Exam Ref 70-347

Prepare for Microsoft Exam 70-347—and help demonstrate your real-world mastery of the skills needed to help securely and efficiently provide Microsoft Office 365 services in any environment. Designed for experienced IT pros ready to advance their status, Exam Ref focuses on the critical-thinking and decision-making acumen needed for success at the MCSA level.

Focus on the expertise measured by these objectives:
- Manage clients and end-user devices
- Provision Microsoft SharePoint Online site collections
- Configure Microsoft Exchange Online and Skype for Business for end users
- Plan for Exchange Online and Skype for Business

This Microsoft Exam Ref:
- Organizes its coverage by exam objectives
- Features strategic, what-if scenarios to challenge you
- Provides exam preparation tips written by a top trainer, consultant, and sysadmin
- Assumes you have experience with the Office 365 Admin Center and an understanding of Exchange Online, Skype for Business, SharePoint Online, Office 365 ProPlus, and Microsoft Azure Active Directory

Exam Ref 70-347 focuses on the skills and knowledge needed to help securely and efficiently provide Office 365 services with SharePoint Online, Exchange Online, and Skype for Business.

About Microsoft Certification
Passing this exam helps you earn an MCSA: Office 365 Solutions Associate certification, demonstrating your skills in transitioning to and administering cloud-hosted business applications with Office 365.

You can earn this certification by passing Exam 70-346, Managing Office 365 Identities and Requirements; and Exam 70-347, Enabling Office 365 Services.

See full details at: microsoft.com/learning

About the Author
Orin Thomas is a consultant, writer, server administrator, speaker, and Microsoft MVP and Regional Director. His more than 30 Microsoft Press books include Exam Ref 70-346 Managing Office 365 Identities and Requirements. He specializes in network security, knowledge management, and collaboration technologies.

Microsoft Press

Enabling Office 365 Services

Exam Ref 70-347

U.S.A. $39.99
Canada $49.99
(Recommended)

Corporate Licensing Available: microsoft.com/mspress


For the latest Microsoft Press releases, go to: microsoft.com/mspress

microsoft.com/mspress

Enabling Office 365 Services

Orin Thomas

Microsoft Press
Exam Ref 70-347
Enabling Office 365 Services

Orin Thomas
Contents at a glance

Introduction xi
Preparation for the exam xv

CHAPTER 1  Manage clients and end-user devices 1
CHAPTER 2  Provision SharePoint Online site collections 81
CHAPTER 3  Configure Exchange Online and Skype for Business
  Online for end users 147
CHAPTER 4  Plan for Exchange Online and Skype for Business Online 229

Index 319
Contents

Introduction xi
  Microsoft certifications xi
  Free ebooks from Microsoft Press xii
  Errata, updates, & book support xii
  We want to hear from you xii
  Stay in touch xiii
  Preparing for the exam xv

Chapter 1  Manage clients and end-user devices 1
  Objective 1.1: Manage user-driven client deployments ................. 1
    Restrict self-provisioning of Office 365 ProPlus 2
    Office 365 and mobile devices 6
    Manage activation 8
    Office for Mac 13
    Objective summary 23
    Objective review 24
  Objective 1.2: Manage IT deployments of Office 365 ProPlus ........... 24
    Manual deployment 25
    Central deployment 29
    Office Deployment Tool 30
    Configuration.xml 32
    Objective summary 35
    Objective review 36

What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can continually improve our
books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/
Objective 1.3: Set up telemetry and reporting ....................... 36
  Set up telemetry service 37
  Telemetry Dashboard details 57
  Configure Telemetry Agent through registry 59
  Report user issues 59
  Objective summary 62
  Objective review 63

Objective 1.4: Plan for Office clients ............................... 64
  Outlook client 64
  Skype for Business Online client 67
  Office on Demand 68
  Office Web Apps 69
  Click-to-Run vs. MSI 70
  Objective summary 73
  Objective review 74

Answers ........................................................................... 75
  Objective 1.1: Thought experiment 75
  Objective 1.1: Review 75
  Objective 1.2: Thought experiment 76
  Objective 1.2: Review 76
  Objective 1.3: Thought experiment 77
  Objective 1.3: Review 77
  Objective 1.4: Thought experiment 78
  Objective 1.4: Review 78

Chapter 2  Provision SharePoint Online site collections 81

  Objective 2.1: Configure external user sharing .................. 81
    Understanding external users 82
    Enabling external user sharing globally 83
    Enabling external user sharing per site collection 86
    Sharing with external users 88
    Removing external user access 93
    Objective summary 96
    Objective review 97
Objective 2.2: Create SharePoint site collection .......................... 98
   Understanding site collection administrators 99
   Understanding resource quotas 100
   Using SharePoint Online Public Websites 102
   Setting storage quota for site collection 103
   Managing site collections 109
   Objective summary 116
   Objective review 117

Objective 2.3: Plan a collaboration solution............................ 118
   Using newsfeeds and Yammer 119
   Documenting coauthoring 122
   Using OneDrive for Business 126
   Understanding the App Store 134
   Understanding Enterprise eDiscovery 135
   Objective summary 139
   Objective review 140

Answers ................................................................. 142
   Objective 2.1: Thought experiment 142
   Objective 2.1: Review 142
   Objective 2.2: Thought experiment 143
   Objective 2.2: Review 143
   Objective 2.3: Thought experiment 145
   Objective 2.3: Review 145

Chapter 3 Configure Exchange Online and Skype for Business
Online for end users ............................................ 147

Objective 3.1: Configure additional email addresses for users........ 147
   Managing email addresses 148
   Managing SIP addresses 158
   Objective summary 166
   Objective review 166
Objective 3.2: Create and manage external contacts, resources, and groups ........................................ 167
  Delegating permissions 167
  Creating shared mailboxes 175
  Managing resource mailboxes 177
  Managing external contacts 183
  Managing distribution groups 185
  Objective summary 194
  Objective review 195

Objective 3.3: Configure personal archive policies ................................. 196
  Enabling personal archive for mailboxes 196
  Understanding retention tags and retention policies 201
  Objective summary 213
  Objective review 214

Objective 3.4: Configure Skype for Business Online end-user communication settings ......................... 215
  Configuring presence 215
  Configuring external communication 216
  Configuring user options 220
  Objective summary 222
  Objective review 223

Answers ................................. 224
  Objective 3.1: Thought experiment 224
  Objective 3.1: Review 224
  Objective 3.2: Thought experiment 225
  Objective 3.2: Review 225
  Objective 3.3: Thought experiment 226
  Objective 3.3: Review 226
  Objective 3.4: Thought experiment 227
  Objective 3.4: Review 228
Chapter 4  Plan for Exchange Online and Skype for Business Online 229

Objective 4.1: Manage anti-malware and anti-spam policies . . . . 229
  Anti-malware policies 230
  Connection filter policies 239
  Spam filter policies 242
  Outbound spam policy 254
  Quarantine 256
  Objective summary 259
  Objective review 260

Objective 4.2: Recommend a mailbox migration strategy . . . . . 262
  Remote move migration method 262
  Staged migration method 264
  Cutover migration method 266
  IMAP migration 268
  Migration comparison 270
  Objective summary 271
  Objective review 271

Objective 4.3: Plan for Exchange Online . . . . . . . . . . . . . . . 272
  Plan client requirements for archive 273
  In-place hold and litigation hold 278
  Configure OWA access 293
  Configure ActiveSync 295
  Objective summary 299
  Objective review 300

Objective 4.4: Manage Skype for Business global external communications settings . . . . . . . . . . . . . . . . . . . . . . 301
  Manage external communication and domains 301
  Manage Skype consumer connectivity 304
  Customize meeting invitations 305
  Disable push notifications 306
  Objective summary 308
  Objective review 309
What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/
Introduction

The 70-347 exam deals with advanced topics that require candidates to have an excellent working knowledge of Office 365, Exchange Online, SharePoint Online, and Skype for Business Online. Some of the exam comprises topics that even experienced Office 365, Exchange Online, SharePoint Online, and Skype for Business Online administrators may rarely encounter unless they are consultants who deploy new Office 365 tenancies on a regular basis.

