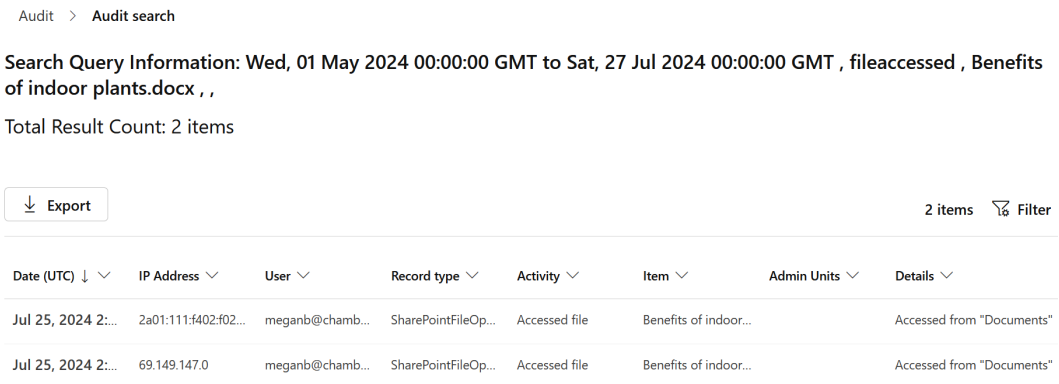


Figure 13.3 – Audit search results

This information is essential for security auditing and ensuring that only authorized users access critical files. It also helps in identifying unauthorized access, assisting in damage control, and preventing information leakage.

There’s more...

From your results page, you can filter results and export them to CSV for further analysis or easier sharing with non-administrators.

From the **Audit | Search** page, you can select a previous search and select **Copy this search** to run a similar audit again. *Figure 13.4* shows this option.

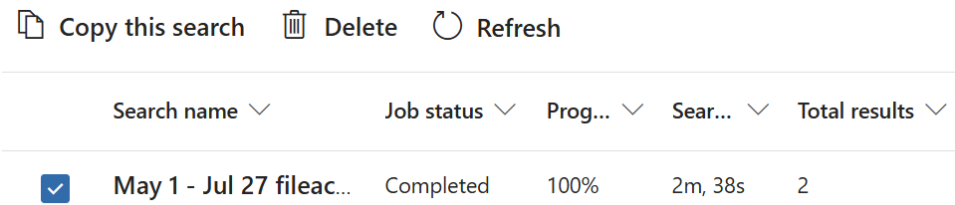


Figure 13.4 – A selected previous search and the option to copy this search

After selecting **Copy this search**, you can change any of the search parameters (such as dates to include) before selecting **Search** to begin the audit.

See also

- *Search the audit log:* <https://learn.microsoft.com/en-us/purview/audit-search>

Accessing Microsoft's HIPAA business associate agreement

The **business associate agreement (BAA)** is an important document for organizations handling **protected health information (PHI)** under the **Health Insurance Portability and Accountability Act (HIPAA)**. The BAA outlines the responsibilities of both Microsoft and your organization in safeguarding PHI. Accessing the standard Microsoft BAA is essential for compliance and audit purposes.

Important note

The BAA is one of many service trust documents available from Microsoft. Documents that can be found in the Microsoft Service Trust Portal are arranged by industry, geography, and more to help you find the documentation and agreements you need for specific contexts, information types, and regulations.

Getting ready

You do not need special permissions to access the Service Trust Portal or its contents.

How to do it...

1. Go to the Microsoft Service Trust Portal at <https://servicetrust.microsoft.com>.
2. Navigate to the **Healthcare and Life Sciences** section.

3. Search the page (*Ctrl + F*) for the HIPAA BAA document, as shown in *Figure 13.5*.







<input type="checkbox"/>	 Azure - Electronic Prescriptions for Controlled Substances (EPCS) 	This is a Microsoft Compliance article link for the Electronic Prescriptions for Controlled Substances (EPCS). Please check out this external link for more information re... Show more	2022-09-19
<input type="checkbox"/>	 Microsoft General - HIPAA BAA (October 2021)  ✓	This document contains the October 2021 version of the Microsoft HIPAA BAA.	2021-12-06
<input type="checkbox"/>	 Azure - HDS (France) Certificate (Sept 2021) 	Microsoft Azure HDS Certification issued Sept, 2021	2021-11-18

Figure 13.5 – Microsoft’s HIPAA BAA in the Microsoft Service Trust Portal

4. Download the BAA for your records and compliance needs.

How it works...

Accessing the Microsoft BAA through the Service Trust Portal ensures that you have the necessary documentation for HIPAA compliance. The BAA details the commitments of both parties in handling and protecting PHI, helping to ensure that all legal and regulatory obligations are met.

There’s more...

While this recipe covers how to access the BAA within a HIPAA context, it is important to note that the Microsoft Service Trust Portal contains a wide range of compliance documents. These include the following:

- **Federal Risk and Authorization Management Program (FedRAMP):** A unified framework for evaluating, authorizing, and continuously monitoring the security of cloud products and services utilized by U.S. federal agencies
- **General Data Protection Regulation (GDPR):** A legal framework established by the **European Union (EU)** to regulate data protection and privacy for individuals within the EU and the European Economic Area, including guidelines for the transfer of personal data beyond these regions

- **Digital Operational Resilience Act (DORA):** An EU regulation focused on bolstering the IT security of financial institutions, ensuring their capacity to endure, respond to, and recover from various ICT-related disruptions and threats

These documents and more are available to provide comprehensive information and assurances regarding Microsoft's compliance with various global standards and regulations.

See also

- *Service Trust Portal:* <https://servicetrust.microsoft.com/>

Creating a DLP policy to protect content with HIPAA-protected data detected

Protecting sensitive health information is an important aspect of maintaining compliance with HIPAA. Microsoft Purview allows you to create DLP policies to detect and protect HIPAA-protected data. This recipe will guide you through creating a DLP policy to identify and secure such data within your organization.

Important note

While we're focusing on HIPAA in this recipe, the steps are similar for other privacy acts and regulations for specific data types across the globe.

Getting ready

Ensure you have Global Administrator, Compliance Administrator, or Security Administrator permissions. Familiarize yourself with the types of data you need to protect and the locations where this data is stored.

How to do it...

1. Sign in to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. If **Data Loss Prevention** appears on your home screen, select it. Otherwise, select **View all solutions | Data Loss Prevention**.

3. Select **Policies** from the left navigation menu and then select **Create policy**, as shown in *Figure 13.6*.

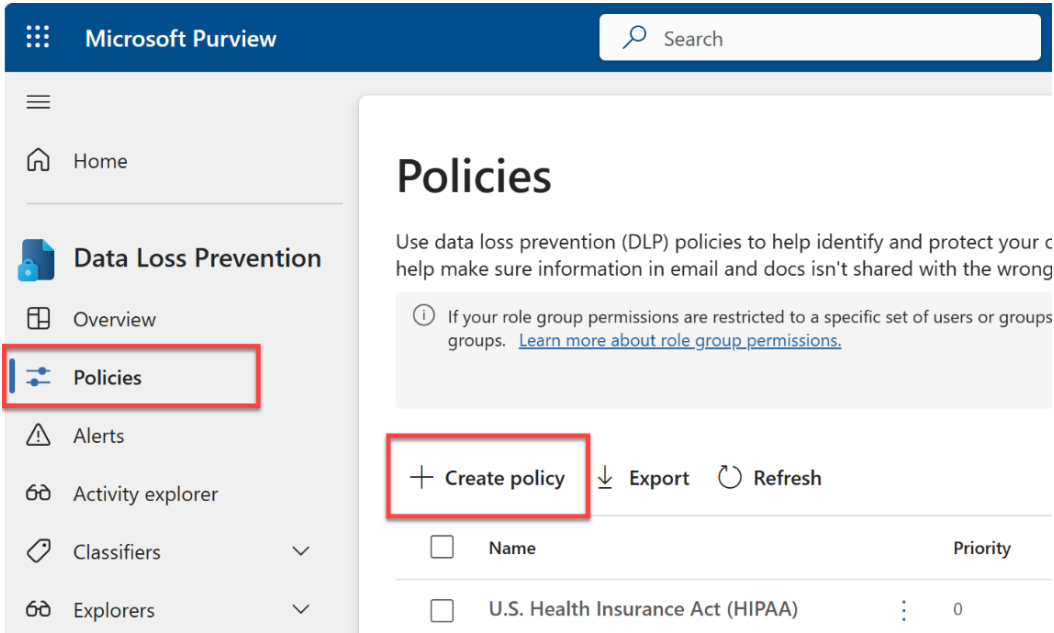


Figure 13.6 – Location of DLP policies and the new policy creation option

4. On the first screen of the wizard that appears, select the **Medical and health** category, then the **Regulations** template named **U.S. Health Insurance Act (HIPAA) Enhanced**, and then select **Next**. These options are shown in *Figure 13.7*.

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. [Learn more about DLP policy templates](#)

Enhanced templates currently aren't supported for following location(s): On-premises file repositories, Power BI, Azure Storage, Azure Sql Server, Aws S3, OpenAI ChatGPT, Google Gemini, Microsoft Bing Chat

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Categories	Regulations	
Enhanced	Australia Health Records Act (HRIP Act) Enhanced	U.S. Health Insurance Act (HIPAA) Enhanced Helps detect the presence of information subject to United States Health Insurance Portability and Accountability Act (HIPAA). This enhanced template extends the original by also detecting people's full names, medical terms and conditions, and U.S. physical addresses. We have also enhanced this template with Trainable Classifier "Business-Healthcare" which can detect healthcare and medical content in your tenant such as Medical records, Health benefits documents, Insurance forms, Prior authorizations and referral forms.
Financial	Canada Health Information Act (HIA)	
Medical and health	Canada Personal Health Information Act (PHIA) - Manitoba	
Privacy	Canada Personal Health Act (PHIPA) - Ontario	
Custom	U.K. Access to Medical Reports Act	
	U.S. Health Insurance Act (HIPAA) Enhanced	

Figure 13.7 – Selected options for HIPAA DLP policies

- Provide **Name** and **Description** values for your policy and then select **Next**. Since you are starting from a provided template, the **Name** and **Description** fields auto-populate to the name of the **Regulations** option you selected. You can modify these, however, to suit your needs.
- Specify the admin units to which this policy will apply (optional). If you don't select any, this policy will apply to all users and groups. Select **Next**.
- Specify the locations where the policy will be applied (e.g., **SharePoint sites**, **OneDrive accounts**, **Exchange email**). DLP policies can be applied to the following:
 - Exchange email
 - SharePoint sites
 - OneDrive accounts
 - Teams chat and channel messages

- **Devices**
 - **Instances**
 - **On-premises repositories**
 - **Power BI workspaces**
8. Select **Next**. On the **Policy settings** screen, configure conditions to detect HIPAA data, actions to take when a match is found, and user notifications. Since we're utilizing a template, it comes with default settings you will review in the next steps.
9. Select **Next** to review the information this policy will protect, such as Social Security numbers, physical addresses, full names, and so on. This screen is shown in *Figure 13.8*.

Info to protect

This policy will protect content that matches these conditions. Review them and make any necessary changes. For example, you can edit the conditions to detect additional sensitive info or content that has specific sensitivity or retention labels applied.

Content contains any of these sensitive info types:

- U.S. Social Security Number (SSN)
- Drug Enforcement Agency (DEA) Number
- U.S. Physical Addresses

And

Content contains any of these sensitive info types:

- International Classification of Diseases (ICD-9-CM)
- International Classification of Diseases (ICD-10-CM)
- All Medical Terms And Conditions

And

Content contains all of these sensitive info types:

- All Full Names

And

Content contains any of these sensitive info types:

- Business - Healthcare
- Employee Insurance Files
- Health/Medical Forms

[Edit](#)

☒ Detect when this content is shared from Microsoft 365: ⓘ

☒ With people outside my organization

☐ Only with people inside my organization

Back

Next

Cancel

Figure 13.8 – The Info to protect screen of a new DLP policy

You can also specify whether you want this policy to detect when content is shared with people outside your organization or restrict it to only detect sharing within your organization. Select **Edit** if you wish to include or exclude specific data types in this policy. Otherwise, select **Next** to proceed without making changes to the chosen template.

10. Enable protection actions, such as showing policy tips or emails to users working with detected information types, sending incident reports or alerts to administrators and other specified individuals to review, or automatically restricting access or encrypting the content containing the detected information. Select **Next**. Depending on your selections so far, you may be asked for additional protection action configurations. Respond to the prompts and select **Next** until you're on the **Policy mode** screen.
11. On the **Policy mode** screen, choose whether you wish to do the following:
 - **Run the policy in simulation mode.** (Review items that match the policy's conditions without taking any enforcement actions. You can choose the **Show policy tips while in simulation mode** option and decide if you want to automatically turn on this policy if it's unedited for 15 days.)

Tip

It is highly recommended to start by running the policy in simulation mode for an extended period. This allows you to validate the policy's effectiveness and fine-tune it based on the results. Running the policy in simulation mode first helps avoid unintentional disruptions to users and ensures that the policy behaves as expected before full enforcement.

- **Turn the policy on immediately.** (This option enables the policy but it may take up to an hour for the policy to start applying.)
 - **Leave the policy turned off.** (Select this option if you prefer to test or further refine the policy before turning it on.)
12. Select **Next**, review your settings, and select **Submit** to finalize the policy.

How it works...

This DLP policy will monitor the locations specified in *Step 7* for HIPAA-protected data. When such data is detected, the policy can block access, notify users and administrators, and ensure that the data is handled according to compliance requirements. This proactive approach helps in maintaining the security and confidentiality of sensitive health information.

There’s more...

In *Step 6*, when specifying locations to which the DLP policy applies, you can specify only certain users, groups, and sites (instead of all) by selecting **Edit**, as shown in *Figure 13.9*.

Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

① Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

① At this time, the following location isn't supported for enhanced DLP templates: On-premises file repositories. Exclude it or go back and choose a non-enhanced template.

Location	Scope	
<input checked="" type="checkbox"/> Exchange email	All groups	<div>Edit</div>
<input checked="" type="checkbox"/> SharePoint sites	All sites	<div>Edit</div>
<input checked="" type="checkbox"/> OneDrive accounts	All users & groups	<div>Edit</div>
<input type="checkbox"/> Teams chat and channel messages	Turn on location to scope	
<input type="checkbox"/> Devices	Turn on location to scope	

Figure 13.9 – Option to provide specific email or OneDrive accounts, SharePoint sites, and so on

See also

- *Learn about data loss prevention*: <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>
- *Create and Deploy data loss prevention policies*: <https://learn.microsoft.com/en-us/purview/dlp-create-deploy-policy>

Using DLP to automatically report HIPAA incident reports

HIPAA compliance requires timely reporting of incidents involving PHI. Microsoft Purview’s DLP policies can be configured to automatically generate and send incident reports whenever HIPAA-protected data is detected, ensuring that all necessary stakeholders are promptly informed even if they’re not Global Administrators or Compliance Administrators.

Getting ready

Ensure you have Global Administrator, Compliance Administrator, or Security Administrator permissions. Understand the incident reporting requirements of HIPAA to properly configure the policy.

How to do it...

1. Sign in to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. If **Data Loss Prevention** appears on your home screen, select it. Otherwise, select **View all solutions | Data Loss Prevention**.
3. Select **Policies** from the left navigation menu and then select the DLP policy you created in the previous recipe followed by the **Edit policy** icon (pencil), as shown in *Figure 13.10*.

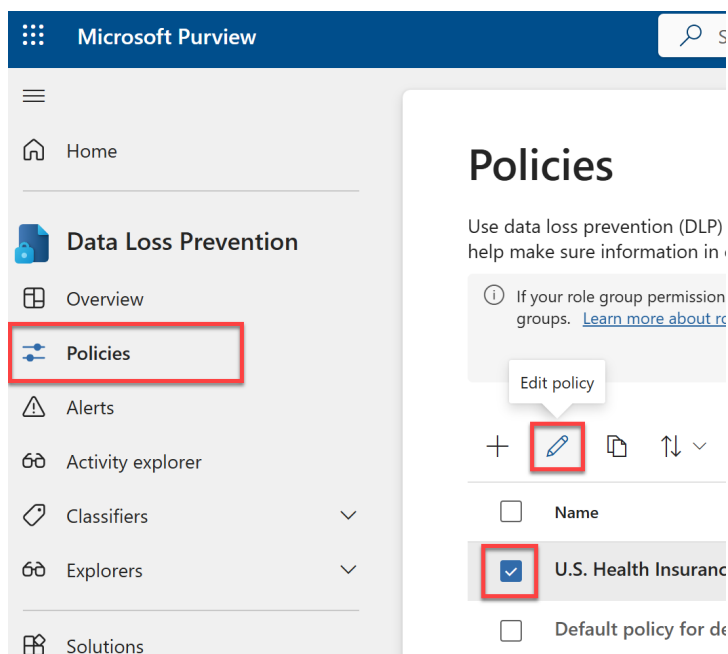


Figure 13.10 – Steps to edit an existing DLP policy

- 4. Select **Next** repeatedly to skip through the wizard until you get to **Customize advanced DLP rules**, as shown in *Figure 13.11*. Then, select the **Edit** icon (pencil) next to the rules you have in place.

