

The ultimate in-depth reference

Hundreds of timesaving solutions

Supremely well-organized, packed
with expert advice



Microsoft 365 Administration Inside **OUT**

Third Edition

Aaron Guilmette • Darryl Kegg • Ed Fisher

FREE SAMPLE CHAPTER |



Microsoft 365 Administration Inside Out, Third Edition

Aaron Guilmette
Darryl Kegg
Ed Fisher

Microsoft 365 Administration Inside Out, Third Edition
Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

Copyright © 2023 by Pearson Education, Inc.

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

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

ISBN-13: 978-0-13-790885-1

ISBN-10: 0-13-790885-7

Library of Congress Control Number: 2022951941

ScoutAutomatedPrintCode

Trademarks

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

Warning and Disclaimer

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

Special Sales

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

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

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

Editor-in-Chief: Brett Bartow

Executive Editor: Loretta Yates

Sponsoring Editor: Charvi Arora

Development Editor: Rick Kughen

Managing Editor: Sandra Schroeder

Senior Project Editor: Tracey Croom

Project Editor: Charlotte Kughen

Copy Editor: Rick Kughen

Indexer: Johnna VanHoose Dinse

Proofreader: Sarah Kearns

Editorial Assistant: Cindy Teeters

Cover Designer: Twist Creative, Seattle

Compositor: Bronkella Publishing, LLC

Graphics: TJ Graham Art

Pearson's Commitment to Diversity, Equity, and Inclusion

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

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

Our ambition is to purposefully contribute to a world where:

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

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

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

Dedications

I'd like to dedicate this book to my kids, several of whom reminded me that I didn't include their names in my last book. Sorry for the oversight. I also want to thank my co-authors, without whom I would have had to write a lot more.

—Aaron Guilmette

I'd like to dedicate this book to my family for their support and understanding, and I'd like to thank my co-authors, a motley crew, for their willingness to collaborate. This book has been a labor of love, and I sincerely hope it can help others to learn and grow.

—Darryl Keggs

I dedicate this book to Connie, without whom this could not have happened and would not have mattered. Thanks for being my better half in every way. And to my partners in crime on this book: It's always a pleasure, gentlemen! And thank you to the great team at Pearson and The Wordsmithery for all your help and patience!

—Ed Fisher



Contents at a Glance

Chapter 1	Chapter 16
Jumping into the cloud 1	Migrating mailboxes to Exchange Online 489
Chapter 2	Chapter 17
Preparing your environment for the cloud 33	Migrating public folders to Exchange Online . . . 515
Chapter 3	Chapter 18
Governance concepts 65	Managing Exchange Online 545
Chapter 4	Chapter 19
Compliance Manager 87	Microsoft Teams overview 589
Chapter 5	Chapter 20
Secure Score 105	Meetings, webinars, and live events 609
Chapter 6	Chapter 21
Labels, retention, and eDiscovery 117	Phone system planning 639
Chapter 7	Chapter 22
Enterprise Mobility + Security 189	Phone System configuration 671
Chapter 8	Chapter 23
Security features of Enterprise Mobility + Security 207	Phone System advanced features 725
Chapter 9	Chapter 24
Identity and authentication planning 237	Managing Teams 761
Chapter 10	Chapter 25
Installing AAD Connect 259	SharePoint Online 781
Chapter 11	Chapter 26
Azure AD Cloud Sync 345	SharePoint Online planning and deployment . . . 791
Chapter 12	Chapter 27
Advanced Azure AD scenarios 381	SharePoint Online Hybrid configuration 809
Chapter 13	Chapter 28
Azure Automation 413	Migrating data to SharePoint Online 845
Chapter 14	Chapter 29
Exchange Online overview 431	SharePoint Online management 867
Chapter 15	Chapter 30
Exchange Online hybrid planning and deployment 455	OneDrive for Business 905
	Index 937



Table of Contents

About the Authors.....	xxiii
Introduction.....	xxii
Who this book is for.....	xxiv
Conventions.....	xxv
Text conventions.....	xxv
Book features.....	xxv
Acknowledgments.....	xxvi
Free ebooks from Microsoft Press.....	xxvi
Errata, updates, & book support.....	xxvii
We want to hear from you.....	xxvii
Stay in touch.....	xxvii
Chapter 1	
Jumping into the cloud.....	1
Getting started.....	1
Which plan is best for me?.....	2
Picking a tenant name.....	3
Adding your domain name to your tenant.....	5
Delegating access to your tenant.....	8
Should I deploy in hybrid mode?.....	9
Exchange Hybrid.....	9
SharePoint Hybrid.....	11
Is your Exchange environment ready?.....	13
Physical Exchange Server infrastructure.....	13
Mail routing.....	14
Mailboxes.....	14
Load balancers, network configurations, proxy servers, and firewall rules.....	16
Is your directory ready?.....	18
User readiness.....	18
Forests and domains.....	21
Stale users.....	23
Are your users ready?.....	25
UPN versus email address.....	25
Multi-forest environments.....	26
Office versions.....	27

	Updates	27
	Mailbox cleanup	28
	Scheduling	29
	The Global Address List	30
	Replying to old emails	30
	What's next?	31
Chapter 2	Preparing your environment for the cloud	33
	Setting up your subscription	33
	Finding your tenant name	33
	Assigning administrators	37
	Configuring DNS, firewalls, and proxy servers	39
	Public DNS records	39
	Firewall configurations	40
	Proxy servers	41
	Preparing your directories	48
	Updating and deploying client software	53
	Installing Microsoft 365 Apps	54
	Activation	57
	Synchronizing your users	58
	Licensing your users	59
	Group-based licensing	59
	PowerShell licensing	61
	Manual license assignment	63
	What's next?	64
Chapter 3	Governance concepts	65
	Identity and access management concepts	66
	Identity lifecycle	67
	Access management lifecycle	68
	Governance for core workloads and features	69
	Azure Active Directory	69
	Exchange Online	71
	SharePoint Online	71
	Microsoft Teams	72
	Retention and data security	72
	eDiscovery	74
	Governance controls	74
	Azure AD	74
	Exchange Online	76
	SharePoint Online	78

	Microsoft Teams	81
	Retention and data security	84
	eDiscovery	85
	What's next?	86
Chapter 4	Compliance Manager	87
	Your organization's compliance score	87
	Understanding improvement actions	89
	Types of improvement actions	89
	Assigning permissions	91
	Conducting an assessment	93
	Creating an assessment	93
	Reviewing controls and actions	96
	Updating improvement actions	98
	Working with alerts	103
	What's next?	104
Chapter 5	Secure Score	105
	Overview	105
	Assessing your security posture	107
	Prioritizing improvements in your security posture	108
	Reporting on your security posture	113
	What's next?	115
Chapter 6	Labels, retention, and eDiscovery	117
	Data governance concepts	117
	Sensitive information types	118
	Classifiers	120
	Labels	121
	Data loss prevention	123
	Retention	124
	Records	126
	Data governance scenarios	127
	Sensitivity labels	127
	Retention labels	147
	Retention policies	153
	Data loss prevention policies	156
	Records search	161
	Audit log search	162
	Content search	164
	eDiscovery	174
	What's next?	187

Chapter 7	Enterprise Mobility + Security	189
	Overview	189
	Identity and access management.....	191
	Simplified access management and security.....	191
	Multifactor authentication	192
	Conditional access.....	193
	Risk-based access.....	194
	Advanced security reporting	197
	Privileged Identity Management	197
	Endpoint management	198
	Mobile application management	199
	Advanced Microsoft Office 365 data protection	199
	Integrated PC management.....	200
	Integrated on-premises management	201
	Information protection	201
	Persistent data protection.....	201
	Intelligent data classification and labeling.....	202
	Document tracking and revocation.....	203
	Encryption key management.....	203
	Identity-driven security	203
	Microsoft Advanced Threat Analytics	203
	Microsoft Cloud App Security	204
	Microsoft Defender for Identity	205
	What's next?	206
Chapter 8	Security features of Enterprise Mobility + Security	207
	Securing identity	207
	Microsoft Defender for Identity	208
	Ensure your hardware is up to the task	208
	Make sure the required connectivity is in place	210
	Create the service account	211
	Create your MDI instance	211
	Monitoring your environment.....	213
	Multifactor authentication	214
	Conditional Access.....	218
	Risk-based Conditional Access.....	223
	Securing devices.....	227
	Mobile Device Management	227
	Mobile Application Management.....	228
	Getting started with Intune	228
	What's next?	235

Chapter 9	Identity and authentication planning	237
	Identity types	237
	Synchronized identities	237
	Cloud identities	238
	Guest identities	246
	User authentication	249
	Password	249
	Password policy	252
	Identity federation	254
	What's next?	257
Chapter 10	Installing AAD Connect	259
	The Custom and Express installation experiences	259
	Express installation	261
	Custom installation	267
	Selecting your authentication method	272
	Password synchronization	273
	Connecting to your directories	284
	The UserPrincipalName and SourceAnchor attributes	287
	Domain and OU filtering	289
	Uniquely identifying your users	290
	User matching	291
	Important notes about GalSync and AAD Connect	299
	SamAccountName and MailNickname	313
	Custom join attribute selection	316
	Source Anchor	319
	Filter users and devices	322
	Optional features	325
	Group Writeback	332
	Device Writeback	333
	Directory Extension Attribute Sync	335
	Finalizing the installation	337
	Configuration complete	339
	When should you start synchronizing?	340
	Starting synchronization	341
	Staging Mode—your ace in the hole	343
	What's next?	344
Chapter 11	Azure AD Cloud Sync	345
	Azure AD Cloud Sync	346
	Device synchronization and hybrid Azure AD Join	347
	Writeback	348
	Pass-through authentication	348
	Directory extensions	348

- Custom attribute flows and rule editing 349
- SourceAnchor 349
- Installing Azure AD Cloud Sync 349
- Configuring Azure AD Cloud Sync 355
 - Deleting attribute mappings 360
 - Editing attribute mappings 361
 - Adding attribute mappings 362
 - Additional complex mapping examples 365
 - Decompressing 370
 - Using the Expression Builder 370
 - Provisioning a user (the validate step) 373
 - Notification and deletion protection 377
 - Enabling the configuration 378
 - Moving from Azure AD Connect to Azure AD Cloud Sync 378
- What's next? 379

Chapter 12 Advanced Azure AD scenarios 381

- Migrations and the SourceAnchor 381
 - What does mS-DS-ConsistencyGuid support add to the configuration? 389
- Performing migrations 395
 - UserPrincipalName 395
 - Email address and Exchange attributes 396
 - Group and user SIDs 396
 - Microsoft options for cross-forest migrations 397
- Additional Azure AD Connect considerations 397
- Password Writeback 398
 - Requirements 398
 - Enabling Password Writeback 398
- Precedence 404
- What's next? 412

Chapter 13 Azure Automation 413

- Azure Automation concepts 413
 - Runbooks 413
 - Hybrid Runbook Worker 414
 - Authentication 414
 - Webhooks 414
- Configuring authentication 414
 - Microsoft 365 service account 415
 - Azure Automation account 416
- Creating a PowerShell runbook 422
 - Prepare an Exchange Online script 423
 - Creating a runbook with a script 424

Testing a PowerShell runbook	426
Publishing a runbook	428
What's next?	430
Chapter 14 Exchange Online overview	431
Exchange Online deployment concepts	431
Recipients	431
Mail routing	432
Autodiscover	432
Migration and coexistence methodologies	435
Exchange and Active Directory on-premises environment	436
Active Directory versions and configuration	436
Autodiscover	437
Certificates	438
Exchange versions, service packs, cumulative updates, and rollups	439
Exchange Best Practices Analyzer	440
IDFix	440
SSL offloading	440
Windows updates	441
Recipients	441
Contacts	441
Mailboxes	441
Mail-enabled users	444
Groups	444
Dynamic distribution groups	445
Microsoft 365 groups	445
Permissions and delegation	446
Public folders	446
Mail routing	447
Data loss prevention	447
Message encryption	447
Message hygiene	447
Networking	448
Bandwidth	448
Firewall	448
Load balancing	449
Proxy	449
DNS	449
Network security appliances	450
Things that don't migrate	451
Additional tools	453
Remote Connectivity Analyzer	453
Exchange Deployment Assistant	453
What's next?	453

Chapter 15	Exchange Online hybrid planning and deployment	455
	Overview of Exchange Online hybrid features	455
	Planning	458
	General	458
	Autodiscover	458
	Azure Active Directory Connect	458
	Cross-premises access and delegation	458
	DNS	459
	Email address policies and proxy addresses	459
	Exchange Server Deployment Assistant	460
	Exchange server versions	460
	Free/busy and hybrid authentication	461
	Message sizes	463
	Mail transport	463
	Networking	464
	Public folders	465
	Office 365 Hybrid Configuration Wizard	465
	Overview	465
	Prerequisites	468
	Installing the Office 365 Hybrid Configuration Wizard	469
	Running the Office 365 Hybrid Configuration Wizard	471
	Rerunning the Hybrid Configuration Wizard	481
	Troubleshooting	482
	Mailbox provisioning	482
	Decommissioning the hybrid environment	485
	What's next?	487
Chapter 16	Migrating mailboxes to Exchange Online	489
	Migration endpoints	489
	Migration batches	493
	Onboarding	493
	Offboarding	507
	Troubleshooting	509
	What's next?	513
Chapter 17	Migrating public folders to Exchange Online	515
	Exchange Online prerequisites	515
	Configuring hybrid public folders	517
	On-premises public folders	518
	Public folder migration	522
	Exchange 2007 or Exchange 2010	523
	Exchange 2013 or later	532

Post-migration configuration	538
Exchange Online public folder location	538
Exchange Online mail-enabled public folder routing	538
Exchange Online mail-enabled public folder external email address	539
Exchange on-premises mail routing domain	539
Exchange on-premises public folder migration complete	539
Apply Send-As permissions	539
Apply Grant-Send-On-Behalf-To permissions	540
Troubleshooting	540
Active Directory Operation Failed. The Object Already Exists	540
Exceeded Maximum Number Of Corrupted Items	541
Subscription Couldn't Be Loaded	541
Make Sure Public Folder Access Is Locked	541
No Such Request Exists	542
Public Folder "/Path" Could Not Be Mail-Enabled	542
Public Folders Could Not Be Mail-Enabled	543
What's next?	544
Chapter 18 Managing Exchange Online	545
Exchange admin center	545
Recipient management	546
Mailboxes	547
Mail-enabled users	553
Contacts	554
Distribution groups	554
Restricting delivery	555
Transport	557
Connectors	557
Transport rules	557
Central mail transport	566
Manage IP filtering lists	567
Enhanced filtering for connectors	569
Message trace	569
Migration of transport settings between Office 365 tenants	570
Migration of transport rules collections	571
DKIM	572
Spam, phishing, and malware filtering	574
Malware filter	574
Phishing filter	574
Spam filter	576
Quarantine	579
Outbound spam	581
Blocked accounts	581

Organization management	582
Organization relationships	583
Sharing policies	586
Hybrid management	587
Provisioning remote mailboxes	587
Updating domains in a hybrid configuration	588
What's next?	588
Chapter 19 Microsoft Teams overview	589
Architecture	589
Identity	592
Files	593
Messaging and chat services	593
Connectors	594
Voicemail	594
Recording	594
Calendars and meetings	594
Contacts	594
Other components	594
Architecture deep dive	595
Microsoft 365 groups	595
Teams	599
User interface	600
Menu bar	601
App bar	601
List pane	601
Main content area	601
Exploring the App bar	601
What's next?	607
Chapter 20 Meetings, webinars, and live events	609
Meetings	609
Types	609
Webinars	613
Administration	616
Live events	625
Live events policies	625
Live events settings	629
Integrated services	631
Configuring Teams Live events with external production	636
What's next?	637

Chapter 21	Phone system planning	639
	Overview of Teams Phone concepts	639
	Teams Phone concepts and terminology	639
	Calling features	643
	Choosing an architecture	646
	Calling Plans for Microsoft 365	647
	Direct Routing	648
	Operator Connect	654
	Planning network requirements	655
	Network requirements	655
	Bandwidth requirements	656
	Ports	657
	Network endpoints	657
	Split-tunnel VPN	658
	Quality of Service	658
	Best practices and additional network tools	667
	Verify all required outbound network ports	667
	Bypass encryption and other filtering devices	668
	Microsoft Teams Network Assessment Tool	668
	Network Planner for Teams	668
	Microsoft 365 Network Connectivity Test	668
	Call Quality Dashboard Report	668
	What's next?	669
Chapter 22	Phone System configuration	671
	Prerequisites	672
	Emergency dialing	672
	Define networks	674
	Configure Location Information Service	675
	Configure emergency policies	681
	Test the emergency location configuration	683
	Phone numbers	683
	Obtain phone numbers	683
	Assign phone numbers	696
	Communications credits	699
	Teams voice policies	700
	Calling restrictions	701
	Calling policies	706
	Call parking policies	712
	Caller ID policies	716
	Voicemail policies	718
	What's next?	723

Chapter 23	Phone System advanced features	725
	Resource accounts	726
	Microsoft Teams advanced calling feature resource accounts	727
	Microsoft Teams Room resource accounts	733
	Holidays	741
	Call queues	743
	Configure call queue prerequisites	743
	Configure a call queue	743
	Voice-enabled channels	748
	Auto attendants	749
	Configure auto attendant prerequisites	750
	Configure an auto attendant	750
	Check auto attendant voicemail	758
	What's next?	759
Chapter 24	Managing Teams	761
	Microsoft 365 Groups and Teams component architecture	761
	Collaboration management	763
	Access control planes	763
	Channel controls	772
	Troubleshooting	777
	This link won't work for people outside your organization	778
	We ran into an issue. Please try again later	778
	Your organization does not allow collaboration with the domain of the user you're inviting	779
	Due to admin policy, you can't add external people to the channel	780
	What's next?	780
Chapter 25	SharePoint Online	781
	SharePoint Online concepts	781
	SharePoint Online capacities	782
	Overall service limits	782
	Individual service plan limits	783
	SharePoint Online features	785
	OneDrive for Business	785
	Office Online	786
	Delve	787
	Yammer	788
	Enterprise search	788
	SharePoint Store apps	789
	Business Connectivity Services	789
	SharePoint Online hybrid	790
	What's next?	790

Chapter 26	SharePoint Online planning and deployment	791
	Planning a modern site architecture	791
	Planning sites and hubs	791
	Planning navigation	794
	Designing site collection structure	796
	Determining site taxonomy and topology	796
	Determining site users	798
	Planning and configuring site and guest access	798
	How external sharing works	798
	Planning and configuring sharing and site access	801
	Planning security options	804
	What's next?	807
Chapter 27	SharePoint Online Hybrid configuration	809
	Planning	810
	General	810
	OneDrive for Business	811
	Search	811
	Taxonomy	813
	App launcher	814
	Business-to-business extranet	814
	Configuration	815
	Set up SharePoint services for hybrid integration	816
	OneDrive for Business and Hybrid Sites	824
	Hybrid search	830
	Hybrid taxonomy	837
	App launcher	842
	Business-to-business extranet	843
	What's next?	844
Chapter 28	Migrating data to SharePoint Online	845
	Inventorying data sources and mapping destinations	846
	What data is being migrated?	846
	Where should it go?	846
	What can't be migrated?	847
	Choosing the migration tools	849
	Planning for requirements and prerequisites	849
	SharePoint Online planning and prerequisites	850
	Network planning and prerequisites	852
	Scanning content	853
	Generating an identity map	854
	Scanning SharePoint content	856
	Customizing the SMAT scanning process	857

	Resolving blocking issues	858
	Planning for content that cannot be migrated.....	858
	Migrating data with SharePoint Migration Tool (SPMT)	859
	What's next?	866
Chapter 29	SharePoint Online management.....	867
	Sites	868
	Policies.....	870
	Sharing	870
	Access control.....	872
	Settings.....	873
	Content services.....	878
	Term Store	879
	Content Type Gallery	879
	Migration	880
	Reports	881
	Content Services.....	881
	Data access governance.....	881
	Advanced	883
	More Features.....	883
	Term Store	884
	User profiles.....	884
	Search	888
	Apps.....	889
	Business Connectivity Services	893
	Secure Store.....	896
	Records management	897
	Infopath	903
	Hybrid Picker.....	903
	What's next?	904
Chapter 30	OneDrive for Business	905
	Accessing OneDrive for Business	905
	OneDrive sync client for Windows	907
	OneDrive sync client for Mac OS X.....	914
	Collaborating with OneDrive for Business.....	915
	Sharing documents and folders	915
	Coauthoring	916
	Document versioning.....	917
	Deploying OneDrive for Business to your users.....	920
	Group Policy	921
	Manage OneDrive for Business.....	928
	Troubleshooting.....	934
	Index.....	937

About the Authors

Aaron Guilmette is a Senior Program Manager for Customer Experience at Microsoft and provides guidance and assistance to customers adopting the Microsoft 365 platform, focusing on messaging, identity, automation, and security solutions. You can follow Aaron on LinkedIn at aka.ms/aaronlinkedin.

Darryl Kegg is a Senior Program Manager at Microsoft, dedicated to deploying Microsoft 365 and Azure technologies with a focus on identity, security, and access management. Darryl has been involved in deploying Microsoft 365 to government, education, healthcare, and commercial customers since its launch in 2011 and has helped migrate 15+ million users to Azure. You can follow Darryl on LinkedIn at aka.ms/darrylkegg.

Ed Fisher is a Technical Solution Leader-Security at Microsoft, focusing on helping customers evaluate, deploy, and adopt Microsoft 365 collaboration technologies, networking, and security solutions. His focus is on Microsoft's XDR and SIEM platforms and Microsoft Defender for Office. Find out more at aka.ms/edfisher.

Introduction

Microsoft's online offerings have continued to evolve since the first debut of the Live@Edu service in 2005. Four years later, in April 2009, Microsoft expanded its cloud services offering with the launch of Microsoft Business Productivity Online Services. Over the last 18 years, Microsoft has steadily rolled out new features to the service and paved the way for today's modern Microsoft 365 platform.

Microsoft 365 enables organizations as small as a single person or as large as the world's biggest multinational retailers and manufacturers to harness the power of cloud scaling, automation, and availability. Microsoft's online services currently enable over 200 million monthly active users to collaborate—whether they're in the same room, across the hall, or around the world.