Candidates for this exam are Information Technology (IT) Professionals who want to validate their advanced Office 365, Exchange Online, SharePoint Online, and Skype for Business Online management skills, configuration skills, and knowledge. To pass this exam, candidates require a strong understanding of how to manage and configure Office 365 clients and user devices, provision SharePoint Online site collections, configure Exchange Online and Skype for Business Online for users, and manage, migrate to, and administer Exchange Online and Skype for Business Online. To pass, candidates require a thorough theoretical understanding, as well as meaningful practical experience implementing the technologies involved.

This book covers every exam objective, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions themselves and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the links you’ll find in text to find more information and take the time to research and study the topic. Great information is available on TechNet, through MVA courses, and in blogs and forums.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.
More Info  All Microsoft Certifications


Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, and are ready for you to download at:

http://aka.ms/mspressfree

Check back often to see what is new!

Errata, updates, & book support

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

http://aka.ms/ER347/errata

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

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

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.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!
Stay in touch

Let’s keep the conversation going! We’re on Twitter: http://twitter.com/MicrosoftPress.
Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam ref and another study guide for your "at home" preparation, and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

Note that this Exam Ref is based on publicly available information about the exam and the author’s experience. To safeguard the integrity of the exam, authors do not have access to the live exam.
CHAPTER 2

Provision SharePoint Online site collections

SharePoint Online allows collaboration for people within an organization, and also allows collaboration with people who are external to the organization. For many organizations, SharePoint Online has taken the place of the traditional shared file server when it comes to sharing documents. Understanding how to configure and manage SharePoint Online site collections is critical for an Office 365 administrator. Administrators must ensure that resources are externally shared when appropriate, and that access to resources is restricted when required.

Objectives in this chapter:

- Objective 2.1: Configure external user sharing
- Objective 2.2: Create SharePoint site collection
- Objective 2.3: Plan a collaboration solution

Objective 2.1: Configure external user sharing

This objective deals with the settings related to allowing people external to your organization’s Office 365 tenancy access to content stored within SharePoint Online. There are a variety of sharing options, from allowing read and edit access to people with Microsoft accounts, to allowing read and edit access to anyone who has the correct URL for a document.

This objective covers the following topics:

- Enable external user sharing globally
- Enable external user sharing per site collection
- Share with external users
- Remove external user access
Understanding external users

External users are people who need to collaborate with people in your organization using content hosted on SharePoint Online, but who haven’t been provisioned with an organizational Office 365 or SharePoint Online license.

The use rights available to external users depend on the features available to the SharePoint Online tenancy with which they will collaborate. For example, if your organization has an E3 Enterprise Plan, and a SharePoint site uses enterprise features, the external user will be able to use and view those enterprise features.

External users can perform the following tasks:

- Can use Office Online to view and edit documents in the browser. Can use their own version of Office to interact with content hosted in SharePoint Online, but are not eligible for licenses to the tenancy’s Office 365 Office ProPlus software.
- Perform tasks on the site commensurate with their permission level. For example, adding an external user to the Members group grants that user Edit permissions. They will be able to add, edit, and delete lists, list items, and documents.
- View other site content, including navigating to subsites to which they have been invited, and view site feeds.

External users are restricted from being able to perform the following tasks:

- Create personal sites
- Edit their profiles
- View the company-wide newsfeed
- Add storage to the tenant storage pool
- Enact searches against “everything” or access the Search Center
- Access site mailbox
- Access PowerBI features, including Power View, Power Pivot, Quick Explore, and Timeline Slicer
- Use eDiscovery
- Open downloaded documents protected by Azure Rights Management (it is still possible to open these documents using Office Online)
- Access SharePoint Online data connection libraries
- Use Excel Services features, such as Calculated Measures and Calculated Members, decoupled Pivot Tables and PivotCharts, Field List and Field support, filter enhancements, and Search Filters
- Use Visio Services
Enabling external user sharing globally

The external sharing options configured at the SharePoint Online tenancy level override those configured at the site collection level. You can configure the following global external sharing options shown in Figure 2-1:

- Don't Allow Sharing Outside Your Organization.
  - Choosing this option prevents all users on all sites within the SharePoint Online tenancy from sharing sites or content with external users.
- Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users.
  - Choosing this option requires external users who have invitations to view content or sites to sign in with a Microsoft account, such as an Outlook.com account.
  - Site owners and users with Full Control permissions are able to share sites with external users.
  - Site owners and users can choose to allow external users View or Edit permissions on documents.
  - All external users must sign in with a Microsoft account before they can access content.
  - Invitations to view content can only be redeemed once, and then are tied to the Microsoft account used for access. After an invitation has been used, it cannot be used by someone else to gain access with a separate set of Microsoft account privileges.
- Allow Both External Users Who Accept Sharing Invitations And Guest Links.
  - Choose this option if you want to allow content to be shared with people who sign in with Microsoft accounts as well as allow anonymous guest links. Anonymous guest links allow access without any form of authentication.
  - Site owners and users with Full Control permission are able to share sites with external users.
  - Site owners and users with Full Control permission are able to choose between requiring sign-in or sending an anonymous guest link when sharing documents.
  - When sharing a document, site owners and users can select between granting View and Edit permissions.
  - All external users will be required to sign in with a Microsoft account before accessing content.
Anonymous links can be shared and forwarded, meaning that unauthorized people can be granted the permission assigned when the document is shared with the anonymous guest link.

To configure external user sharing for the SharePoint Online tenancy, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This opens the SharePoint Admin Center.
3. In the SharePoint Admin Center, click Settings, as shown in Figure 2-2.