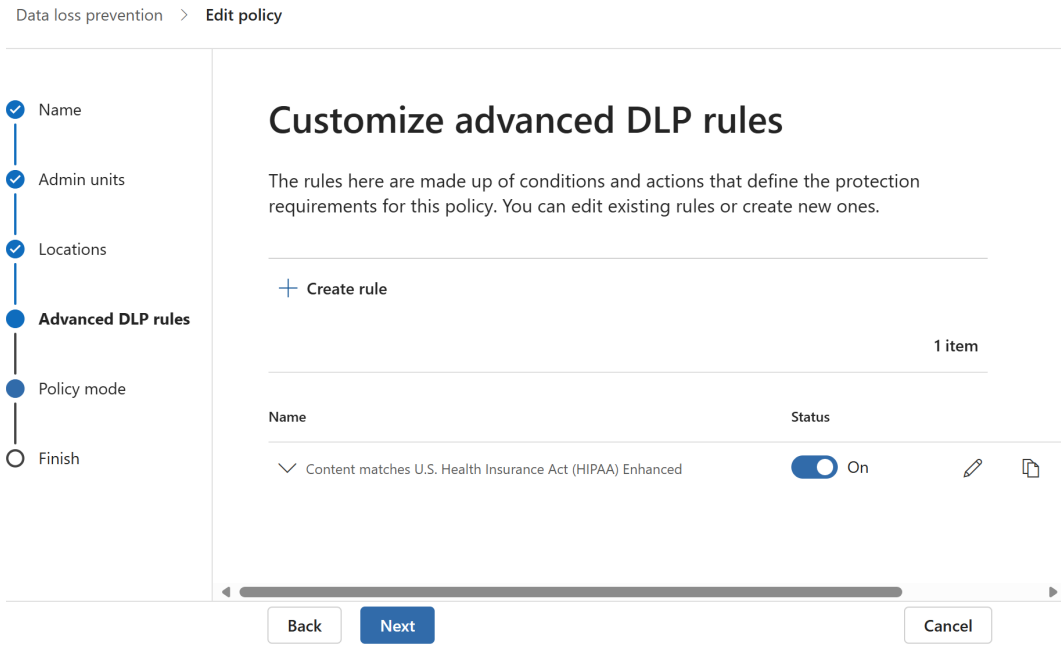


Figure 13.11 – Customize advanced DLP rules screen of a DLP policy

- 5. Scroll down to the **Incident reports** section and turn on **Use email incident reports to notify you when a policy match occurs** if it's not already enabled. *Figure 13.12* shows the options available related to incident reports when enabled.

Use email incident reports to notify you when a policy match occurs.



Send notifications to these people

heather@natechamberlain.com

molly@natechamberlain.com

[+ Add or remove users](#)

All incident reports include information about the item that was matched, where the match occurred, and the rules and policies it triggered.

You can also include the following information in the report:

- ☒ The name of the person who last modified the content
- ☒ The types of sensitive content that matched the rule
- ☒ The rule's severity level
- ☒ The content that matched the rule, including the surrounding text
- ☒ The item containing the content that matched the rule

▼ **Additional options**

Save

Cancel

Figure 13.12 – DLP policy action settings for incident reports

6. Configure the recipients of the reports by selecting **Add or remove users**. Consider delivering these reports to a non-person object, such as a group mailbox, rather than individual user mailboxes. This ensures that the incident reports are not isolated in a single person's inbox, enabling multiple stakeholders to stay informed and respond promptly.
7. Specify the details to include in the alerts by checking the box for the desired content, including the following:
 - **The name of the person who last modified the content**
 - **The types of sensitive content that matched the rule**
 - **The rule's severity level**
 - **The content that matched the rule, including the surrounding text**
 - **The item containing the content that matched the rule**
8. Select **Save** to apply the changes.
9. Select **Next** repeatedly until you can review the updated policy on the **Review and finish** screen. Then, select **Submit** when finished.

How it works...

By modifying a DLP policy to include incident reporting, you ensure that any detection of HIPAA-protected data automatically triggers a detailed report. This report is sent to specified users who don't have to necessarily be administrators, allowing for quick response and documentation of the incident, which is crucial for compliance and audit purposes.

There's more...

If you require different levels of detail in incident reports for different departments or recipients, you need to create multiple DLP policies with specific incident report configurations for each department. For the HR department, create a DLP policy with detailed incident reports. Configure it to include all available details. For the marketing department, set up a separate yet identical DLP policy with general incident reports that notify of breaches without exposing detailed personal information. This approach ensures that each department receives the appropriate level of detail in incident reports based on their specific needs and data sensitivity.

To help make this process of creating identical policies easier, you can copy an existing DLP policy to get started. Simply select the policy you wish to copy then **Copy policy**, as shown in *Figure 13.13*.

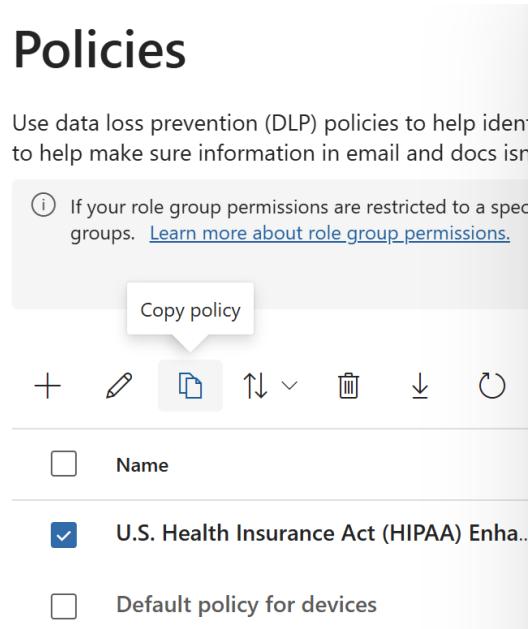


Figure 13.13 – Steps to copy an existing DLP policy

Then, in the copy's settings, be sure to specify different recipients and incident report details before saving it.

See also

- *Learn about data loss prevention*: <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>
- *Create and Deploy data loss prevention policies*: <https://learn.microsoft.com/en-us/purview/dlp-create-deploy-policy>

Creating a custom sensitive information type based on keywords

Before we can create policies that can respond to contents and activities involving custom keywords, such as confidential project or product names or unique sensitive identifiers you use within your organization, we will need to establish a new sensitive information type to use in later policies.

Getting ready

Ensure you have Global Administrator, Compliance Administrator, or Security Administrator permissions. Identify the custom keywords that are critical to your organization and need protection.

How to do it...

1. Sign in to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. If **Data Loss Prevention** appears on your home screen, select it. Otherwise, select **View all solutions | Data Loss Prevention**.

3. Select **Classifiers** | **Sensitive info types** from the left navigation menu, then **Create sensitive info type**, as shown in *Figure 13.14*.

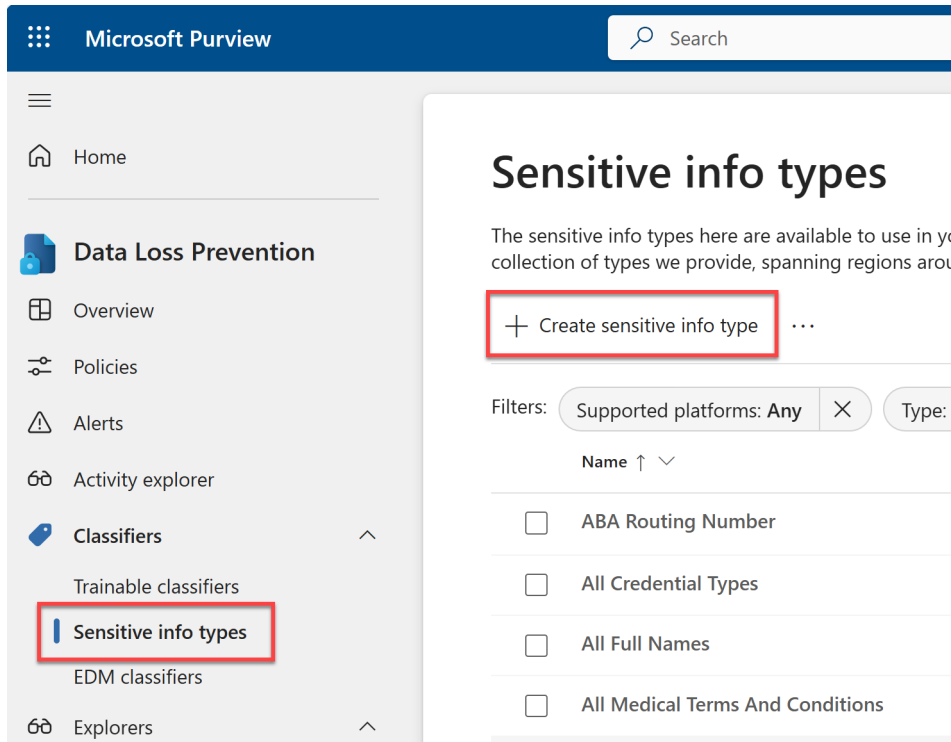


Figure 13.14 – Steps to create a new sensitive info type

4. Provide **Name** and **Description** values for the sensitive information type, such as the confidential project or product name and/or number. Select **Next**.
5. Select **Create pattern** and then choose the default confidence level for the pattern (**Low**, **Medium**, or **High** confidence in a match).
6. Select **Add primary element** | **Keyword list**, as shown in *Figure 13.15*.

Define pattern

Sensitive info type element and configuration to further refine the

+ Create pattern

At least one pattern

New pattern

At minimum, a pattern should have a confidence level and primary element to detect. Adding supporting elements, character proximity, and additional checks will help increase accuracy.

Regular expression

Keyword list

Keyword dictionary

Functions

+ Add primary element

Character proximity

Detect primary AND supporting elements within 300 characters

☐ Anywhere in the document

Back Next Create Cancel

Figure 13.15 – Steps to add a keyword list as a pattern for a sensitive info type

7. Enter a name for the keyword list, such as the name of the confidential project, then enter keywords in the **Keyword group #1** section, as shown in *Figure 13.16*. Note that there are separate boxes for keywords that should be case-sensitive when matching and those that are case-insensitive.


Add a keyword list

Keyword lists identify the words and phrases you want this info type to detect. For example, the keyword list to identify Netherlands VAT numbers is 'VAT number, vat no, vat number, VAT#'. [Learn how to create keyword lists](#)

Choose from existing keyword lists

ID * 

Project Moon

Keyword group #1 * 



Case insensitive

project moon
moon project
Project 19826
P19826

Case sensitive

Moon
Project Moon

Done

Cancel

Figure 13.16 – Keyword list for a new sensitive info type

8. Select **Done** to review your pattern configuration and then click **Next**.
9. Select **Next** again, leaving the confidence level unchanged. This is because the confidence level is pre-populated based on your pattern's confidence level, which applies when you are configuring only one pattern as we are in this recipe.
10. Review your new sensitive info type's setup and then select **Create**.

How it works...

Sensitive info types can be used in multiple types of security and compliance policies. When you create a custom sensitive info type, it appears alongside the hundreds of others provided by Microsoft based on generic sensitive information types, as shown in *Figure 13.17*.

Sensitive info types

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

Create sensitive info type

...

325 items

Search

Filters:

Supported platforms: Any

Type: Any

Publisher: Any

Add filter

Name

Supported pl...

Type

Publisher

<input type="checkbox"/>	Project Moon	Link	All	Entity	chambernate
<input type="checkbox"/>	ABA Routing Number	Link	All	Entity	Microsoft Corpor...
<input type="checkbox"/>	Argentina National Identity (DNI) Number	Link	All	Entity	Microsoft Corpor...
<input type="checkbox"/>	Argentina Unique Tax Identification Key (CUI...)	Link	All	Entity	Microsoft Corpor...
<input type="checkbox"/>	Australia Bank Account Number	Link	All	Entity	Microsoft Corpor...



Figure 13.17 – A custom sensitive info type shown alongside Microsoft's

Now that you have a custom sensitive info type for your organization, you can refer to that sensitive info type when building DLP and retention policies, as we will in this chapter.

There's more...

In addition to primary elements, your sensitive info type can consider supporting elements and additional checks. *Figure 13.18* shows the **Patterns** screen of the sensitive info type setup showing these additional areas for configuration.

Primary element * ⓘ

Keyword list: Project Moon  

Character proximity ⓘ

Detect primary AND supporting elements within characters

☐ Anywhere in the document

Supporting elements ⓘ

+ Add supporting elements or group of elements ▾

Additional checks ⓘ

+ Add additional checks ▾

Figure 13.18 – The Supporting elements and Additional checks sections of a sensitive info type

Supporting elements are useful when your primary element is a five-digit product number or employee ID pattern, and you don't want your policies to flag every five-digit number, as not all five-digit numbers are relevant. If your primary element is a five-digit number pattern, supporting elements can include keywords such as *product number*, *product*, *employee*, or *badge*. In the **Character proximity** section, you specify how close in characters the primary and supporting elements must be to be recognized as this sensitive information type.

Additional checks you can add are as follows:

- **Exclude specific values**
- **Starts or doesn't start with characters**
- **Ends or doesn't end with characters**
- **Exclude duplicate characters**

- **Include or exclude prefixes**
- **Include or exclude suffixes**

These additional checks might be helpful for scenarios in which you wish to exclude IDs that were used for tests or for products that have already launched and are now public knowledge (no longer sensitive).

See also

- *Create custom sensitive information types*: <https://learn.microsoft.com/en-us/purview/sit-create-a-custom-sensitive-information-type>

Creating a DLP policy for content with custom keywords in the name or subject

Organizations often have specific terms or projects that need extra security, such as projects the public or competitors should not know about. By creating a DLP policy that targets custom keywords, you can protect sensitive information related to these terms, ensuring that it does not get shared inappropriately.

Getting ready

Ensure you have Global Administrator, Compliance Administrator, or Security Administrator permissions.

You will also need to create a custom sensitive info type that includes the keywords and conditions for the specific subject you're protecting. See the previous recipe, *Creating a custom sensitive information type based on keywords*, and complete its steps prior to beginning this recipe.

How to do it...

1. Sign in to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. If **Data Loss Prevention** appears on your home screen, select it. Otherwise, select **View all solutions | Data Loss Prevention**.
3. Select **Policies** from the left navigation menu, then **Create policy**, as previously shown in *Figure 13.6*.

4. On the first screen of the wizard, select the **Custom** category, then select the **Custom policy** option under the **Regulations** section, and select **Next**. These options are shown in *Figure 13.19*.

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. [Learn more about DLP policy templates](#)

① **Check out our new enhanced policy templates.** These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Search for specific templates

All countries or regions

Categories	Regulations	Custom policy
Enhanced		
Financial		
Medical and health		
Privacy		
Custom	Custom policy	Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

Figure 13.19 – Options to choose for a custom DLP policy

5. Provide **Name** and **Description** values for your policy, then select **Next**.
6. Skip the **Assign admin units** screen by selecting **Next** again since we want this policy to apply to all users and groups. If you wanted to limit the admin units to which this policy applied, you would instead select **Add or remove admin units** and specify them before proceeding.
7. Define the locations for the policy (e.g., SharePoint, OneDrive, Exchange), as shown in *Figure 13.20*, and then select **Next**.

Data loss prevention > Create policy

Template or custom policy

Name

Admin units

Locations

Policy settings

Policy mode

Finish

Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

1

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply this policy to those users or groups. [Learn more about role group permissions.](#)

View role groups

1

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Location	Scope	
<input checked="" type="checkbox"/> Exchange email	All groups	Edit
<input checked="" type="checkbox"/> SharePoint sites	All sites	Edit
<input checked="" type="checkbox"/> OneDrive accounts	All users & groups	Edit
<input checked="" type="checkbox"/> Teams chat and channel messages	All users & groups	Edit
<input type="checkbox"/> Instances	Turn on location to scope	
<input type="checkbox"/> On-premises repositories	Turn on location to scope	

Back

Next

Cancel

Figure 13.20 – DLP policy locations

8. **Create or customize advanced DLP rules** is already selected for you. Select **Next** again.

9. Select **Create rule**. Provide **Name** and **Description** values.

10. Under **Conditions**, select **Add condition** | **Content contains**, as shown in *Figure 13.21*.

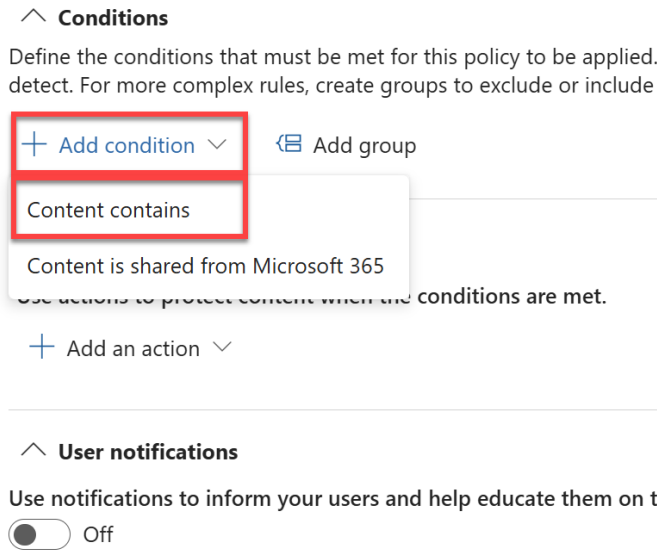


Figure 13.21 – Option to add DLP policy conditions based on contents

11. Within the **Default** group provided, select **Add** | **Sensitive info types** to add a condition to detect custom keywords in document names, subjects, and messages (depending on the locations you've chosen). This is shown in *Figure 13.22*.

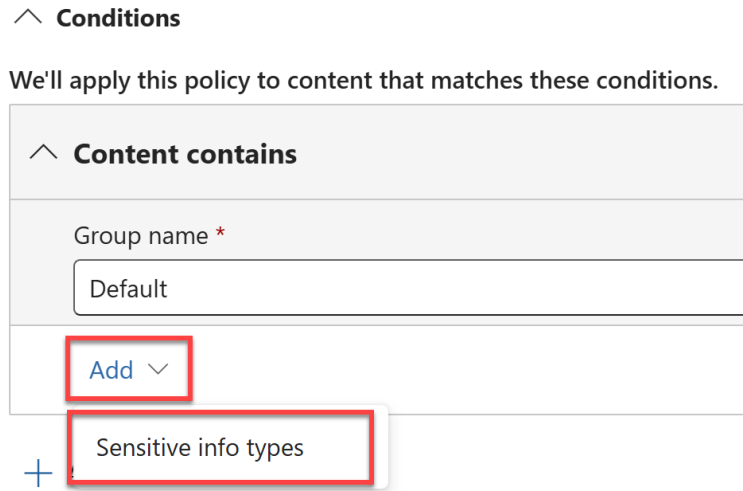


Figure 13.22 – Sensitive info types option for a DLP policy's condition

12. Search for and select the sensitive info type you created containing the custom keywords you wish to monitor. Then, select **Done**.
13. Specify the **Instance count** value for the sensitive info type. For example, an **Instance count** value of 3 to *Any* will require that the info type is found at least 3 times in a document, message, and so on before this policy's actions are triggered.
14. Scroll down and select **Add an action** in the **Actions** section. Note in *Figure 13.23* how you can choose to restrict file access or encrypt it or restrict third-party apps from accessing the content.