The service is evergreen—built around the ideas of continuous improvement and feature release—to ensure that customers always receive the latest capabilities and enhance their ability to be more agile, productive, and secure. With the launch of the Microsoft 365 product suite in 2017, Microsoft added Windows platform, mobility, and enterprise security capability to the already popular Office 365 software-as-a-service offering.

Microsoft has a vision for a cloud-first, mobile-first future—built on the broad capabilities of Microsoft 365 and Azure. This book equips you with the knowledge you need to tackle the deployment of one of the largest transformational products available as well as insider tips that help you avoid the mistakes that might slow you down.

Who this book is for

This book is written for IT professionals responsible for deploying, migrating to, and managing some (or all) of an organization's Microsoft 365 environment. Microsoft 365 isn't just a single application or service; it's a suite of software-as-a-service tools that can touch every part of the business.

For some, Microsoft 365 might seem like just one more thing to learn. In reality, though, if you've been administering on-premises versions of Active Directory, Exchange, or SharePoint, you're already familiar with many of the core concepts you need to hit the ground running. The Microsoft 365 platform enables myriad hybrid capabilities, allowing your organization to adopt the cloud on its terms and timeline. There are a lot of compelling cloud-only features that you'll want to explore as well.

We at Microsoft believe that the Microsoft 365 platform is an extension of your own datacenter. The management patterns and practices you've built for your on-premises environment can be updated and adapted to the cloud, enabling you to achieve quicker results.

We've organized this book to try to take you from the very beginning through progressively more advanced concepts. However, you don't have to read it in order—you can skip around to the parts that address your most immediate needs. Our goal with this book is to help you at any stage of your cloud journey—whether you're a consultant looking for architecture and planning guidance or an IT pro tasked with deployment and management.

Conventions

This book uses special text and design conventions to make it easier for you to find the information you need.

Text conventions

The following conventions are used in this book:

- **Boldface type** is used to indicate text that you should type where directed.
- For your convenience, this book uses abbreviated menu commands. For example, "Click Tools > Track Changes > Highlight Changes" means you should click the Tools menu, point to Track Changes, and then click the Highlight Changes command.
- Elements with the Code typeface are meant to be entered on a command line or inside a dialog box. For example, "type `cd \Windows` to change to the Windows subdirectory" means that you should be entering `cd \Windows` with your keyboard or text input device.
- The first letters of the names of menus, dialog boxes, dialog box elements, and commands are capitalized—for example, the Save As dialog box.
- *Italicized type* indicates new terms.

Book features

In addition to the text conventions, this book contains sidebars to provide additional context, tips, or suggestions.

Inside OUT

These are the book's signature tips. In these tips, you'll get the straight scoop on what's going on with the software or service—inside information about why a feature works the way it does. You'll also find field-tested advice and guidance as well as details that give you the edge on deploying and managing like a pro.

READER AIDS

Reader aids are exactly that—Notes, Tips, and Cautions provide additional information on completing a task or specific items to watch out for.

Acknowledgments

We would like to thank the teams at Pearson and Microsoft Press for giving us the opportunity to share our knowledge, experiences, and lessons learned in this update. We'd also like to thank our coworkers and peers for content ideas, suggestions, and feedback during the writing and revising process. And, of course, we want to thank the countless engineers, programmers, and technical experts who tirelessly work behind the scenes to expand the capabilities of the platform, giving all of us the ability to achieve more.

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book in the form of a list of submitted errata and their related corrections—at:

MicrosoftPressStore.com/365AdminInsideOut/errata

If you discover an error that is not already listed, please submit it to us at the same page.

For additional book support and information, please visit MicrosoftPressStore.com/Support.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to:

<http://support.microsoft.com>.

Stay in touch

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



Preparing your environment for the cloud

Setting up your subscription	33	Updating and deploying client software.....	53
Assigning administrators.....	37	Synchronizing your users.....	58
Configuring DNS, firewalls, and proxy servers	39	Licensing your users	59
Preparing your directories.....	48	What's next?	64

In the previous chapter, we identified some high-level tasks involved in a Microsoft 365 deployment. In this chapter, we will use your understanding of those tasks to

- Continue setting up your Microsoft 365 subscription
- Assign administrators
- Configure your network
- Run the IDFix tool to clean up your directory
- Update and install client software
- Start synchronizing your users to your tenant

Once these tasks are complete, you will be able to start using your Microsoft 365 subscription and migrating your users.

Setting up your subscription

If you have not already set up your Microsoft 365 subscription, that is the best place to start. Please review the steps in the previous chapter to select and begin a subscription. As discussed, the tenant name you select will become permanent and branded across your subscription, so choose carefully.

Finding your tenant name

Once the tenant name selection is complete, each of the services within your Microsoft 365 subscription (such as Exchange, SharePoint, or Teams) will be branded with the name you selected. As mentioned previously, this branding process is permanent, and the name will be visible in several locations—the Microsoft 365 service, your users, and external parties.

Exchange Online

Exchange Online uses your tenant name in the routing email address stamped on every mail-enabled object you create.

The Exchange Hybrid process (discussed in more detail in Chapter 15, “Exchange Online hybrid planning and deployment”) configures a recipient policy in your Exchange on-premises organization that automatically assigns an email address suffix of `@tenantName.mail.onmicrosoft.com` for every mail-enabled object. This `@tenant.mail.onmicrosoft.com` address is typically referred to as the *service routing address*.

This service routing address is required for every mailbox that will be migrated to Exchange Online. It will not appear on cloud-only mailboxes because it is applied in an on-premises environment. However, within the Exchange Online service, there is another automatic email address assignment that is not optional and cannot be changed.

As seen in Figure 2-1, Exchange Online automatically assigns an email address ending in `@tenantName.onmicrosoft.com` to every mail-enabled object.

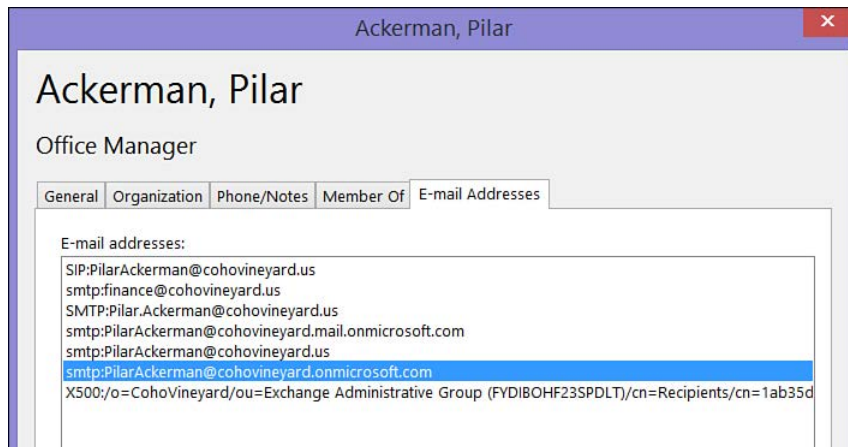


Figure 2-1 The tenant.onmicrosoft.com email address

The email address seen in the example above is only visible to your internal users when viewing the contact properties of another mail-enabled object. It is also important to note that this address does NOT contain the word *mail*, like in the service routing address mentioned above.

This additional `onmicrosoft.com` routing address is not visible outside your organization, nor is it present in the email header when sending messages to external recipients over the Internet.

TIP

The domain suffix `mail.onmicrosoft.com` is not added automatically to the tenant during the Exchange Online setup; instead, this domain suffix is added to every mail-enabled object in on-premises Exchange via an email address policy added during the Exchange Hybrid setup.

SharePoint Online

Of all the services in Microsoft 365, your tenant name appears most prominently in SharePoint Online. It is visible internally in site content URLs and in the shared URLs provided to external parties.

As shown in Figure 2-2, the tenant name is present in the URL for every external sharing request sent via email.

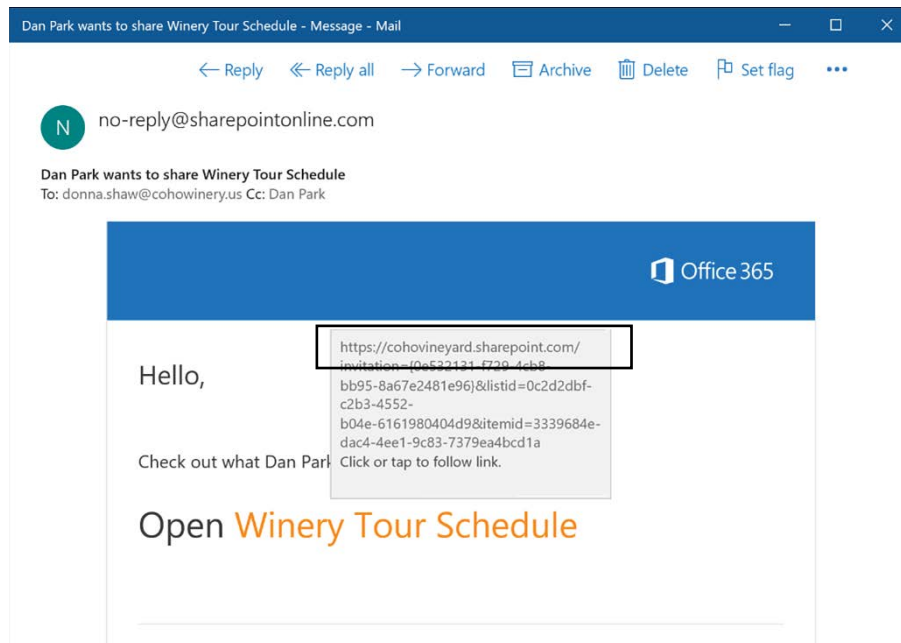


Figure 2-2 The tenant name visible in the URLs for SharePoint sharing requests

OneDrive for Business

Because OneDrive is part of the SharePoint Online service and takes the place of MySites in SharePoint Server, your tenant name will appear in any OneDrive URLs shared via email to internal or external recipients. Additionally, when OneDrive content is viewed when navigating between folders or stored files, it will display the tenant name in the URL (visible in the address bar at the top of the browser). See Figure 2-3.

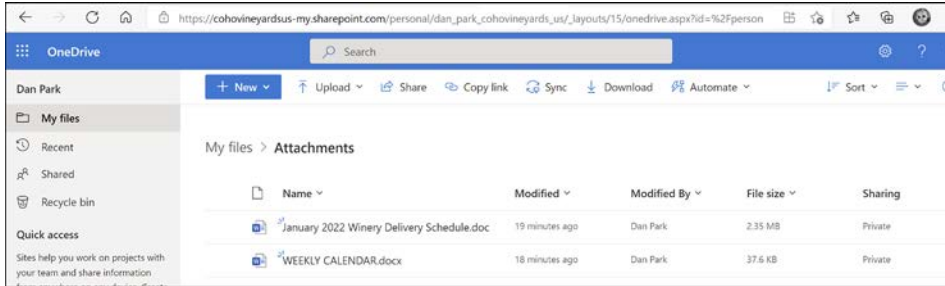


Figure 2-3 The tenant name visible in OneDrive URLs

Microsoft Teams

In past versions, the tenant name in Microsoft Teams was visible when viewing the meeting URL in meeting requests sent via email. However, it no longer contains references to your tenant name.

The meeting URL can be viewed by right-clicking or hovering over the Join Teams Meeting hyperlink in email invites, as shown in Figure 2-4.

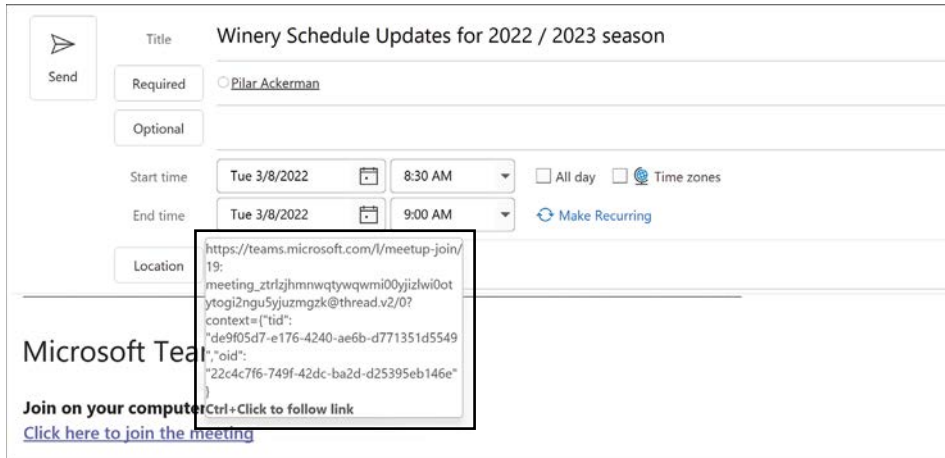


Figure 2-4 Viewing the tenant name in a Teams sharing request

Microsoft 365 Apps

The tenant name is not visible when viewing the properties of the Microsoft 365 Apps (formerly Microsoft Office 365 ProPlus) applications, nor is it visible in any of the additional licensed Office-suite applications like Visio or Project.

Office Online

Office Online applications automatically use OneDrive for Business as the default save location for newly created documents, as shown in Figure 2-5. This is visible to your user in the browser address bar, and if these documents are shared with external parties, the file's URL will contain the tenant name.

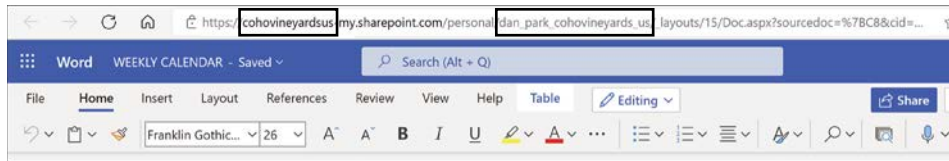


Figure 2-5 Tenant name visibility when using Office Online applications

Assigning administrators

Using the information you learned in Chapter 1, you can either create cloud accounts and delegate administrative privileges or wait until you've started synchronizing your users (discussed later in this chapter) and assigning permissions.

In either case, you might need to delegate permissions to one or more additional administrators. Keep in mind that the Global Administrator role has the right to create other Global Administrators, so you should limit administrative delegation to one of the other administrative roles discussed in Chapter 1 and avoid creating other Global Administrator accounts unless necessary.

Follow the steps below to create a new administrative account with User administration privileges:

1. Navigate to the Microsoft 365 admin center (<https://admin.microsoft.com>).
2. Select Add A User from the Home or Users views, as shown in Figure 2-6.

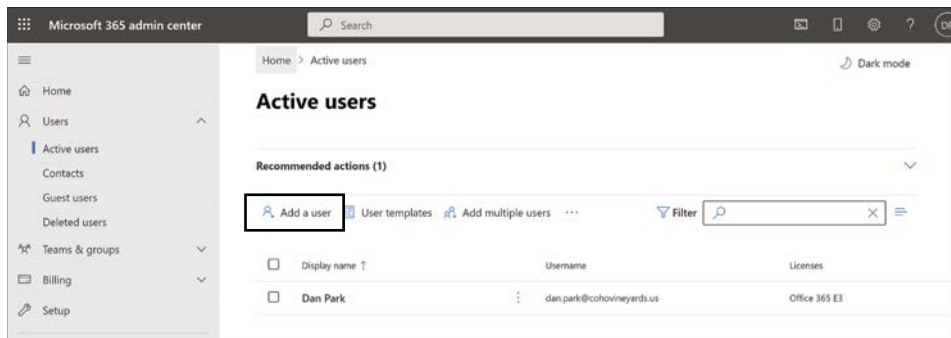
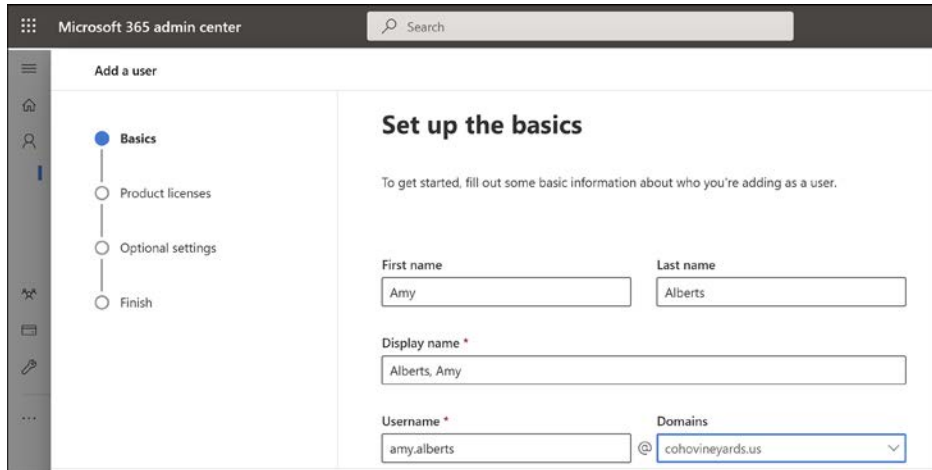


Figure 2-6 The Active Users view in the Microsoft 365 admin center

3. Enter the necessary First Name, Last Name, Display Name, and User Name in the boxes provided, as shown in Figure 2-7.



Microsoft 365 admin center

Search

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: Amy

Last name: Alberts

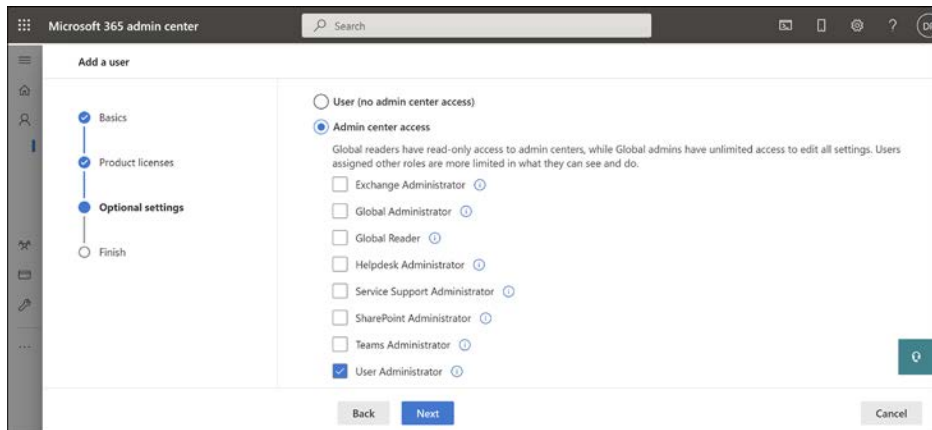
Display name *: Alberts, Amy

Username *: amy.alberts

Domains: cohovineyards.us

Figure 2-7 Creating a cloud user with administrative privilege

4. When creating the account, select the Roles dropdown under Optional Settings, select Admin Center Access, and check the User Administrator box, as shown in Figure 2-8.



Microsoft 365 admin center

Search

Add a user

Basics

Product licenses

Optional settings

Finish

User (no admin center access)

Admin center access

Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned 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

Back Next Cancel

Figure 2-8 Selecting an administrator role for a Microsoft 365 user account

5. Click Add to create the cloud user account.

6. This process can be used to modify existing cloud accounts or even accounts that have been synchronized from on-premises Active Directory using the AAD Connect synchronization tool.
7. Once you have completed the creation of any administrator accounts in your new tenant, you can move on to creating DNS records to verify your domains, as well as any other services that you wish to add.

Configuring DNS, firewalls, and proxy servers

As discussed in Chapter 1, several network devices could affect your Microsoft 365 deployment, connectivity, and continued success with the services provided. Therefore, it is strongly recommended that all network devices be updated to their latest versions, and each device vendor should be contacted to ensure that your device supports Microsoft 365 connectivity.

Often, it is merely a matter of upgrading your existing devices to support Microsoft 365. However, this upgrade process can be time-consuming and disruptive if not done correctly. Therefore, it is strongly recommended that any infrastructure changes required to support Microsoft 365 be made before starting your Microsoft 365 deployment.

Public DNS records

The first necessary configuration changes will be to your public DNS records, which will allow you to verify any domain names and configure the necessary DNS records for things like mail exchange (MX), Exchange AutoDiscover, and Teams.

Proof of domain ownership

When setting up your domain name, as discussed in Chapter 1, the Microsoft 365 admin center configuration steps will walk you through making the necessary DNS changes with your registrar to provide domain ownership proof, typically in the form of a TXT record.

This TXT record can be removed once ownership is verified, and in many cases, the admin center configuration will automatically connect to your registrar and make the necessary addition if you provide credentials.

The network changes will need to be made manually by an authorized administrator if your public DNS infrastructure is managed internally or hosted on Microsoft Windows Server via the Domain Name Services role or another network appliance.

MX, SRV, and other DNS records

Once you have completed the setup process described previously using the Microsoft 365 admin center, your domain will automatically be registered in Microsoft 365, and it can be used as the domain suffix for the `UserPrincipalName` for the user login and Exchange Online mail

routing. This is because the automated configuration process will add MX records to your DNS configuration, allowing email to be delivered to Microsoft 365 automatically.

Additionally, the Exchange AutoDiscover, Sender Policy Framework (SPF), and required Server Resource (SRV) records will exist in Microsoft 365 tenant's initial domain namespace (tenant.onmicrosoft.com). These will allow Outlook and mobile client connectivity to your tenant and Teams client. Also, they will allow you to send and receive email directly to or from your tenant or communicate using Instant Message (IM) and Voice Over IP (VOIP) communications via Teams.

TIP

If your existing domain name (cohovineyards.us in this chapter's examples) is already configured with MX, SIP, SMTP, CNAME, or SPF records in your public DNS and routing to your on-premises infrastructure, you will want to select the manual configuration options in the previous configuration process and make only the necessary changes to support your Microsoft 365 setup.

NOTE

Additional configuration changes for Exchange mail routing as part of the Exchange or Teams hybrid processes are covered in later chapters and can be performed later so as not to impact existing functionality.

Firewall configurations

Microsoft 365 is a cloud-based solution, so it is a requirement that your internal infrastructure can communicate with your tenant without any connectivity issues introduced by your networking infrastructure.

If your internal infrastructure cannot communicate with Azure, your Microsoft 365 experience will be impacted—possibly resulting in email delays. Also, this can prevent you from authenticating and using services or provisioning or licensing users. It can even prevent access to cloud data.