![SharePoint Admin Center](image)

**FIGURE 2-2 SharePoint Admin Center**

4. Scroll down within the settings area until you get to the External Sharing section and choose between one of the three following options shown in Figure 2-3:
   - Don’t Allow Sharing Outside Your Organization
   - Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users
   - Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links
Objective 2.1: Configure external user sharing

CHAPTER 2

85

FIGURE 2-3 External Sharing settings

Turning off external sharing has the following consequences:

- If you disable and then re-enable external sharing, external users who have been granted access to content will regain access.
- If you disable and then re-enable external sharing, site collections that had sharing enabled will have sharing re-enabled.
- If you want to block specific site collections from having sharing re-enabled, disable external sharing on a per site collection basis prior to re-enabling external sharing.
- When you disable external sharing on a specific site collection, any configured External User permissions for that site collection are permanently deleted.
- Turning off external sharing at the site collection level disables guest links, but does not remove them. To remove access to specific documents, you need to disable anonymous guest links.
- Changes made to external access do not occur immediately, and might take up to 60 minutes.

MORE INFO EXTERNAL SHARING

You can learn more about external sharing at https://support.office.com/en-us/article/Manage-external-sharing-for-your-SharePoint-Online-environment-c8a462eb-0723-4b0b-8d0a-70feae4be85.
Enabling external user sharing per site collection

Only SharePoint Online administrators are able to make changes to the SharePoint Online tenancy’s external user sharing settings. Site collection administrators are allowed to configure sharing settings on a per site collection basis as long as external user sharing is set to one of the following options:

- Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users.
- Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links

The sharing options at a site collection level are similar to those that are available at the SharePoint Online tenancy level, and are shown in Figure 2-4.

These options have the following properties:

- Don’t Allow Sharing Outside Your Organization
  - Prevents all users on all sites in the collection from sharing sites or content with external users.
  - Users are unable to share content or sites with users who are not members of their organization’s Office 365 tenancy.
  - If sharing had been enabled previously, any permissions assigned to external users will be deleted.
- Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users
Allow users with Microsoft accounts who have been sent invitations to access sites and content in a site collection.

Site owners and users with Full permission can share sites and documents with external users who sign in with a Microsoft account.

Invitations that are redeemed by external users are tied to the redeeming Microsoft account, and access cannot be shared with other Microsoft accounts.

 Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links

Site owners and users with Full Control permissions are able to share sites and documents with external users.

Allows sites within a site collection that have been authenticated with Microsoft accounts to be shared with users.

Invitations that are redeemed by external users are tied to the redeeming Microsoft account. Access cannot be shared with other Microsoft accounts.

Site owners and users with Full Control permissions are able to share documents through an anonymous link.

When sharing documents with external users or through anonymous links, View or Edit permission can be assigned.

Anonymous links can be shared with the original sharer, having no control over which external parties access anonymously shared content after the guest link has been forwarded.

Settings configured at the SharePoint Online tenancy level determine those available at the individual site collection level. If sharing is only allowed for external users at the SharePoint Online tenancy level, the option to allow anonymous guest links to be sent at the site collection level will not be available. If sharing is blocked at the SharePoint Online tenancy level, then sharing will not be possible at the site collection level. Modifications to the external sharing settings for the My Site site collection apply to any existing personal sites as well as any personal sites created in the future.

To configure sharing at the site collection level, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.

2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.

3. In the Site Collections area, select the site collection for which you want to configure sharing, and click Sharing in the Site Collections toolbar shown in Figure 2-5.

![Site Collections](image)

**FIGURE 2-5** Site Collections
4. On the Sharing dialog box, shown in Figure 2-6, specify the type of sharing you want to enable, and click Save.

![Sharing dialog box]

**FIGURE 2-6** Sharing options

Sharing settings configured at the site collection level determine the sharing options available at the document level. If sending anonymous links is not allowed at the site collection level, it will not be allowed from a document hosted within a site in that collection.

**MORE INFO SITE COLLECTION SHARING**

You can learn more about sharing at the site collection level at [https://support.office.com/en-us/article/Manage-external-sharing-for-your-SharePoint-Online-environment-c8a462eb-0723-4b0b-8d0a-70fefa4b85](https://support.office.com/en-us/article/Manage-external-sharing-for-your-SharePoint-Online-environment-c8a462eb-0723-4b0b-8d0a-70fefa4b85).

**Sharing with external users**

After sharing is appropriately configured at the SharePoint Online tenancy level and at the site collection level, there are three basic methods that allow you to share content with external users:

- Share an entire site and invite users to sign in using a Microsoft account (including Office 365 accounts from separate organizations, such as workplaces or schools).
- Share individual documents by inviting external users to sign in using a Microsoft account.
Send users a guest link that allows users external to the organization access to each individual document that you want to share anonymously.

Sharing a site
To share a site with an external user, perform the following steps:

1. Sign in to Office 365 with an account that has permission to share the site. Select Sites from the list of My Apps as shown in Figure 2-7.

   ![Office 365 Apps](image)

   **FIGURE 2-7** Office 365 Apps

2. In the list of sites, select the site that you want to share.

3. In the upper right-hand corner of the Site page, click Share, as shown in Figure 2-8.

   ![Share](image)

   **FIGURE 2-8** Share

4. On the Share Site dialog box, shown in Figure 2-9, provide the name of the person with whom you want to share the site, specify the permission level, and click Share. You can choose between the following levels:
   - Excel Services Viewers [View Only]
   - Team Site Members [Edit]
   - Team Site Owners [Full Control]
   - Team Site Visitors [Read]
An invitation will automatically be sent to the person or people who you invited. If the invitation isn’t accepted within seven days, it will expire. Users accepting an invitation must sign in with a Microsoft account, such as an Outlook.com or Hotmail.com account, or an Office 365 account.

You can determine which external users a SharePoint Online site collection has been shared with by performing the following steps:

1. Sign in to Office 365 with an account that has permission to share the site and select Sites from the list of My Apps.
2. In the list of sites, select the site that you want to share.
3. In the upper right-hand corner of the Site page, click Share, as shown in Figure 2-10.
4. On the Share Site dialog box, click Shared With, as shown in Figure 2-11. The dialog box will list all users with whom the site collection has been shared.
Sharing a document

There are two ways to share a document: sharing with an external user who must authenticate and sharing through an anonymous guest link.

To share with an external user who must authenticate using a Microsoft account, which includes the option of using an Office 365 account, perform the following steps:

1. Sign in to Office 365 with an account that has permission to share the site, and select Sites from the list of My Apps.
2. In the list of sites, select the site that hosts the document that you want to share.
3. Next to the document that you want to share, click the ellipses and then click Share, as shown in Figure 2-12.

![Share Document](image-url)
4. On the Share page, select Invite People and then type the Microsoft account addresses of the people with whom you want to share the document. You can choose between the permissions Can Edit and Can View. Select the Require Sign-In check box to require the account be used to sign in. If this option is not selected, a link will be generated and forwarded to the email address provided. Figure 2-13 shows the document Example1 shared to the Microsoft account orin.thomas@outlook.com, with the permission that allows the user of that account to edit the document.

![Figure 2-13: Share document](image)

5. Click Share to share the document.

You can view the Shared With section of the Shared dialog box to view a list of users who have access to this shared document. Figure 2-14 shows the document Example1 shared with Orin Thomas.

![Figure 2-14: Shared With](image)
The process of creating a shared link is similar. Sign in to Office 365, locate the document that you want to share, and then open the Sharing dialog box by clicking the ellipses next to the file and clicking Share. On the Get A Link section, you have the option of creating a View Only link, an Edit link, or both. Figure 2-15 shows a document where a View Only link and an Edit link have been created. You can click Disable on this dialog box to disable one or both links.