^ **Actions**

Use actions to protect content when the conditions are met.

+ Add an action ▾

Restrict access or encrypt the content in Microsoft 365 locations

Restrict third-party apps

Restrict access or remove on-premises files

Figure 13.23 –The action options for a DLP policy rule

15. Scroll down to **User notifications** and **Incident reports**. Configure the messages or reports you want to send when the sensitive info type is detected, like what you did in the recipe titled *Using DLP to automatically report HIPAA Incident Reports*.
16. Select **Save**, then **Next**.
17. On the **Policy mode** screen, choose whether you wish to do the following:
 - **Run the policy in simulation mode.** (Review items that match the policy's conditions and choose whether to **Show policy tips while in simulation mode** and if you want to automatically turn on this policy if it's unedited for 15 days.)
 - **Turn the policy on immediately.** (This may take up to an hour to begin enforcing.)
 - **Leave the policy turned off.** (Do this in case you'd rather test it or turn it on later.)
18. Select **Next**, review your settings, and select **Submit** to finalize the policy.

How it works...

A DLP policy with custom keywords allows you to monitor and protect documents containing specific terms or project names. This ensures that any sensitive information related to those keywords is securely managed and prevented from unauthorized sharing through restricting access, encrypting, or notifying the involved users and/or administrators.

There's more...

Incorporate **sensitivity labels** in conjunction with your DLP policies. Sensitivity labels can help auto-classify and protect content based on its level of confidentiality. By using both DLP policies and sensitivity labels, you create a multi-layered security approach that better safeguards your organization's data.

To get started with sensitivity labels, go to Microsoft Purview at <https://purview.microsoft.com>, then select **View all solutions | Information Protection | Sensitivity labels**.

See also

- *Learn about data loss prevention:* <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>
- *Create and Deploy data loss prevention policies:* <https://learn.microsoft.com/en-us/purview/dlp-create-deploy-policy>
- *Learn about sensitivity labels:* <https://learn.microsoft.com/en-us/purview/sensitivity-labels>

Tuning a DLP policy's sensitivity

Fine-tuning a DLP policy's sensitivity ensures that it effectively detects and prevents data leaks while minimizing false positives. Adjusting the confidence level of sensitive information types is an essential part of this process.

Getting ready

Ensure you have Compliance Administrator or Security Administrator permissions.

How to do it...

1. Sign in to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. If **Data Loss Prevention** appears on your home screen, select it. Otherwise, select **View all solutions | Data Loss Prevention**.

3. Choose **Classifiers | Sensitive info types**, as previously shown in *Figure 13.14* in this chapter's recipe titled *Creating a custom sensitive information type based on keywords*.
4. Search for and select the name of the custom sensitive information type you want to adjust, then select **Edit**, as shown in *Figure 13.24*.

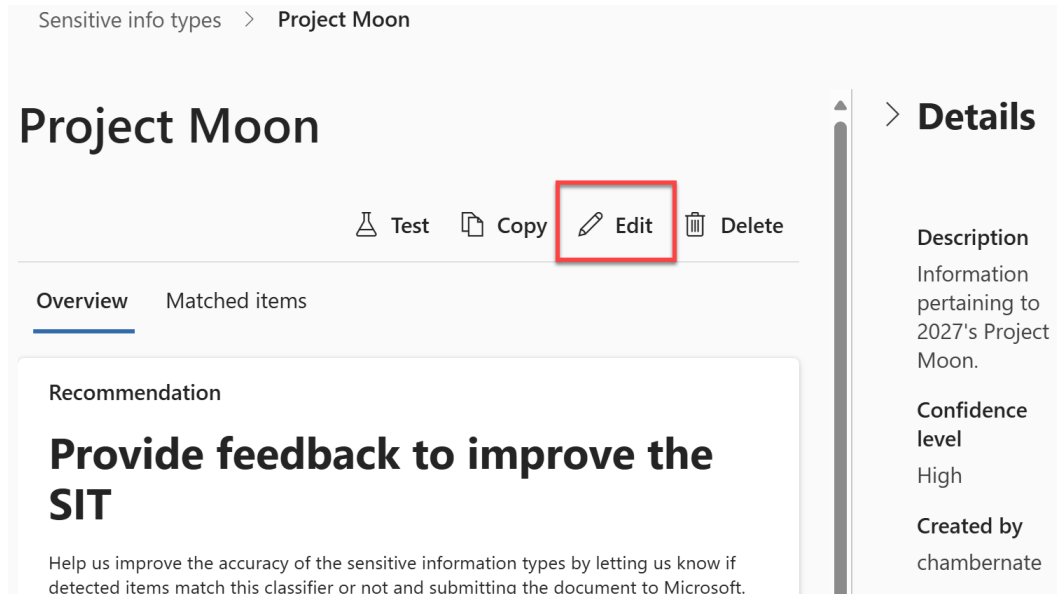
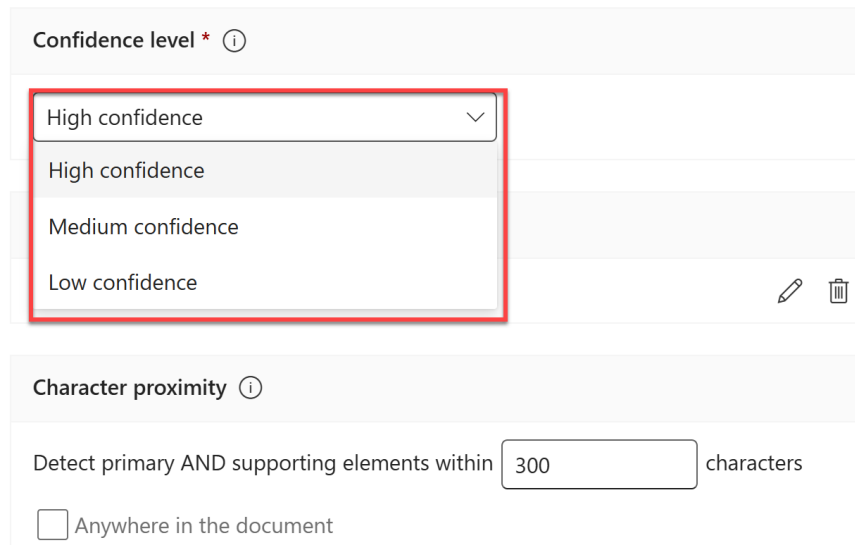


Figure 13.24 – Option to edit a sensitive info type

5. Select **Next** to go to the **Patterns** screen and then select **Edit** (the pencil icon) next to the pattern for which you're modifying the sensitivity.
6. Adjust the **Confidence level**, as shown in *Figure 13.25*, to the desired setting (see the *How it works...* section of this recipe for more information on the options: **Low confidence**, **Medium confidence**, or **High confidence**).

Edit pattern

At minimum, a pattern should have a confidence level and primary element to detect. Adding supporting elements, character proximity, and additional checks will help increase accuracy.



The screenshot shows the 'Edit pattern' configuration interface. The 'Confidence level' section has a dropdown menu with three options: 'High confidence', 'Medium confidence', and 'Low confidence'. The 'High confidence' option is currently selected. Below this, the 'Character proximity' section is visible, featuring a text input field containing '300' and the label 'characters'. There is also an unchecked checkbox labeled 'Anywhere in the document'.

Figure 13.25 – Confidence level for a sensitive info type's pattern

7. Select **Update** to apply the changes. Then, select **Next** twice, and click **Save**.
8. Now that your sensitive info type's confidence level has been adjusted, any policy (including DLP policies) that looks for this sensitive info type will be more or less sensitive based on your selection in *Step 6*.

How it works...

By tuning the confidence level of a pattern within a sensitive info type's configuration, you can control the balance between catching true positives and avoiding false positives. Higher confidence levels result in fewer, more accurate detections, while lower levels increase sensitivity but may capture more false positives. Specifying more supporting elements requires selecting a higher confidence level to ensure the matched items contain the targeted sensitive information. For instance, matches with a high confidence level will have more supporting elements near the primary element, while matches with a low confidence level will have few or no supporting elements in close proximity.

There's more...

After tuning your DLP policy's sensitivity (by adjusting your sensitive info type's confidence levels), consider implementing a monitoring phase where you track the policy's effectiveness and adjust as necessary. Regularly consult the DLP reports and dashboards in Microsoft Purview to identify trends and refine your policy settings.

See also

- *Learn about data loss prevention:* <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>
- *Create custom sensitive information types:* <https://learn.microsoft.com/en-us/purview/sit-create-a-custom-sensitive-information-type>

Creating a retention policy to retain content for seven years

Retention policies help organizations manage the lifecycle of their data, ensuring that important information is retained for compliance and operational purposes. This recipe focuses on creating a retention policy that applies to all users' and groups' mailboxes, OneDrive accounts, and SharePoint sites. It will retain content for 7 years (a regulatory requirement in this fictional scenario) before it allows the content to be deleted.

Getting ready

Ensure you have Global Administrator, Compliance Administrator, or Security Administrator permissions.

How to do it...

1. Sign in to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. Select **View all solutions | Data lifecycle management** then select **Policies | Retention** from the left navigation menu.
3. Select **New retention policy** and provide **Name** and **Description** values for the new policy, such as **7-year Retention**. Select **Next**.
4. Select **Next** again to keep **Policy scope** set to all users and guests. Alternatively, you can add admin units to restrict the policy's application to specific individuals. This is useful if only certain people are working on a confidential project, and it is unlikely that anyone outside this group will be creating and managing the confidential content that needs to be retained.

5. Choose how you want to specify locations to which your new retention policy will apply:

- **Adaptive:** You don't specify a static list of locations, as it might grow over time. Instead, you want anything matching specific properties (e.g., site URL contains *HR* or site name contains *Moon*).
- **Static:** Specify exact locations if you know the locations won't change.

For this recipe, we'll select **Static**, as shown in *Figure 13.26*, as we want this to apply to all locations.

Data lifecycle management > Create retention policy

Choose the type of retention policy to create

Locations can be specified dynamically with an adaptive scope using attributes or properties, or if you know the specific target locations, you can select them individually from a list. An advantage of using an adaptive scope to determine target locations is that it will automatically update where it's applied based on the attributes or properties you define.

☐ **Adaptive**
After selecting adaptive policy scopes, which consist of attributes or properties (e.g. 'Department' or 'Site URL') that define the users, groups, or sites in your org, you'll choose supported locations containing the content you want to retain. The policy will automatically update to match the criteria defined in the scopes.

☒ **Static**
You'll choose locations containing the content you want to retain. If locations change after this policy is created (for example if a SharePoint site is added or removed), you'll need to manually update the policy.

Back Next Cancel

Figure 13.26 – Retention policy type settings

6. Select **Next**. Specify the locations to which this retention policy will apply from the following options:

- **Exchange mailboxes** (all or specific)
- **SharePoint classic and communication sites** (all or specific)
- **OneDrive accounts** (all or specific)
- **Microsoft 365 Group mailboxes & sites** (all or specific)

- **Skype for Business** (all or specific)
- **Exchange public folders** (all or specific)
- **Teams channel messages** (all or specific)
- **Teams chats and Copilot interactions** (all or specific)
- **Teams private channel messages** (all or specific)
- **Yammer community messages** (all or specific)
- **Yammer user messages** (all or specific)

Unless otherwise specified, any locations you toggle on will include all locations within that service automatically. For this recipe, toggle on **Exchange mailboxes**, **SharePoint classic and communication sites**, **OneDrive accounts**, and **Microsoft 365 Group mailboxes & sites**, as shown in *Figure 13.27*.

Data lifecycle management > Create retention policy

✓ Name

✓ Administrative Units

● Type

● Locations

○ Retention settings

○ Finish

Choose where to apply this policy

The policy will apply to content that's stored in the locations you choose.

i You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. [Set up now](#)

Status	Location	Applicable Content
<input checked="" type="checkbox"/> On	Exchange mailboxes	Items in user, shared, and resource mailboxes: emails, calendar items with an end date, notes, and tasks with an end date. Doesn't apply to items in Microsoft 365 Group mailboxes. More details
<input checked="" type="checkbox"/> On	SharePoint classic and communication sites	Files in classic sites or communication sites or team sites that aren't connected to a Microsoft 365 group, and files in all document libraries (including default ones like Site Assets). More details
<input checked="" type="checkbox"/> On	OneDrive accounts	All files in users' OneDrive accounts. More details
<input checked="" type="checkbox"/> On	Microsoft 365 Group mailboxes & sites	Items in the Microsoft 365 Group mailbox, and files in the corresponding group-connected SharePoint team site. Doesn't apply to files in SharePoint classic or

Back

Next

Cancel

Figure 13.27 – Locations specified in a retention policy

7. Select **Next**. On the **Retention settings** screen, configure the following as shown in *Figure 13.28*:
- **Retain items for a specific period: 7 years.**
 - **Start the retention period based on: When items were last modified.**
 - **At the end of the retention period: Do nothing.** (We simply want to prevent deletion until it has been seven years since the modifications. After seven years, we can choose to keep or delete the content, but it will be kept unless some other action is taken.)

Data lifecycle management > Create retention policy

✓ Name

✓ Administrative Units

✓ Type

Retention settings

○ Finish

Decide if you want to retain content, delete it, or both

☒ Retain items for a specific period
Items will be retained for the period you choose.

Retain items for a specific period

7 years

Start the retention period based on

When items were last modified

At the end of the retention period

☐ Delete items automatically

☒ Do nothing

☐ Retain items forever
Items will be retained forever, even if users delete them.

☐ Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Back

Next

Cancel

Figure 13.28 – Retention settings for a new retention policy

8. Select **Next**, review your policy, then select **Submit**.

How it works...

This retention policy will automatically apply to all content within the selected locations, ensuring that important information is preserved according to organizational and regulatory requirements. After the defined time period, users can choose to keep or delete the content that has passed its retention period.

There's more...

Combining retention policies with **retention labels** offers several benefits for managing your organization's data. Retention labels allow you to apply specific retention settings to individual items or documents, offering a finer level of control than broad retention policies. This is particularly useful for handling exceptions to your overarching retention policy. For instance, while a general retention policy might require retaining all content for seven years, as it did in this recipe, certain documents might need to be retained longer due to legal requirements or shorter due to operational needs. Retention labels let your users manually mark these exceptions without altering the entire policy.

Additionally, integrating retention labels with retention policies enhances data governance by aligning retention requirements with the sensitivity and classification of the data. Sensitive or confidential information can be given retention labels that not only ensure the data is kept for the appropriate duration but also include security measures such as encryption and access controls. This dual approach helps in complying with regulations, protecting sensitive information, and ensuring that data lifecycle management is both effective and compliant with organizational policies.

Get started by configuring retention labels in Microsoft Purview at <https://purview.microsoft.com>. Once there, select **View all solutions | Data lifecycle management | Retention labels**. Here, you can create labels that override your broader retention policies and have the following settings, as shown in *Figure 13.29*:

- **Retain items forever or for a specific period**
- **Enforce actions after a specific period** (such as deleting or relabeling)
- **Just label items** (more for classification, not for changing retention actions)

Create retention label

☒ Name

☒ **Label Settings**

☐ Period

☐ Finish

Define label settings

We'll apply the settings you choose to labeled items

- ☒ **Retain items forever or for a specific period**
Items won't be retained but when they reach the age you specify, they'll be deleted from where they are stored.
- ☐ **Enforce actions after a specific period**
Labeled items won't be retained. You can decide whether they should be deleted, or relabeled when the period you specify in the next step ends.
- ☐ **Just label items**
Choose this setting if you only want to classify labeled items. The items won't be retained and your users won't be restricted from editing, moving, or deleting them.

Figure 13.29 – Retention label settings

Once you've saved your label, you can choose to allow users to manually apply it as needed, or you can choose to auto-apply it to content matching certain criteria, such as those defined by the sensitive info type we created in this chapter's recipe titled *Creating a custom sensitive information type based on keywords*.

See also

- *Learn about retention policies and retention labels:* <https://learn.microsoft.com/en-us/purview/retention>

Creating and using an eDiscovery case

Standard eDiscovery cases in Microsoft Purview allow organizations to identify, hold, and manage **electronically stored information (ESI)** that may be relevant to legal cases or investigations. This ensures that necessary data is preserved and accessible for legal review. In this recipe, we'll set up a standard eDiscovery case.

Tip

Check out this recipe's *There's more...* section to learn how premium cases differ from standard cases.

Getting ready

Ensure you have Global, Administrator, eDiscovery Administrator, or eDiscovery Manager permissions. Familiarize yourself with the types of data that may be relevant to legal inquiries within your organization.

How to do it...

1. Sign in to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. Select **View all solutions | eDiscovery | Standard Cases**.
3. Select **Create a case**.
4. Provide **Name** and **Description** values for the case, and then select **Save**.
5. Open the newly created case by selecting its name from the **eDiscovery (Standard)** screen, as shown in *Figure 13.30*.

eDiscovery (Standard)

After creating an eDiscovery case and choosing who has access to it, use the case to search for email, documents, Skype f Teams data, and other content in your organization. You can then preserve the content and export the search results for f [more](#)

+ Create a case

↓ Download list

↻ Refresh1 item

🔍 Search

☰ Group

▼

🔎 Filter

Name	Status	Created date	Last modified
<div><div><input type="checkbox"/></div><div>Project Moon eDiscovery</div><div>⋮</div></div>	Active	Jul 28, 2024 8:40 AM	Jul 28, 2024 8:40 AM

Figure 13.30 – A newly created eDiscovery case

6. Add members to the case, or update existing permissions, by selecting **Settings | Access & permissions | Select**, as shown in *Figure 13.31*.

eDiscovery (Standard) > Project Moon eDiscovery

Home

Searches

Hold

Exports

Settings

📷 Case Information

Edit general information about your case, such as:

- Case name
- Case number
- Description
- Status
- Delete case

Select

🔗 Access & permissions

Manage who can access your case and what they can do.