It is strongly recommended that all network devices responsible for packet filtering, load balancing, and network port access control be configured to allow unrestricted outbound traffic to the Microsoft datacenters.

The Microsoft datacenter IP ranges include all the Microsoft 365 services and are maintained on the Microsoft 365 support site. The IP ranges can be viewed and downloaded here: https://aka.ms/M365_IPs

Proxy servers

Traditionally, proxy servers are used to relay requests to the Internet via a single host, though this behavior can create issues when setting up certain services for Microsoft 365 connectivity.

Primarily, traffic to Microsoft 365 is outbound traffic. Some services, like Exchange AutoDiscover, AD FS authentication, and mail routing, might be an exception; however, it is important to understand that proxy server configurations can cause interruptions.

Many proxy servers or services rely on some form of user authentication (either explicit or implicit) to allow the infrastructure to track users and filter requests according to business requirements. This proxy authentication feature primarily impacts directory synchronization.

The directory synchronization process, performed by the AAD Connect tool, connects to Microsoft 365 every 30 minutes to synchronize any directory updates. Additionally, depending on the AAD Connect tool's configuration, it will retrieve password changes and other data. If the connectivity between AAD Connect and Microsoft 365 is affected, the synchronization might fail, resulting in incomplete data in Microsoft 365.

Therefore, we recommend the AAD Connect tool be exempted from any proxy server configurations and allowed to communicate with Azure without any proxy configuration.

CAUTION

The AAD Connect tool does not support authenticated proxy servers. Instead, you must bypass any authenticated proxy servers, or you will be unable to synchronize your directories with Microsoft 365.

If you cannot bypass proxy servers for the AAD Connect implementation, we recommend configuring both Internet Explorer and the shell to use the same proxy server. Both methods are used during the AAD Connect setup for communication with Microsoft 365, so failure to enable both might result in a failed installation.

To set up Internet Explorer on the server where the synchronization tool will be installed, you will need to do the following:

1. Launch Internet Explorer.
2. Select Tools and Internet Options from the Internet Explorer main menu.
3. Select Connections > LAN Settings from the Internet Options menu.
4. Make sure the Proxy Server box is checked and a proxy server and port are provided in the Address and Port fields, as shown in Figure 2-9.

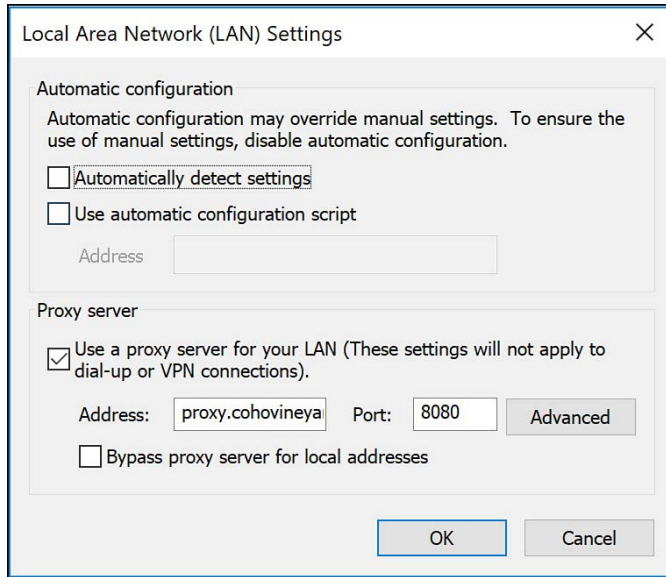


Figure 2-9 Configuring Internet Explorer proxy server

5. Click OK to close the Local Area Network (LAN) Settings dialog box and OK again to close the Connections dialog box.

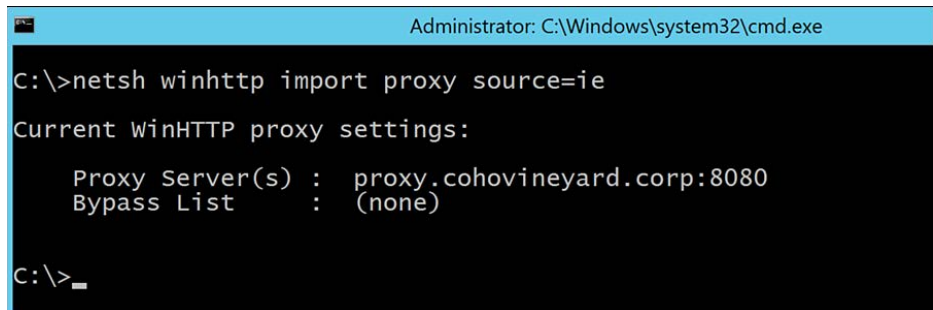
Once the proxy server has been properly configured in Internet Explorer, perform the following steps to configure the proxy server for the Windows Shell:

1. Open an administrative command prompt by clicking Start, Run (or Win+R), typing CMD. EXE, and pressing Enter.
2. Enter the `netsh winhttp show proxy` command and press Enter.
3. If the command returns the `Direct access (no proxy server)` result, as shown in Figure 2-10, proceed to the next step to configure the proxy server.

```
Administrator: C:\Windows\system32\cmd.exe
C:\>netsh winhttp show proxy
Current WinHTTP proxy settings:
    Direct access (no proxy server).
C:\>_
```

Figure 2-10 Displaying current WinHTTP proxy server configuration

4. Enter the Netsh WinHTTP Import proxy Source=IE command and press Enter.
5. If the command completes successfully, it should display the same proxy server that is configured in Internet Explorer, as seen in Figure 2-11.



```

Administrator: C:\Windows\system32\cmd.exe

C:\>netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) : proxy.cohovineyard.corp:8080
    Bypass List      : (none)

C:\>

```

Figure 2-11 Configuring Netsh proxy using Internet Explorer

6. Finally, in some circumstances, it might also be necessary to modify the `machine.config` file used by the Windows .Net configuration to also define the proxy server that should be used by any .Net applications.

If the AAD Connect setup fails to properly communicate with Azure—even after the settings in Internet Explorer and the Windows Shell have been configured—the .Net configuration file can be modified via the following steps:

1. On the AAD Connect server, navigate to `C:\Windows\Microsoft.NET\Framework64\v4.xxxxxx\Config`, where `x4.xxxxx` is the `v4.0` or `v4.5` directory located under the `Framework64` folder. This directory name will depend upon the .Net 4 version installed on your AAD Connect server.
2. Edit the `machine.config` file, shown in Figure 2-12, using Notepad.

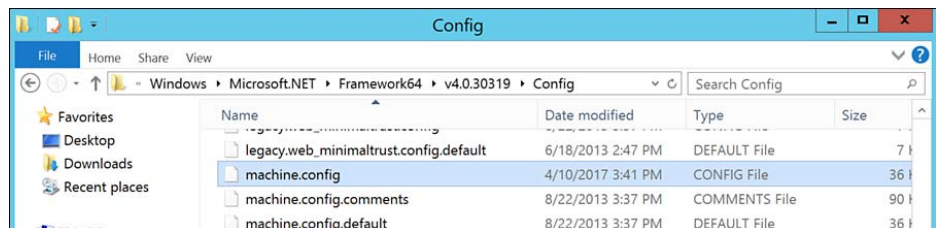
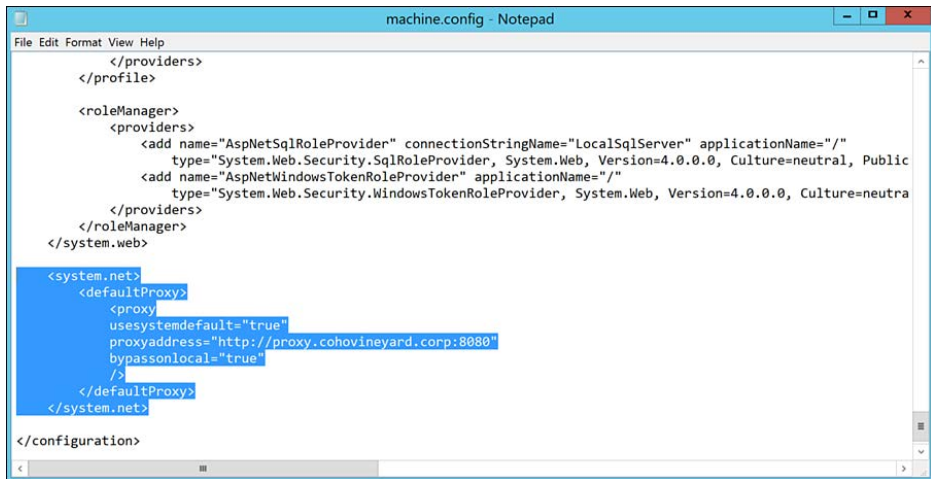


Figure 2-12 The Microsoft .Net machine.config file location

- At the bottom of the file, insert the following block of text before the `</configuration>` line, substituting `<PROXYADDRESS>` with the name or IP address of your proxy server and `<PROXYPORT>` with the correct port number:

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy
      usesystemdefault="true"
      proxyaddress="http://<PROXYADDRESS>:<PROXYPORT>"
      bypassonlocal="true"
    />
  </defaultProxy>
</system.net>
```

- Save the updated file, as shown in Figure 2-13.