![Share 'Example1' dialog box](image)

**FigURE 2-15** Get A Link

MORE INFO SHARE SITES OR DOCUMENTS WITH EXTERNAL USERS

You can learn more about sharing sites or documents with external users at [https://support.office.com/en-us/article/Share-sites-or-documents-with-people-outside-your-organization-80e49744-e30f-44db-8d51-16661b1d4232](https://support.office.com/en-us/article/Share-sites-or-documents-with-people-outside-your-organization-80e49744-e30f-44db-8d51-16661b1d4232).

**Removing external user access**

You can revoke external user access to a site only after a user has accepted their invitation. You can revoke access by removing the external user’s permission to the site. To revoke access, perform the following steps:

1. Sign in to Office 365 with an account that has permission to share the site and select Sites from the list of My Apps.
2. In the list of sites, select the site that you want to share.
3. Select Settings, which is represented as a cogwheel, and then click Site Settings, as shown in Figure 2-16.
4. Under Users And Permissions, click People And Groups, as shown in Figure 2-17.

5. Select the external user from whom you want to revoke access. Figure 2-18 shows the Orin Thomas external user selected.
6. From the Actions menu, click Remove Users From Group, as shown in Figure 2-19.

![Figure 2-19 Remove Users From Group](image)

FIGURE 2-19 Remove Users From Group

7. When prompted about removing users from the group, as shown in Figure 2-20, click OK.

![Figure 2-20 Confirmation message](image)

FIGURE 2-20 Confirmation message

There is no way, at the SharePoint Online tenancy level, to determine all of the sites to which an external user has been granted access. It is necessary to view the settings for individual sites to determine if a specific external user has been granted access to the site. There is also no method, at the SharePoint Online tenancy level, to determine which documents have been shared externally.

MORE INFO REVOKE USER ACCESS

You can learn more about revoking user access at https://support.office.com/en-us/article/Share-sites-or-documents-with-people-outside-your-organization-80e49744-e30f-44db-8d51-16661b1d4232.

EXAM TIP

Remember that the sharing settings configured at the SharePoint Online level will override the settings that can be configured at the site collection level.
**Thought experiment**

**Removing external user access at Contoso**

In this thought experiment, apply what you learned about this objective. You can find answers to these questions in the “Answers” section at the end of this chapter.

After performing an audit of how content was being shared from your organization’s SharePoint Online tenancy, management has decided that it will no longer allow users to share content with users anonymously. In the future, all content shared with external users can only be shared if the user has a Microsoft or an Office 365 account. Management is also concerned about one external user, Kim, who has had content shared with her across multiple site collections. Kim has recently started working for a competitor and management wants to remove her current access to information in your organization’s SharePoint Online site collections. With this information in mind, answer the following questions:

1. What’s the quickest method of stopping anonymous users from accessing SharePoint Online content?
2. What steps need to be taken to remove the external user’s access from site collections?

**Objective summary**

- External users are people with whom Office 365 SharePoint Online content can be shared.
- External users can authenticate with a Microsoft account, including an Office 365 account that is not part of the organization’s tenancy.
- At the global level, you can configure an option for block sharing to external users, allow external users who have authenticated with Microsoft, or allow users who have authenticated with a Microsoft account and who have been provided with an anonymous link.
- Site owners and users who have Full Control permissions on a site are able to share sites with external users.
- Invitations sent to external users remain valid for seven days.
- Sharing settings configured at the SharePoint Online tenancy level determine the sharing options available at the site collection level. If sharing is blocked at the tenancy level, it is not available at the site collection level.
- Sharing settings configured at the site collection level determine the sharing options available at the document level.
Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. How many days does an invitation to access shared content sent to an external user from an Office 365 SharePoint Site collection remain valid before it expires?
   A. 7 days
   B. 14 days
   C. 21 days
   D. 28 days

2. You want to block users sharing links and require all external users accessing shared content to authenticate using a Microsoft account. Which of the following steps can you take to accomplish this goal with a minimum amount of administrative effort?
   A. Disable sharing at the SharePoint Online tenancy level
   B. Restrict sharing to authenticated users at the SharePoint Online tenancy level
   C. Restrict sharing to authenticated users in each site collection
   D. Disable sharing in each site collection

3. You want to allow users in your organization’s Office 365 tenancy to email links that will allow anonymous access to specific documents hosted in a specific site collection. Which of the following settings must be configured to allow this to occur? (Choose two. Each answer forms part of a complete solution.)
   A. Configure the Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links option at the site collection level
   B. Configure the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users option at the site collection level
   C. Configure the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users option at the SharePoint Online tenancy level
   D. Configure the Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links option at the SharePoint Online tenancy level

4. In most circumstances, you want to allow users in your organization to be able to send anonymous links to people outside your organization to documents hosted in site collections in your organization’s Office 365 SharePoint Online tenancy. However, you want to ensure that anonymous links can’t be used for documents hosted in a specific site collection. Documents in the site collection should be able to be shared with external users who have authenticated with a Microsoft account. With this in mind, which of the following settings should be configured to accomplish this goal? (Choose two. Each answer forms part of a complete solution.)
   A. Configure the Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links option at the SharePoint Online tenancy level
B. Configure the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users option at the SharePoint Online tenancy level
C. Configure the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users option at the site collection level for the specific site collection where you want to block anonymous links
D. Configure the Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links option at the site collection level for the specific site collection where you want to block anonymous links

5. After sensitive documents were leaked from your organization, you want to block all sharing of content hosted in SharePoint Online to people external to your organization. Which of the following steps could you take to accomplish this goal with a minimum amount of administrative effort?
A. Configure the Don’t Allow Sharing Outside Your Organization option in the sharing settings of each site collection
B. Configure the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users at the SharePoint Online tenancy level
C. Configure the Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links at the SharePoint Online tenancy level
D. Configure the Don’t Allow Sharing Outside Your Organization option at the SharePoint Online tenancy level

**Objective 2.2: Create SharePoint site collection**

This objective deals with creating and managing SharePoint site collections. To master this objective, you’ll need to understand how to configure a user as a site collection administrator, how to configure resource quotas, how to apply storage quotas, and other aspects of managing site collections within SharePoint Online.

This objective covers the following topics:
- Site collection administrators
- Resource quotas
- Configure public website
- Set storage quota for site collection
- Manage site collections
Understanding site collection administrators

Site collection administrators are users who have permission to manage SharePoint Online at the top of a specified site collection. A site collection administrator has permissions over all content in the site collection, including all subsites. Each site collection is a separate permissions root. For example, a site collection that has the URL http://contoso347er.sharepoint.com/sites/Research does not have the same permissions as the site collection http://contoso347er.sharepoint.com.

A site collection has only one primary administrator, but can have multiple site collection administrators. A primary site collection administrator receives administrative email alerts for the site collection.

To configure site collection administrators for a site collection, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. Click Site Collections.
4. In the list of Site Collections, select the site for which you want to configure the site collection administrators. Figure 2-21 shows the site collection https://contoso347er.sharepoint.com/sites/TeamSiteTemp selected.