- Add / remove members
- Add / remove role groups

Select

Figure 13.31 – Steps to manage an eDiscovery case's permissions

- 7. Add users or role groups that should have access to the case, then select **Close**.
- 8. To preserve content matching a specific query, go to the **Hold** tab and select **Create** to create a hold.
- 9. Provide **Name** and **Description** values for your hold and select **Next**.
- 10. Define the hold locations, choosing to include or exclude **Exchange mailboxes** (all or specific), **SharePoint sites** (all or specific), and **Exchange public folders** (all or none). For this recipe, enable all locations, as shown in *Figure 13.32*.

New Hold

✓

Name your hold

●

Choose locations

○

Query

○

Review your settings

Choose locations

Status	Location	Included	Excluded
<div><div></div>On</div>	<div><div></div>Exchange mailboxes</div> <div><div></div>Microsoft 365 Groups</div> <div><div></div>Teams</div> <div><div></div>Yammer user messages</div>	None Choose users, groups, or teams	None
<div><div></div>On</div>	<div><div></div>SharePoint sites</div> <div><div></div>OneDrive sites</div> <div><div></div>Microsoft 365 Group Sites</div> <div><div></div>Team Sites</div> <div><div></div>Yammer Networks</div>	None Choose sites	None
<div><div></div>On</div>	<div><div></div>Exchange public folders</div>	All	None

Back

Next

Cancel

Figure 13.32 – All locations selected for a new hold

- 11. Select **Next** to configure the keywords and conditions under which a hold should be placed on content and then select **Save**. Notice in *Figure 13.33* how there are many different properties on which you can build conditions.

New Hold

✓ Name your hold

✓ Choose locations

Query

○ Review your settings

Query

☒ Query builder
 ☐ KQL editor

Keywords

Enter keywords

☐ Show keyword list

+ Add condition ▾

Date
Sender/Author
Size (in bytes)
Subject/Title
Retention label
Message kind
Participants
Type
Received
Recipients
Sender
Sent
Subject
To
Author
Title
Created
Last modified
File type

Back

Next

Figure 13.33 – Condition properties for a new hold

12. Select **Next**, review your new hold configuration, and then select **Submit** and **Done**.
13. As opposed to a hold that preserves content, you can also perform searches instead that just find matching content. This doesn't take action on the content but allows you to easily find content that would otherwise be held or protected. Select the **Searches** tab and then click **New search** to get started. Searches are set up nearly identically to how a hold is configured, so repeat *Steps 9-12* to set up your search.
14. When the eDiscovery case is no longer active or needed, you can open the case and select **Close case** from its **Home** tab.

How it works...

An eDiscovery case functions as a container to manage all activities related to a legal investigation. It allows you to place holds on relevant data, perform searches, and manage access to ensure all necessary information is preserved and reviewed appropriately. You, and those you've added in *Steps 6-7*, can review and export the content being held or appearing in searches by opening the case from Microsoft Purview's **eDiscovery | Standard cases** screen.

There's more...

While standard eDiscovery cases in Microsoft Purview provide essential tools for identifying, holding, and managing information relevant to legal cases, **eDiscovery (Premium) cases** offer advanced capabilities tailored for more complex legal matters. eDiscovery (Premium) enhances the standard features by providing robust data analysis, deeper content insights, and more efficient workflows. Note that a Microsoft 365 E5 license (or equivalent) is required to use eDiscovery (Premium).

To get started with eDiscovery (Premium), go to <https://purview.microsoft.com> and select **View all solutions | eDiscovery | Premium Cases**.

One of the key differences is the inclusion of advanced analytics and machine learning in eDiscovery (Premium). This allows for features such as **optical character recognition (OCR)** so you can find content with text in images matching your query, relevance scoring, near-duplicate detection, email threading, and theme identification, which significantly improve the accuracy and efficiency of document review processes. These tools help legal teams quickly identify the most pertinent information, reducing the time and cost associated with large-scale data reviews.

Another advantage of eDiscovery (Premium) is its capability to manage and review large volumes of data with enhanced scalability. It offers more comprehensive reporting and tracking features, enabling better oversight and documentation of the eDiscovery process.

Furthermore, eDiscovery (Premium) includes additional security and compliance features, such as custodial data sources and legal hold notifications, which help ensure that all relevant data is preserved in compliance with legal requirements. This level of control and precision is important for organizations dealing with highly sensitive or extensive legal inquiries.

See also

- *Overview of Microsoft Purview eDiscovery (Premium)*: <https://learn.microsoft.com/en-us/purview/ediscovery-overview>
- *Get started with eDiscovery (Standard)*: <https://learn.microsoft.com/en-us/purview/ediscovery-standard-get-started>

Assigning permissions for non-IT users to Microsoft Purview

Assigning appropriate permissions to non-IT users in Microsoft Purview ensures that they can access necessary compliance and security features without compromising overall system security. **Role-based access control (RBAC)** allows you to assign specific roles to users based on their job functions, enabling them to perform tasks related to compliance and security effectively.

In this recipe, we will assign the Compliance Manager Reader role to a user so that they will have read-only access to the organization's compliance score and its related factors via Compliance Manager.

Tip

While we are focusing on a specific role within Microsoft Purview, keep in mind the steps are similar for other roles that grant limited access to other Microsoft Purview solutions.

Getting ready

Ensure you have Global Administrator permissions. Identify the specific roles and permissions required by non-IT users to perform their tasks in Compliance Manager.

How to do it...

1. Sign in to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. Select **Settings | Roles and scopes** from the left navigation menu.

3. Select **Role groups**, as shown in *Figure 13.34*.

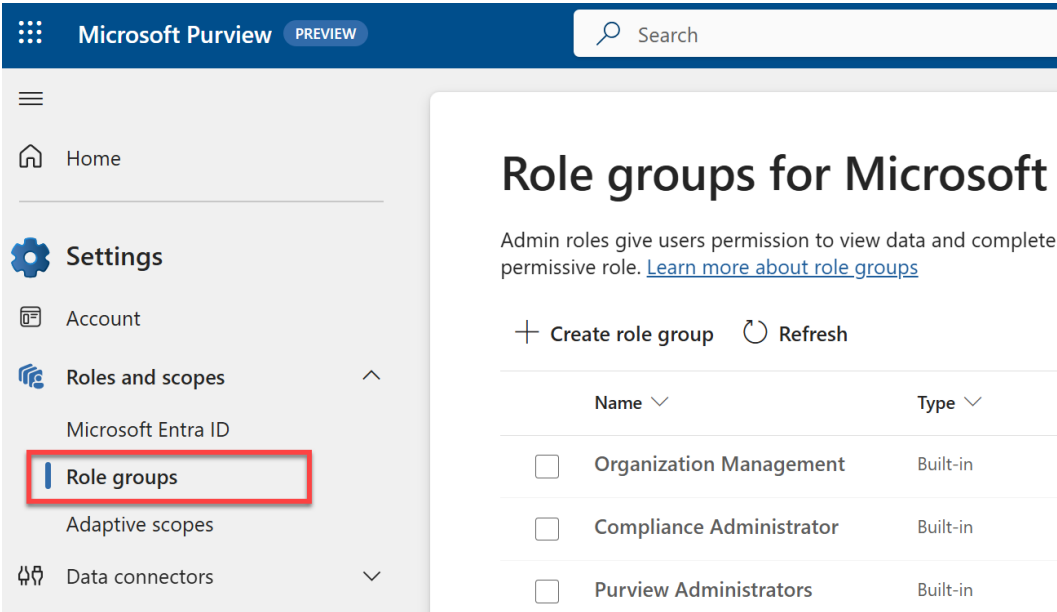


Figure 13.34 – Location of Role groups within Microsoft Purview settings

4. Now, choose the role group you want to assign (e.g., Compliance Administrator, Global Reader). For this recipe, select **Compliance Manager Readers**.
5. Select **Edit**.
6. On the **Edit members of the role group** page shown in *Figure 13.35*, select either **Choose users** or **Choose groups**.

Compliance Manager Readers

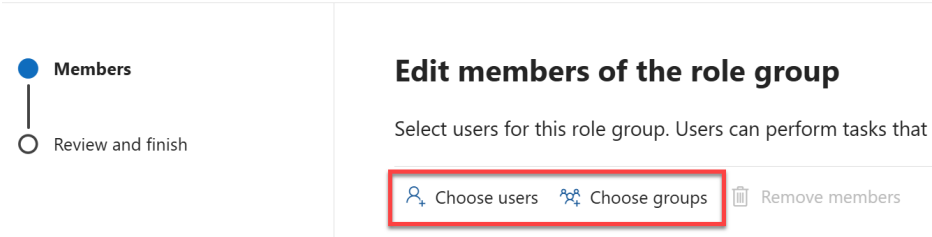


Figure 13.35 – Option to add users or groups to the Compliance Manager Readers role group

7. Search for and select the users or groups to which you want to assign the role.
8. Select **Next** to review the pending role changes, and then click **Save** to apply them.

How it works...

Assigning specific roles to non-IT users allows them to access the necessary compliance and security features within Microsoft Purview without granting full administrative rights. This approach ensures proper RBAC, enhancing security and efficiency. In this case, the newly assigned Compliance Manager Readers can access Compliance Manager and read, but not edit, data.

Tip

Another role you may wish to assign to a non-IT user is the **eDiscovery Manager role**. This allows users to view and edit all eDiscovery cases but doesn't give them control over Microsoft Purview's many other compliance features and tools.

There's more...

Compliance Manager is like Microsoft Defender's Secure Score feature, except it scores your organization's compliance score instead. *Figure 13.36* shows Compliance Manager within Microsoft Purview. It can be found by navigating to Microsoft Purview at <https://purview.microsoft.com> and selecting **View all solutions | Compliance Manager**.

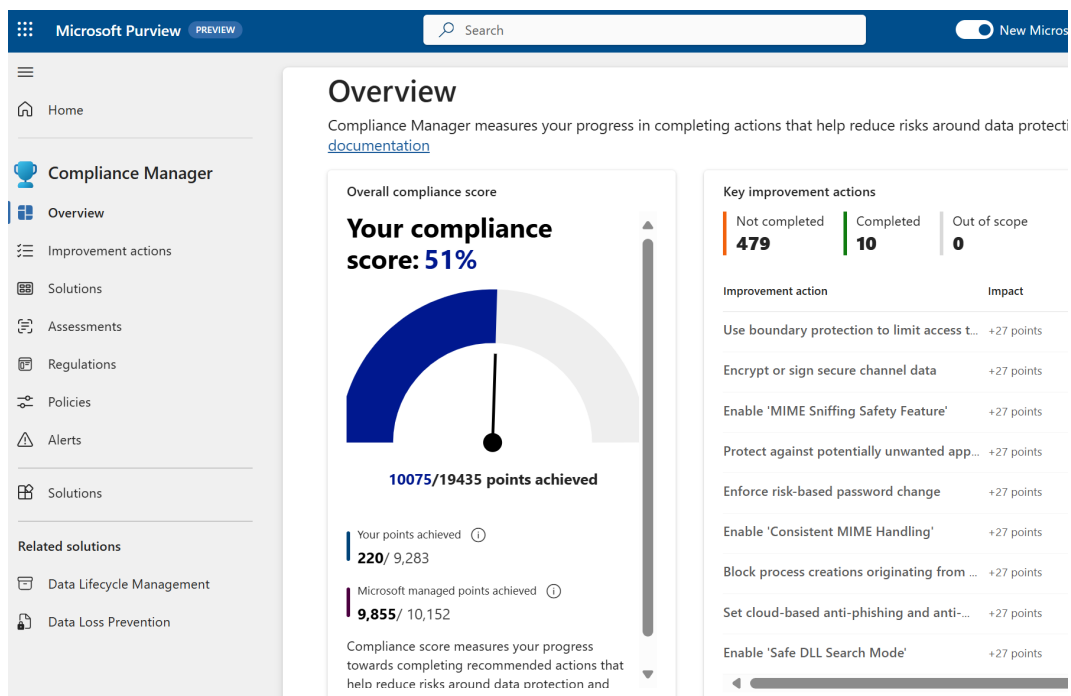


Figure 13.36 – Compliance Manager in Microsoft Purview

Compliance Manager users will be able to view this score and, depending on their specific role, take action to improve it.

See also

- *Permissions in the Microsoft Purview portal*: <https://learn.microsoft.com/en-us/purview/purview-permissions>

Using Communication Compliance to identify potential policy violations in messages

Communication Compliance in Microsoft Purview helps organizations monitor and review communications to identify potential policy violations. This tool is essential for maintaining compliance with organizational policies and regulatory requirements, and for ensuring a safe and respectful communication environment.

In this recipe, we will add the predefined policy from Microsoft that monitors messages for offensive language.

Getting ready

Ensure you have the necessary roles assigned, such as Global Administrator or Compliance Administrator.

How to do it...

1. Sign in to the Microsoft Purview portal at <https://purview.microsoft.com>.
2. Select **View all solutions | Communication Compliance**.
3. Select **Policies** from the left navigation menu, then **Create policy | Detect inappropriate text**, as shown in *Figure 13.37*.

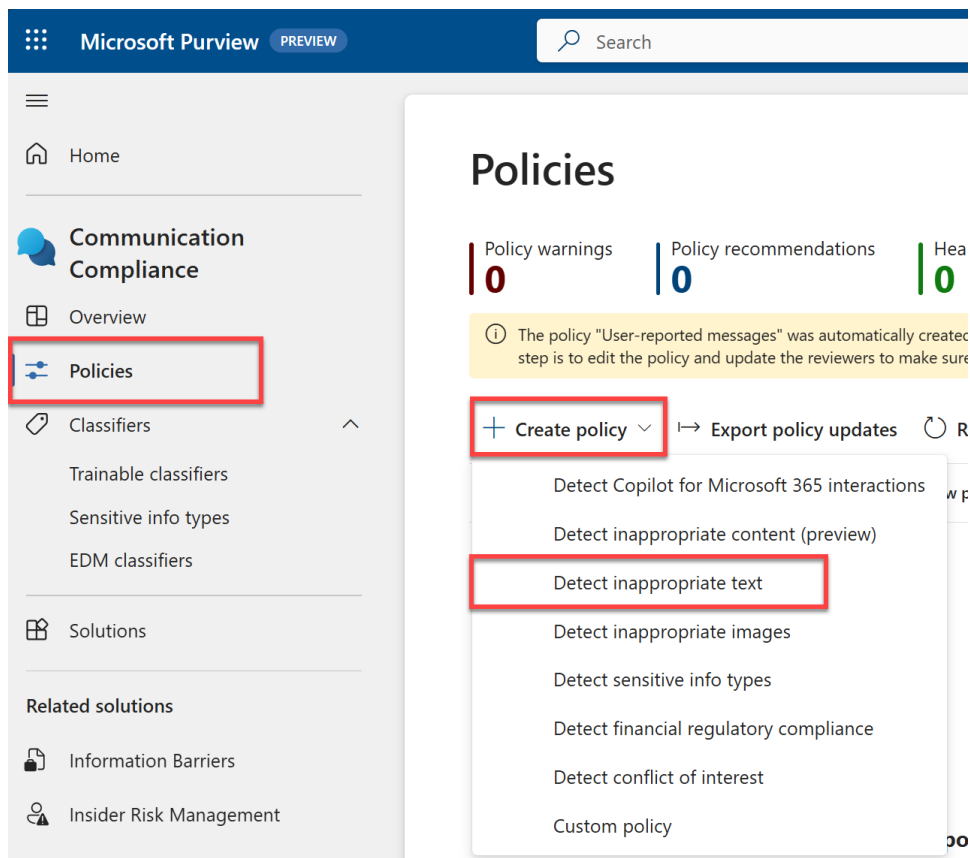


Figure 13.37 – Steps to create a Communication Compliance policy for inappropriate text

4. Provide a name for the policy and choose the users and/or groups to monitor under **Users or groups in scope**.
5. Specify the reviewers who will receive alerts for policy violations. Since we selected a template, it pre-populated the following:
 - Exchange, Teams, and Viva Engage as locations
 - Conditions and percentage to review

- The default **Targeted Harassment**, **Threat**, and **Discrimination** trainable classifiers for the policy to monitor. The policy configured thus far is shown in *Figure 13.38*.

Detect communications for inappropriate text

Policy name *

Inappropriate Text

Users or groups in scope *

☒ All users

☐ Select users

Start typing to find users or groups

Reviewers *

NW Nestor Wilke × NC Nate Chamberlain × Start typing to find users

Settings we've filled in for you ^

Communications to detect ⓘ

Scoped locations Exchange, Teams, Viva Engage

Conditions and percentage

Communication direction Inbound, Outbound, Internal

Percentage to review 100

Optical character recognition(OCR) Enabled

Filter email blasts Enabled

Detect content matching these trainable classifiers ⓘ

- Targeted Harassment
- Threat
- Discrimination

Create policy Customize policy ...

Figure 13.38 – A new Communication Compliance policy for inappropriate text

6. Select **Create policy** to finalize the setup.

How it works...

The Communication Compliance policy will take up to an hour to take effect, but then will continuously monitor the specified communication locations for offensive language or other risky content, including text found in images by using OCR. Alerts will be sent to designated reviewers when potential violations are detected, allowing for prompt investigation and remediation.

There's more...

While we chose one template in this recipe, there are several other templates that are built-in that you may want to consider implementing, such as **Detect communications for inappropriate content**, which will monitor for content matching **Sexual**, **Violence**, **Hate**, or **Self-harm** trainable classifiers provided by Microsoft.

You can also use Communication Compliance to detect any sensitive info types, including custom types you've configured, as we did in this chapter's recipe titled *Creating a custom sensitive information type based on keywords*. After selecting **Create policy**, choose **Detect sensitive info types** and select your custom type from the **Add sensitive info or keyword dictionary** options.

You can also create a custom policy from scratch by selecting **Create policy | Custom policy** or even customize one of the templates' predefined settings by selecting the template, and then clicking **Customize policy** after you've begun configuring it, as shown in *Figure 13.39*.