```
File Edit Format View Help
</providers>
</profile>
<roleManager>
  <providers>
    <add name="AspNetSqlRoleProvider" connectionStringName="LocalSqlServer" applicationName="/"
      type="System.Web.Security.SqlRoleProvider, System.Web, Version=4.0.0.0, Culture=neutral, Public
    <add name="AspNetWindowsTokenRoleProvider" applicationName="/"
      type="System.Web.Security.WindowsTokenRoleProvider, System.Web, Version=4.0.0.0, Culture=neutra
    </providers>
  </roleManager>
</system.web>
<system.net>
  <defaultProxy>
    <proxy
      usesystemdefault="true"
      proxyaddress="http://proxy.cohovineyard.corp:8080"
      bypassonlocal="true"
    />
  </defaultProxy>
</system.net>
</configuration>
```

Figure 2-13 The machine.config file, updated to include default proxy information

- Once the proxy server configurations have been made to Internet Explorer, the Windows Shell, and the .Net configuration, you may proceed with installing and configuring the AAD Connect tool for directory synchronization.

Network tracing

Occasionally, during the implementation or configuration of proxy server or network firewall changes, it might be necessary to review the communication between your application and Microsoft 365. Understanding the route that Microsoft 365 communication must take to reach Azure will help troubleshoot network connectivity issues.

Other than mailbox moves, the synchronization process is the most common reason for connectivity tracing with Microsoft 365. Unless configured differently, the AAD Connect sync engine

will connect to Azure every 30 minutes to synchronize directory changes from on-premises to the cloud.

Depending on the additional features selected during installation, the AAD Connect engine might connect as frequently as every 1 to 2 minutes to retrieve password change and other authentication requests from the Azure service bus.

If you need to review traffic between your AAD Connect server and Microsoft 365, you can use tools like NetMon3, Fiddler, or WireShark to capture network traces from the server to ensure no other devices are preventing proper communication.

In the example below, we are using Fiddler to capture and import from the Microsoft 365 tenant using the AAD Connect tool. Fiddler is installed on the AAD Connect server and has been configured to decrypt HTTPS traffic.

The trace was captured by using the following steps:

1. Download and install Fiddler (<https://www.telerik.com/fiddler/fiddler-everywhere>).
2. Launch Fiddler and press F12, or select File and choose Capture Traffic.
3. Start the AAD Connect Synchronization Service Manager.
4. Select Connectors.
5. In the Connections window, select the Windows Azure Active Directory connector.
6. In the Actions pane, select Run.
7. Choose Full Import and click OK, as shown in Figure 2-14.

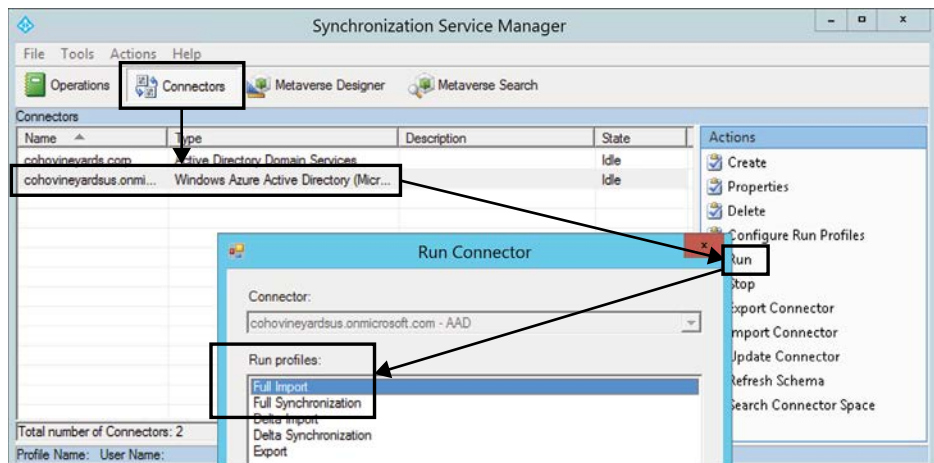


Figure 2-14 Starting a Full Import on the Azure Connector in AAD Connect

- Once the Full Import has been completed, review the results of the Fiddler trace, as shown in Figure 2-15.

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process
1	200	HTTP	Tunnel to	login.windows.net:443	0			miserver:1876
2	200	HTTPS	login.windows.net	/common/UserRealm/Sync_COHOVINEYARD-DC_c8cd2f06f4ae@cohovineyard.onmicrosoft.com...	181	private	application/...	miserver:1876
3	200	HTTPS	login.windows.net	/cohovineyard.onmicrosoft.com/oauth2/token	3,434	no-cac...	application/...	miserver:1876
4	200	HTTP	Tunnel to	adminwebservice.microsoftonline.com:443	0			miserver:1876
5	200	HTTPS	adminwebservice.mi...	/provisioningservice.svc	192,438		application/...	miserver:1876
6	200	HTTP	Tunnel to	adminwebservice.microsoftonline.com:443	0			miserver:1876
7	200	HTTPS	adminwebservice.mi...	/provisioningservice.svc	192,398		application/...	miserver:1876
8	200	HTTP	Tunnel to	adminwebservice.microsoftonline.com:443	0			miserver:1876
9	200	HTTPS	adminwebservice.mi...	/provisioningservice.svc	192,445		application/...	miserver:1876
10	200	HTTP	Tunnel to	adminwebservice.microsoftonline.com:443	0			miserver:1876
11	200	HTTPS	adminwebservice.mi...	/provisioningservice.svc	192,435		application/...	miserver:1876
12	200	HTTP	Tunnel to	adminwebservice.microsoftonline.com:443	0			miserver:1876

Figure 2-15 Fiddler trace of the AAD Connect Full Import run step

In the screen capture above, each line represents a packet in the communication between the AAD Connect server and Azure Active Directory. The packets are performing the following actions:

- Communication is established between the synchronization engine and Azure via the `login.windows.net` URL over secure SSL port 443.
- Home realm discovery is initiated using the `Sync_COHOVINEYARD-DC_c8cd2f06f4ae@cohovineyard.onmicrosoft.com` account. This account, discussed in detail in Chapter 4, is the account used to authenticate with Microsoft 365 for synchronization.
- The home realm discovery process results in an authentication token with the `cohovineyard.onmicrosoft.com` tenant.
- The synchronization engine is redirected to the `adminwebservice.microsoftonline.com` URL over secure SSL port 443.
- The synchronization engine begins reading data from the `adminwebservice.microsoftonline.com/provisioningservice.svc` endpoint URL, which returns the tenant data to the sync engine.
- The process continues until all the directory data has been read from the Microsoft 365 tenant into the Azure connector in the synchronization engine, at which point, communication ceases.
- As you can see from the preceding example, despite the existence of a proxy server in the configuration, there was no effect on the traffic between the synchronization engine and the Microsoft 365 tenant. If there had been issues with the traffic, you would have experienced retransmissions or transmission failures like the example in Figure 2-16.

Inside Out

Do I need ExpressRoute?

Microsoft 365 services are designed to work best over the Internet because the multi-pathing characteristics of the Internet provide the best service routes and reliability. Microsoft does not recommend using ExpressRoute to connect to Office 365 or Microsoft 365 services. Purchasing ExpressRoute for Microsoft 365 requires Microsoft approval. For more information, see <https://aka.ms/erguide>.

If you are considering ExpressRoute connectivity to the Microsoft cloud during your implementation of Microsoft 365, we strongly recommend implementation be done before the rest of your Microsoft 365 readiness milestones. An ExpressRoute implementation changes your network routing internally and affects things like load balancers, proxy servers, and firewalls. These changes will affect communication, so they should be made before establishing synchronization and starting mailbox migrations.

Preparing your directories

Much like preparing your network for a successful Microsoft 365 implementation, it is equally important to ensure that your on-premises directories are free from any issues that might impact a successful synchronization of users, groups, and contacts to your tenant.

Microsoft provides the IDFix tool, which will review your environment and highlight any problem areas or data inconsistencies. Follow these steps to install IDFix:

1. Download the IDFix setup media from <https://aka.ms/idfix> and launch it.
2. Launch the IDFix setup media and click Install, as shown in Figure 2-17.
3. If prompted with an Open File–Security Warning, as shown in Figure 2-18, click Run to proceed with the installation.

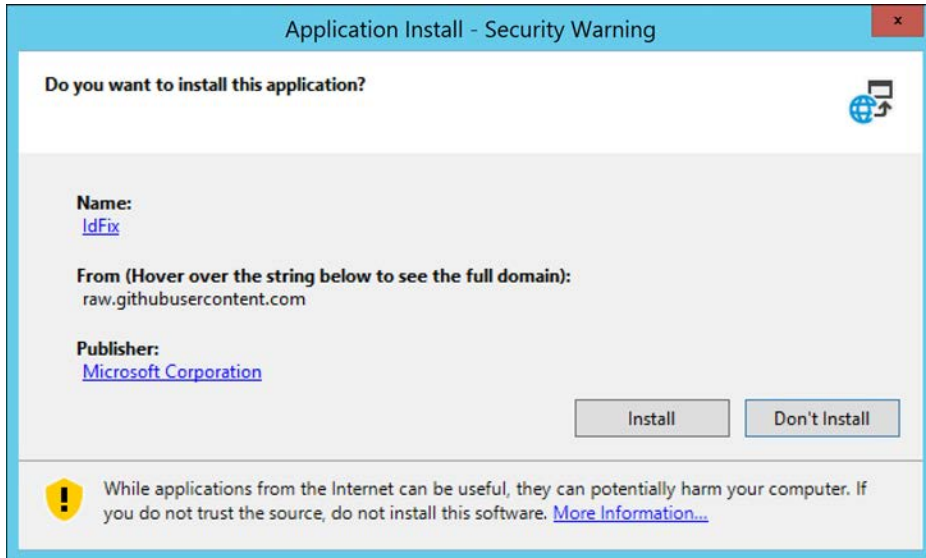


Figure 2-17 Application Install Security Warning dialog

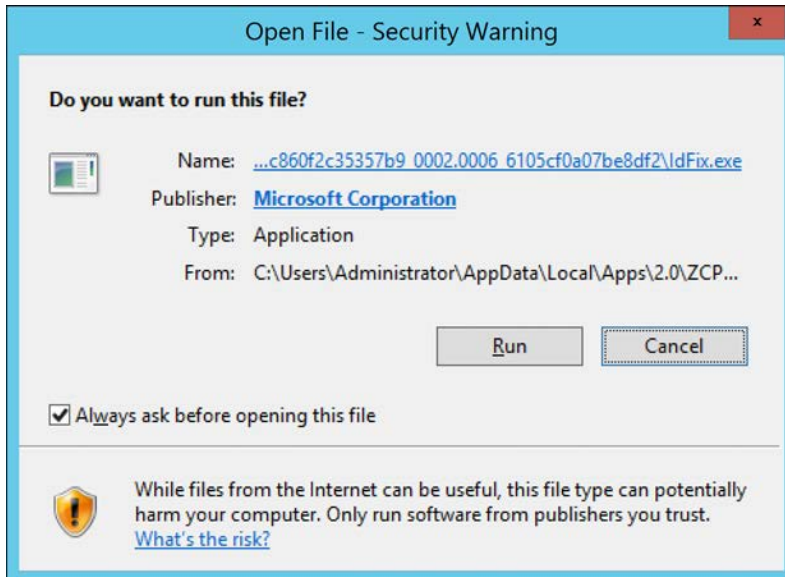


Figure 2-18 Open File Security Warning dialog

4. Click OK to proceed past the IdFix Privacy Statement dialog shown in Figure 2-19. This dialog is displayed because the IDFix application will review your data and provide reports containing sensitive information.

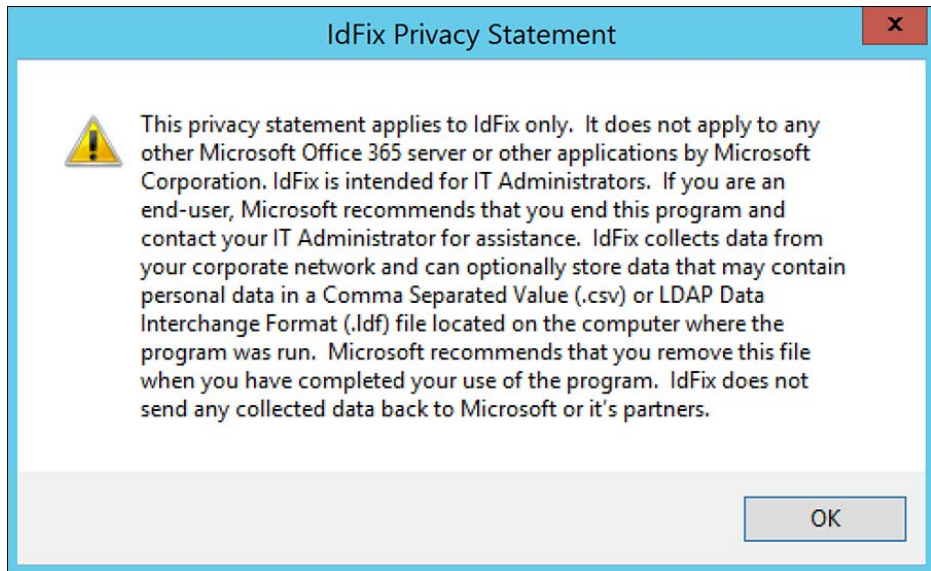


Figure 2-19 The IDFix Privacy Statement

5. Select the Query option from the topmost menu, as shown in Figure 2-20.

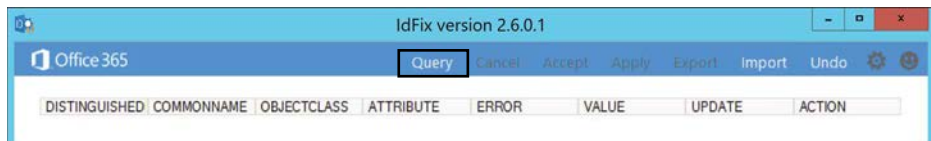


Figure 2-20 The IDFix tool main menu

6. While the query is running, a status will be displayed in the lower-left corner.
7. As shown in Figure 2-21, once the query has been completed, a list of all detected issues will be displayed with an error description for each. The total object and error counts will be displayed in the lower-left corner.

DISTINGUISHED	COMMONNAME	OBJECTCLASS	ATTRIBUTE	ERROR	VALUE	UPDATE	ACTION
CN=Tom O'Neill...	Tom O'Neill	user	userPrincipalNa...	Character	Tom.O'Neill@C...	Tom.O'Neill@C...	
CN=Reuben D'sa...	Reuben D'sa	user	userPrincipalNa...	Character	Reuben.D'sa@...	Reuben.Dsa@...	
CN=Erin O'Connell...	Erin O'Connell	user	userPrincipalNa...	Character	Erin.O'Connell...	Erin.O'Connell@...	
CN=Jr. Smith,O...	Jr. Smith	user	proxyAddresses	Format, LocalPart	SMTP:Jr.Smith...	SMTP:Jr.Smith...	
CN=Jr. Bacon...	Jr. Bacon	user	userPrincipalNa...	Format, LocalPart	Jr.Bacon@Co...	Jr.Bacon@Coh...	
CN=B.J. Haberkom...	B.J. Haberkom	user	userPrincipalNa...	Format, LocalPart	B.J.Haberkom...	B.J.Haberkom...	
CN=Jr. Smith,O...	Jr. Smith	user	userPrincipalNa...	Format, LocalPart	Jr.Smith@Coh...	Jr.Smith@Coh...	
CN=Jr. Bacon...	Jr. Bacon	user	proxyAddresses	Format, LocalPart	SMTP:Jr.Baco...	SMTP:Jr.Baco...	
CN=B.J. Haberkom...	B.J. Haberkom	user	proxyAddresses	Format, LocalPart	SMTP:B.J.Ha...	SMTP:B.J.Hab...	
CN=Bego H. Hurtado...	Bego H. Hurtado	user	userPrincipalNa...	LocalPart	Bego.H.Hurtad...	Bego.H.Hurtado...	
CN=Bego H. Hurtado...	Bego H. Hurtado	user	proxyAddresses	LocalPart	SMTP:Bego.H...	SMTP:Bego.H...	
CN=Bjorn Tolle...	Bjorn Tolle	user	proxyAddresses	LocalPart	SMTP:Bjorn.T...	SMTP:Bjorn.Toll...	
CN=Castrejón J...	Castrejón Javier	user	proxyAddresses	LocalPart	SMTP:Castrej...	SMTP:Castrej...	
CN=Castrejón J...	Castrejón Javier	user	userPrincipalNa...	LocalPart	Castrejón.Javie...	Castrejón.Javie...	
CN=Bjorn Tolle...	Bjorn Tolle	user	userPrincipalNa...	LocalPart	Bjorn.Tolleve...	Bjorn.Tollevsen...	
CN=Daniel Koczka...	Daniel Koczka	user	userPrincipalNa...	LocalPart	Daniel.Koczka...	Daniel.Koczka@...	
CN=Daniel Koczka...	Daniel Koczka	user	proxyAddresses	LocalPart	SMTP:Dniel.Ko...	SMTP:Dniel.Ko...	
CN=Erzsébet B...	Erzsébet Balázs	user	proxyAddresses	LocalPart	SMTP:Erzsébe...	SMTP:Erzabet...	
CN=Erzsébet B...	Erzsébet Balázs	user	userPrincipalNa...	LocalPart	Erzsébet.Balá...	Erzabet.Balzs@...	
CN=Arturo López...	Arturo López	user	userPrincipalNa...	LocalPart	Arturo.Lopez@...	Arturo.Lpez@C...	
CN=Balázs Beli...	Balázs Belinski	user	proxyAddresses	LocalPart	SMTP:Balázs...	SMTP:Balzs.Be...	

Total Error Count: 85

Figure 2-21 IDFix error report summary

8. Selecting a single error will allow you to use the Action column to define the behavior that should be used to resolve it. As shown in Figure 2-22, you can choose to Edit, Remove, or Complete the object in question.

DISTINGUISHED	COMMONNAME	OBJECTCLASS	ATTRIBUTE	ERROR	VALUE	UPDATE	ACTION
CN=Tom O'Neill...	Tom O'Neill	user	userPrincipalNa...	Character	Tom.O'Neill@C...	Tom.O'Neill@C...	
CN=Reuben D'...	Reuben D'sa	user	userPrincipalNa...	Character	Reuben.D'sa@...	Reuben.Dsa@...	EDIT
CN=Erin O'Connell...	Erin O'Connell	user	userPrincipalNa...	Character	Erin.O'Connell...	Erin.O'Connell@...	
CN=Jr. Smith,O...	Jr. Smith	user	proxyAddresses	Format, LocalPart	SMTP:Jr.Smith...	SMTP:Jr.Smith...	
CN=Jr. Bacon...	Jr. Bacon	user	userPrincipalNa...	Format, LocalPart	Jr.Bacon@Co...	Jr.Bacon@Coh...	
CN=B.J. Haberkom...	B.J. Haberkom	user	userPrincipalNa...	Format, LocalPart	B.J.Haberkom...	B.J.Haberkom...	
CN=Jr. Smith,O...	Jr. Smith	user	userPrincipalNa...	Format, LocalPart	Jr.Smith@Coh...	Jr.Smith@Coh...	
CN=Jr. Bacon...	Jr. Bacon	user	proxyAddresses	Format, LocalPart	SMTP:Jr.Baco...	SMTP:Jr.Baco...	
CN=B.J. Haberkom...	B.J. Haberkom	user	proxyAddresses	Format, LocalPart	SMTP:B.J.Ha...	SMTP:B.J.Hab...	
CN=Bego H. Hurtado...	Bego H. Hurtado	user	userPrincipalNa...	LocalPart	Bego.H.Hurtad...	Bego.H.Hurtado...	
CN=Bego H. Hurtado...	Bego H. Hurtado	user	proxyAddresses	LocalPart	SMTP:Bego.H...	SMTP:Bego.H...	

Figure 2-22 Selecting actions for error objects in IDFix

9. Once you have selected the appropriate action for each object, selecting Apply at the top of the menu returns the confirmation dialog shown in Figure 2-23.

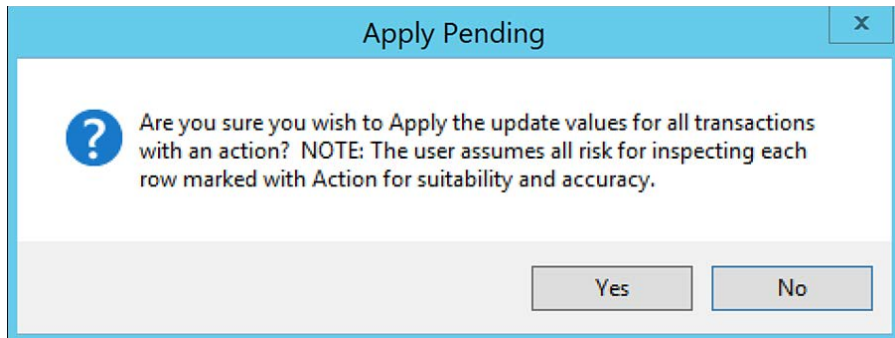


Figure 2-23 IDFix Apply Pending dialog

10. Click Yes to apply all selected updates.
11. Once complete, all updates that have been applied will be marked as Complete, as shown in Figure 2-24.

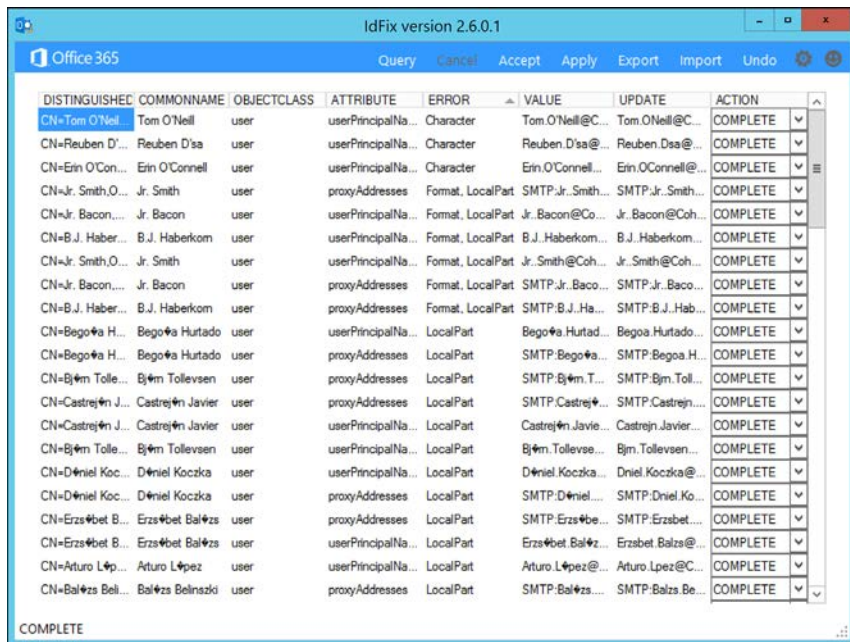


Figure 2-24 IDFix tool with Actions updated

12. Following are a few important notes:
 - When selecting Edit, you will not be allowed to edit the value in error manually. Instead, the IDFix tool will simply apply the update displayed in the Update column. You should review this new value below, allowing IDFix to make the change.

- Optionally, you can use the Accept option on the IDFix main menu to automatically apply the updated value shown in the Update column to each object in an error state, as shown in Figure 2-25.

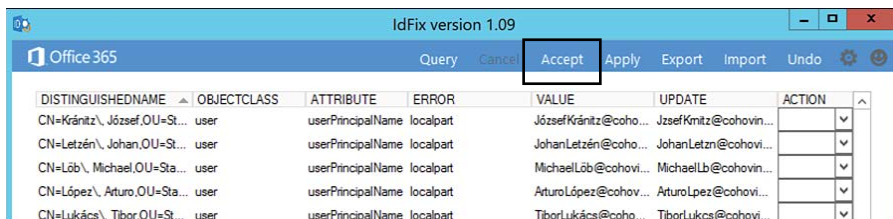


Figure 2-25 The IDFix Accept option

- Like the Apply option, the Accept option will also display a dialog warning that the changes being made represent a risk as they are changing data in your directory. See Figure 2-26.

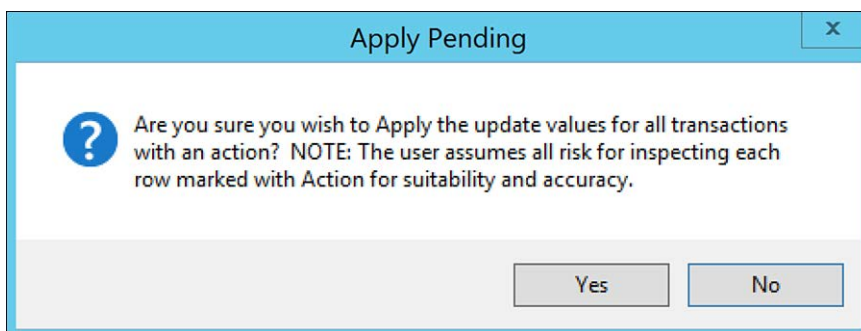


Figure 2-26 Apply Pending dialog

- Using the Accept All option in the Accept dropdown menu will simply change all Action fields to Edit, and it is then necessary to use the Apply option to make the changes.
- Once the changes have been applied, select Query to re-run the IDFix process against your directory and confirm no additional changes are required.