![Site Collections](image1)

FIGURE 2-21 Site Collections

5. In the Site Collections section, click Owners and then click Manage Administrators as shown in Figure 2-22.

![Manage Administrators](image2)

FIGURE 2-22 Manage Administrators
6. On the Manage Administrators dialog box, you can change the name of the Primary Site Collection Administrator, which is set when the site collection is created, and add the names of additional Site Collection Administrators. Figure 2-23 shows Don Funk set as the Primary Site Collection Administrator with Kim Akers and Dan Jump set as Site Collection Administrators.

![Manage Administrators dialog box](image)

**FIGURE 2-23** Manage Administrators

7. You can use the Check Names button to verify that the names entered are correct. When entering more than one name in the Site Collection Administrators text box, separate each name using a semicolon.

8. Click OK to assign the site collection administrator settings to the site collection.

**MORE INFO SITE COLLECTION ADMINISTRATORS**

You can learn more about site collection administrators at [https://support.office.com/en-au/article/Manage-administrators-for-a-site-collection-9a7e46f9-3fc4-4297-955a-82cb292a5be0](https://support.office.com/en-au/article/Manage-administrators-for-a-site-collection-9a7e46f9-3fc4-4297-955a-82cb292a5be0).

### Understanding resource quotas

Server resources are a numerical way of representing server resources, including RAM and CPU utilization. Each SharePoint Online deployment is allocated a server resource figure based on the number of user licenses. This server resource figure is shared across all site collections. You can view the amount of resources available for a collection on the Site Collections page. Figure 2-24 shows a tenancy where 5,300 resources are available.
Organizations that have customized site collections or sandboxed solutions can use resource quotas to ensure that resources, such as server CPU and RAM, aren’t exhausted across the tenancy. If the number of resources used in a 24-hour period exceeds the resources available, SharePoint Online turns off the sandbox. When the sandbox is turned off, custom code will not run. The sandbox will be turned back on when the 24-hour period expires and the resource number is reset.

By applying resource quotas to specific collections, administrators can ensure that custom code running in specific site collections does not deplete all server resources assigned to the tenancy. Purchasing extra user licenses will increase the overall resource allocation to the tenancy.

To configure a resource quota for a specific site collection, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. Click Site Collections.
4. Select the site collection for which you want to configure the resource quota and then click Server Resource Quota. Figure 2-25 shows the site collection https://contoso347er.sharepoint.com/sites/TeamSiteTemp selected.
5. On the Set Server Resource Quota page, specify the number of server resources to be assigned to the collection. You can also configure an email to be sent to the primary site collection administrator when the resource utilization reaches a specific percentage of the assigned quota. Figure 2-26 shows a quota set to 300 and an email alert configured to be sent when the quota reached 95 percent.

![](set_server_resource_quota.png)

**FIGURE 2-26** Server Resource Quota

6. Click Save to apply the new quota to the site collection.

**MORE INFO RESOURCE QUOTAS**


---

**Using SharePoint Online Public Websites**

SharePoint Online Public Websites were a feature that allowed organizations to create an online presence accessible to clients on the Internet without requiring authentication. As of March 2015, the SharePoint Online Public Website feature was not available to new Office 365 customers. Existing Office 365 customers will be able to use the SharePoint Online Public Website feature until March 2017. While this feature appears in the current 70-347 exam objectives, the feature becoming unavailable means that items related to it will be withdrawn from the exam.
Setting storage quota for site collection

Storage quotas determine how much storage space can be used. Office 365 tenancies are allocated an amount of storage space for SharePoint Online based on the number of users associated with the tenancy. The amount of storage space allocated to SharePoint Online uses the formula 10 GB plus 500 MB per user. For example, if an organization has 40 users associated with its Office 365 tenancy, the amount of storage space allocated to SharePoint Online is: 10 GB plus (500 MB * 40) equals 20 GB. It’s possible for organizations to purchase additional storage on top of this initial allocation, as needed. Additional storage is allocated and on a GB per month basis. A site collection can be allocated a maximum of 1 TB of storage.

You can view the current amount of storage allocated to the tenancy by performing the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. Click Site Collections. In the Site Collections area, you will be able to see the resources available as well as the remaining storage available. Figure 2-27 shows 30.42 GB available out of 30.45 GB.

![Figure 2-27: Storage use](image-url)
This storage allocation is available to all site collections associated with the tenant. It functions as a central storage pool from which all SharePoint Online storage can be allocated.

You can purchase additional storage for a tenancy by performing the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. In the Site Collections area, shown in Figure 2-28, click Buy Storage.

![Site Collections menu](FIGURE 2-28)

4. You will need to re-sign in to Office 365 with an account with tenancy Administrator permissions or Billing Administrator permissions.
5. On the Manage Subscription page, select the subscription that you would like to add additional storage to and click the Add More link next to the text that indicates the number of current licenses.
6. In the section named Optional Add-Ons, enter the additional storage in GB that you want to add to the tenancy. It is not necessary to enter information in the user license field, though you can also use this section of the Manage Subscription page to add additional user licenses to a subscription.
7. Click Add licenses and then click Place Order.

There are two ways of allocating storage:

- **Automatically** You can choose to use the pooled storage model.
- **Manually** Allows you to manually configure storage allocations on a per-site collection basis.

**MORE INFO ADD STORAGE TO SHAREPOINT ONLINE**

Pooled storage model

The pooled storage model is a feature of SharePoint Online introduced in 2015. The pooled storage model allows SharePoint Online to manage storage automatically rather than storage management being a task performed manually by an administrator. The pooled storage model will be the default setting for new subscriptions created after late 2015.

If your organization has an existing Office 365 subscription, will need to enable the pooled storage model manually. When you do this, SharePoint Online removes the existing limits that you have configured for site collections and reset the limits to 1 TB.

To configure an Office 365 tenancy to use the pooled storage model for SharePoint Online, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center as shown in Figure 2-29.
3. In the SharePoint Admin Center, select Settings, as shown in Figure 2-30.
4. Under Site Collection Storage Management, select Auto and then click OK. Note that the pooled storage feature is being rolled out in 2015. The Site Collection Storage Management area might not be available through the settings section of all Office 365 subscriptions until the end of 2015.

Per-site collection storage management

The default option for Office 365 tenancies created before mid-2015 was that storage management occurred on a per-site collection basis. If you have switched to the pooled storage model and want to switch back, or have an Office 365 tenancy created after mid-2015, you can switch to per-site collection storage management by performing the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. In the Settings section, in the Site Collection Management area, select Manual and then click OK. The Site Collection Storage Management area might not be available through the settings section of all Office 365 subscriptions until the end of 2015.
Setting site collection storage limits

You can configure storage limits on a per site-collection basis. To do this, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. Select the Site Collections area as shown in Figure 2-31.

![FIGURE 2-31 List of Site Collections](image)

4. Select the site collection for which you want to configure the quota. Figure 2-32 shows the selection of the site collection with the URL `https://contoso347er.sharepoint.com/sites/TeamSiteTemp`. 