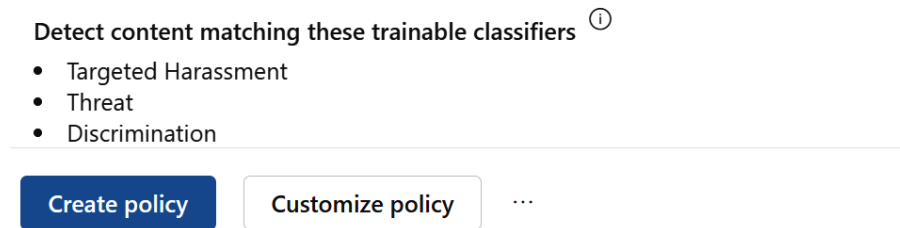


Figure 13.39 – Option to customize policy at the bottom of a new policy configuration panel

See also

- *Learn about communication compliance:* <https://learn.microsoft.com/en-us/purview/communication-compliance>
- *Create and manage communication compliance policies:* <https://learn.microsoft.com/en-us/purview/communication-compliance-policies>

Monitoring Microsoft 365 Apps and Services

Regularly monitoring Microsoft 365 apps and services helps you maintain a secure, compliant, and efficiently functioning environment. This chapter focuses on providing administrators with the tools and techniques necessary to track and analyze the usage and performance of various Microsoft 365 services. Through these recipes, you will learn how to identify at-risk users, create alerts for specific activities, review email handling histories, and monitor the health and usage of SharePoint, Teams, Power Apps, and more.

Monitoring activities helps in the early detection of potential security issues, ensuring compliance with organizational policies, and optimizing the overall use of Microsoft 365 services. By leveraging the monitoring capabilities discussed in this chapter, Administrators can maintain a proactive stance in managing their Microsoft 365 environment.

We will cover the following recipes in this chapter:

- Finding at-risk users
- Creating alerts for specific activities performed by users in OneDrive
- Reviewing mail handling to see spam and malware history
- Identifying your least active SharePoint sites
- Analyzing search activity throughout Microsoft 365
- Checking service health status and known issues
- Checking general usage data for Microsoft 365 apps and services
- Checking Teams usage and user activity
- Monitoring Power Apps and Power Automate usage and activity

Technical requirements

This chapter requires administrative access to Microsoft 365. Users assigned the Global Administrator role will have the capability to execute all tasks presented. Those holding specific app or function administration roles such as Compliance or Security Administrators will find many of these recipes within their reach. Additionally, audit logging must be enabled in your organization to track user activities and system events comprehensively.

Finding at-risk users

At-risk users are those flagged for unusual behavior, such as suspicious sign-ins or unfamiliar sign-in properties. Identifying and addressing these users is critical for maintaining the security of your organization. This recipe will guide you through the steps to find and manage at-risk users using Microsoft Entra ID Protection.

Getting ready

Ensure that you have a Microsoft Entra ID P1 or P2 license and are a Global or Security Administrator.

How to do it...

1. Go to the Microsoft Entra admin center at <https://entra.microsoft.com>.
2. Select **Protection** from the left navigation menu and then **Identity Protection**, as shown in *Figure 14.1*.

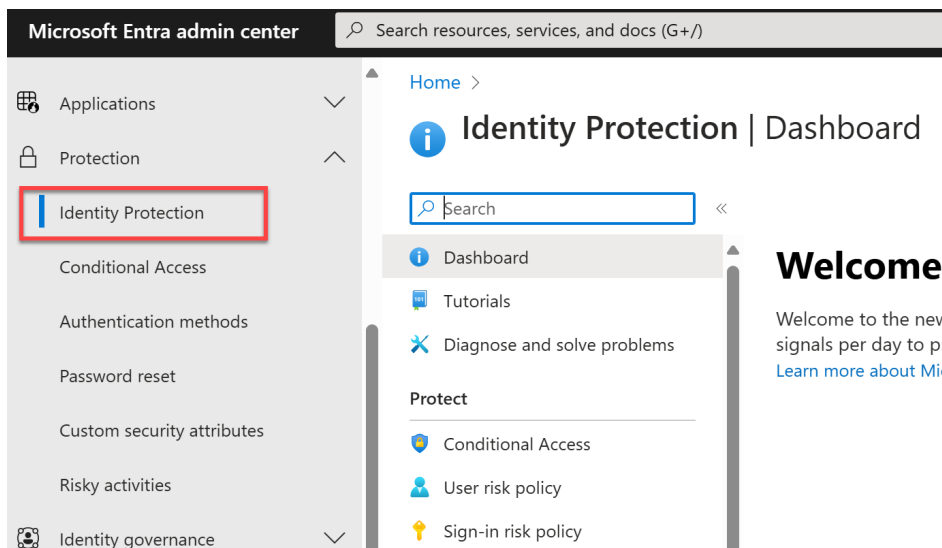


Figure 14.1 – Location of Identity Protection in Microsoft Entra

3. Under the **Report** section, select **Risky users**.
4. Review the list of users with a risk state of **At risk** or change the list's filters to view users who are **Confirmed compromised**, **Remediated**, **Dismissed**, or **Confirmed safe**.
5. Select **Risk detections** on the left to get detailed information about each user's detected risks, including date and time, IP address, and location.
6. For each user, choose one of the following actions:
 - **Reset password**
 - **Block sign-in**
 - **Confirm user compromised**
 - **Dismiss user risk**

How it works...

Microsoft Entra ID Protection analyzes user sign-in patterns to detect risky activities, such as sign-ins from unusual locations or devices, and flags these users for review. Administrators can then take appropriate actions to secure these accounts.

There's more...

Consider setting up automated notifications for detected risks and enabling user risk-based conditional access policies to enhance your security posture. These policies can automatically enforce actions such as requiring multifactor authentication for risky sign-ins.

See also

- *What is Identity Protection?*: <https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection>
- *View and manage risky users in Microsoft 365 Lighthouse*: <https://learn.microsoft.com/en-us/microsoft-365/lighthouse/m365-lighthouse-view-manage-risky-users>
- *Remediate risks and unblock users*: <https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-remediate-unblock>

Creating alerts for specific activities performed by users in OneDrive

Creating alerts for specific actions in OneDrive, such as external file sharing, helps prevent data loss and ensures compliance by notifying administrators of important activities. This recipe details the process of setting up alert policies in the Microsoft 365 Defender portal to monitor and respond to specific user activities.

Getting ready

You must be a Global Administrator to complete this recipe.

How to do it...

1. Go to the Microsoft 365 Defender portal at <https://security.microsoft.com>.
2. Select **Email & collaboration** | **Policies & rules** from the left navigation menu, then **Alert policy**, as shown in *Figure 14.2*.

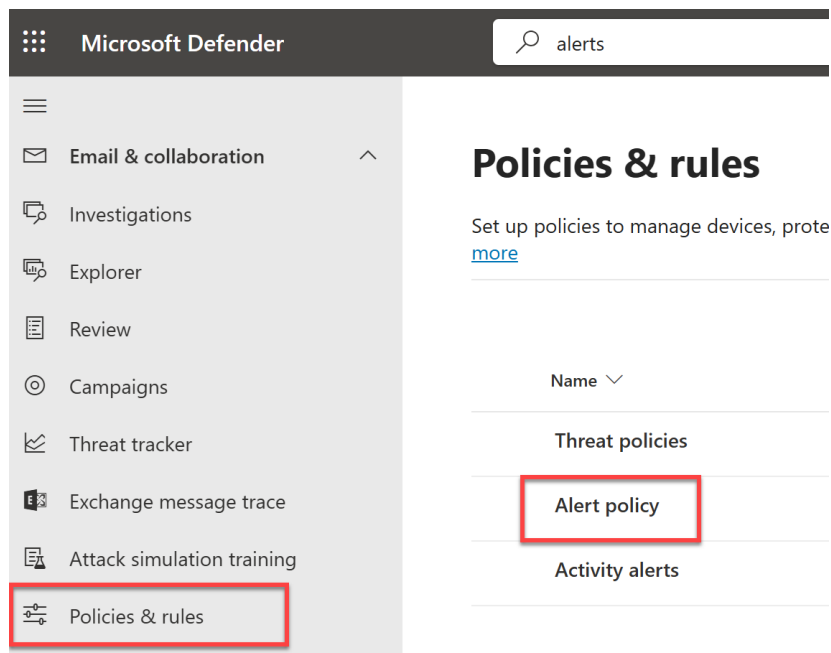


Figure 14.2 – Location of Alert policy in Microsoft Defender

3. Select **New Alert Policy**.

4. Fill in the **Name**, **Description**, **Severity**, and **Category** fields for the alert, as shown in the example in *Figure 14.3*.

Name your alert, categorize it, and choose a severity.

Assign a category and severity level to help you manage the policy and any alerts it triggers. You'll be able to filter on these settings from both the 'Alert policies' and 'View alerts' pages.

Name *

OneDrive External Sharing Activity

Description

An alert when a OneDrive user shares content outside the organization.

Severity * ⓘ

● Medium

Category *

Threat management

Figure 14.3 – A new alert policy configuration screen

5. Select **Next**, then set the **Activity is** dropdown to **Shared file externally** and include your OneDrive site collection URL followed by an asterisk (e.g., `https://<yourtenant>-my.sharepoint.com/*`), as shown in *Figure 14.4*.


What do you want to alert on?

^ **Activity is**

Shared file externally ×

User shared, granted access of a file or folder to an external user, or created an anonymous link for it.

AND

^ **File: Site collection URL is** 

Like any of ▾

https://contoso-my.sharepoint.com/*

Figure 14.4 – Activity and site scope settings of an alert policy

6. Scroll down, select **Every time an activity matches the rule** for frequency, and select **Next**.
7. Choose who should receive the alert and set the notification's daily limit (no limit up to 200 notifications per day).
8. Select **Next**, review your alert settings, and then select **Submit**.

How it works...

This setup creates a new alert policy in the Microsoft 365 Defender portal, notifying specified users when someone shares a OneDrive file externally. Such alerts help prevent data loss and maintain compliance by providing immediate awareness of potential data breaches or unauthorized sharing activities.

There's more...

You can customize alerts for various other activities, such as file deletions or permission changes, to further enhance security and compliance monitoring. Some common options are shown in *Figure 14.5*.

New Alert Policy

- ✓ Name your alert
- **Create alert settings**
- Set your recipients
- Review your settings

Common user activities

- Detected malware in an email message
- Phishing email detected at time of delivery
- User submitted email
- Detected malware in file
- Shared file or folder
- Created mail forward/redirect rule
- Any file or folder activity
- Changed file or folder
- Shared file externally

Select an activity

+ Add condition ▾

Figure 14.5 – Common user activity options for a new alert policy

These alerts can be fine-tuned to meet the specific needs of your organization, ensuring comprehensive oversight of potentially risky activities.

See also

- *Alert policies in Microsoft 365*: <https://learn.microsoft.com/en-us/purview/alert-policies>

Reviewing mail handling to see spam and malware history

Analyzing mail activity for spam and malware helps maintain email security and detect potential threats. This recipe will guide you through the steps to review email handling history, including spam and malware metrics, using the Microsoft 365 Defender portal.

Getting ready

You need to be a Global Administrator, Global Reader, or Reports Reader.

How to do it...

1. Go to the Microsoft 365 Defender portal at <https://security.microsoft.com>.
2. Select **Reports** from the left navigation menu, then select **Email & collaboration reports**, as shown in *Figure 14.6*.

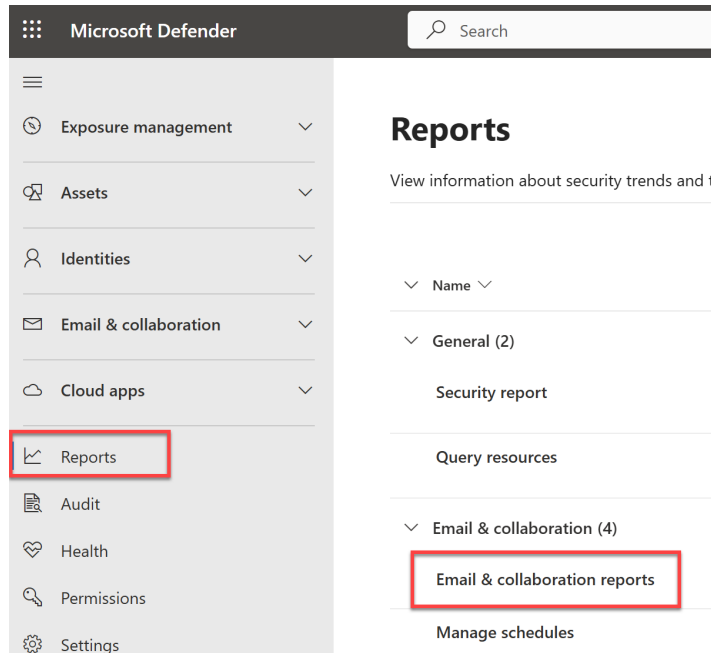


Figure 14.6 – Location of Threat management reports in Microsoft Defender

3. Select the **Threat protection status** report and review the **Email malware** metrics.
4. Similarly, review the **Email spam** metrics on the same report for detailed insights.

How it works...

These reports provide detailed information on detected malware and spam, helping administrators identify and address potential threats to email security.

There's more...

Consider setting up alert policies to be notified when malware or spam activities take place so you can respond more quickly. See the previous recipe for guidance on setting up an alert policy but choose **Detected malware in an email message** or **Malicious email detected** for **Activity** is.

See also

- View email security reports in the Microsoft Defender portal: <https://learn.microsoft.com/en-us/defender-office-365/reports-email-security>

Identifying your least active SharePoint sites

Identifying inactive SharePoint sites helps in maintaining an organized and efficient SharePoint environment. This recipe explains how to find and manage the least active SharePoint sites, allowing you to take actions such as archiving or deleting them to maintain a clean environment.

Getting ready

Ensure that you are a Global Administrator, SharePoint Administrator, Global Reader, or Reports Reader.

How to do it...

1. Access the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Select **Reports | Usage** from the left navigation menu.
3. Select **SharePoint**, then **Site usage**, as shown in Figure 14.7.

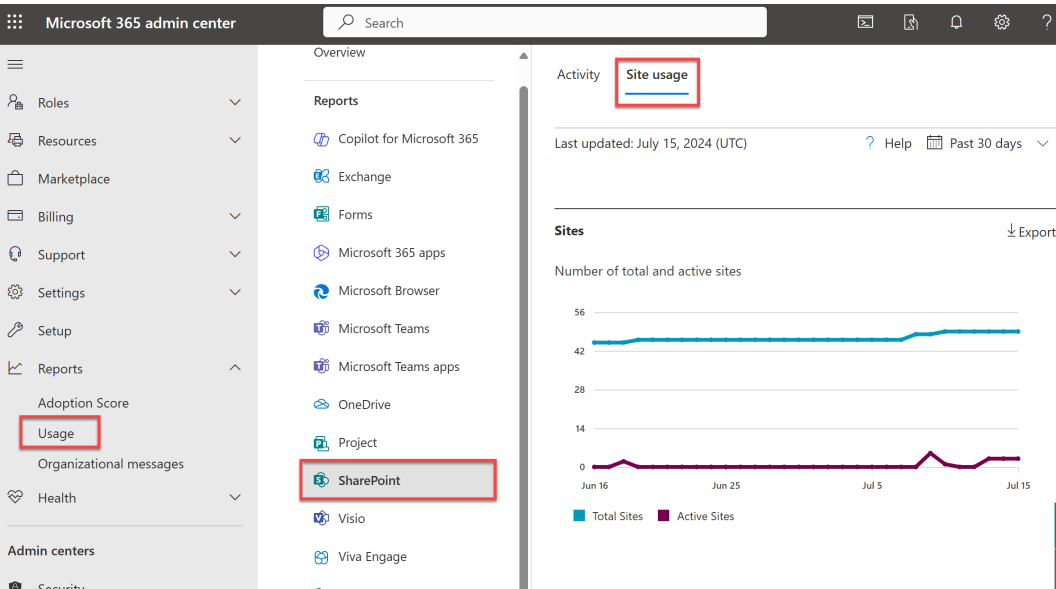


Figure 14.7 – Location of Site usage reports for SharePoint in the Microsoft 365 admin center

4. Scroll down, where you'll find a list of sites in detail, and sort the list by **Last activity date** in ascending order.
5. The sites listed at the top are the least active. Select **Export** to download the data for further analysis.

How it works...

This process helps identify the least used SharePoint sites, allowing you to take actions such as archiving or deleting them to maintain a clean environment.

There's more...

In addition to total versus active SharePoint sites, the site usage reports also show you storage usage, active versus total files in SharePoint, and total page views.

See also

- *Microsoft 365 Reports in the admin center - SharePoint site usage*: <https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/sharepoint-site-usage-ww>

Analyzing search activity throughout Microsoft 365

Monitoring search activity across Microsoft 365 applications helps organizations understand user behavior, improve content discoverability, and enhance the overall search experience. This recipe provides steps to access and analyze search usage reports, enabling administrators to identify trends, gaps in search adoption, and areas for improvement.

Getting ready

You need to be a Global Administrator, Search Administrator, or Search Editor to access and analyze search usage data.

How to do it...

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Select **All admin centers** from the left navigation menu, then select **Search & intelligence**, as shown in *Figure 14.8*.