Updating and deploying client software

Before migrating mailboxes to Microsoft 365, any machines with Microsoft Outlook installed must be updated to the latest public update (PU) so there is no interruption in the user experience after mailbox migrations have begun.

Even a mailbox that has not yet migrated to Exchange Online might experience connectivity issues or constant credential prompts if that mailbox is delegated permission to another mailbox that HAS been migrated to Microsoft 365. For this reason, it is strongly recommended that Microsoft Office and Windows updates be approved and applied in advance of the Microsoft 365 implementation.

Frequently, customers will choose to apply the Microsoft 365 Apps license to all users ahead of the mailbox moves (or even SharePoint Online and Teams deployments) so all Microsoft Office versions are current and support the Microsoft 365 workloads.

Installing Microsoft 365 Apps

Installation of the Microsoft 365 Apps software is straightforward:

1. Log in to the Microsoft 365 portal at <https://portal.office.com>.
2. When prompted, log in to Microsoft 365 using your username and password.
3. On the Microsoft 365 portal page shown in Figure 2-27, select Install Office in the upper-right corner.

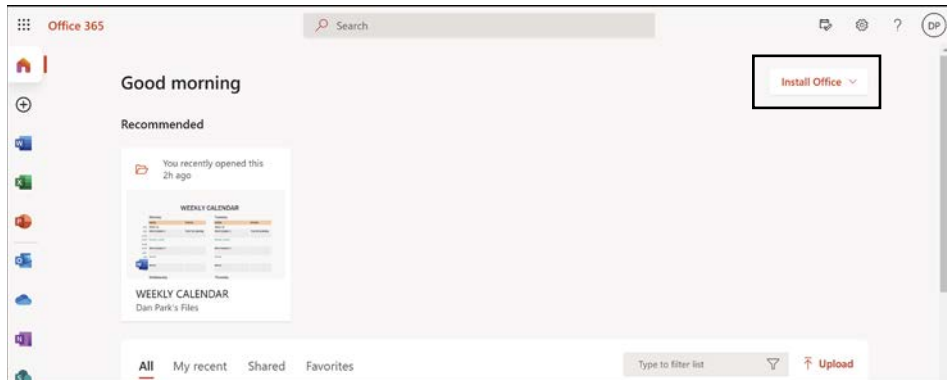


Figure 2-27 Installing Office from the Microsoft 365 portal

4. The Microsoft 365 portal will display additional information, as shown in Figure 2-28, which will assist in the Microsoft 365 Apps installation.
5. Click Run to begin the Microsoft 365 Apps installation.
6. If any conflicting software versions are already installed on the workstation, there is a lack of local disk space, or issues connecting to the Internet, you will receive a pop-up dialog showing the issue, as shown in Figure 2-29.

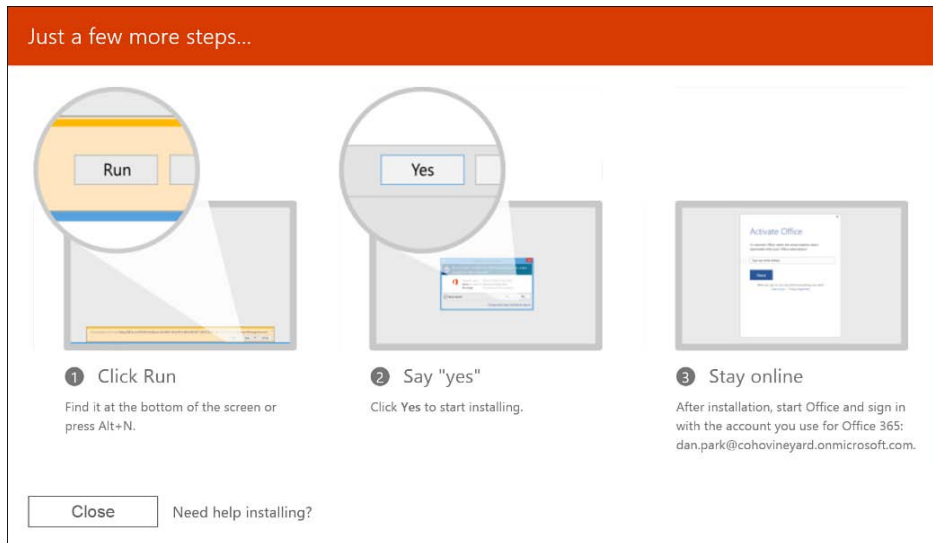


Figure 2-28 Microsoft 365 portal's Just A Few More Steps page

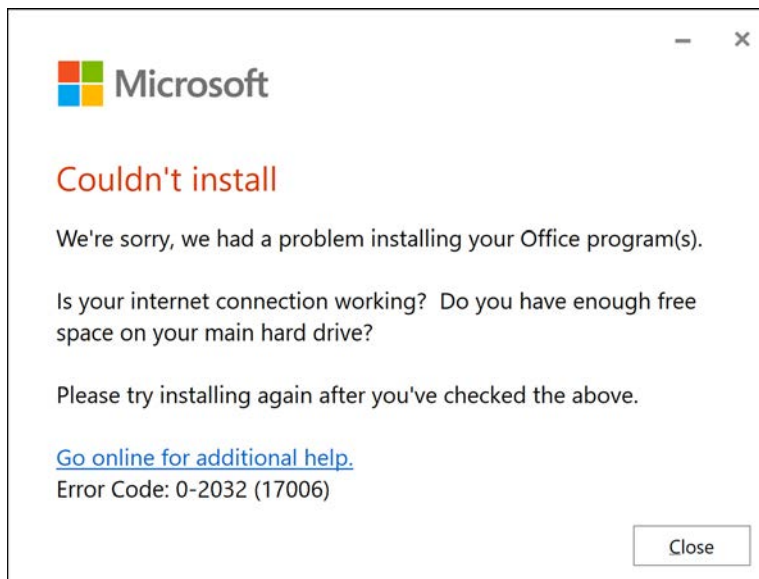


Figure 2-29 The Microsoft 365 Apps setup conflicts with existing installed versions

- If conflicting versions are already installed on the computer, you can click the I Understand box and select Install Anyway if you want to proceed with the installation. This will remove the conflicting software version(s) and proceed with the installation. Clicking I'll Wait will end the Office installation process.

7. As shown in Figure 2-30, once the installation has been completed, a new window will be displayed, indicating the installation is complete.

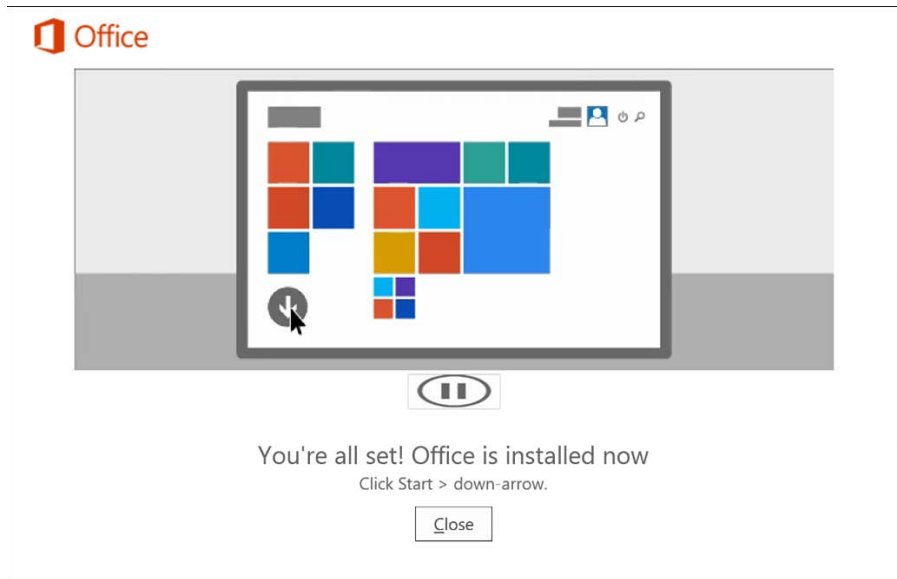


Figure 2-30 Microsoft 365 Apps installation completion page

8. Click Close to complete the installation process.

Once the installation is complete, the Office products will be available for use, and when applicable, you will be prompted to update any previous documents created in past versions of the applications.

Inside Out

Microsoft 365 Apps

Apps installed with the Microsoft 365 portal will be enabled for automatic updating. These updates will occur over the Internet, not via any internal automatic update services (such as Windows Server Update Services) configured in your organization. Microsoft also provides resources for centralized deployment of Microsoft 365 Apps using either Group Policy, System Center Configuration Manager, or Microsoft Endpoint Manager (Intune). You can learn more about additional deployment methods for Microsoft 365 Apps at <https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365>.

Activation

Activation is the last step and is a process whereby the Office application will connect to Microsoft 365 to ensure that the user is properly licensed by the tenant to use it.

The good news is that activation is automatic. No additional action is required on the user's part to activate their Office installation. Activation does, however, require that the computer has Internet access available to complete the process.

TIP

As you've already learned, Microsoft 365 Apps are typically licensed in a per-user model. (A per-device model is available under some license agreements, but it is outside the scope of this book.) Each user is entitled to five desktop installations. If you have roaming or shared computer scenarios, you might find that each time a user logs into a new machine, they consume one of their five allotted licenses. To account for this, you can configure Shared Computer Activation for those computers. User logins for Shared Computer Activation won't count against the user's total count. A user still must be licensed for Microsoft 365 Apps for Shared Computer Activation. Shared Computer Activation can be enabled through the setup configuration file or Group Policy. For more information, see <https://docs.microsoft.com/en-us/deployoffice/overview-shared-computer-activation>.

Once Office is installed on a user's workstation, the system will try daily to reach the Microsoft Office Licensing Service activation endpoint on the Internet. If it is unsuccessful, it will retry daily for up to 30 days before the applications enter reduced functionality mode.

In reduced functionality mode, the software will remain installed on the workstation, though your users will only be able to view and print documents. Any features related to document editing or the creation of new documents will remain disabled until they either enter a product key or successfully authenticate with Microsoft 365.

If Office cannot reach the licensing service for more than 30 days, the reduced functionality mode will display a Product Deactivated dialog screen, as shown in Figure 2-31.

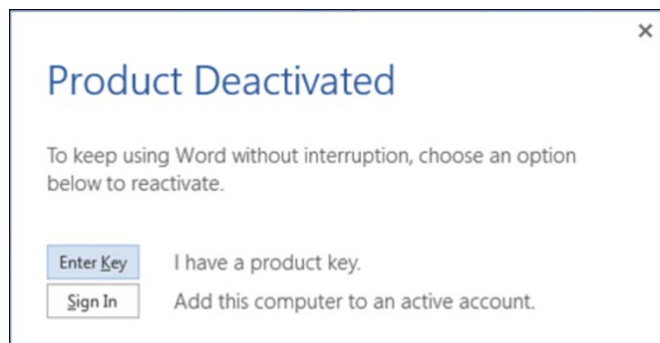


Figure 2-31 Product Deactivated dialog box

Synchronizing your users

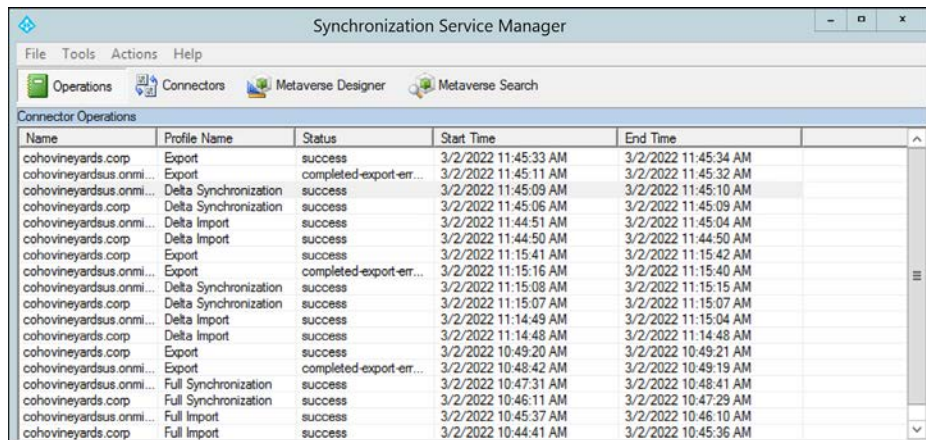
The next step in your deployment of Microsoft 365 will be the synchronization of your users to Azure Active Directory.

Synchronization is performed using the Azure Active Directory Connect tool, typically referred to as Azure AD Connect or AAD Connect. AAD Connect is a free download from Microsoft for Microsoft 365 users and is based upon the Microsoft Identity Manager (MIM) product line.

While simple in theory, the directory synchronization process can be very involved when installing and configuring the AAD Connect tool. In addition to selecting objects and organizational units, the AAD Connect tool can also be configured to support features like pass-through authentication, group writeback, password writeback, Exchange Hybrid writeback, and device writeback.

Chapter 9, “Identity and authentication planning,” and Chapter 10, “Installing AAD Connect,” contain an in-depth look into directory synchronization, features, and installation options.

Once the synchronization engine has been installed, it is important to pay attention to the synchronization statistics for each of the run profile steps on the Operations tab of the AAD Connect tool, as shown in Figure 2-32.



Name	Profile Name	Status	Start Time	End Time
cohovineyards.corp	Export	success	3/2/2022 11:45:33 AM	3/2/2022 11:45:34 AM
cohovineyards.onmi...	Export	completed-export-err...	3/2/2022 11:45:11 AM	3/2/2022 11:45:32 AM
cohovineyards.onmi...	Delta Synchronization	success	3/2/2022 11:45:09 AM	3/2/2022 11:45:10 AM
cohovineyards.corp	Delta Synchronization	success	3/2/2022 11:45:06 AM	3/2/2022 11:45:09 AM
cohovineyards.onmi...	Delta Import	success	3/2/2022 11:44:51 AM	3/2/2022 11:45:04 AM
cohovineyards.corp	Delta Import	success	3/2/2022 11:44:50 AM	3/2/2022 11:44:50 AM
cohovineyards.corp	Export	success	3/2/2022 11:15:41 AM	3/2/2022 11:15:42 AM
cohovineyards.onmi...	Export	completed-export-err...	3/2/2022 11:15:16 AM	3/2/2022 11:15:40 AM
cohovineyards.onmi...	Delta Synchronization	success	3/2/2022 11:15:08 AM	3/2/2022 11:15:15 AM
cohovineyards.corp	Delta Synchronization	success	3/2/2022 11:15:07 AM	3/2/2022 11:15:07 AM
cohovineyards.onmi...	Delta Import	success	3/2/2022 11:14:49 AM	3/2/2022 11:15:04 AM
cohovineyards.corp	Delta Import	success	3/2/2022 11:14:48 AM	3/2/2022 11:14:48 AM
cohovineyards.corp	Export	success	3/2/2022 10:49:20 AM	3/2/2022 10:49:21 AM
cohovineyards.onmi...	Export	completed-export-err...	3/2/2022 10:48:42 AM	3/2/2022 10:49:19 AM
cohovineyards.onmi...	Full Synchronization	success	3/2/2022 10:47:31 AM	3/2/2022 10:48:41 AM
cohovineyards.corp	Full Synchronization	success	3/2/2022 10:46:11 AM	3/2/2022 10:47:29 AM
cohovineyards.onmi...	Full Import	success	3/2/2022 10:45:37 AM	3/2/2022 10:46:10 AM
cohovineyards.corp	Full Import	success	3/2/2022 10:44:41 AM	3/2/2022 10:45:36 AM

Figure 2-32 The Operations view in AAD Connect

While it is important to review all errors reported in the Status column, those operations for the Azure connector, typically named `tenant.onmicrosoft.com`, should be reviewed carefully.

Any errors on the Azure connector will mean either bad or missing data in Microsoft 365. In fact, if the IDFix tool has been run and all issues are resolved before installation of the AAD Connect tool, the Azure connector should not show any errors related to data problems.

If errors do appear in the synchronization statistics view, the data provided there might not be sufficient to diagnose the issue adequately. In those cases, we recommend reviewing the Application Event Log for more detail.

While it's not 100 percent inclusive of events returned by the AAD Connect engine (primarily because the tool is constantly evolving and maturing), this data represents the most common and important events that should be reviewed and included in any event log monitoring utilities.

Licensing your users

Once a cloud user has been created, and you have started synchronizing identities to your tenant, you will need to assign licenses to your users before they can begin consuming Microsoft 365 services.

Licensing plans and subscriptions were explained in detail in Chapter 1, though there are several methods available for licensing users in Microsoft 365. It is important to understand each available method so you can pick the best option for you. Currently, there are three primary methods for license assignment in Microsoft 365:

- Azure Active Directory group-based licensing
- PowerShell licensing cmdlets included in the MSOnline PowerShell module
- Manual licensing via the Microsoft 365 portal

Group-based licensing

One of the most popular features available for licensing in Microsoft 365 is group-based licensing, commonly referred to as GBL.

Group-based licensing is a feature that requires either Azure AD Premium Plan 1 or Azure AD Premium Plan 2. It is one of the quickest, easiest, and most effective ways to manage Azure AD licenses. As the name implies, group-based licensing uses Azure AD groups for the assignment of licenses to users.

Licenses are assigned to either security groups, which are synchronized to Azure via the Azure AD Connect tool, or to cloud-only groups created directly in Azure.

In the example shown in Figure 2-33, an on-premises security group and its membership has been synchronized to Azure AD, and the Exchange Online Enterprise E3 license is assigned (1 of 26 enabled services).

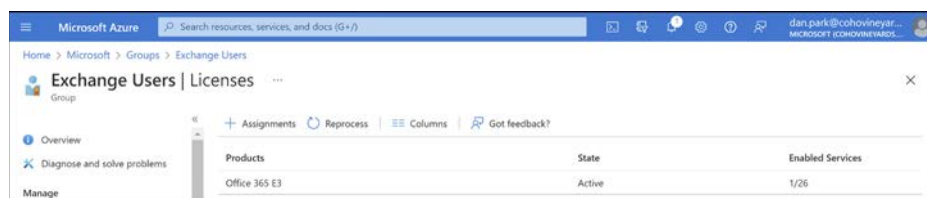


Figure 2-33 Group-based license assignment in the Azure portal

Additionally, dynamic groups can be created in the Azure portal and configured to define membership based on synchronized attributes. The creation of Azure AD dynamic groups, shown in Figure 2-34, requires an Azure AD Premium license.

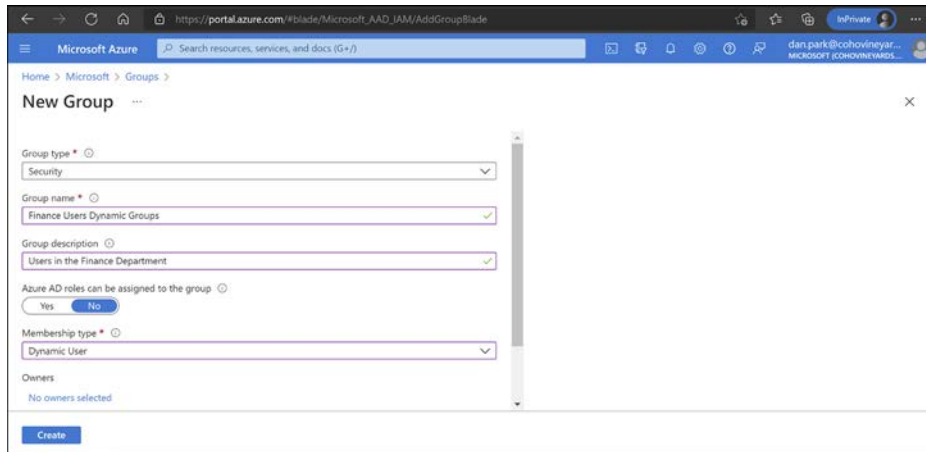


Figure 2-34 Creating a dynamic group in the Azure portal

Once a dynamic group has been created in the Azure portal, the group can then be used for automatic license assignment via group-based licensing, as shown in Figure 2-35.

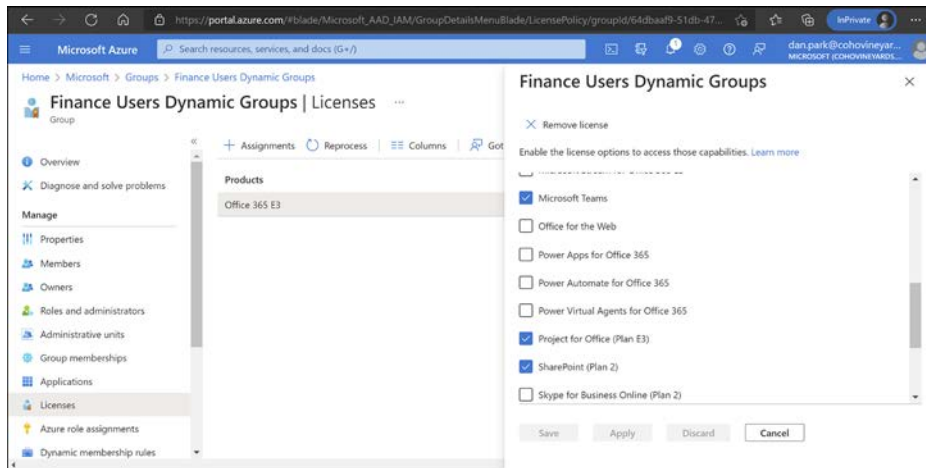


Figure 2-35 Assigning licenses to an Azure dynamic group

It is important to note the following details regarding Azure AD group-based licensing:

- All existing Microsoft Azure license types are supported by Azure AD group-based licensing.

- Group membership updates made in on-premises groups synced to Azure AD are effective within just a few minutes of a membership change.
- Users can be members of multiple groups, and licenses across groups are combined.
- If no licenses are available within the tenant, group-based licensing will be unable to assign licenses to a user, and no error will be returned.
- Licenses assigned via a group cannot be manually removed via PowerShell or the portal.
- Users can have licenses assigned via multiple groups or direct assignment (PowerShell and manual).
- Users can have licenses through multiple means, such as manual licensing applied through PowerShell or group-based licensing.

PowerShell licensing

The second licensing method is using the provided PowerShell cmdlets in the Azure Active Directory PowerShell for Graph module.

This Powershell module includes several cmdlets that can be used for user license assignment in Azure AD. These cmdlets can assign users SKUs and enable or disable specific plans under the SKU.

1. All users must have a Usage Location assigned to be licensed. Define the list of sub-plans that you wish to have disabled (not enabled) and assign the options directly to the user.
2. A user's Usage Location is set automatically via the AAD Connect tool, provided the `msExchUsageLocation` value in the on-premises Active Directory is populated with a valid two-digit ISO country code. If the value is not set, the AAD Connect tool can be customized to synchronize any other Active Directory attribute (such as `CountryCode`) as Usage Location, provided it is a valid two-digit ISO country code.
3. If the Usage Location is not set via AAD Connect, it can be set programmatically using the Azure Active Directory PowerShell for Graph cmdlets as follows:

```
Set-AzureADUser -ObjectId userUPN@domain.com -UsageLocation YY
```

In the example shown in Figure 2-36, the user Pilar Ackerman's Usage Location has been set to US.



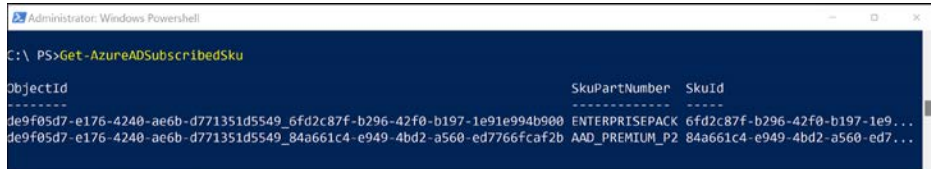
```
Administrator: Windows Powershell
C:\PS> Set-AzureADUser -ObjectId pilar.ackerman@cohovineyards.us -UsageLocation US
```

Figure 2-36 Setting UsageLocation via PowerShell

- Next, it is necessary to retrieve a list of Subscribed SKUs available in the tenant; these can be identified using the following command:

```
Get-AzureADSubscribedSkus
```

- As shown in Figure 2-37, the `Get-AzureADSubscribedSkus` command returns a list of the `SkuIds` and their `ObjectIds` for licenses available in the tenant.



```
Administrator: Windows PowerShell
C:\> PS>Get-AzureADSubscribedSkus

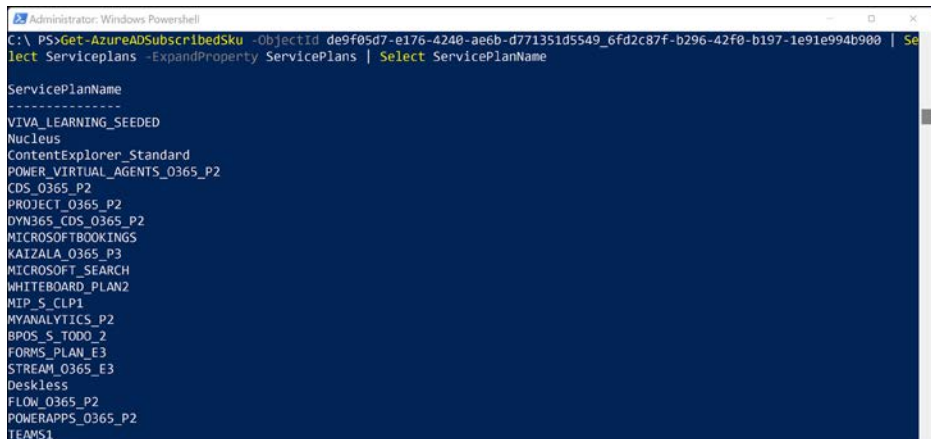
ObjectId                                     SkuPartNumber  SkuId
-----
de9f05d7-e176-4240-ae6b-d771351d5549_6fd2c87f-b296-42f0-b197-1e91e994b900 ENTERPRISEPACK 6fd2c87f-b296-42f0-b197-1e9...
de9f05d7-e176-4240-ae6b-d771351d5549_84a661c4-e949-4bd2-a560-ed7766fc2b AAD_PREMIUM_P2 84a661c4-e949-4bd2-a560-ed7...
```

Figure 2-37 Returning a list of Azure SKUs available in a tenant

- Next, it is necessary to retrieve a list of service plans available for a particular SKU so they can be assigned to a user. The list of service plans available can be displayed using the following command:

```
Get-AzureADSubscribedSkus -ObjectId <ObjectID of the desired SKU>
```

- In Figure 2-38, you can see that the `Get-AzureADSubscribedSkus` command is used in conjunction with a `Select` statement to return a list of service plans.



```
Administrator: Windows PowerShell
C:\> PS>Get-AzureADSubscribedSkus -ObjectId de9f05d7-e176-4240-ae6b-d771351d5549_6fd2c87f-b296-42f0-b197-1e91e994b900 | Se
lect Serviceplans -ExpandProperty ServicePlans | Select ServicePlanName

ServicePlanName
-----
VIVA_LEARNING_SEEDED
Nucleus
ContentExplorer_Standard
POWER_VIRTUAL_AGENTS_0365_P2
CDS_0365_P2
PROJECT_0365_P2
DYN365_CDS_0365_P2
MICROSOFTBOOKINGS
KATZALA_0365_P3
MICROSOFT_SEARCH
WHITEBOARD_PLAN2
MIP_5_CLP1
MYANALYTICS_P2
BPOS_5_TODO_2
FORMS_PLAN_E3
STREAM_0365_E3
Deskless
FLOW_0365_P2
POWERAPPS_0365_P2
TEAMS1
```

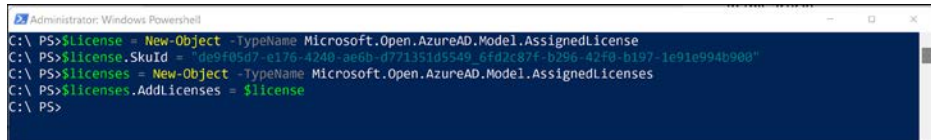
Figure 2-38 Returning a list of service plans from a SubscribedSku

- Once a `SubscribedSku` Object ID and service plan name has been identified, the license can be assigned to a user with the following command:

```
Set-AzureADUserLicense -ObjectId <user UPN> -AssignedLicenses $LicenseObject
```

- To create the LicenseObject needed for license assignment, it is necessary to create an Azure AD License object that can be applied to the user. In Figure 2-39, you can see the steps necessary to set the License and LicenseObject.

```
$License = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
$License.SkuId = "SkuID of the license you wish to assign"
$Licenses = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
$Licenses.AddLicenses = $License
```

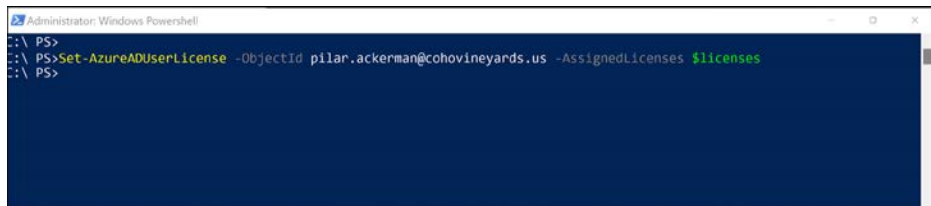


```
Administrator: Windows PowerShell
C:\ PS> $License = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
C:\ PS> $License.SkuId = "de9f85d7-e175-4240-ae6b-d771351d5549_6fd2c87f-b296-42f8-b197-1e91e994b908"
C:\ PS> $Licenses = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
C:\ PS> $Licenses.AddLicenses = $License
C:\ PS>
```

Figure 2-39 Creating a LicenseObject for user assignment

- Finally, the License object created in the previous step can be used with the following command to assign the License object to the user, as shown below and in Figure 2-40:

```
Set-AzureADUserLicense -ObjectID <User UPN> -AssignedLicenses $Licenses
```



```
Administrator: Windows PowerShell
::\ PS>
::\ PS> Set-AzureADUserLicense -ObjectID pilar.ackerman@cohovineyards.us -AssignedLicenses $Licenses
::\ PS>
```

Figure 2-40 Assigning a license to a user with Powershell

Manual license assignment

The final method available for license assignment is using the Microsoft 365 portal to assign user licenses manually.

Manual license assignment can be done on an individual user basis by selecting the user and editing assigned licenses or by selecting multiple users, as shown in Figure 2-41.

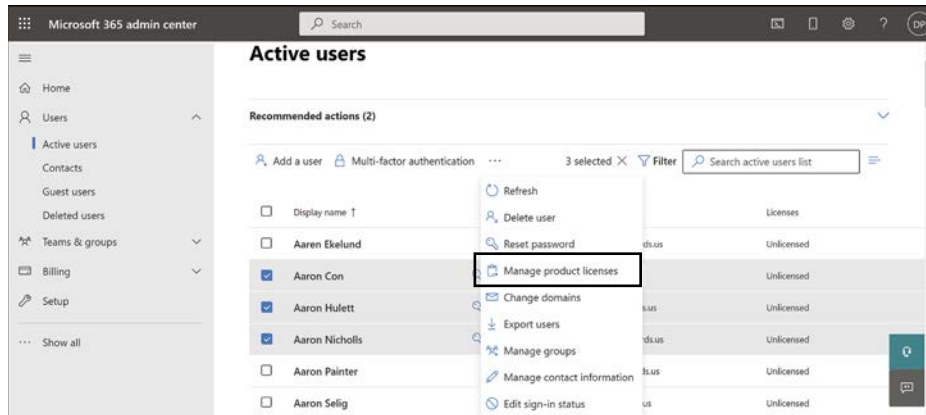


Figure 2-41 Bulk user license assignment via the Microsoft 365 portal

While the ability to assign user licenses is available via the Microsoft 365 portal for both individual and bulk assignment, it does not typically scale well for large organizations with many thousands of users. Also, it does not scale well with licensing requirements because doing so can create the need to assign licenses in various combinations based on role, location, or department.

This is why the manual assignment of licenses should be used on an ad-hoc basis and as a supplement to one of the other options for license assignment.

What's next?

Now that we have discussed the major milestones involved in your Microsoft 365 tenant setup and provided guidance on each of these steps, we will move on to discussing more advanced topics such as Federation, Directory Synchronization, Exchange Hybrid setup, and tasks that will be required to help you get the most from your Microsoft 365 experience.



Index

Symbols

2FA (two-factor authentication), 192

100,000 items, SQL Server, 269–270

A

AAA (Authentication, Authorization, Accounting), 66

AAD Connect, 8, 346

Custom installation, 267

Azure AD app and attribute filtering, 326–328

completion, 339

directories, 284–286

Domain And OU Filtering dialog, 289–290

GalSync, 299–313

group filtering, 322, 324

joins, custom, 316–318

location, 268

MailNickname, 313–316

Optional Features, 325–337

Option Features, 326, 331, 335

Password Synchronization, 273–278, 280–281, 283

SamAccountName, 313–316

service accounts, 270–272

Source Anchor attribute, 319–322

SQL Server, 269–270

Staging Mode, 340–341

synchronization, 340–343

synchronization settings, 272

Uniquely Identifying Your Users dialog, 290–299

UPN suffixes, 287–290

Express mode installation, 259–260, 265

Active Directory account, 263

Configuration Complete dialog, 267

credentials, 261

directory synchronization, 262

Exchange Hybrid deployment, 266

Global Administrator, 261

OU (organizational unit), 263

Replicating Directory Changes, 264

SQL Express and, 266

synchronization, 266

.NET configuration file, 43

Password Writeback, 398

enabling, 398–403

requirements, 398

proxy servers and, 41

SourceAnchor

migration, 382–388

mS-DS-ConsistencyGuid and, 382–394

sync engine, connections, 45

synchronization, rule precedence, 404–412

traffic, reviewing, 45

user synchronization, 58–59

AADSync, 345

accepted domains, 443–444

access

Azure AD Conditional Access, 218, 220, 222

risk-based, 223–224, 227

channels, private, 772

channels (Teams), 772–777

Exchange Administrator, 8

Global Administrator, 8

Global Reader, 8

Helpdesk Administrator, 8

read-only, 106

read/write, 106

risk-based, 194–195

Service Support Administrator, 9

SharePoint Administrator, 9

Teams Administrator, 9

User Administrator, 9

access control

SharePoint Online, 872–878

SharePoint Online admin center, 770–771

access control planes, 763–767, 769–771

access management lifecycle, 68

access protocols, migration, 451

Accidental Delete Threshold, 377

accounting, 66

activation, 57

Active Directory (AD)

forests, multi-forest environment, 26

RODC (read-only domain controller), 437

SCPs (service connection points), 432

syncing to Azure, 18

disabled users, 24

domains, 22–23

empty groups, 24

forests, 21

invalid characters, 20

MailNickname attribute, 19

SamAccountName attribute, 20–21

stale users, 23

unused groups, 24

UserPrincipalName attribute, 19

synchronization, users, 58–59

Active Directory forest, credentials, 262

ADD condition, 370

ADFS (Active Directory Federation Services), 255–257

AD FS components, 276–278

ADGMS (Active Directory Group Modernization Service), 445

ad hoc meetings (Teams), 610

admin center, Exchange Online, 546

AdminDescription attribute, 346

administrator access

Exchange Administrator, 8

Global Administrator, 8

Global Reader, 8

Helpdesk Administrator, 8

Service Support Administrator, 9

SharePoint Administrator, 9

Teams Administrator, 9

User Administrator, 9

administrators, assigning, 37–39

ADMS (Active Directory Migration Service), 397

AF (Assured Forwarding) model, network traffic, 659

App bar (Microsoft Teams), 601

Activity feed, 601–602

added apps, 606

App store, 607

Calendar app, 603

Calls app, 605

Chat app, 602–603

Download Mobile App, 607

Files view, 605

presence, 602–603

Teams view, 603

app launcher icon, 6

App Management service (SharePoint), hybrid integration setup, 822–823

app management, SharePoint Online, 889–890

ATA (Advanced Threat Analytics), 203

ATA (analog telephone adapter), 653

attribute flows, complex, 349

attributes

data sanitization, 365

email-related, 396

mail, 396

mappings

adding, 362–365

complex, 365–370

deleting, 360–361

editing, 361–362

migrations, 365

SourceAnchor, 349

audio conferencing (Teams Phone), 640

audio (Teams), 617–619

Audit log searches, 162, 164

authentication, 66

2FA (two-factor authentication), 192

AAD Connect Password Synchronization, 273–283

Azure Automation, 414

Conditional Access, 193

DKIM (Domain Keys Identified Mail), 572–573

Exchange, 10

Exchange Online, 10

hardware tokens, 193

IWA (Integrated Windows Authentication), 823

MFA (multifactor authentication), 192–193

MDI (Microsoft Defender for Identity), 214–218

notification, 218

OATH tokens, 193

pass-through, 274–276

passwords, 192

Azure AD, 249–253

synchronization, 273

PTA (pass-through authentication), 348

SharePoint Online Hybrid, 823–824

SSO (single sign-on), 283

text messages, 218

usernames, 192

verification code, 218

Authenticator App, 193**authorization, 66****Auto attendants (Teams Phone System), 749–750**

Call Flow, 752

Call Flow For After Hours, 755

Call Routing, 752

Dial By Extension, 754

Director Search, 754

greeting, 753, 756

operator options, 751

redirect, 753

Voice Command, 754

voice mail, 758–759

Autodiscover, 437, 458

configuration, 438

DNS and, 449

free/busy and, 461

hybrid public folders, 519

Autodiscover, Outlook, 432–434**Autodiscover URL, 586****Autodiscovery, HTTPS and, 434****automation. *See* Azure Automation****Azure**

Active Directory syncing, 18

*disabled users, 24**domains, 22–23**empty groups, 24**forests, 21**invalid characters, 20**MailNickname attribute, 19**SamAccountName attribute, 20–21**stale users, 23**unused groups, 24**UserPrincipleName attribute, 19*

MAPS (Microsoft Azure Peering Service), 654

Azure AD (Azure Active Directory)

AAD Connect tool, 237

controls, 74

governance and, 69–71

groups, 70

identities

*cloud, 238–241, 244–246**guest identities, 246–248**synchronized, 237–238**synchronized identities, 243*

identity federation, 254–257

*ADFS (Active Directory Federation Services), 255–257**configuration required, 255*

MTR (Microsoft Teams Rooms) deployment, 736

passwords, 249–253

rights, deleting, 70

user accounts, guest, 69

service account, 415–416

UserPrincipalName, 395–396

Azure AD Cloud Sync, 346

AAD Connect features not supported, 347

configuration, 355–356

*attribute mappings, 361–370**deletions, 377**enabling, 378**Expression Builder, 370–373**OUs, 357–359**provisioning users, 373–376**users, 357*

gMSA (Group Managed Service Account), 346

installation, 349, 352

*agent configuration, 354**directories, 354**Download Agent, 350**installation wizard, 351**Provisioning Agent, 350*

PHS (Password Hash Sync), 348

provisioning agents, 347

Azure AD Conditional Access, 218, 220–224, 227**Azure AD Connect**

Active Directory forests, 347

Exchange Online hybrid configuration, 458

Group Writeback, 446

synchronization engine, 21

*disabled users, 24**domains, 22–23**empty groups, 24**forests, 21**stale users, 23**unused groups, 24*

Azure AD Portal, external identity controls, 767–769

Azure Automation

- authentication, 414
- automation account
 - creating, 416–418*
 - credentials, 421–422*
 - modules, 418, 420–421*
- runbooks
 - graphical, 414*
 - graphical PowerShell workflow, 414*
 - Hybrid Runbook Worker, 414*
 - PowerShell, 413, 422–429*
 - PowerShell workflow, 413*
 - Python, 414*
- service account, 415–416
- webhooks, 414

Azure automation account

- creating, 416–418*
- credentials, 421–422*
- modules, 418, 420–421*

Azure Data box, 849

B

bandwidth, 448

- Teams Phone, 656

Basic Authentication, enabling, 515–517

BCS (Business Connectivity Services), 12

Best Practices Analyzer, 440

blocked accounts, spam filtering and, 581

blocking phone numbers, 702–703

body pane (Microsoft Teams), 601

Business Basic plan, 2

Business Connectivity Services (SharePoint Online), 789, 893

- Hybrid picker, 903–904
- Infopath, 903
- Manage BDC Models And External Content Types, 894
- Manage Connections To Online Services, 895
- Records Management, 897–903
- Secure Store, 896

Business Premium plan, 2

Business Standard plan, 2

BYOK (Bring Your Own Key), 203

C

Calendar app (Teams), 610

calendar (Exchange Online)

- automatic processing, 552–553
- booking policies, 552
- users, mail-enabled users, 553

calendar processing, migration and, 451

calendars, Microsoft Teams, 594

caller ID (Teams Phone), 643

caller ID (Teams Phone System), 716–718

Calling Plans, 647–648, 672

calling policies (Teams Phone System), 706

- assigning, 709–711
- configuring, 707–709

calling restrictions (Teams Phone System), 701

- inbound calling, 701–702
 - blocking numbers, 702*
 - exceptions, 703*
 - unblocking numbers, 703*
- outbound calling, 703–705

call parking (Teams Phone System), 712

- park and pick up, 712–714
- policies, 714–716

call queues (Teams Phone System), 743–744

- Call Overflow Handling, 747
- Conference Mode, 746
- greeting, 745–746
- prerequisites, 743
- Presence-Based Routing, 747
- Routing Method, 747
- timeout handling, 748

CASB (Cloud Access Security Broker), 204

CAS (Client Access Server), 14, 457

CDN (Content Delivery Network), 630–633

Central Mail Transport, 566–567

certificates, 438

- channels (Teams)**
 - private, 772–773
 - org-level settings*, 775–776
 - team-level settings*, 773–774
 - shared, 776–777
- chats (Teams)**, 593, 602–603
- child hubs**, 793
- civic address, LIS (Location Information Service)**, 675–676
- classifiers**, 120–121
- clauses, groups**, 316
- CLID (calling line ID)**, 643
- client software**
 - updating/deploying, 53
 - activation*, 57
 - Microsoft 365 Apps*, 54–56
- cloud identities**, 238–246
 - CSV files, 240–241
- CMT (centralized mail transport)**, 463–464
- CNAM (calling party name)**, 643
- coauthoring documents in OneDrive for Business**, 916–917
- collaboration (OneDrive for Business)**
 - document coauthoring, 916–917
 - document sharing, 915
 - document versioning, 917–920
 - folder sharing, 915
- collaboration, access control planes**, 763–771
- communications credits (Teams Phone System)**, 699–700
- Compliance Manager**
 - alerts, 103–104
 - assessments, 93–95
 - template*, 88
 - compliance score, 87–88
 - Controls tab, 96–97
 - documentation, 99–100
 - Improvement Actions tab, 97
 - Key Improvement Actions, 89
 - assigning actions*, 98–99
 - corrective actions*, 91
 - detective actions*, 90
 - discretionary actions*, 90
 - documentation actions*, 89
 - enforcement type*, 90
 - mandatory actions*, 90
 - operational actions*, 90
 - preventative actions*, 90
 - risk type*, 90
 - status*, 102
 - technical actions*, 90
 - permissions, 91–93
- Conditional Access**, 193
 - Azure AD Conditional Access, 218–222
 - risk based*, 223–227
- Configuration Manager**, 200–201
- connectors (Teams)**, 594
- contacts**, 441
 - Exchange Online, 554
 - Microsoft Teams, 594
- Content Search**, 164
 - Condition Cards, 164
 - downloading results, 169–174
 - exporting results, 169–174
 - performing, 165–168
 - responsive content, 164
- Content Services reports (SharePoint Online)**, 881
- controls**
 - Azure Active Directory, 74
 - Exchange Online, 76
 - Microsoft Teams, 81
 - SharePoint Online, 78
- corrective actions, Compliance Manager**, 91
- credentials, AAD Connect installation**, 261
- cross-premises access, hybrid configuration**, 458–459
- cryptography, DKIM (DomainKeys Identified Mail)**, 572
- CSR (Customer Service Record)**, 689
- CSV (comma-separated value) files**
 - cloud identities, 240–241
 - migration batches and, 495

Custom installation**AAD Connect, 267**

- Azure AD app and attribute filtering, 326–328*
- completion, 339*
- directories, 284–286*
- Domain And OU Filtering dialog, 289–290*
- GalSync, 299–313*
- group filtering, 322–324*
- joins, custom, 316–318*
- location, 268*
- MailNickname, 313–316*
- Optional Features, 325–337*
- Password Synchronization, 273–283*
- SamAccountName, 313–316*
- service accounts, 270–272*
- Source Anchor attribute, 319–322*
- SQL Server, 269–270*
- Staging Mode, 340–341*
- synchronization, 340–343*
- synchronization settings, 272*
- Uniquely Identifying Your Users dialog, 290–299*
- UPN suffixes, 287–290*

cutover migration, 435**D****data controls, 84****data classification, 202****data governance**

- classifiers, 120–121
- Content Services reports (SharePoint Online), 881
- disposition reviews, 126
- DLP (data loss prevention) policies, 123–124
- labels, 121
 - application, 122*
 - Exchange Online and, 121*
 - OneDrive for Business and, 121*
 - retention labels, 122, 147–153*
 - sensitivity labels, 122, 127–147*
 - SharePoint Online and, 121*
- policies
 - DLP (data loss prevention), 156–161*
 - retention policies, 153–156*

- records, 126–127

- retention policies, 124–126, 155

- SIT (sensitive information type), 118–119

data labeling, 202**data lifecycle, governance and, 72–73****data loss prevention, 447****data protection, persistent, 201****DAuth (Delegated Authentication), 461–462****decryption rules, 564****Defender**

- Anti-phishing settings, 575

- Anti-Spam policies, 576–577

delegation (Microsoft Outlook), cross-premises access, 459**deletions, 377****Delve, 787****deployment**

- client software, 53

- activation, 57*

- Microsoft 365 Apps, 54–56*

- Exchange Online, 431–436

Deployment Assistant, migration and, 453**detective actions, Compliance Manager, 90****devices**

- QoS (Quality of Service), 663–664

- security, 227

- Intune, 228–234*

- MDM (Mobile Device Management), 227*

- mobile application management, 228*

- synchronization, 347–348

Device Writeback, 333–334**DID (direct inward dial), 726, 728****directories**

- AAD Connect Custom installation, 284–286

- adding, 287*

- objects, 284–285*

- Azure AD Cloud Sync, 354

- extensions, 348

- IDFix and, 48–53

- synchronization, 10, 287

- synchronized service accounts, 286

- user joins, 314

Directory Extension Attribute Sync, 335–337

Direct Routing (Teams), 648–650, 672

- ATA (analog telephone adapter), 653
- LBR (location-based routing), 652
- LMO (Local Media Optimization), 651–652
- Media Bypass, 650
- SBA (survivable branch appliances), 653

DirSync, 345

disabled users, 24

discretionary actions, Compliance Manager, 90

dispatchable locations, emergency calling, 644

disposition reviews, 126

DKIM (DomainKeys Identified Mail), 572–573

DKIM records, 450

DLP (data loss prevention)

- Central Mail Flow, 566
- policies, 156
 - application mode, 159*
 - document fingerprinting, 160–161*
 - template-based content, 156–160*

DLP (data loss prevention) policies, 123–124

DMARC records, 450

DNS (domain name system)

- Autodiscover, 449
- DKIM records, 450
- DMARC records, 450
- Exchange AutoDiscover records, 40
- Exchange Online configuration, 459
- IM (Instant Message), 40
- Microsoft Federation Gateway, 450
- MX (Mail eXchanger) records, 450
- proof of ownership, 39
- public records, 39
- records, domain registrar and, 6–7
- SPF records, 450
- SPF (Sender Policy Framework) records, 40
- SRV (Server Resource) records, 40
- verification records, 450
- VOIP (Voice Over IP), 40

DNS CNAME records, 449

DNS TXT records, 450

documentation, Compliance Manager, 89, 99–100

document fingerprinting, 119, 156, 160–161

documents (OneDrive for Business)

- coauthoring, 916–917
- revocation, 203
- sharing, 915
- tracking, 203
- versioning, 917–920

Domain And OU Filtering dialog, 289–290

domain names, 4

- tenant and, 5

domain registrar, 6, 7

domains

- accepted, 443–444
- Active Directory, 22
 - OU filtering, 22–23*
- hybrid configuration, 588
- ownership verification
 - MX DNS record, 5*
 - TXT record, 5*
- RODC (read-only domain controller), 437

Download Agent, 350

DSCP (Differentiated Services Code Point) values, 659–660

DTMF (dual tone multi-frequency) keypresses, 749

dynamic distribution groups, 445

E

E3 tier, Enterprise, 3

E5 tier, Enterprise, 3

E911 (Enhanced 911), 672–673

- emergency calling policies, 681–683
- ESRP (Emergency Service Routing Provider), 683
- LIS (Location Information Service), 675–676
 - access point definition, 678–679*
 - civic address, 675–676*
 - places, 676*
 - ports, 680–681*
 - subnets, 677–678*
 - switches, 680–681*
- networks, 674

EAC (Exchange Administrative Center), 10

EAPs (email addressing policies), 16

ECP (Exchange Control Panel), certificates, 438

ECRC (Emergency Call Relay Center), 673

eDiscovery, 74, 174

case management, 174

closing, 185–186

content holds, 178

content searches, 182–183

content holds, 180–181

creating cases, 176–177

member creation, 176–177

permissions, 174–176

search result export, 183–185

search scope limits, 177

controls, 85

EF (Expedited Forwarding) model, network traffic, 659

email

addresses

Exchange Hybrid process, 34

Exchange Online, 551

Exchange Online hybrid configuration, 459

attributes, migrations, 396

domain setup, 6

GAL (Global Address List), 30

GalSync, 295–296, 299

configuration modification, 300

contact objects, 300–313

Junk Email folder, 579

MailNickname, 313–316

replying to old messages, 30–31

SamAccountName, 313–316

emergency dialing. See E911

EMS (Enterprise Mobility + Security), 189, 207

advanced data protection, 199

ATA (Advanced Threat Analytics), 203

Authenticator App and, 192

data classification, 202

data labeling, 202

devices, 227

Intune, 228–234

MDM (Mobile Device Management), 227

mobile applications, 228

documents

revocation, 203

tracking, 203

EMS E3

advanced data protection, 199

advanced security reporting, 197

EMS E5 comparison, 190

products, 190

EMS E5

advanced data protection, 199

advanced security reporting, 197

EMS E3 comparison, 190

products, 190

encryption keys, 203

Endpoint Manager, 198

MAM (Mobile Application Management), 199

identity

Azure AD Conditional Access, 218–224, 227

MDI (Microsoft Defender for Identity), 208–218

integrated PC management, 200

MCAS (Microsoft Cloud App Security), 204

MDCA (Microsoft Defender for Cloud Apps), 204

MDI (Microsoft Defender for Identity), 205

on-premises data management, 201

persistent data protection, 201

encryption, 563

keys, 203

mail messages, 447

passwords, 273

removing, 565

RMS (Rights Management Service), 563

rules, 564

Endpoint Manager, 198–199

endpoints

Outlook Anywhere, 531

Teams Phone, 657

EOP (Exchange Online Protection), 447

ESRP (Emergency Service Routing Provider), 683

EWS (Exchange Web Services), certificates and, 438**Exchange**

- AutoDiscover, 11
- AutoDiscover DNS records, 10
- Best Practices Analyzer, 440
- CAS (Client Access) servers, 14
- EAC (Exchange Administrative Center), 10
- Hybrid, 10, 11, 17
- mailboxes, 14
 - domains, 15–16*
 - large items, 15*
 - linked, 292–294*
 - proxy addresses, 15–16*
 - recipient types, 15*
- network
 - configurations, 17*
 - load balancers, 17*
 - proxy servers, 17*
 - server placement, 17*
- physical infrastructure, 13
 - mailboxes, 14*
 - mail routing, 14*
 - migration, stages, 14*
 - MRS (Mailbox Replication Service), 13*
 - public folders, 16*
- support matrix, 439
- updates, 441
- versions, 439
- Web Services, 11

Exchange 2007, hybrid public folder configuration, 519–520**Exchange 2010, hybrid public folder configuration, 520****Exchange 2013, hybrid public folder configuration, 521****Exchange Administrator, 8****Exchange AutoDiscover records, 40****Exchange Hybrid**

- AAD Connect installation, 266
- firewalls, 448
- MTR (Microsoft Teams Rooms) deployment, 736–738

Optional Features settings, 325–326

service routing address, 34

Writeback, 286, 307

GalSync and, 303, 305

Exchange Management Servers, hybrid configuration, 469**Exchange Management Shell, certificates, 438****Exchange Online**

- admin center, 546
- Autodiscover, 432–434
- coexistence, 435–436
- controls, 76
- deployment, 431, 436
- DLP (data loss prevention policies), 123
- governance and, 71
- hybrid configuration, 458
 - AAD Connect, 458*
 - Autodiscover, 458*
 - CMT (centralized mail transport), 463–464*
 - cross-premises access, 458–459*
 - DAuth, 461–462*
 - decommissioning, 485–487*
 - DNS and, 459*
 - domain updates, 588*
 - edge transport servers, 478*
 - email addresses, 459*
 - Exchange Server Deployment Assistant, 460*
 - Exchange Servers, 469*
 - Exchange server versions, 460*
 - free/busy and, 461–462*
 - Hybrid Configuration Wizard, 466*
 - mailbox provisioning, 482–485*
 - mail transport, 463*
 - message size, 463*
 - network requirements, 464*
 - OAuth, 461–462*
 - public folders, 465*
 - remote mailboxes, 482, 484–485, 587*
- Hybrid Configuration Wizard, 457, 465
 - completing, 473*
 - connectivity testing, 475*
 - connector configurations, 479*
 - federation trust, 471–473*

- FQDN*, 480
- free/busy and*, 466
- HTTPS and*, 466
- Hybrid Features page*, 475
- Hybrid Topology page*, 475
- improvements*, 465–466
- installation*, 469–471
- mail transport options*, 477
- MailTips*, 466
- MRSProxy (Mailbox Replication Service Proxy)*, 466
- OST (Outlook Offline Storage)*, 466
- prerequisites*, 468–469
- rerunning*, 481
- running*, 471–481
- SMTP and*, 466
- task sequence*, 467, 468
- troubleshooting*, 482
- Web Services Virtual Directory*, 477
- hybrid environment
 - features overview*, 455–457
 - Hybrid Agent*, 456
- labels, 121
- mailboxes
 - calendar processing*, 552–553
 - contacts*, 554
 - delivery restriction*, 555–557
 - distribution groups*, 554–555
 - email addresses*, 551
 - mail-enabled users*, 553
 - permissions*, 547–551
 - rights*, 547–551
- mail routing, 432
- malware filter, 574
- migration, 365
 - cutover*, 435
 - express*, 435
 - hybrid*, 436
 - IMAP*, 436
 - staged*, 435
- organizations
 - relationships*, 583, 585–586
 - sharing policies*, 586
- phishing
 - Anti-phishing settings*, 575
 - filter*, 574–576
- public folders
 - location*, 538
 - mail-enabled, external email address*, 539
 - mail-enabled, routing*, 538
 - on-premises, mail routing*, 539
- recipients, 431
- Send-As permissions, 539
- spam
 - blocked accounts*, 581
 - filter*, 576–578
 - outbound, filtering*, 581
 - quarantine*, 579–580
- tenant name, 34
- transport
 - Allow list*, 567–568
 - Block list*, 567–568
 - Central Mail Transport*, 566–567
 - connectors*, 557
 - DKIM*, 572–573
 - enhanced filtering*, 569
 - IP filtering lists*, 567–568
 - message attachment*, 565–566
 - Message Encryption*, 563–565
 - Message Trace*, 569–570
 - rules*, 557–563
 - rules export*, 571
 - rules import*, 571–572
 - rules migration*, 571
 - settings migration*, 570
- Exchange Server**
 - Exchange Online hybrid configuration, 460
 - Exchange Server Deployment Assistant, 460
- export, transport rules**, 571
- Expression Builder**, 370–373
- expressions, VBA**, 366–369
- express migration**, 435
- Express mode installation, AAD Connect**, 259–260, 265
 - Active Directory account, 263
 - Configuration Complete dialog, 267

- credentials, 261
- directory synchronization, 262
- Exchange Hybrid deployment, 266
- Global Administrator, 261
- OU (organizational unit), 263
- Replicating Directory Changes All, 264
- SQL Express and, 266
- synchronization, 266
- ExpressRoute, 47**
- extensions, directories, 348**
- external sharing, 763, 798–801**

F

- F3 tier, Enterprise, 3**
- Fiddler, 45, 47**
- filtering**
 - enhanced, 569
 - groups, 322, 324
 - MDI (Microsoft Defender for Identity), 214
- filters**
 - malware, 560–574
 - phish, 574–576
 - Secure Score reports, 113
 - spam, 576–578
 - outbound, 581*
- FIM + WAAD, 345**
- FIM (Forefront Identity Manager), 345**
- firewalls, 448**
 - configuration, 40
- FOIA (Freedom of Information Act), 174**
- folders**
 - Exchange, 16
 - mailbox sorting, 28
 - public, 522
 - Exchange 2007, 523–532*
 - Exchange 2010, 523–532*
 - Exchange 2013 or later, 532–537*
 - Exchange Online hybrid configuration, 465*
 - hybrid, 517–521*
 - migration, 446, 523–534*
 - number of users, 530*

- Outlook Anywhere endpoints, 531*
- post-migration, 538–540*
- sharing, OneDrive for Business, 915

forests

- Active Directory, 21
- cross-forest migration, 397
 - ADMT, 397*
 - PowerShell, 397*

- free/busy, Exchange Online hybrid configuration, 461–462**

G

- GAL (Global Address List), 30, 396**
- GalSync, 295–296, 299**
 - configuration modification, 300
 - contact objects, 300–313
 - DLL, 307
 - rule configuration, 306
- Global Administrator, 8**
- global navigation, 795**
- Global Reader, 8**
- gMSA (Group Managed Service Account), 346**
 - MDI (Microsoft Defender for Identity), 211
- governance, 65**
 - Azure Active Directory, 69–71
 - controls
 - Azure Active Directory, 74*
 - eDiscovery, 85*
 - Exchange Online, 76*
 - Microsoft Teams, 81*
 - retention, 84*
 - SharePoint Online, 78*
 - core workloads and, 69–74
 - data lifecycle, 72–73
 - eDiscovery, 74
 - Exchange Online, 71
 - IAM (Identity and Access Management)
 - access management lifecycle, 68*
 - identity lifecycle, 67–68*
 - Microsoft Teams, 72
 - SharePoint Online, 71
- graphical PowerShell workflow runbook, 414**

graphical runbook, 414

group-based licensing, 59–61

group object, Microsoft Teams, 599–600

Group Policy (OneDrive for Business), 921

Documents folder, redirection, 925–926

folder path changes, preventing, 921–923

syncing personal account, preventing, 923

syncing with other tenants, preventing, 924

user account silent configuration, 926–928

groups

ADGMS (Active Directory Group Modernization Service), 445

Azure Active Directory, 70

call parking, 716

call policies, 711

clauses, 316

empty, 24

filtering, 322–324

gMSA (group-managed service account)

MDI (Microsoft Defender for Identity), 211

Hybrid OneDrive for Business, 825

Microsoft Teams

guests, 596

members, 596

owners, 596

properties, 596, 599

provisioning, 595

synchronization and, 444–445

dynamic distribution, 445

Microsoft 365 groups, 445–446

unused, 24

group SIDs, 396

Group Writeback, 332–333, 446

guest access, Microsoft Teams admin center, 770

guest identities, 246–248

guest user accounts, Azure Active Directory, 69

GUID, migration batch offboarding, 508

H

hardware

authentication, tokens, 193

MDI (Microsoft Defender for Identity), 208–210

HCW (Hybrid Configuration Wizard), 11

Helpdesk Administrator, 8

home realm discovery, 46

How You'll Sign In page, 4

HRIS (human resources information systems), 67

hubs

associated sites, 793

child, 793

designating, 792

parent, 793

hub site navigation, 795

hub sites (SharePoint Online), 868

Hub Transport role, 457

Hybrid Agent (Exchange Online), 456

Hybrid App Launcher (SharePoint), 842–843

Hybrid Auditing (SharePoint Online), 809

Hybrid Configuration Wizard, 457, 465

completing, 473

connectivity testing, 475

connector configurations, 479

edge transport servers, 478

federation trust, 471, 473

FQDN, 480

free/busy and, 466

HTTPS and, 466

Hybrid Features page, 475

Hybrid Topology page, 475

improvements, 465–466

installation, 469–471

MailTips, 466

mail transport options, 477

MRSProxy (Mailbox Replication Service Proxy), 466

OST (Outlook Offline Storage), 466

prerequisites, 468–469

rerunning, 481

running, 471–481

selection options, 471

SMTP and, 466

task sequence, 467–468

troubleshooting, 482

Web Services Virtual Directory, 477

hybrid migration, 436

Hybrid OneDrive for Business (SharePoint), 824

- groups, 825
- Hybrid Picker, 829–830
- permissions, 825–826
- prerequisites, 824
- redirection, 826, 828
- subscription plan, 824

Hybrid OneDrive for Business (SharePoint Online), 809, 811**Hybrid Picker**

- Hybrid App Launcher, 842–843
- Hybrid Taxonomy, 839–841

hybrid public folders, 517

- on-premises, 518–521
 - Exchange 2007, 519,–520*
 - Exchange 2010, 520*
 - Exchange 2013, 521*
 - online, 521*

Hybrid Runbook Worker, 414**Hybrid Search (SharePoint), 830**

- cloud Search service application, 831–832
- content sources, 833–835
- prerequisites, 830–831
- results included, 835, 837
- subscription, 831
- troubleshooting, 835

Hybrid Search (SharePoint Online), 809, 811–813

- cloud hybrid search, 811
- hybrid federated search, 811

Hybrid Taxonomy (SharePoint), 837

- copying to SharePoint Online, 838–839
- Hybrid Picker and, 839–841
- prerequisites, 837–838
- Timer service, 838

Hybrid Taxonomy (SharePoint Online), 809, 813**HYOK (Host Your Own Key), 203****I****IAM (Identity and Access Management), 66, 191**

- access management lifecycle, 68
- identity lifecycle, 67–68

- MFA (multifactor authentication), 192–193
- simplified access management, 191

identities (Azure AD), 592

- cloud, 238–246
- Custom View option, 245
- guest, 246–248
- synchronized, 237–238, 243

identity

- external controls, Azure AD portal, 767–769
- lifecycle, 67–68

MDI (Microsoft Defender for Identity), 208

- connectivity, 210*
- gMSA, 211*
- hardware requirements, 208–210*
- instance creation, 211–213*
- service account, 211*

identity federation (Azure AD), 254–257

- ADFS (Active Directory Federation Services), 255–257
- configurations required, 255

identity map (SharePoint Online), 854–856**IDFix, 48–53, 314, 440****IDP (Identity Provider), 192****IDSs (intrusion detection systems), 450, 853****IF statements, 369****IMAP migration, 436****IM (Instant Message), DNS configuration and, 40****impersonation, 574****instant meetings (Teams), 610****Internet Explorer, 41****Intune, 200****IOAs (indicators of attack), 208****IOCs (indicators of compromise), 208****IPSs (intrusion protection systems), 450, 853****IRM (Information Rights Management), 877****ITAR (International Traffic in Arms), 459****IVR (interactive voice response), 640****IWA (Integrated Windows Authentication), 823**

J-K

Junk Email folder, 579

KFM (Known Folder Move), 925

KQL (Keyword Query Language), 187

L

labels, 121

application, 122

automatic, 122

manual, 122

Exchange Online and, 121

OneDrive for Business and, 121

retention labels, 122

adaptive scopes, 149–151

creating, 148–149

publishing, automatic application, 152–153

publishing, manual application, 151–152

sensitivity labels, 122, 127

creation, 131–138

deploying, 128

encryption, 133

environment preparation, 129–130

publishing, automatic application, 142–144, 147

publishing, manual application, 139–142

sharing, 137

synchronization, 129–131

SharePoint Online and, 121

LBR (location-based routing), 619

least privilege rights, 69

licensing

OneDrive for Business, 905–907

SharePoint Online, 892–893

users, 59