Objective 2.2: Create SharePoint site collection  

CHAPTER 2  

107
5. On the Site Collections toolbar, click Storage Quota.

6. On the Set Storage Quota dialog box, shown in Figure 2-33, configure the following options and then click Save:

   - **Limit Storage Quota For Each Selected Site Collection To A Maximum Of** This option allows you to configure the maximum amount of storage allocated to each site collection. A figure of 0 indicates that no quota is set for the site collection.

   - **Send Email To Site Collection Administrators When A Site Collection’s Storage Reaches** Allows you to configure an email to be automatically sent after the storage allocated to the site collection reaches the specified percentage.
Managing site collections

A user with SharePoint Online Administrator permissions is able to create, delete, and restore deleted site collections.

Creating site collections

To create a site collection, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. In the site collections area, shown in Figure 2-34, click New and then click Private Site Collection.
4. On the New Site Collection page, shown in Figure 2-35, provide the following information and click OK:

- **Title**  The name of the site collection.
- **Website Address**  Allows you to specify the address of the website. Drop-down menus allow you to select the domain name and the URL path. The URL path can either have /sites/ or /teams/ after the domain name.
- **Template Selection**  Allows you to select which template to use for the site collection. Available templates are separated across the following categories: Collaboration, Enterprise, Publishing, and Custom. You also use this section to select a language from a drop-down list. Choosing the correct language at this stage of the process is critical because it is not possible to alter the language selection for the site collection after the collection is created. You can enable SharePoint's multiple language interface on a site collection, but the primary language will always be the one selected during site collection creation.
- **Time Zone**  Allows you to specify the time zone for the site collection.
- **Administrator**  Use this option to specify the administrator of the site collection. You can type the user name, or browse for a site collection administrator. You can alter the site collection administrator after the creation of the site collection.
- **Storage Quota**  Use this option to specify the storage quota in GB for the site collection up to a maximum value of 1 TB.
- **Server Resource Quota**  Use this option to specify the resources you want to allocate to this collection in terms of available resources. Resources are a combination of performance metrics related to the execution of code for sandboxed solutions.
FIGURE 2-35 New Site Collection

**Delete site collection**

As part of ensuring that data stored on SharePoint Online is not retained past the point where no one is using it, you will occasionally need to delete site collections. For example, you might want to delete a site collection used for a specific project that has long since ended. Site collections that you delete are moved to the Recycle Bin. You will read more about the Recycle Bin later in this chapter.

Deleting a site collection deletes the site hierarchy hosted within the collection. It also deletes the following user and content data stored within the site collection, including:

- Documents and document libraries
- Lists and list data
- Site configuration settings
- Site and subsite role and security information
Provision SharePoint Online site collections

- Subsites of the top-level website
- Web parts
- Document workspaces
- Content types
- User associations

To delete a site collection, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. In the Site Collections area, select the site collection that you want to delete. Figure 2-36 shows the selection of the site collection with the address https://contoso347er.sharepoint.com/sites/TeamSiteTemp.

4. In the Site Collections area, shown in Figure 2-37, click Delete.

5. On the Delete Site Collections page, shown in Figure 2-38, click Delete.
Objective 2.2: Create SharePoint site collection

**MORE INFO** CREATING AND DELETING SHAREPOINT ONLINE SITE COLLECTIONS

You can learn more about creating and deleting SharePoint Online site collections at [https://support.office.com/en-us/article/Create-or-delete-a-site-collection-3a3d-7ab9-5d21-41f1-b4bd-5200071dd539](https://support.office.com/en-us/article/Create-or-delete-a-site-collection-3a3d-7ab9-5d21-41f1-b4bd-5200071dd539).

**Restore deleted site collection**

When you delete a SharePoint Online site collection, it is moved to the Recycle Bin for 30 days before it is purged. If you need a site collection restored after this 30-day period has elapsed, you have an additional 14 days in which you can have Microsoft perform the restoration through a Service Request.

You can view the site collections in the Recycle Bin and the number of days remaining before being purged by performing the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. In the Site Collections area, shown in Figure 2-39, click Recycle Bin.

![Recycle Bin](image)

**FIGURE 2-39** Recycle Bin
4. In the Recycle Bin, you can see the list of site collections that have been deleted, and also when deleted, along with the number of days before being purged from the Recycle Bin. Figure 2-40 shows the Recycle Bin.

![Recycle Bin contents](image)

FIGURE 2-40 Recycle Bin contents

You can restore a deleted site collection under the following circumstances:

- The site collection has been in the Recycle Bin for less than 30 days.
- The usage quota for the SharePoint Online tenancy has not been exceeded.
- The storage quota for the SharePoint Online tenancy has not been exceeded.

Site collection URLs must be unique. This means that an active site collection cannot have the same URL as a deleted site collection that is still in the Recycle Bin. Should you need to create a new site with the same URL as a site in the Recycle Bin, the interface will prompt you to permanently delete the site collection. This will remove the site from the Recycle Bin.

To restore a deleted site collection, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. In the Site Collections area, shown in Figure 2-41, click Recycle Bin.

![Recycle Bin](image)

FIGURE 2-41 Recycle Bin
4. In the Recycle Bin area, select the site collection that you want to restore. Figure 2-42 shows the site collection https://contoso347er.sharepoint.com/sites/TeamSiteTemp selected. Click Restore Deleted Items.

![Figure 2-42 Recover Site Collection](image)

5. On the Restore Site Collections page, shown in Figure 2-43, click Restore.

![Figure 2-43 Restore Site Collections](image)

**MORE INFO** RESTORE DELETED SITE COLLECTION

You can learn more about restoring deleted SharePoint Online site collections at [https://support.office.com/en-us/article/Restore-a-deleted-site-collection-91c18651-c017-47d1-9c27-3a22f325d6f1](https://support.office.com/en-us/article/Restore-a-deleted-site-collection-91c18651-c017-47d1-9c27-3a22f325d6f1).
EXAM TIP
Remember the amount of time that a site collection remains in the Recycle Bin before being purged.

Thought experiment
Managing site collections at Fabrikam
In this thought experiment, apply what you learned about this objective. You can find answers to these questions in the “Answers” section at the end of this chapter.

You have recently deleted a number of site collections from your organization’s SharePoint Online tenancy. Several of these collections are still present in the Recycle Bin and others have been removed after exceeding the Recycle Bin retention period. With this information in mind, answer the following questions:

1. One of the site collections disappeared from the Recycle Bin yesterday. What steps could you take to recover it?
2. You want to create a new site collection with the URL of a recently deleted site collection. What steps must you take before you can perform this task?