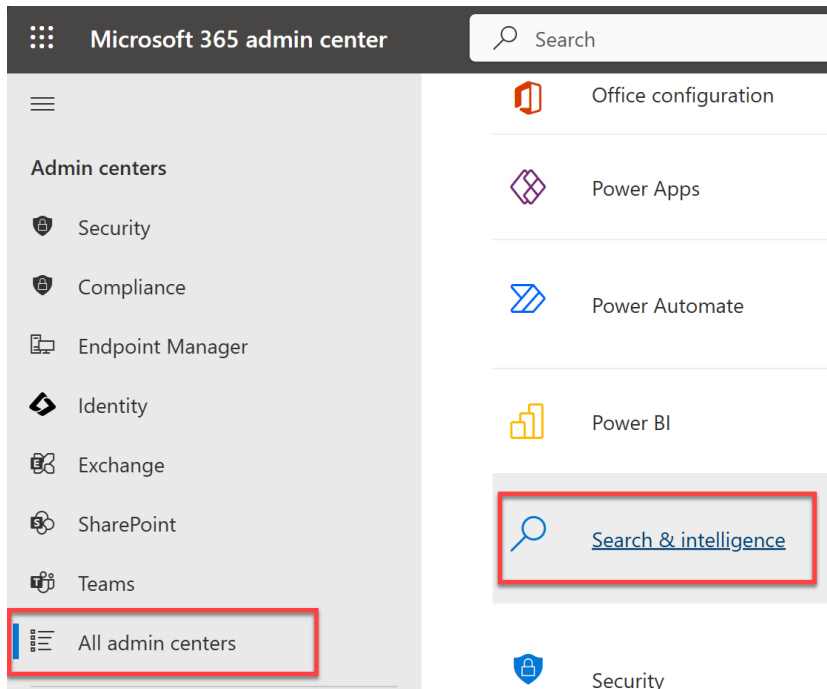


Figure 14.8 – Location of Search & intelligence in admin center

3. Select **Insights** from the ribbon menu.
4. Here, you can access various search usage reports:
 - **Summary:** Shows key metrics from each of the individual reports that follow.
 - **User analytics:** Shows user engagement across different search applications and displays usage based on job title and geography.
 - **Query analytics:** Provides key metrics and trends for search queries such as no-result queries, the most popular search terms, and abandoned queries. Part of **Most popular search terms** can be seen in the **Query analytics** screenshot shown in *Figure 14.9*.

Search & intelligence

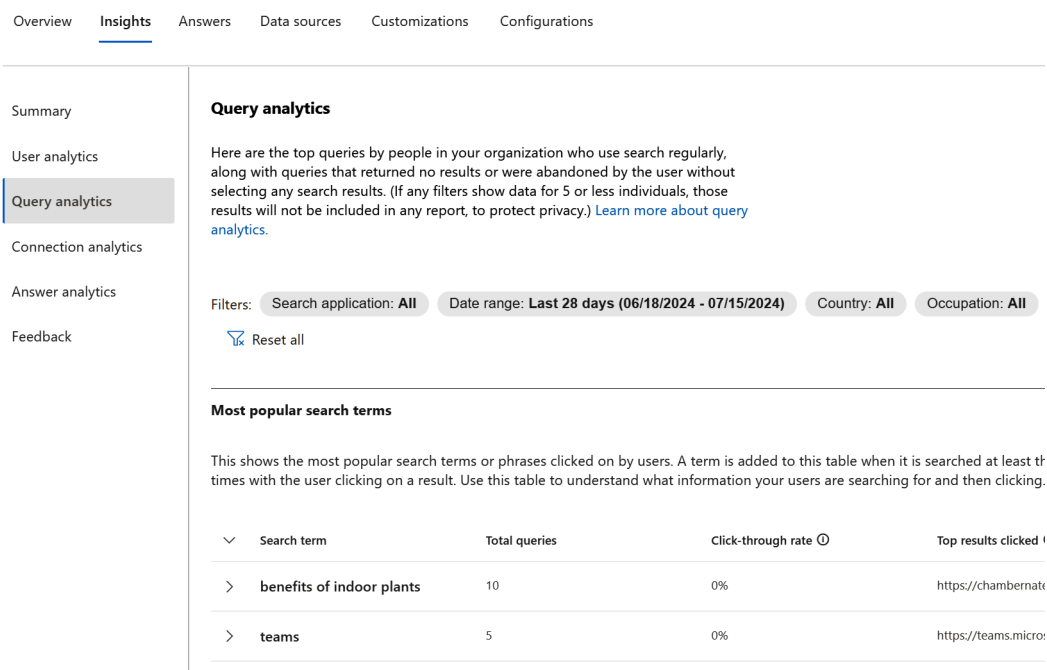


Figure 14.9 – Query analytics report

- **Connection analytics:** Analyzes search result interactions with any connected data sources, such as third-party systems or external websites.
 - **Answer analytics:** Tracks the performance of editorial content such as bookmarks, Q&A results, and acronyms.
5. Use filters at the top of each report page to refine your data by date range, search application, country, occupation, or department/division.

How it works...

The search usage reports provide detailed insights into how users interact with search across various Microsoft 365 applications:

- **User analytics** tracks search engagement and adoption across applications such as SharePoint, Teams, and Outlook
- **Query analytics** highlights the most popular search terms, queries that returned no results, and abandoned searches

- **Connection analytics** evaluates user interactions with search results
- **Answer analytics** measures the effectiveness of editorial content such as bookmarks and Q&As

By analyzing these reports, administrators can identify patterns, address gaps in search adoption, and enhance the search experience for users.

There's more...

Regularly reviewing these reports helps organizations stay informed about search trends and user behavior. Additionally, administrators can use insights from these reports to conduct targeted training sessions, optimize content for searches, and improve overall user satisfaction.

Also, on the **Summary** page of **Insights**, you can select **Download Report**, as shown in *Figure 14.10*, for any of the key metrics shown, such as **Query analytics**, **Query distribution**, or **Connection analytics**. This provides an Excel spreadsheet of the report's data you can use or share for further analysis.

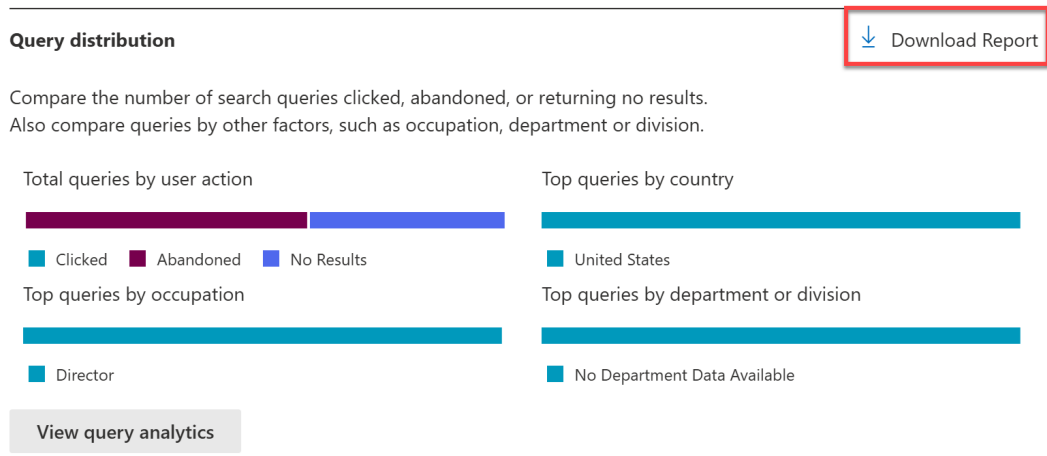


Figure 14.10 – Download Report option for key metrics on the Summary page of Insights

You'll find the same **Download Report** option available for specific reports on other pages in **Insights** as well.

See also

- *Microsoft Search Usage Reports*: <https://learn.microsoft.com/en-us/microsoftsearch/usage-reports>

Checking service health status and known issues

Monitoring service health helps you stay informed about current issues and advisories affecting your Microsoft 365 services. This recipe outlines how to check the service health status and known issues using the Microsoft 365 admin center, enabling proactive management of service disruptions.

Getting ready

You need to be a Global Administrator, Service Administrator, or Global Reader.

How to do it...

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Select **Health** | **Service health** from the left navigation menu, as shown in *Figure 14.11*.

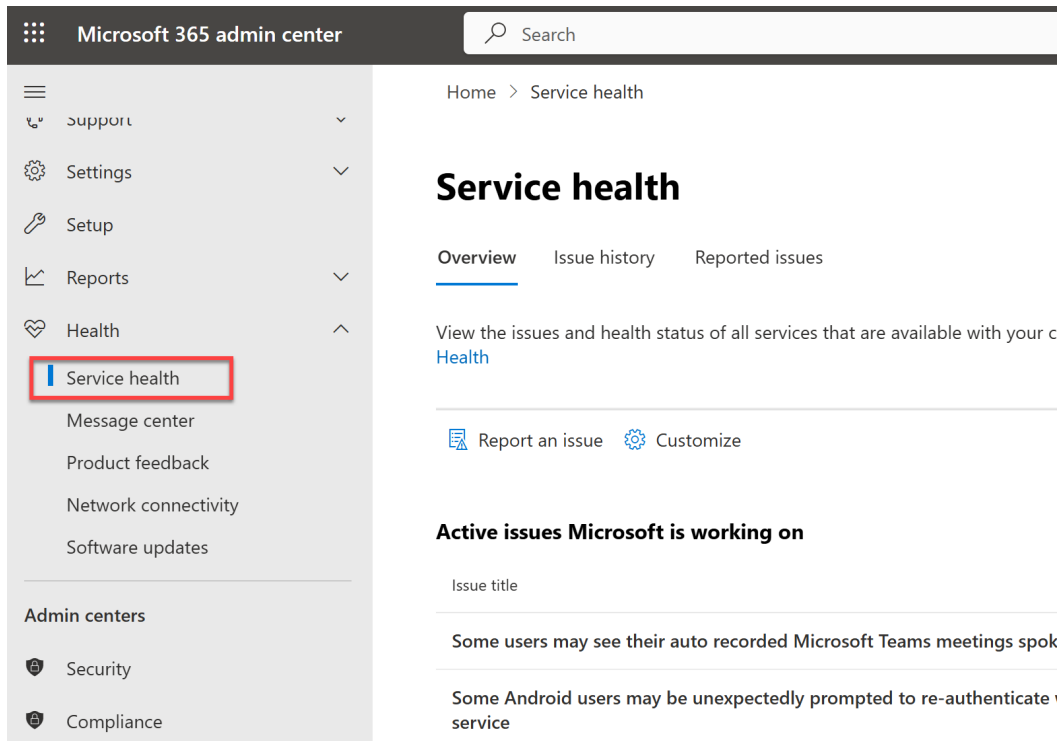


Figure 14.11 – Service health in the Microsoft 365 admin center

3. Review the list of services and any known issues or advisories. You can select any of the issues listed to review more details and find any updates if available. A service degradation issue example is shown in *Figure 14.12*.

Some users may be unable to accept calendar sharing invites in Outlook on the web

 Manage notifications for this issue  Copy text

User impact

Users may be unable to accept calendar sharing invites in Outlook on the web.

More info

This issue occurs when invites are shared to external users; those who are inviting users internal to their organization aren't impacted by this event. Impact is further limited to users that are on Windows 11 or the 64-bit version of Windows 10. Those who are on the 32-bit version of Windows are unaffected.


Scope of impact

Users who are attempting to accept calendar sharing invites that are external from their organization and are on either Windows 11 or the 64-bit version of Window 10 may be impacted.

Root cause

A code issue within a section of Outlook on the web service infrastructure is causing the inability to accept calendar invites in Outlook on the web.

Issue ID
EX803094

Affected services
 Exchange Online

Status
Service degradation

Start time
Jun 19, 2024, 4:00 AM CDT

Issue type
Advisory

Give feedback
[Are you experiencing this issue?](#)
[Is this post helpful?](#)

Updates

Figure 14.12 – Service health issue example

4. On the **Service health** screen, select **Report an issue** if you encounter problems not listed.

How it works...

The **Service health** page provides real-time information on the status of Microsoft 365 services, helping you address issues proactively.

There's more...

You can subscribe to notifications to receive alerts about changes in service health, ensuring you stay informed about potential disruptions. To do so, select **Customize | Email | Send me email notifications about service health**, as shown in *Figure 14.13*.

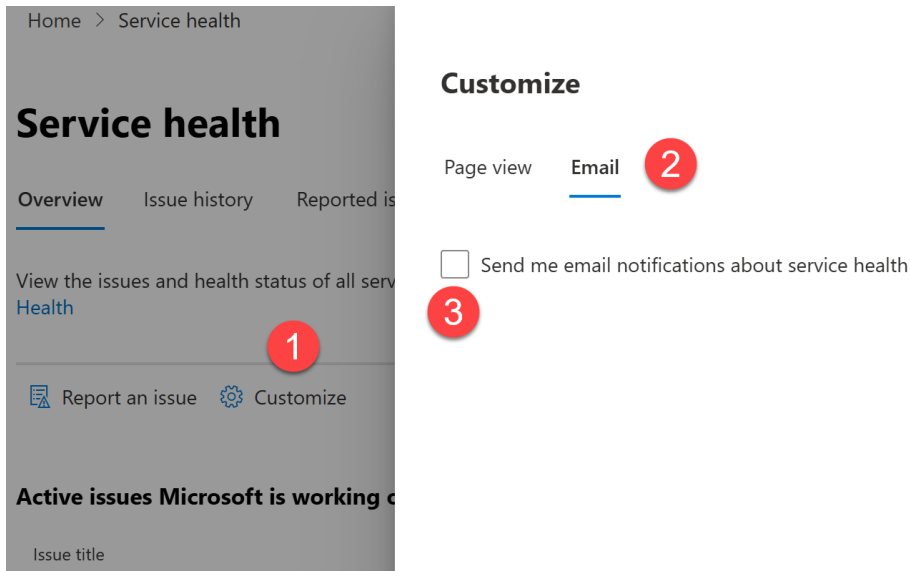


Figure 14.13 – Steps to subscribe to Service health email updates

See also

- *How to check Microsoft 365 service health:* <https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health>

Checking general usage data for Microsoft 365 apps and services

Monitoring usage data helps understand the adoption and utilization of Microsoft 365 apps and services within your organization. This recipe provides steps to access and review general usage data, helping you make informed decisions about training, support, and resource allocation.

Getting ready

You need to be a Global Administrator or Global Reader.

How to do it...

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Select **Reports | Usage** from the left navigation menu.
3. Review the usage data for various Microsoft 365 apps and services including:
 - Copilot for Microsoft 365
 - Exchange
 - Forms
 - Microsoft 365 apps
 - Microsoft Browser
 - Microsoft Teams
 - Microsoft Teams apps
 - OneDrive
 - Project
 - SharePoint

Home > Usage > Exchange

[Enable Dark mode](#)

Usage

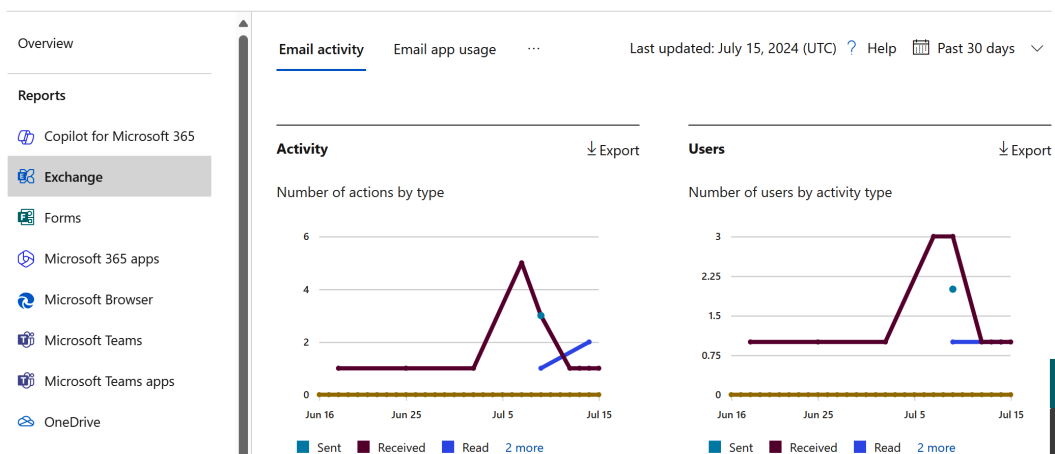


Figure 14.14 – Usage reports in Microsoft 365 admin center

- 4. Use the calendar filter at the top of each app's reports to adjust the time span as needed. You can select the previous 7, 30, 90, or 180 days.

How it works...

The usage reports provide insights into how different services are being used, helping you make informed decisions about training and resource allocation.

There's more...

Regularly reviewing these reports can help identify areas where additional support or training might be needed to improve service adoption. You can also export any report's data by selecting **Export** in the upper-right corner of a visual to further analyze or share the visual's data in CSV format. This option is shown in *Figure 14.15*.

Usage

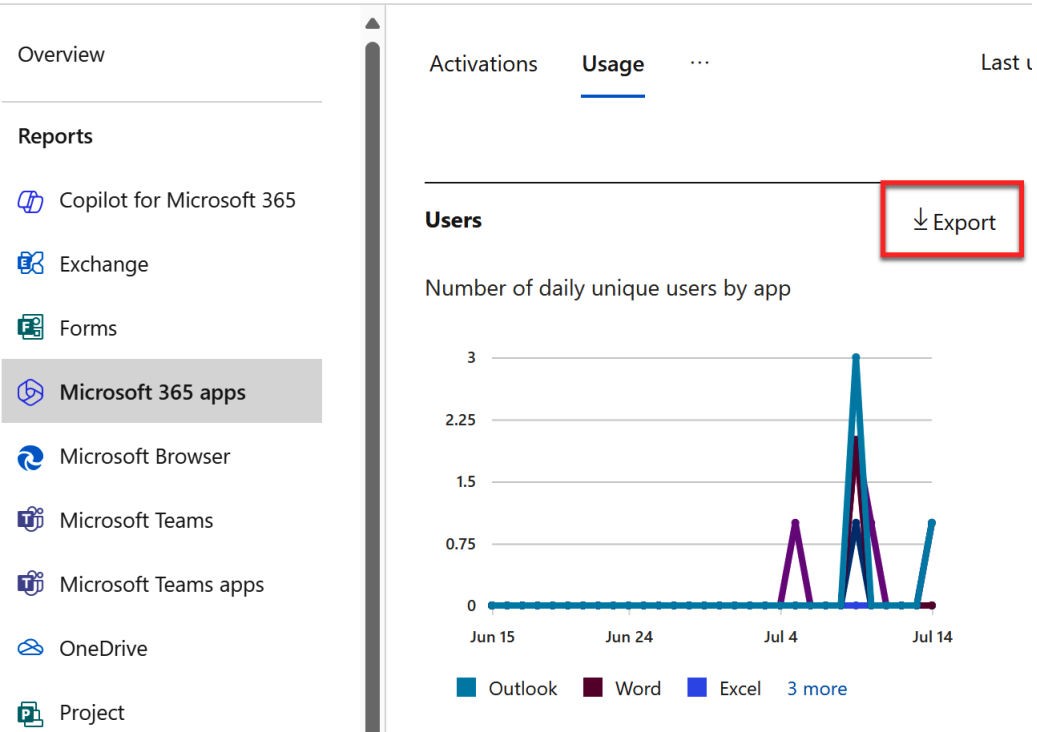


Figure 14.15 – Option to export usage data

Consider using Power BI to visualize exported data in visuals you can customize further than what's given to you out of the box via the admin center.