group based, 59–61

manual assignment, 63–64

PowerShell, 61–63

LIS (Location Information Service), 675–676

access point definition, 678–679

civic address, 675–676

places, 676

ports, 680–681

subnets, 677–678

switches, 680–681

List pane (Microsoft Teams), 601

live events (Teams), 625

external production, 636–637

policies, 626–628

assigning, 628–629

settings, 629

Support URLs, 630

video distribution, 630

Stream, 631–633

Yammer, 634

LMO (Local Media Optimization), 619

load balancing, 17, 449

LOB (line of business), 67

local navigation, 795

login

sign-in prompts, 26

UPN (UserPrincipalName), 25–26

M

MAD (merger, acquisition, and divestiture), 381

mail

Autodiscover, 432–434

contacts, 441

Exchange Online hybrid configuration

CMT (centralized mail transport), 463–464

transport plans, 463

routing, 432

mail attribute, migrations, 396

Mail attribute, 294–295

mailboxes, 14, 441

EAPs (email addressing policies), 16

Exchange

domains, 15–16

proxy addresses, 15–16

recipient types, 15

forwarding addresses, 451

large items, 15

- linked, 292–294
- migration
 - alternate interface*, 496
 - MRSProxy (Mailbox Replication Service Proxy)*, 489–492
 - schedule*, 29
 - troubleshooting*, 509–513
- MTR (Microsoft Teams Rooms), 734
- Outlook
 - cleanup*, 28–29
 - sorting*, 28
- remote, 482–485
 - hybrid configuration*, 587
- mailboxes (Exchange Online)**
 - calendar, booking policies, 552
 - calendar processing, 552–553
 - contacts, 554
 - cross-premises access, 459
 - delivery restriction, 555
 - allowed senders*, 555
 - distribution group, moderating*, 556
 - message approval*, 556–557
 - outside senders*, 555
 - distribution groups, 554–555
 - email addresses, 551
 - SMTP*, 551
 - permissions, 547, 551
 - AutoMapping*, 548
 - folders*, 549–550
 - full access*, 547–548
 - roles*, 550
 - Send-As*, 549
 - Send-On-Behalf*, 549
 - provisioning hybrid configuration, 482–485
 - rights, 547–551
 - users, mail-enabled, 553
- Mailbox Replication Service migration method**, 463
- mailbox users, mail-enabled users and**, 442
- mail-enabled users**, 444
 - mailbox users and, 442
 - Exchange Online, 553
- mail messages**
 - encryption, 447
 - EOP (Exchange Online Protection), 447
 - hygiene, 447
- MailNickname attribute**, 19, 292, 313–316
- mail routing, data loss prevention**, 447
- MailTips**, 466
- malware**, 574
 - filters, 560–563, 574
- MAM (Mobile Application Management)**, 199, 227
- managed metadata service (SharePoint), hybrid integration setup**, 816–818
- mandatory actions, Compliance Manager**, 90
- manual licensing assignment**, 63–64
- MAPS (Microsoft Azure Peering Service)**, 654
- MCAS (Microsoft Cloud App Security)**, 204
- MCS (Microsoft Consulting Services)**, 397
- MDCA (Microsoft Defender for Cloud Apps)**, 204
- MDI (Microsoft Defender for Identity)**, 205, 208
 - connectivity, 210
 - environment monitoring, 214
 - filtering, 214
 - gMSA account, 211
 - hardware requirements, 208–210
 - instances, 211–213
 - MFA (multifactor authentication), 214–218
 - service account, 211
- MDM (Mobile Device Management)**, 227
- Media Bypass (Teams Phone)**, 650
- meetings (Teams)**
 - anonymous people, 621–622
 - channel, 612–613
 - policies, 616
 - assigning*, 623–624
 - Audio And Video settings*, 617–620
 - Content Sharing settings*, 621
 - general settings*, 616–617
 - Participants & Guests settings*, 621–623
 - Recording & Transcription settings*, 620
 - settings, 624–625
 - standard, 612

standard (traditional), 610–612

ad hoc meetings, 610

instant meetings, 610

options, 611

scheduled meetings, 610

versus webinars, 615

Menu bar (Teams), 601

Message Encryption, 563

Azure RMS (Rights Management Service), 563

removing, 565

rules, 564

decryption, 564

messages

Exchange Online hybrid, 463

migrating

attachments, 443

size, 443

NDR (non-delivery report), 124

Message Trace, 569–570

messaging (Teams), 593

MFA (multifactor authentication), 192–193

Conditional Access, 193

MDI (Microsoft Defender for Identity), 214–218

methods, 192

risk-based access, 194–195

Microsoft 365 admin center

Microsoft 365 Groups settings, 765–766

sharing management, 766–767

Teams settings, 763–764

Microsoft 365 Apps

conflicting versions, 55

installing, 54–56

tenant name, 36

Microsoft 365 Groups, 765–766

Microsoft Federation Gateway, 450

Microsoft Intune, 227–234

Microsoft Purview, 131

Microsoft Purview Compliance Manager. *See* Compliance Manager

Microsoft Teams, 589

adding members, 778–779

admin center, guest access, 770

administration

meeting policies, 616–623

meeting settings, 624–625

App bar, 601

Activity Feed, 601–602

added apps, 606

App store, 607

Calendar app, 603

Calls app, 605

Chat app, 602–603

Download Mobile App, 607

Files view, 605

presence, 602–603

Teams view, 603

architecture overview, 591

audio and video settings, 617–619

body pane, 601

Calendar app, 610

calendars, 594

channels, 590

people, troubleshooting, 780

private, 591, 772–776

shared, 776–777

chats, 593

connectors, 594

contacts, 594

controls, 81

files, 593

governance and, 72

group object integration, 599–600

groups

guests, 596

members, 596

owners, 596

properties, 596, 599

provisioning, 595

identities, Azure AD, 592

List pane, 601

live events, 625

external production, 636–637

policies, 626–628

policies, assigning, 628–629

settings, 629–630

- Stream*, 631–633
- Yammer*, 634
- meetings
 - anonymous people*, 621–622
 - channel*, 612–613
 - standard*, 612
 - standard (traditional)*, 610–612
- meetings versus webinars, 615
- Menu bar, 601
- messaging, 593
- networks, 619
- objects, converting to, 589
- PowerShell module, 672
- recording, 594
- rooms. *See* Microsoft Teams Rooms (MTR)
- settings, Microsoft 365 admin center, 763–764
- sharing invitation troubleshooting, 778
- Stream and, 631–633
- Teamifying, 589
- teams as container object, 590
- Teams Phone, 639
 - architectures*, 646–655
 - audio conferencing*, 640
 - auto attendants*, 640
 - call parking*, 644
 - Call Quality Dashboard Report*, 668
 - call queues*, 640
 - caller ID*, 643
 - calling plans*, 642, 647–648
 - CLID (calling line ID)*, 643
 - CNAM (calling party name)*, 643
 - contact centers*, 641
 - dial plans*, 641
 - direct routing*, 642
 - Direct Routing*, 648–653
 - emergency calling*, 644–645
 - inbound call blocking*, 645
 - Network Assessment Tool*, 668
 - network best practices*, 667–668
 - Network Connectivity Test tool*, 668
 - Network Planner for Teams*, 668
 - network requirements*, 655–667
 - Operator Connect*, 642, 654–655
 - phone numbers*, 642
 - poring numbers*, 642
 - PSTN (public switched telephone number)*, 643
 - resource accounts*, 643
 - SBC (Session Border Controller)*, 642–643
 - service numbers*, 643
 - shared lines*, 645
 - SIP (Session Initiation Protocol)*, 643
 - voicemail*, 646
 - VoIP (Voice over Internet Protocol)*, 643
- tenant name, 36
- user domain troubleshooting, 779–780
- voicemail, 594
- webinars, 613
 - registration*, 614–615
- Yammer and, 634
- Microsoft Teams Rooms (MTR)**
 - deployment
 - Exchange hybrid*, 736–738
 - online only*, 734–736
 - licensing, 733
 - resource accounts, 733
 - deployment scenarios*, 733–738
 - room features*, 739–740
 - room lists*, 738–739
- migration**
 - access protocols, 451
 - calendar processing and, 451
 - cross-forest, 397
 - ADMT*, 397
 - PowerShell*, 397
 - Deployment Assistant, 453
 - email-related attributes, 396
 - endpoints, 489–492
 - Exchange Online
 - cutover migration*, 435
 - express migration*, 435
 - hybrid migration*, 436
 - IMAP migration*, 436
 - staged migration*, 435
 - folders, public, 523, 533–534
 - forwarding addresses and, 451

Mailbox Replication Service migration method, 463

Messages, 443

permissions, 446

public folders, 446

Remote Connectivity Analyzer, 453

retention policies, 452

schedule, 446

to SharePoint Online, 880

- Azure Data box, 849*
- blocking issues resolved, 858*
- content not migrated, 858*
- content scanning, 856–858*
- custom script, 851–852*
- excluded items, 847–849*
- identity map generation, 854–856*
- mapping, 846–847*
- network, 852–853*
- planning, 850–852*
- preparation, 846*
- prerequisites, 850–852*
- SharePoint Migration Manager, 849*
- SMAT (SharePoint Migration Assessment Tool), 850, 856–858*
- SPMT (SharePoint Migration Tool), 849–851, 859–864*

SIDs (Security Identifiers), 396

SourceAnchor attribute, 381–388

transport rules, 571

transport settings, 570

UserPrincipalName value, 395–396

migration batches, 493

offboarding, 507, 508

- database GUIDs, 508*
- PowerShell, 508*

onboarding, 497–505

- completing a batch, 501–502*
- completing user in batch, 503–506*
- creating a batch, 494–496*
- monitoring, 498–499*
- removing users, 506*
- retrying users, 500*
- start method, 497*

MIM (Microsoft Identity Manager), 58

MRS (Mailbox Replication Service), 13

MRSProxy (Mailbox Replication Service Proxy), 466, 489–492

mS-DS-ConsistencyGuid, 321–322, 382–389

MX DNS record, 5

MX (Mail eXchanger) record, 14, 450

My Sites (SharePoint), hybrid integration setup, 818–819

N

NAT (Network Address Translation), 449

navigation

- global, 795
- hub sites, 795
- local, 795

NDI (network device interface), 619

NDR (non-delivery report), 124

NetMon3, 47

networking

- bandwidth, 448
- CIR (Committed Information Rate), 659
- DSCP (Differentiated Services Code Point) values, 659–660
- E911, 674
 - trusted IP, 674*
- EIR (Excess Information Rate), 659
- Exchange
 - configurations, 17*
 - load balancers, 17*
 - proxy servers, 17*
- Exchange Online hybrid configuration, 464
- firewalls, 448
- load balancing, 449
- Microsoft Teams, 619
- migration to SharePoint Online, 852
 - IDS (intrusion detection systems, 853*
 - IPS (intrusion protection systems, 853*
 - proxies, 852*
- network tracing, 44–47
- proxies, 449

- proxy servers, 41–44
 - network tracing*, 44–47
- security appliances, 450–451
- Teams Phone, 655
 - bandwidth*, 656
 - best practices*, 667–668
 - Call Quality Dashboard Report*, 668
 - endpoints*, 657
 - Network Assessment Tool*, 668
 - Network Connectivity Test tool*, 668
 - Network Planner for Teams*, 668
 - ports*, 657
 - QoS (Quality of Service)*, 658–667
 - VPN (virtual private networks)*, 658
- notifications, deletion**, 377

O

- OAB (Offline Address Book)**, 438
- OATH tokens**, 193
- OAuth (Open Authorization)**, 461–462
- ObjectGUID**, 319–322
- ObjectSID/msExchMasterAccountSID**, 292–293
- Office versions**, 27
- Office Graph, Delve and**, 787
- Office Online**, 786–787
- OneDrive**
 - DLP (data loss prevention), 123
 - folder backup, 910
 - Offline Attribute, 913
 - Pinned Attribute, 913
 - setup, 908
 - sync client, 783
 - Mac OS X*, 914–915
 - Windows*, 907–913
 - Unpinned Attribute, 913
- OneDrive for Business**, 785–786
 - access, 905–907
 - administrators, secondary, 928–929
 - documents
 - coauthoring*, 916–917
 - sharing*, 915
 - versioning*, 917–920
 - Documents folder, redirection, 925–926
 - folder sharing, 915
 - Group Policy and, 921
 - folder path changes, preventing*, 921–923
 - labels, 121
 - licensing, 905–907
 - OneDrive sync client
 - Mac OS X*, 914–915
 - Windows*, 907–913
 - provisioning
 - disabling*, 931–933
 - pre-provisioning sites*, 933
 - sharing, restricting, 931
 - synchronization
 - device restriction*, 929–931
 - troubleshooting*, 934–935
 - syncing personal account prevention, 923
 - syncing with other tenants prevention, 924
 - tenant name, 35
 - user account silent configuration, 926–928
- on-premises management**, 201
- on-premises public folders**, 518–521
 - Exchange 2007, 519–520
 - Exchange 2010, 520
 - Exchange 2013, 521
 - online, 521
- operational actions, Compliance Manager**, 90
- Operator Connect (Teams)**, 654–655, 672
- Optional Features settings**, 325
 - Azure AD app and attribute filtering, 326–328
 - Device Writeback, 333–334
 - Directory Extension Attribute Sync, 335–337
 - Exchange Hybrid, 325–326
 - Group Writeback, 332–333
 - Password Synchronization, 330–331
 - Password Writeback, 331
- Organization Management RBAC group**, 519, 523
- organizations**
 - relationships, 583–586
 - sharing policies, 586
- OST (Offline Store)**, 10
- OST (Outlook Offline Storage)**, 466

OU (Office Update), 28

OUs (Organizational Units), 22–23, 263

Azure AD Cloud Sync, 357–359

Outlook

Autodiscover, 432–434

local XML, 433

mailboxes, 28–29

updates, 27

Outlook Anywhere, 531

OWA (Outlook Web App), certificates and, 438

P

parent hubs, 793

pass-through authentication (PTA), 274–276, 348

Password Hash Sync, 255

passwords

Azure AD, 249–252

complexity policy, 253

expiration policy, 252

requirements, 251

brute-forced, 192

encryption, 273

scope, 274

synchronization, 330–331

pass-through authentication and, 275

TOTP (Time-Based One-Time Passwords), 193

Password Synchronization, AAD Connect, 273–274

Password Writeback, 331–332

enabling, 398

password reset, 398–399

password reset policy, 400–401

user registration data, 401–403

requirements, 398

PAW (Protocol Agnostic Workflow), 504–506

PBX (public branch exchange) phone system, 640

PC management, integrated, 200

permissions, 274

Compliance Manager, 91–93

delegating, 382

eDiscovery case management, 174–176

Hybrid OneDrive for Business, 825–826

mailboxes (Exchange Online), 547–551

AutoMapping, 548

folders, 549–550

full access, 547–548

roles, 550

Send-As, 549

Send-On-Behalf, 549

migration, 446

policies, 274

RMS (Rights Management Service), 563

Send-As, 539

Send-On-Behalf, 540

service accounts, 286

persistent data protection, 201

phish, 574

Anti-phishing settings, 575

filters, 574–576

impersonation, 574

spoofing, 575

phone numbers (Phone System)

acquiring, 683–696

assigning, 696–699

ordering through Microsoft, 684–688

porting, 688–694

canceling request, 695–696

porting out, 695

troubleshooting, 696

PII (Personally Identifiable Information), 320

PIM (Privileged Identity Management), 197

policies

DLP (data loss prevention), 156

application mode, 159

document fingerprinting, 160–161

template-based content, 156–160

passwords, 274

retention policies, 153–156

SharePoint Online

Access Control page, 872–873

Settings page, 873–878

Sharing page, 870–871

ports, Teams Phone, 657

PowerShell

- identity federation and, 256
- licensing, 61–63
- migration offboarding, 507–508
- PSRemoting, 280
- splatting, 735

PowerShell module, 672**PowerShell runbook, 413, 422**

- Exchange Online script, 423–424
- publishing, 428–429
- testing, 426, 428

PowerShell workflow runbook, 413**Preservation Hold library, 125****pre-trained classifiers, 120****preventative actions, Compliance Manager, 90****private channels (Teams), 772–773**

- org-level settings, 775–776
- team-level settings, 773–774

Privileged Identity Management, 69**provisioning, OneDrive for Business**

- disabling, 931–933
- pre-provisioning sites, 933

Provisioning Agent, 350**proxies**

- networking and, 449
- networking migration, 852

proxy servers, 17, 41–44

- network tracing, 44–47
- Windows Shell, 42

PSAP (Public Safety Answering Point), 644, 673**PSH (Password Hash Sync), 348****PSRemoting, 280****PSTN (Public Switched Telephone Network), 605, 639, 643****PTA (pass-through authentication), 348****public folders, 522**

- Exchange, 16
- Exchange 2007, 523–532
- Exchange 2010, 523–532
- Exchange 2013 or later, 532–537
- Exchange Online hybrid configuration, 465

hybrid, 517

- on-premises, 518–521*

migration, 523–534

number of users, 530

Outlook Anywhere endpoints, 531

post-migration, 538–540

publishing labels

- automatic application, 142–147, 152–153

- manual application, 139–142, 151–152

publishing a runbook, 428–429**PU (public update), 28****Python runbook, 414****Q****QoS (Quality of Service)**

- Teams Phone, 658–660

- AF (Assured Forwarding) model, 659*

- desktop clients, 660–663*

- devices, 663–664*

- EF (Expedited Forwarding) model, 659*

- Group Policy, 660–663*

- mobile devices, 663–664*

- Surface Hub devices, 664–667*

quarantining spam, 579–580**R****Ray Baum's Act, 644****RBAC (role-based access control) groups, 519, 523****RBAC (role-based administrative control), 70****read-only access, Secure Score, 106****read/write access, Secure Score, 106****recording (Teams), 594, 620, 627****records, 126**

- actions, 127

- classification, 72

- controls, 84

- retention, 72

records search

- Audit log, 162–164

- Content Search, 164
 - Condition Cards*, 164
 - downloading results*, 169–174
 - exporting results*, 169–174
 - performing*, 165–168
 - responsive content*, 164

- eDiscovery, 174
 - case closing*, 185–186
 - case creation*, 176–177
 - case management*, 174
 - case member permissions*, 174–176
 - case members*, 176–177
 - case search results, exporting*, 183–185
 - content holds*, 178–181
 - content searches*, 182–183

- Recycle Bin retention policies, 125

- RegEx (regular expressions), blocked numbers and, 645

- Remote Connectivity Analyzer, migration and, 453

- remote mailboxes, hybrid configuration, 587

- reporting (SharePoint Online)

- Content Services, 881

- data governance, 881

- resource accounts (Microsoft Teams Rooms), 733

- deployment

- Exchange hybrid*, 736–738

- online only*, 734–736

- room features, 739–740

- room lists, 738–739

- resource accounts (Teams Phone System), 730

- licenses, 728

- acquiring*, 729–730

- assigning*, 730

- service numbers, 730

- assigning*, 731–732

- ordering*, 730–731

- retention labels, 122

- adaptive scopes, 149–151

- creating, 148–149

- publishing

- automatic application*, 152–153

- manual application*, 151–152

- retention of records, 72

- retention policies, 124–126, 153–156

- document versioning, 125

- migration and, 452

- Recycle Bin stages, 125

- rights, mailboxes (Exchange Online), 547–551

- risk-based access, 194–195

- risk-based conditional access, 223–224, 227

- RMS (Rights Management Service), 563

- RODC (read-only domain controller), 437

- room features (MTR (Microsoft Teams Rooms), 739–740

- room lists (MTR (Microsoft Teams Rooms), 738–739

- routing mail, Exchange Online, 432

- RTMP (Real-Time Messaging Protocol), 636

- rule editing, 349

- rule precedence, AAD Connect synchronization, 404–412

- rules

- decryption, 564

- encryption, 564

- runbooks

- graphical PowerShell workflow, 414

- Hybrid Runbook Worker, 414

- PowerShell, 413, 422

- Exchange Online script*, 423–424

- publishing*, 428–429

- testing*, 426–428

- workflow*, 413

- Python, 414

S

- SamAccountName attribute, 20–21, 313–314, 316

- SBA (survivable branch appliance), 653

- SBC (Session Border Controller), 642

- SCPs (service connection points), 432

- SDI (serial digital interface), 619

searches

- Hybrid Search (SharePoint), 830
 - cloud Search service application, 831–832*
 - content sources, 833–835*
 - prerequisites, 830–831*
 - results included, 835, 837*
 - subscription, 831*
 - troubleshooting, 835*

SharePoint Online, 888–889

SEC (Securities and Exchange Commission), 124**Secure Score, 105**

- actions for improvement, 107
- changes, 108
- Overview tab, 108
- products licensed, 106
- read-only access, 106
- read/write access, 106
- security posture
 - improvements, prioritizing, 108–112*
 - reports, 113–114*
- security posture assessment, 107–108

security

- Azure AD Conditional Access, 218–222
 - risk-based, 223–227*
- defaults, 216
- devices
 - Intune, 228–234*
 - MDM (Mobile Device Management), 227*
 - mobile application management, 228*
- DLP (data loss prevention), 566
- identity-driven, 203–206
- IOAs (indicators of attack), 208
- IOCs (indicators of compromise), 208
- MDI (Microsoft Defender for Identity), 208–218
- networks, 450–451
- Threat Policies, 560–563

security breaches, causes, 106**Send-As permission, 539, 549****Send-On-Behalf permission, 540, 549****sensitivity labels, 122, 127**

- creating, 131–138
- deploying, 128

- encryption, 133
- environment preparation, 129–130
- publishing
 - automatic application, 142–144, 147*
 - manual application, 139–142*
- sharing, 137
- synchronization, 129–131

Server Management RBAC group, 519, 523**service account**

- Azure Automation and, 415–416
- MDI (Microsoft Defender for Identity), 211

service accounts

- AAD Connect installation, 270–272
- permissions, 286

service numbers (Teams Phone System), 730

- assigning, 731–732
- ordering, 730–731

Service Support Administrator, 9**shadow IT, 204****shared channels (Teams), 776–777****SharePoint**

- files, 593
- Hybrid, 11, 13
 - one-way inbound, 11*
 - one-way outbound, 11*
 - two-way, 12*

SharePoint Administrator, 9**SharePoint Foundation Subscription Settings service (SharePoint), 823****SharePoint Migration Manager, 849****SharePoint Online**

- API access, 883
- Business Connectivity Services, 789, 893
 - Hybrid picker, 903–904*
 - Infopath, 903*
 - Manage BDC Models And External Content Types, 894*
 - Manage Connections To Online Services, 895*
 - Records Management, 897–903*
 - Secure Store, 896*

content services

Term Store, 879

controls, 78

Delve, 787

enterprise search, 788

filenames

character limits, 783

reserved characters, 783

files

blocked file types, 783

size limits, 782

governance and, 71

groups, size limits, 782

hosted applications, 783

hybrid experience, 790

labels, 121

lists, limits, 783

migrating to, 846

Azure Data box, 849

blocking issues resolved, 858

content not migrated, 858

content scanning, 856–858

custom script, 851–852

excluded items, 847–849

identity map generation, 854–856

mapping, 846–847

network, 852–853

planning, 850–852

prerequisites, 850–852

SharePoint Migration Manager, 849

SMAT (SharePoint Migration Assessment Tool),

850, 856–858

SPMT (SharePoint Migration Tool), 849,

850–851, 859–864

Migration page, 880

More Features menu, 883

Office Online, 786–787

OneDrive for Business, 783–786

policies

Access Control page, 872–873

Classic settings, 875

Settings page, 873–878

Sharing page, 870–871

reports

Content Services, 881

data governance, 881

service limits, 782

service plan limits, 783–784

site collection, 783, 868

active, 869

Active Sites page, 869

deleted, 869

hub sites, 868, 869

provisioning, automatic, 870

Store, 789

tenant name, 35

Term Store, 782, 884

User Profiles, 884

Manage Apps section, 889–893

My Site Settings section, 887

People section, 885, 887

Search Administration section, 888–889

users, limits, 783

versions, limits, 783

views, 783

Yammer, 788

SharePoint Online admin center, access control settings, 770–771

SharePoint Online Hybrid

App Launcher, 809, 814

Hybrid Picker and, 842–843

App Management service, integration setup, 822–823

authentication, server-to-server, 823–824

business-to-business extranet, 809, 814, 843

B2B (business-to-business) sites, enabling, 844

invitation model, 814

licensing, 814

Hybrid Auditing, 809

Hybrid OneDrive for Business, 809–811, 824

groups, 825

Hybrid Picker, 829–830

permissions, 825–826

prerequisites, 824

redirection, 826–828

subscription plan, 824

- Hybrid Search, 809–813, 830
 - cloud hybrid search, 811*
 - cloud Search service application, 831–832*
 - content sources, 833–835*
 - hybrid federated search, 811*
 - prerequisites, 830–831*
 - results included, 835–837*
 - subscription, 831*
 - troubleshooting, 835*
- Hybrid taxonomy, 809, 813, 837
 - copying to SharePoint Online, 838–839*
 - Hybrid Picker and, 839–841*
 - prerequisites, 837–838*
 - Timer service, 838*
- managed metadata service, integration setup, 816–818
- My sites, integration setup, 818–819
- need for, 815
- requirements, 810–811
- SharePoint Foundation Subscription Settings service, 823
- User Profile service, integration setup, 820–822
- sharing**
 - documents, OneDrive for Business, 915
 - external, 798–801
 - Microsoft 365, 763*
 - folders, OneDrive for Business, 915
 - invitation troubleshooting, 778
 - organizations, 586
- sharing management, Microsoft 365 admin center, 766–767**
- Sharing page (SharePoint Online), 870–871**
- Sharing policy, 804–806**
- SID (Security Identifier), 396**
- Sign-In Risk Policy, 195**
- sign-in status, synchronized identities, 243**
- site architecture**
 - access, 798
 - external sharing, 798–801*
 - guest identities, 799*
 - site level, 803–804*
 - tenant level, 801–803*
 - Azure B2B SharePoint integration, 800–801
 - hubs
 - designating, 792*
 - planning, 791–793*
 - navigation
 - global, 795*
 - hub sites, 795*
 - local, 795*
 - security options, 804–806
 - Sharing policy, 804–806
 - site planning, 791–793
 - taxonomy, 796–797
 - topology, 796–797
 - users, 798
- site collection (SharePoint Online), 868**
 - active, 869
 - Active Sites page, 869
 - deleted, 869
 - hub sites, 868–869
 - provisioning, automatic, 870
- site level access, 803–804**
- SIT (sensitive information type), 118**
 - built-in, 118
 - custom, 119
 - document fingerprinting, 119
- SMAT (SharePoint Migration Assessment Tool), 850, 856–858**
- SOA (Source of Authority), 396**
- Social Security Number, 320**
- source data, migrating to SharePoint Online, 846**
- SourceAnchor attribute, 349**
 - migration and, 381–388
 - mS-DS-ConsistencyGuid and, 382–389
- SourceAnchor Metaverse attribute, 389**
- SourceAnchorBinary attribute, VBA Expressions, 389**
- spam, 574**
 - filters, 576–578
 - outbound
 - blocked accounts, 581*
 - filtering, 581*
 - quarantine, 579–580

- SPF records, 450
- SPF (Sender Policy Framework) records, DNS configuration, 40
- splatting (PowerShell), 735
- split-tunnel VPN, Teams Phone, 658
- SPMT (SharePoint Migration Tool), 849–851, 859–864
- spoofing, 575
- SQL Server
 - 100,000 items, 269–270
 - AAD Connect installation, 269–270
- SRV (Server Resource) records, DNS configuration, 40
- SRV (service locator) record, 434
- SSL (Secure Sockets Layer), offloading, 440
- SSO (single sign-on), 283
- staged migration, 435
- Staging Mode, ADD Connect, 340–343
- standard meetings (Teams), 610
- Stream, Microsoft Teams and, 631–633
- Surface Hub, QoS (Quality of Service), 664–667
- synchronization
 - AAD Connect, 8, 266, 272, 340–343
 - devices, 347–348
 - directories, 10, 287
 - filter scoping, 313
 - groups and, 444–445
 - dynamic distribution*, 445
 - Microsoft 365 groups*, 445–446
 - on-premises and cloud users, 442–443
 - passwords, 330–331
 - rule precedence, 404–412
 - users, 58–59
- synchronized identities, 237–238

T

- TargetApplicationUri, 585
- TargetAutodiscoverEpr, 586
- TargetOwaURL, 586
- TargetSharingEpr, 586
- taxonomy, sites architecture, 796–797
- Teamifying, 589
- Teams Administrator, 9
- Teams Phone System
 - Auto attendants, 749–750
 - Call Flow*, 752
 - Call Flow For After Hours*, 755
 - Call Routing*, 752
 - Dial By Extensions*, 754
 - Directory Search*, 754
 - greeting*, 753–756
 - operator options*, 751
 - redirect*, 753
 - Voice Command*, 754
 - voice mail*, 759
 - voice mail, checking*, 758
 - caller ID, 716–718
 - calling policies, 706
 - assigning*, 709–711
 - configuring*, 707–709
 - calling restrictions, 701
 - inbound calling*, 701–703
 - outbound calling*, 703–705
 - call parking, 712
 - park and pick up*, 712–714
 - policies*, 714–716
 - call routing, 726
 - call queues, 743–744
 - Call Overflow Handling*, 747
 - Conference Mode*, 746
 - greeting*, 745–746
 - prerequisites*, 743
 - Presence-Based Routing*, 747
 - Routing Method*, 747
 - timeout handling*, 748
 - communications credits, 699–700
 - E911, 672–673
 - emergency calling policies*, 681–683
 - emergency routing*, 673
 - ESRP (Emergency Service Routing Provider)*, 683
 - LIS (Location Information Service)*, 675–681
 - networks*, 674
 - trusted IP*, 674

Holidays configuration, 741–743

phone numbers

- acquiring*, 683–696
- assigning*, 696–699
- blocking*, 702
- ordering from Microsoft*, 684–688
- porting*, 688–696
- unblocking*, 703

PowerShell module, 672

resource accounts

- creating*, 727–728
- licensing*, 728–730
- service numbers*, 730–732

service numbers, 730

- assigning*, 731–732
- ordering*, 730–731

VECs (voice-enabled channels), 748–749

voicemail, 718

- policies*, 719–721
- settings*, 721–723

technical actions, Compliance Manager, 90

tenant

- access, 8–9
- domain name, 5
- name, 3–4
 - Domain Name and*, 4
 - Exchange Online*, 34
 - Microsoft 365 Apps*, 36
 - MicrosoftTeams*, 36
 - Office Online apps*, 37
 - OneDrive for Business*, 35
 - SharePoint Online*, 35

tenant level access, 801–803

Term Store (SharePoint Online), 879, 884

- Content Type Gallery, 879

text messages, authentication code, 218

Threat Policies, 560–563

topology, site architecture, 796–797

TOTP (Time-Based One-Time Passwords), 193

traditional meetings (Teams), 610

trainable classifiers, 121

transcribing meetings (Teams), 620

transport (Exchange Online)

- Allow list, 567–568
- Block list, 567–568
- Central Mail Transport, 566–567
- connectors, 557
- DKIM, 572–573
- encryption, 563–564
- enhanced filtering, 569
- IP filtering lists, 567–568
- message attachments, 565–566
- Message Trace, 569–570
- rules, 557
 - actions*, 558
 - attachment blocking*, 560–563
 - conditions*, 558
 - creating*, 558–559
 - exceptions*, 558
 - export*, 571
 - import*, 571–572
 - migration*, 570–571

troubleshooting

- Hybrid Configuration Wizard, 482
- mailbox migration, 509–513
- OneDrive for Business synchronization, 934–935
- public folder migration, 540–543
- sharing invitations, 778
- Teams
 - adding members*, 778–779
 - channels, external people*, 780
 - user domains*, 779–780

TXT record, 5, 10**U****Uniquely Identifying Your Users dialog, 290–299****updates**

- Exchange, 441
- OU (Office Update), 28
- Outlook, 27
- PU (public update), 28
- software client, 53–57
- Windows, 441

UPNs, 260

- AAD Connect Custom installation, 287–290

UPN (UserPrincipalName), 25–26**URI (Uniform Resource Identifier), 585****User Administrator, 9**

- user joins, directories, 314

- usernames, 192

UserPrincipalName attribute, 19

- migration and, 395–396

User Profile service (SharePoint), hybrid integration setup, 820–822**User Profiles (SharePoint Online), 884**

- Manage Apps section, 889–890

- Manage license, 892–893*

- Monitor Apps, 893*

- SharePoint store, 891–892*

- My Site Settings section, 887

- People section, 885–887

- Search Administration section, 888–889

User Risk Policy, 194**users**

- Azure AD Cloud Sync, 357

- call parking, 715

- call policies, 709–710

- guest accounts, Azure Active Directory, 69

- identities, cloud identities, 239–240

- licensing, 59

- group based, 59–61*

- manual assignment, 63–64*

- PowerShell, 61–63*

- mail-enabled

- Exchange Online, 553*

- mailbox users and, 442*

- OU (organizational unit), 263

- plans, 2

- provisioning, Azure AD Cloud Sync, 373–376

- site architecture and, 798

- synchronization to Active Directory, 58–59

- synchronizing on-premises and cloud, 442–443

user SIDs, 396**User Writeback, 346****V****VBA Expressions, 366–369**

- SourceAnchorBinary attribute, 389

VECs (voice-enabled channels), 748–749

- versioning documents in OneDrive for Business, 917–920

- video (Teams), 617–619

voicemail

- Auto attendants (Teams Phone System), 758–759

- Microsoft Teams, 594

- Teams Phone System, 646, 718

- policies, 719–721*

- settings, 721–723*

VoIP (Voice over Internet Protocol), 643

- DNS configuration, 40

- VPNs (virtual private networks), Teams Phone, 658

W

- WAAD (Windows Azure Active Directory), 345

- waffle icon, 6

- WAP (Web Application Proxy) server, ADFS and, 255

- webhooks, 414

- webinars (Teams), 613

- registration, 614–615

- versus meetings, 615

- Windows updates, 441

- Windows Shell, 42

writeback

- Device Writeback, 348

- Exchange Hybrid Writeback, 348

- Group Writeback, 348

X–Y–Z

- XML, Outlook, 433

- Yammer, 788

- Microsoft Teams and, 634