Objective summary
- Site collection administrators are users who have permission to manage SharePoint Online at the top of a specified site collection.
- A site collection administrator has permissions over all content in the site collection, including all subsites.
- Server resources are a numerical way of representing server resources, including RAM and CPU utilization.
- Each SharePoint Online deployment is allocated a server resource figure based on the number of user licenses.
- If the number of resources used in a 24-hour period exceeds the resources available, the sandbox turns off and custom code will not run.
- SharePoint Online Public Websites is a functionality not available in new Office 365 subscriptions and only available in some existing subscriptions until March 2017.
- Office 365 tenancies are allocated an amount of storage space for SharePoint Online based on the number of users associated with the tenancy.
- You can assign storage quotas on a per-site collection basis to limit the amount of storage space consumed by individual site collections.
- When creating a site collection, you configure the name, URL, primary site collection administrator, template, storage quota, and server resource quota.
- A deleted site collection can be recovered from the Recycle Bin for 30 days.
Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. An organization has 40 users associated with its Office 365 tenancy. You are planning allocation of SharePoint Online storage. How much storage space will be allocated to SharePoint Online by default given this number of users?
   A. 10 GB
   B. 20 GB
   C. 30 GB
   D. 40 GB

2. What is the maximum amount of storage that can be allocated to an individual SharePoint Online site collection?
   A. 100 GB
   B. 500 GB
   C. 1 TB
   D. 5 TB

3. You have allocated a 50 GB quota to a SharePoint Online site collection. You want to be notified when 48 GB of that quota has been consumed. Which of the following steps should you take to accomplish this goal?
   A. Set the quota to 48 GB
   B. Set the quota to 52 GB
   C. Set the quota warning email threshold to 48 percent
   D. Set the quota warning email threshold to 96 percent

4. Which of the following settings cannot be changed after the creation of a site collection?
   A. Site collection administrators
   B. Storage quota
   C. Server resource quota
   D. Primary language

5. How long do deleted site collections remain in the Recycle Bin before being purged?
   A. 15 days
   B. 30 days
   C. 60 days
   D. 90 days
6. In which of the following cases will you be unable to recover a site collection from the Recycle Bin? (Choose all that apply.)
   A. Usage quota for the SharePoint Online tenant has been exceeded
   B. Storage quota for SharePoint Online tenant has been exceeded
   C. Site collection was deleted more than 50 days ago
   D. Site collection was deleted less than 20 days ago

7. How many primary site collection administrators can be assigned to a site collection?
   A. 5
   B. 1
   C. 2
   D. 10

8. You want to ensure that the custom code running in a specific site collection doesn’t consume all of the CPU and RAM resources allocated to your organization’s SharePoint Online tenancy. Which of the following steps would you take to accomplish this goal?
   A. Configure a storage quota
   B. Configure a resource quota
   C. Configure site collection administrator
   D. Purchase additional user licenses

**Objective 2.3: Plan a collaboration solution**

This objective deals with using a variety of Office 365 tools for collaboration and coauthoring. To master this objective you’ll need to understand the differences between Yammer and SharePoint newsfeeds, the settings related to coauthoring, the functionality of OneDrive For Business, the SharePoint App Store, and Enterprise eDiscovery.

**This objective covers the following topics:**
- Yammer versus newsfeeds
- Coauthoring
- Project Online
- Excel Services
- Visio Services
- OneDrive for Business
- App Store
- Enterprise eDiscovery
Using newsfeeds and Yammer
Newsfeeds and Yammer provide different methods for allowing users to share information throughout the organization.

Newsfeeds
Newsfeeds in SharePoint Online function as an organizational blog where members of the organization can post and reply to posts. A newsfeed exists at the SharePoint Online tenancy level. Newsfeeds also exist at the team site level. Figure 2-44 shows a post to the newsfeed in a SharePoint Online tenancy’s team site.

![Newsfeed](image)

FIGURE 2-44 Newsfeeds

As is the case with other social networks, users can choose to like or reply to newsfeed posts. It is also possible to follow specific users. This allows for the newsfeed filter to be switched between those users a person is following and all users in the organization. People are also able to filter newsfeed posts so that only those posts that reference them are displayed.

In the event that you want to use a newsfeed to have a conversation with a small number of users rather than everyone in the organization, and you have permission to create new sites, you can do the following:

1. Create a new SharePoint Online site.
2. Share the site with the people who you want to have included in the conversation.
3. Use the site-specific newsfeed to have the conversation.
4. Ensure that users accessing the site select the Follow option, as shown in Figure 2-45, so that the users are subscribed to the newsfeed.

![Follow option](image)

FIGURE 2-45 Follow option
Users can access all of the newsfeeds of sites that are followed through the newsfeed app. To access the newsfeed app, perform the following steps:

1. In the list of apps, shown in Figure 2-46, click Newsfeed.

![List of apps](image)

**FIGURE 2-46** List of apps

2. The Newsfeed page will show you all existing posts on sites that you are following. Figure 2-47 shows a newsfeed where a user is following two sites.

![Newsfeed app](image)

**FIGURE 2-47** Newsfeed app

3. If you are following multiple sites, you are able to select which site you post to from the Newsfeed app by using the drop down menu, as shown in Figure 2-48.
Yammer

Yammer is a private social network that has features similar to many of the larger social networks. Yammer allows people in your organization to collaborate with one another. Only people with company email addresses are able to join a company Yammer network.

To use Yammer with SharePoint Online, you need to configure Yammer as the SharePoint social collaboration option. To configure Yammer as the SharePoint social collaboration option, perform the following steps:

1. Sign in to the Office 365 Admin Center with a user account that has SharePoint Online administrator privileges.
2. Under Admin, click SharePoint. This will open the SharePoint Admin Center.
3. Click Settings. Next to Enterprise Social Collaboration, click Use Yammer.com Service, as shown in Figure 2-49.
4. Click Save.
Switching to Yammer doesn’t disable Newsfeed functionality, though it does disable the ability to make posts to everyone in the organization. Newsfeeds associated with specific sites remain in place after you have enabled Yammer.

**MORE INFO YAMMER VS. NEWSFEED**

You can learn more about Yammer versus Newsfeed at [https://support.office.com/en-us/article/Pick-your-enterprise-social-experience-Yammer-or-Newsfeed--21954c85-4384-47d4-96c2-dfa1c9d56e66](https://support.office.com/en-us/article/Pick-your-enterprise-social-experience-Yammer-or-Newsfeed--21954c85-4384-47d4-96c2-dfa1c9d56e66).

### Documenting coauthoring

The coauthoring feature of SharePoint Online allows multiple users to work on a document. This occurs in such a way that the changes made by one user do not interfere with the changes made by another. The ability to coauthor documents is enabled by default for documents stored in SharePoint Online.

Office 365 ProPlus provides coauthoring support for Word, PowerPoint, OneNote, and Visio. Coauthoring is also possible through the Word, PowerPoint, Excel, and OneNote Online web apps. The only restriction is that the Excel client application supports a Shared Workbook feature rather than direct coauthoring of workbooks stored in SharePoint Online.

When planning for document coauthoring in SharePoint Online, take the following into account:

- **Correct permissions** Every user who will coauthor a document needs to have appropriate permissions to edit the document. One method of accomplishing this goal is to give all users who need to edit the document access to the SharePoint site where the document is stored. SharePoint permissions can also be used to limit which documents within a SharePoint site can be edited by particular users.

- **Versioning** Versioning keeps track of documents and stores previous versions of a document. SharePoint Online supports major and minor versioning, with major versioning being the default value. Microsoft recommends that monitor versioning not be used for document libraries that are used with OneNote coauthoring, as it can interfere with OneNote’s built-in versioning functionality.