See also

- *Microsoft 365 Reports in the admin center*: <https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports>

Checking Teams usage and user activity

Tracking Teams usage and user activity helps gauge adoption and identify opportunities for improvement. The previous recipe, *Checking general usage data for Microsoft 365 apps and services*, includes some Microsoft Teams usage data, including the following:

- **User activity**
- **Teams usage**
- **Device usage**
- **App usage**
- **User activity** (app-specific)

The reports we'll explore in this recipe, however, give you more insight, at a deeper level, into user activity in Teams.

Getting ready

You must be a Global Administrator or Teams Administrator to complete the steps in this recipe.

How to do it...

1. Go to the Teams admin center at <https://admin.teams.microsoft.com>.
2. Select **Analytics & reports | Usage reports** from the left navigation menu.
3. Choose **Teams usage** or **Teams user activity** from the dropdown and select a time span (7, 30, 90, or 180 days).

4. Select **Run report** to view the data. *Figure 14.16* shows part of the 30-day Teams usage report for a fictional tenant.

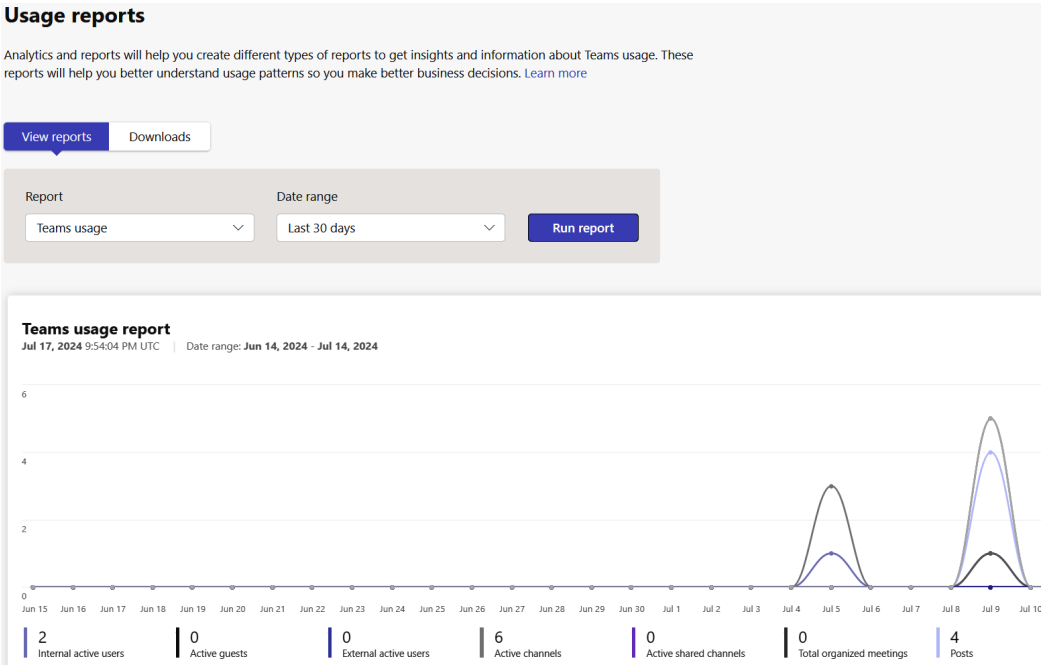


Figure 14.16 – Teams usage report example

How it works...

These reports provide detailed insights into Teams usage, helping you identify active (or inactive) teams, channels, meetings, and user activities such as chats and posts.

There's more...

Figure 14.17 illustrates how there are many more than just this recipe's two suggested reports to choose from. These include reports specific to meeting types, connectivity, Teams app usage, user activity, phone activity, premium feature usage, and more. These Microsoft Teams admin center report options give you much more insight into Teams adoption and usage than the Microsoft 365 admin center currently offers.

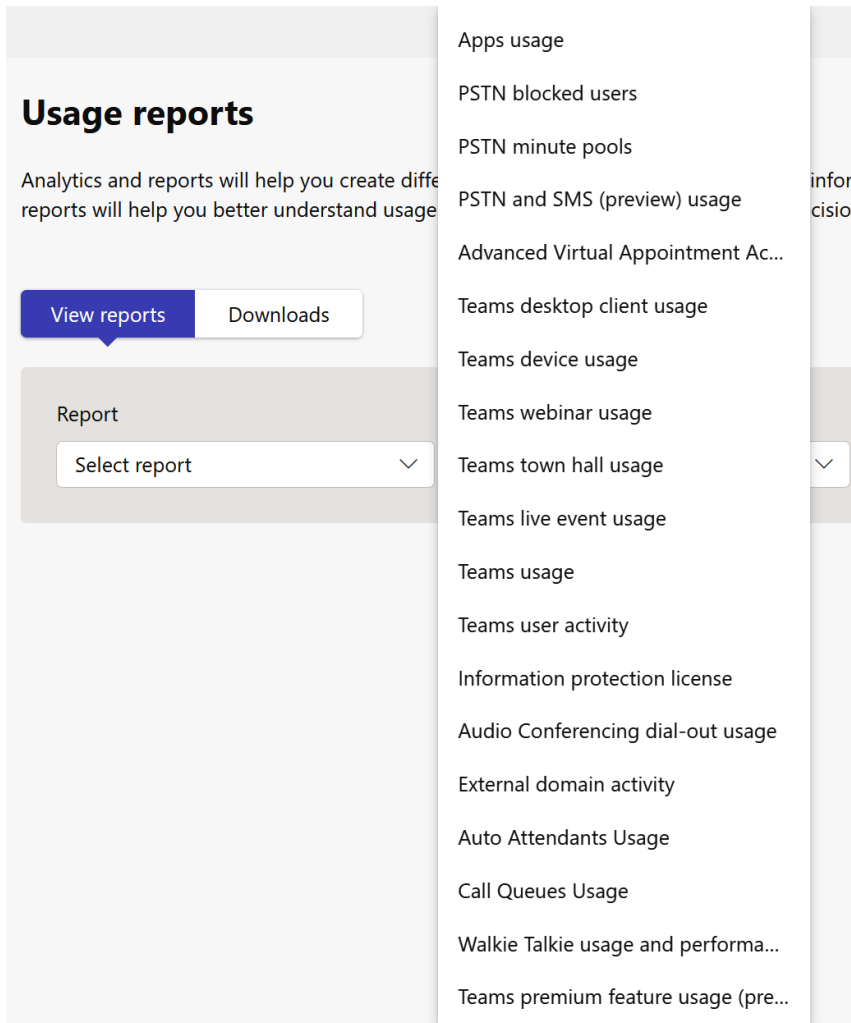


Figure 14.17 – Report options in the Microsoft Teams admin center

Exporting this data to Excel allows for deeper analysis and sharing with stakeholders. Each report visualization has an Excel icon at the upper right, which will export the visual's data for further analysis and sharing.

See also

- *Microsoft Teams analytics and reporting*: <https://learn.microsoft.com/en-us/microsoftteams/teams-analytics-and-reports/teams-reporting-reference>

Monitoring Power Apps and Power Automate usage and activity

Monitoring the usage of Power Apps and Power Automate is essential for understanding adoption, ensuring efficient use of licenses, and maintaining a healthy and secure environment. This recipe guides administrators in finding metrics that aid in tracking usage, identifying performance issues, and optimizing the utilization of these tools using the Power Platform admin center.

Getting ready

You need to be a Global, Power Platform, Dynamics 365, or Environment Administrator. A Power Platform or Global Administrator also must have enabled tenant-level analytics prior to following the steps in this recipe. To do so, follow *steps 1-2* in this recipe, then select **Enable** and wait 24-48 hours for tenant analytics to become available.

How to do it...

1. Access the Power Platform admin center at <https://admin.powerplatform.microsoft.com/>.
2. Choose **Power Apps** or **Power Automate** to view license consumption and usage and activity details such as the following:
 - Successful versus failed flows
 - Count of flows and users
 - Counts of canvas and model-driven apps
 - Top apps by users/sessions
 - Top flow and app makers
 - Connector dependencies

Figure 14.18 shows visualizations available if you select **Power Automate | Environment View**. By default, you'll see daily, weekly, and monthly flow run activity here.



Figure 14.18 – Weekly and monthly flow run activity in the Power Platform admin center

3. On the **Environment View** tab, you can select **Usage** to see which flows specifically are being utilized in your environment.
4. In the Power Platform admin center, select **Analytics | Dataverse** to view environment-specific metrics. To change environments, select **Change filters**, then choose your environment, as shown in *Figure 14.19*.

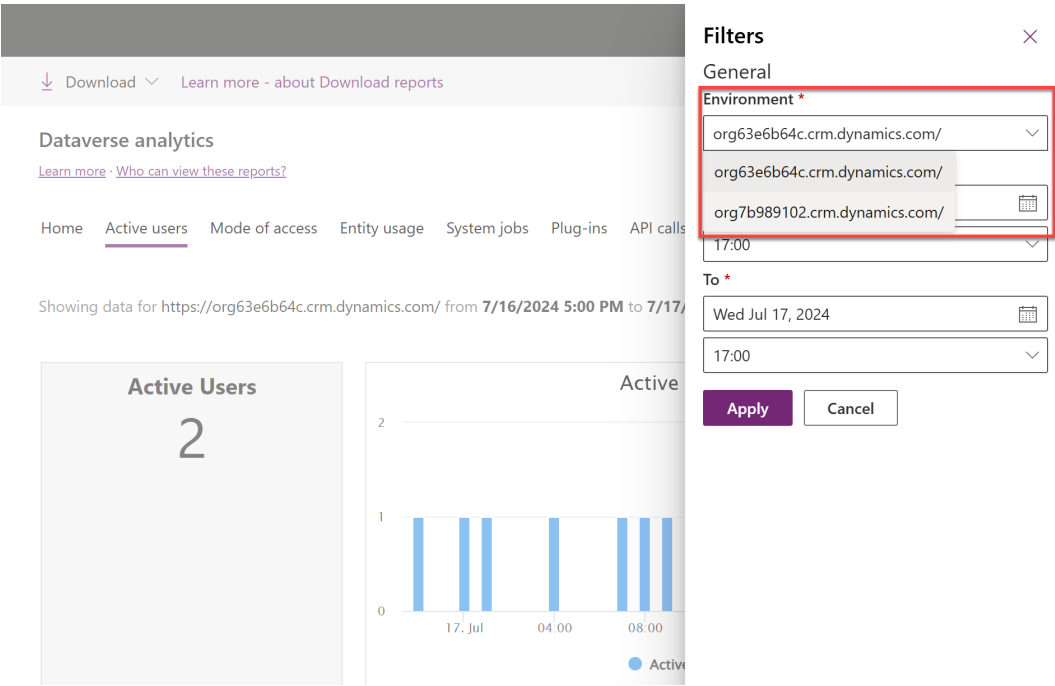


Figure 14.19 – How to change environments when viewing Dataverse analytics

5. Review the various tabs available to review **Active users**, **Mode of access** (devices and operating systems), and so on.

How it works...

By leveraging the Power Platform admin center, administrators can gain comprehensive insights into how Power Apps and Power Automate are being used within the organization. This involves tracking consumption and creation, monitoring solution health and performance, and analyzing usage patterns. These insights help in optimizing resources, ensuring compliance, and improving the overall efficiency of automation processes.

There's more...

Regularly reviewing these metrics helps in identifying training needs and adoption gaps. Additionally, using the **Center of Excellence (CoE) Starter Kit** can provide a more structured approach to governance and management. The CoE Starter Kit comes with templates and dashboards that offer tenant-wide insights and help in establishing best practices for using Power Platform tools. Learn more at <https://learn.microsoft.com/en-us/power-platform/guidance/coe/starter-kit>.

See also

- *Management and monitoring*: <https://learn.microsoft.com/en-us/power-platform/admin/wp-management-monitoring>
- *Tenant-level analytics for Power Automate*: <https://learn.microsoft.com/en-us/power-platform/admin/power-automate-analytics-reports>
- *Tenant-level analytics for Power Apps*: <https://learn.microsoft.com/en-us/power-platform/admin/powerapps-analytics-reports>
- *Microsoft Power Platform Center of Excellence (CoE) Starter Kit*: <https://learn.microsoft.com/en-us/power-platform/guidance/coe/starter-kit>

Appendix

Microsoft 365 Subscriptions and Licenses

Navigating Microsoft 365 subscriptions and licenses can be complex due to frequent updates and varying offerings. This appendix provides a high-level overview to help you manage your Microsoft 365 subscriptions and licenses effectively.

Purchase a subscription

You can purchase a Microsoft 365 subscription directly through the Microsoft 365 website at <https://www.microsoft.com/microsoft-365>. The site offers various plans tailored for personal, family, business, and enterprise use. Each plan provides different features and services to meet diverse needs.

Compare Microsoft 365 subscriptions

Microsoft 365 offers a range of subscription plans with varying features:

- **Microsoft 365 Personal and Family:** Designed for individual or family use, offering premium Office apps, 1 TB of OneDrive storage per user, and advanced security.
- **Microsoft 365 Business:** Includes plans like Business Basic, Business Standard, and Business Premium, catering to small and medium-sized businesses with features such as email hosting, file storage, and advanced security and device management. Each Microsoft 365 Business plan has a maximum limit of 300 licenses per tenant. This means that a single organization can assign up to 300 licenses for each of these plans. If additional licenses are needed beyond this limit, an organization must either switch to an Enterprise plan or manage the additional users with a combination of different Business plans.
- **Microsoft 365 Enterprise:** Enterprise-level plans (E1, E3, E5) provide advanced security, compliance, and productivity tools suitable for large organizations. Note that Microsoft Teams is now licensed separately from the core Enterprise subscriptions, so be sure to check the latest licensing options.

See *Find the right Microsoft 365 enterprise plan for your organization* at <https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft365-plans-and-pricing> for more information.

Compare additional services

In addition to core Microsoft 365 plans, several additional services are available:

- **Microsoft 365 Apps for Business/Enterprise:** Provides the latest Office applications without additional services like email or OneDrive.
- **Microsoft 365 F3:** Tailored for frontline workers, offering essential tools and services for communication and collaboration. Frontline workers typically include employees who are directly involved with the public or operations, such as retail staff, factory workers, and healthcare professionals.
- **Microsoft 365 Education:** Designed for educational institutions, offering tools for classroom collaboration and learning management.

See *Find the best Microsoft 365 plan for your business* at <https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products>.

Purchase licenses

Licenses for Microsoft 365 can be purchased through the Microsoft 365 admin center at <https://admin.microsoft.com> or via a Microsoft partner. Each user within your organization needs a valid license to access Microsoft 365 services. Administrators can assign, reassign, or remove licenses as needed.

See *Buy or remove licenses for a Microsoft business subscription* at <https://learn.microsoft.com/en-us/microsoft-365/commerce/licenses/buy-licenses> for more information.

Upgrade a license

Upgrading a license is straightforward through the Microsoft 365 admin center. Administrators can select users and upgrade their licenses to higher-tier plans that offer more features and capabilities. For example, upgrading from Microsoft 365 Business Standard to Business Premium adds advanced security and device management features.

See *Upgrade or change to a different Microsoft 365 for business plan* at <https://learn.microsoft.com/en-us/microsoft-365/commerce/subscriptions/upgrade-to-different-plan> for more information.

Renew a license

Microsoft 365 subscriptions typically auto-renew to ensure uninterrupted service. Administrators can manage renewal settings through the admin center, including opting out of auto-renewal or making changes to the subscription plan.

See *Manage recurring billing in the Microsoft 365 admin center* at <https://learn.microsoft.com/en-us/microsoft-365/commerce/subscriptions/renew-your-subscription> for more information.

Useful resources

Given the dynamic nature of Microsoft 365 offerings, staying current with the latest information is essential. Here are some valuable resources:

- Microsoft 365 Licensing Resources at <https://www.microsoft.com/en-us/licensing>: Comprehensive guides and updates on licensing models and programs.
- Microsoft 365 and Office 365 Service Descriptions at <https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-service-descriptions-technet-library>: Detailed descriptions of the services included in each plan.
- Microsoft 365 Admin Center at <https://admin.microsoft.com>: A hub for managing subscriptions, licenses, and administrative tasks. Be sure to specifically check out the **Billing** and **Settings** options from the left navigation menu.

For the most accurate and up-to-date information, always refer to the official Microsoft 365 documentation. Get started at <https://learn.microsoft.com/en-us/microsoft-365/>.

Index

A

Access review report

- creating, in Entra ID 351-357
- reviewing and completing, in
Entra ID 358-360

acronym

- creating, in Microsoft Search 146-149

Active Directory (AD) 4

Add-MgGroupMember command 84

admin center home page

- personalizing 34-37

admin center navigation

- customizing 32-34

admin centers

- accessing 2-5
- reference link 5

administrative units

- reference link 79

admin roles

- managing, in Microsoft 365
admin center 76-78
- reference link 76, 79

admin roles in Microsoft 365 admin center

- reference link 5

admin roles, Viva Engage

- Answers Administrator 312
- Community Administrator 312
- Corporate Communicator 312
- Engage Administrator 312
- Global Administrator 311
- Network Administrator 312
- Verified Administrator 312

Advanced Threat Protection (ATP) 195

alerts, for specific actions in OneDrive

- creating 446-448
- customizing 448

All Company community

- posts, restricting 327, 328

Analytics

- using, in Microsoft Power Platform 225-227

Answers Administrator role 312

ATP features

- enabling 140-144

at-risk users

- finding 444, 445

Automated Investigation and Response (AIR) 394

B

bookmark

- creating, in Microsoft Search 149-152
- importing, in bulk from CSV 155, 156
- reference link 154, 157

branding

- adding, to Entra ID sign-in page 337-339

bulk upload

- errors, when importing users 46-48

business associate agreement (BAA) 399

business associate agreement, HIPAA

- accessing 399, 400

C

Center of Excellence (CoE) 466

channels 279

cmdlets 348, 349

Communication Compliance

- used, for identifying potential policy violations 438-440

Community Administrator role 312

Compliance Manager 437, 438

compliance safeguards

- audit and activity logs 194
- Data Loss Prevention (DLP) 194
- data retention policies 195
- information barriers 194
- sensitivity labels 194
- setting up 193-195

Connect-MgGraph command 84

connectors, in Power Apps and Power Automate

- restricting, from accessing business data 221-224

Connect-SPOService cmdlet 95

Corporate Communicator role 312, 316

- assigning, to user 316, 317

cover image

- configuring, for Power BI 241, 242

cross-tenant migration 268

CSV file

- bookmark, importing in bulk from 155, 156

current gateway installer

- removing 236

custom domain

- setting up 25

custom sensitive information type

- creating, based on keywords 411-417

D

Dashboard view to Health

- switching, option 37

data, from network locations

- importing, with Migration Manager or SPMT 265-268

Data Loss Prevention

- (DLP) 221, 223, 255, 395

data migration

- performing, with SPMT 207-211

Dataverse

- creating 220, 221

Dataverse analytics 227

default logo

- configuring, for Power BI 241, 242

default share link type

- setting 199-202, 258-261

default storage allocation and retention periods, OneDrive for Business

- adjusting 203-206

deleted OneDrive site

- restoring 100, 101

development environments 217

Digital Operational Resilience**Act (DORA) 401****direct sign-on links**

obtaining, for organizational apps 344-346

distribution list

creating 114, 119, 120

DLP policy

creating, for content protection 401-405

creating, for content with custom
keywords 417-421

sensitivity, tuning 422-424

using, to automatically report HIPAA
incident reports 406-411**domain**

adding 23, 24

modifying, for users 26, 27

Domain Name System (DNS) 24**dynamic distribution groups 120****dynamic distribution list**

creating 121-123

message approval, enabling 124

dynamic Viva Engage community

creating 324-326

E**eDiscovery case**

creating 430-434

using 430-434

eDiscovery Manager role 437**electronically stored information (ESI) 430****Engage Administrator role 312****Entra ID**

Access review report, creating in 351-357

Access review report, reviewing
and completing 358-360**Entra ID, sign-in page**

branding elements, adding 337-339

privacy statement, adding to 340, 341

European Union (EU) 400**Events policy**

creating, in Microsoft Teams 288, 289

Exchange admin center 105**Exchange Online 105**

new user, creating with mailbox 106-108

shared mailbox, creating 115-117

Exchange-specific retention policy

creating 124-127

external access

configuring, in Microsoft Teams 300-302

external senders

preventing, from emailing internal

Microsoft 365 groups 103, 104

external sharing abilities

limiting 250-255

external sharing, OneDrive for Business

enabling 174-179

permission levels, configuring 179-182

restricting, to specific domains 183, 184

external sharing settings

setting, for site 255-257

external users 305**F****FedRAMP 400****G****General Data Protection Regulation
(GDPR) 341, 400****general usage data**reviewing, for Microsoft 365 apps
and services 458-461

Get-Command cmdlet 83
Get-Help cmdlet 84
Get-MgGroup command 84
Get-MgUser command 84
Get-MgUser cmdlet 91
Gigabytes (GBs) 263
Global Address List (GAL)
 Microsoft 365 groups, hiding from 102
Global Administrator role 311
Government Community Cloud (GCC) 9
graphical user interface (GUI) 81
group 279
 license, assigning to 30, 31
group creation, in Microsoft
 365 admin center
 reference link 53
guest access
 configuring, in Microsoft Teams 304, 305
guest users 305
 adding 64
 managing 60-63
 reference link 64

H

Health Insurance Portability and Accountability Act (HIPAA) 399
 business associate agreement,
 accessing 399, 400
health status and known issues
 checking 456, 457
HIPAA incident reports
 reporting, automatically with DLP 406-411
hubs 270
hub site
 benefits 272, 273
 navigation, editing 273, 274

 other sites, associating with 270-273
 site, designating as 270-273

I

inactive SharePoint sites
 identifying 451, 452
indicators of attack (IOAs) 389
indicators of compromise (IOCs) 389
Information Rights Management (IRM) 195
Integrated Scripting Environment (ISE) 82
IP address
 access, restricting by 274, 275
issues with group-based license
 management, in Microsoft Entra ID
 reference link 32

L

license
 assigning, to group 30, 31
 assigning, to users 28, 29
license assignment issues,
 addressing and resolving
 reference link 32
local sync of files, OneDrive for Business
 enabling 185-189
 restricting, to PCs on specific
 domains 190-192
location
 adding 157-159

M

mail activity, for spam and malware
 analyzing 449, 450
mailboxes
 creating, with PowerShell 109

mail-enabled security group 110, 114

creating 110-113

mail flow rule

creating 128-132

mail tips 121**Meeting policy**

creating, in Microsoft Teams 285-287

meeting settings

configuring, in Microsoft Teams 283-285

Message center

Planner syncing option 15, 16

Planner syncing option 15

reference link 17

Message center reader role 11**Messaging policy**

creating, in Microsoft Teams 290-292

Microsoft 365

apps, monitoring 443

group, creating 48-51

services, monitoring 443

useful resources 471

Microsoft 365 admin center

admin roles, managing 76-78

settings 52, 53

Microsoft 365 Admin mobile app

download link 14

Microsoft 365 email address, modification to use custom domain

reference link 27

Microsoft 365 groups 114

hiding, from Global Address List 102

Microsoft 365 groups creation

reference link 73

users, restricting from 69-72

Microsoft 365 Groups, for administrators

reference link 53

Microsoft 365 Message center

upcoming changes, discovering via 11-14

Microsoft 365 plan for business

reference link 30

Microsoft 365 Reports in admin center

reference link 59

Microsoft 365 roadmap

filtering 8-10

viewing 8-10

Microsoft 365 roadmap, usage

reference link 11

Microsoft 365 subscriptions

additional services, comparing 470

purchasing 469

subscription plans, comparing 469

Microsoft Defender 365

Automated Investigation and Response (AIR) 394

permissions to non-IT users, assigning 384-386

RBAC, using 386-388

reports, monitoring 388-392

report, viewing on users with specific SharePoint file access 396-399

Safe Attachments policy, setting up 373-375

Safe Links policy, setting up 369-372

threat investigation and response capabilities, utilizing 393

threat protection policy, creating 366, 367

Microsoft Entra built-in roles

reference link 76

Microsoft Entra ID 31, 302, 331

creating 332-336

external collaboration settings 302, 303

populating 332-336

Microsoft Entra ID Protection 445**Microsoft Graph PowerShell**

reference link 8

Microsoft Graph PowerShell module

list of available commands, obtaining 82, 83

Microsoft Graph PowerShell SDK

user, creating in Microsoft 365 tenant 85, 86
user, disabling in Microsoft 365 tenant 87

Microsoft Graph PowerShell Software Development Kit (SDK) 6**Microsoft Graph SDK**

connecting, via PowerShell 346-349
installing, via PowerShell 346-349

Microsoft Places

reference link 146

Microsoft Power Platform 213

Analytics, using 225-227
existing environment 218, 219
new environment, creating 214-218

Microsoft Purview

Communication Compliance 438
Compliance Manager 437, 438
DLP policy, creating 401-405
permissions, assigning for
non-IT users 435-437

Microsoft Purview portal 395**Microsoft Search in Bing**

reference link 166
usage, setting up 164-166

Microsoft Search, setup

reference link 169

Microsoft Search Usage Reports

reference link 172

Microsoft Secure Score 144**Microsoft Teams**

Events policy, creating 288, 289
external access, configuring 300-302
guest access, configuring 304, 305
Meeting policy, creating 285-287
meeting settings, configuring 283-285
Messaging policy, creating 290-292
multiple policies, assigning to larger
batch of users 294-297

owners, reviewing 306, 307
policy, applying to specific users 293, 294
setup policies, configuring 298, 299
team, creating 278-280
Team policy, creating 281, 282
teams, reviewing 306, 307
Viva Engage, pinning 313-315

Migration Manager

used, for data import from network
locations 265-268

mover 268**multi-factor authentication
(MFA) 7, 39, 94, 362**

options 55, 56

multiple users

adding 43, 44

multiple users, addition at same time

reference link 48

N

Network Administrator role 312

user, assigning via Viva Engage
admin center 310, 311

New-MgGroup command 84**New-MgUser cmdlet 86****New-MgUser command 84**

O

OneDrive

alerts, creating for specific actions 446-448

OneDrive for Business

default share link type, configuring 199-202
default storage allocation and retention
periods, adjusting 203-206
external sharing, enabling 174-179

- individuals access, providing to
 - another user's content 196-199
 - local sync of files, enabling 185-189
- on-premises data gateway**
 - in admin center 232, 233
 - installing 228-231
- optical character recognition (OCR) 434**
- organizational apps**
 - direct sign-on links, obtaining for 344-346

P

- permissions**
 - assigning, for non-IT users to
 - Microsoft Purview 435-437
- permissions, Microsoft Defender**
 - assigning, to non-IT users 384-386
- posts**
 - restricting, in All Company
 - community 327, 328
- potential policy violations**
 - identifying, with Communication
 - Compliance in messages 438-440
- Power Apps analytics 227**
- Power Apps and Power Automate**
 - usage and activity**
 - monitoring 464-466
- Power Automate analytics 227**
- Power BI**
 - cover image, configuring 241, 242
 - default logo, configuring 241, 242
 - embed codes created by organization,
 - auditing 238-240
 - Publish to web (anonymous share)
 - ability, restricting to specific
 - security members 236-238
 - theme, configuring 241, 242

Power Platform admin center

- Data policies screen 224, 225

PowerShell 81

- mailboxes, creating 109
- Microsoft Graph SDK, installing
 - and connecting via 346-348
- permissions, managing efficiently 97
- setting up 5-8
- site configurations, automating 97
- used, for connecting to SharePoint
 - Online 94, 95

PowerShell, in Microsoft Graph

- users, adding and removing via 349-351

privacy statement

- adding, to Entra ID sign-in page 340, 341

Private groups 50

production environments 217

protected health information (PHI) 399

Public groups 50

Publish to web option

- restricting, to specific security
 - group members 236-238
- settings, refining 238

purchase licenses

- renewing 471
- upgrading 470

Q

Q&A result

- adding, in Microsoft Search 161-163
- reference link 164

R

Really Simple Syndication (RSS) 10

Remove-MgGroup command 84

Remove-MgGroupMember command 84

Remove-MgUser command 84, 88

report

- viewing, on users with specific
SharePoint file access 396-399

reports, Microsoft Defender

- monitoring 388-392

retention labels 429

retention policies 128

retention policy 425

- combining, with retention labels 429, 430
- creating, to retain content for
seven years 425-428

Role-Based Access Control

(RBAC) 110, 386, 435

- using, in Microsoft Defender 386-388

room and equipment mailboxes

- creating 136-139

S

Safe Attachments policy, Microsoft Defender

- setting up 373, 374
- working 375

Safe Links policy, Microsoft Defender

- setting up 369-371
- working 372

search activity

- analyzing, across Microsoft 365
applications 452-455

Search Administrator role

- assigning 167, 168

Search Editor role

- assigning 167, 168

Search Insights dashboard reports

- using 169-172

Secure Score

- accessing 375-378
- reviewing 375-378
- security configuration
recommendations 380-382
- tags, managing 383

security defaults 53

security defaults, in Microsoft Entra ID

- enabling 53-55
- reference link 56

security groups 114

self-service password reset (SSPR)

- enabling 360-362

sensitivity labels 422

service-level agreements (SLAs) 17

- Standard Support 17
- Unified Support 17

Service Principals (S2S) 224

service request

- creating 17-20

service request status

- existing request editing 21, 22
- monitoring 20, 21

Session Initiation Protocol (SIP) 297

Set-UnifiedGroup cmdlet 104

SharePoint Migration Tool (SPMT) 173

- used, for data import from network
locations 265-268
- using, for data migration 207-211

SharePoint Online

- connecting, via PowerShell 94, 95

SharePoint Online Management Shell 94

SharePoint Online site

- creating 96, 97
- new site admin, adding 98, 99

SharePoint PnP PowerShell

- reference link 98

SharePoint site

- access, regaining 100
- configuring, with permission groups 247
- creating 244-247
- deleting 248, 249
- managing 247

single sign-on (SSO) 331

- adding, for application 341-344

site collection storage

- configuring 261-264

spam filter policies

- configuring 132-135

subsite creation button

- hiding 268-270

T**team**

- creating, in Microsoft Teams 278-280

Team policy

- creating, in Microsoft Teams 281, 282

Teams Premium license 290**Teams usage and user activity**

- checking 461-463

template, creation and usage to add users

- reference link 68

test environments 217**theme**

- configuring, for Power BI 241, 242

threat investigation and response**capabilities, Microsoft Defender**

- utilizing 393, 394

threat protection policy, Microsoft Defender

- creating 366, 367
- working 368, 369

time-based one-time password (TOTP) 55**U****Uniform Resource Identifier (URI) 343****uniform resource locators (URLs) 5****Update-MgUser cmdlet 350****Update-MgUser command 84, 89, 94****usage data**

- monitoring 458

user

- Corporate Communicator role,
 - assigning to 316, 317
- creating, in Microsoft 365 tenant 85, 86
- disabling, in Microsoft 365 tenant 87
- properties 86
- settings or profile information, modifying 89

User Administrator role

- assigning 73-76

user password

- modifying 93

User Principal Name (UPN) 86, 280, 350**users**

- adding and removing, via PowerShell
 - in Microsoft Graph 349-351
- creating 40-43
- domain, modifying 26, 27
- exporting 56-59
- importing, in bulk 44-46
- license, assigning to 28, 29
- list of users with user properties,
 - obtaining 91, 92
- restricting, from installing on-premises
 - data gateways 233-235
- restricting, from new Microsoft
 - 365 groups creation 69-72

user template

- creating 65-67

V

Verified Administrator role 312

Viva Engage 309

admin roles 311, 312

community, creating 320-322

network look, customizing 318, 319

pinning, in Microsoft Teams 313-315

Viva Engage admin center

Network Administrator role,
assigning to user 310, 311



packtpub.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

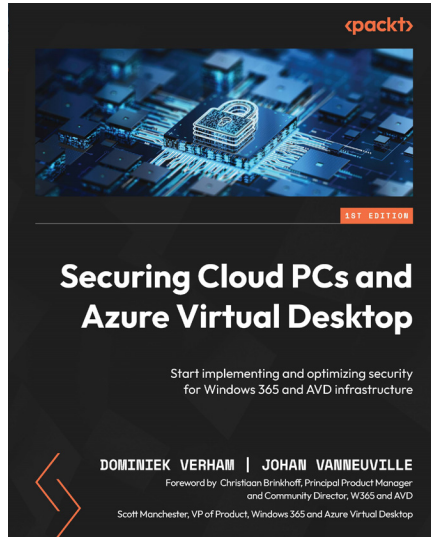
- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at packtpub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at customercare@packtpub.com for more details.

At www.packtpub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Other Books You May Enjoy

If you enjoyed this book, you may be interested in these other books by Packt:

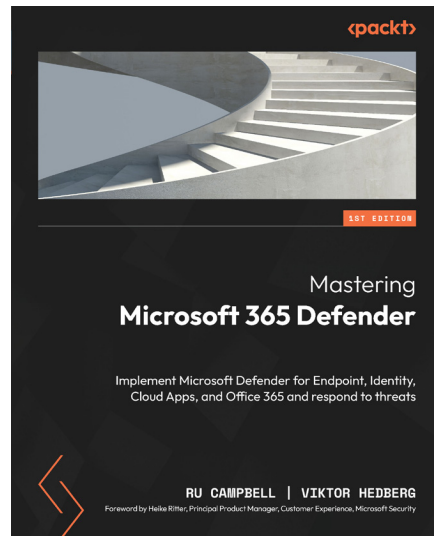


Securing Cloud PCs and Azure Virtual Desktop

Dominiek Verham, Johan Vanneuville

ISBN: 978-1-83546-025-2

- Become familiar with Windows 365 and Microsoft Azure Virtual Desktop as a solution
- Uncover the security implications when company data is stored on an endpoint
- Understand the security implications of multiple users on an endpoint
- Get up to speed with network security and identity controls
- Find out how to prevent data leakage on the endpoint
- Understand various patching strategies and implementations
- Discover when and how to use Windows 365 through use cases
- Explore when and how to use Azure Virtual Desktop through use cases



Mastering Microsoft 365 Defender

Ru Campbell, Hedberg

ISBN: 978-1-80324-170-8

- Understand the Threat Landscape for enterprises
- Effectively implement end-point security
- Manage identity and access management using Microsoft 365 defender
- Protect the productivity suite with Microsoft Defender for Office 365
- Hunting for threats using Microsoft 365 Defender

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit authors.packtpub.com and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Share Your Thoughts

Now you've finished *Microsoft 365 Administration Cookbook*, we'd love to hear your thoughts! If you purchased the book from Amazon, please [click here](#) to go straight to the Amazon review page for this book and share your feedback or leave a review on the site that you purchased it from.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Download a free PDF copy of this book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere?

Is your eBook purchase not compatible with the device of your choice?

Don't worry, now with every Packt book you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there, you can get exclusive access to discounts, newsletters, and great free content in your inbox daily

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the link below



<https://packt.link/free-ebook/978-1-83588-802-5>

2. Submit your proof of purchase
3. That's it! We'll send your free PDF and other benefits to your email directly