- **Number of versions** The number of versions kept doesn’t directly impact coauthoring, but it will impact the amount of storage space consumed by versions. The default value for SharePoint Online is 500 versions.

- **Check out** If a document is checked out by an author, the document is locked until the check out is released. This blocks coauthoring. Check out is disabled by default in SharePoint Online, but users can manually check out documents using the Advanced menu, as shown in Figure 2-50. You should warn users not to check out documents when engaging in the coauthoring process.
To configure versioning and check out settings in a SharePoint Online document library, perform the following steps:

1. In the SharePoint Site, click Documents and then click Library, as shown in Figure 2-51.

2. On the Library toolbar, shown in Figure 2-52, click Library Settings.

FIGURE 2-50 Check Out

FIGURE 2-51 Documents

FIGURE 2-52 Library Settings
3. Under the General settings area, click Versioning Settings, as shown in Figure 2-53.

4. Next to Document Version History, shown in Figure 2-54, choose whether you want to configure No versioning, Create Major Versions, or Create Major And Minor (Draft) Versions. You can also specify the number of major and minor versions to be kept. The default is to use major versions and to keep 500 major versions of a document.

5. In the Require Check Out section, shown in Figure 2-55, specify whether documents should be checked out before editing. Remember that enabling this option disables coauthoring.

6. Click OK to apply the new settings.
Objective 2.3: Plan a collaboration solution

CHAPTER 2

MORE INFO OFFICE 365 COAUTHORING

Project Online
Project Online is a standalone web service that provides browser-based portfolio and project management tools. Project Online includes Project Web App. Depending on an organization's Office 365 subscription level, it might also include Project Pro for Office 365. Project Pro for Office 365 is a desktop application that runs on client computers.

MORE INFO PROJECT ONLINE
You can learn more about Project Online at https://support.office.com/en-us/article/Get-started-with-Project-Online-e3e5f64f-ada5-4f9d-a578-130b2d4e5f11.

Excel Services
When you open an Excel file hosted in a SharePoint Online tenancy in a browser, the file opens in Excel Online. When you perform the same task with an Excel file hosted in an on-premises SharePoint 2013 deployment, the file might be opened either in Excel Services or in Excel Web App if an Office Web Apps server is present.

MORE INFO EXCEL SERVICES

Visio Services
Visio Services is included with SharePoint 2013 and Office 365. It allows Visio diagrams stored in SharePoint 2013 or SharePoint Online to be viewed in a browser without requiring a full Visio client or Visio Viewer. Visio Services works with the .VSDX Visio file format. Older Visio files in .VDW format will also be visible in a web browser through Visio Services.

MORE INFO COLLABORATION WITH VISIO SERVICES
You can learn more about collaboration with Visio Services at https://blogs.office.com/2012/09/18/sharing-diagrams-with-visio-services/.
Using OneDrive for Business

OneDrive for Business, formerly known as SkyDrive Pro, is a location that allows you to store, sync, and share work files. OneDrive for Business is separate from OneDrive, which was formerly known as SkyDrive. OneDrive for Business differs from OneDrive in the following ways:

- OneDrive is associated with a personal Microsoft account. People in your organization cannot access or manage OneDrive.
- OneDrive for Business is managed by an organization and is made available through an Office 365 subscription. This means that files stored in OneDrive for Business can be accessed by Office 365 administrators. OneDrive for Business allows Office 365 users to share files with each other for the purposes of collaboration. OneDrive for Business can also be used with an on-premises SharePoint deployment. As this is an Office 365-related exam, using OneDrive for Business is not covered.

Accessing OneDrive for Business

A user can access OneDrive for Business by performing the following steps:

1. Sign in to Office 365 with your user account.
2. On the list of apps, shown in Figure 2-56, click OneDrive.

![App list](image)

**FIGURE 2-56** App list

3. The OneDrive for Business site, which is a SharePoint Online personal site, will be opened. Documents can be uploaded to this site or created and added to this location. It is also possible to create a folder hierarchy in this location. Figure 2-57 shows a OneDrive for Business page with several documents and folders.
Collaborating with OneDrive for Business

Collaborating with someone using OneDrive for Business is very similar to collaborating using SharePoint Online. This makes sense considering OneDrive for Business stores data in SharePoint Online. The main difference is that the sharing done through SharePoint Online directly is usually managed by an administrator. The sharing done through OneDrive for Business is usually managed directly by an end user.

An end user can choose to share individual files or can create and share folders. As is the case with SharePoint Online, it’s possible to share with people using a Microsoft account, or by sending an external link. Sharing settings are dependent on the sharing settings configured in the SharePoint Online tenancy.

- If the Don’t Allow Sharing Outside Your Organization option is selected at the tenancy level, users will only be able to share with other users in the tenancy. If the users attempt to share with external users, they will see the message shown in Figure 2-58, explaining that sharing with external users is not possible.
If the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users option is selected at the tenancy level, sharing with external users will be possible as long as those users have a Microsoft account or an Office 365 account.

If the Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links option is selected at the tenancy level, it will be possible to share with external users with Office 365 or Microsoft accounts. It will also be possible to forward links to shared documents or folders to users so that they can access content without having to authenticate.

To share an individual document, perform the following steps:

1. Sign in to Office 365 with your user account.
2. On the list of apps, click OneDrive.
3. In the OneDrive for Business site, select the document that you want to share. Figure 2-59 shows the DonFunkExcel workbook selected.

---

**FIGURE 2-58** No sharing with external users

**FIGURE 2-59** Select document
4. Click the Share icon. If the Allow Both External Users Who Accept Sharing Invitations And Anonymous Guest Links option is selected at the tenancy level, users will be able to share to external users and generate links. To share with external users, enter the user’s email address and determine if the users have read-only or edit access. Figure 2-60 shows the user orin.thomas@outlook.com granted the edit permission.

![FIGURE 2-60 Share document](image)

5. If you want to share the document with anonymous users, click the Get A Link section. On this page, you can click View Only or the Edit option, as shown in Figure 2-61.

![FIGURE 2-61 Anonymous sharing](image)

You can view who a document is shared with on the document’s Share page. Note that if you’ve invited someone to a document and they haven’t accepted the invitation, their account will not be listed on the Shared With section of the Share page. Invitations remain valid for seven days.

To view who a document is shared with, perform the following steps:
1. Sign in to Office 365 with your user account.
2. On the list of apps, click OneDrive.
3. In the OneDrive for Business site, select the document of which you want to view the sharing properties. Any documents that are shared will have Shared in the Sharing column, as shown in Figure 2-62.

![FIGURE 2-62 Document shown as Shared](image)

4. On the toolbar, click Share.
5. The Shared With section will show with whom the document has been shared.
6. As Figure 2-63 shows, you can choose to remove someone's permission to access a document from this page.

![FIGURE 2-63 Who the document is shared with](image)

You can share folders from OneDrive for Business. All of the content in a folder inherits the sharing settings of the parent folder. This makes sharing documents a matter of placing them in the appropriately configured folder.

To share a folder, perform the following steps:

1. Sign in to Office 365 with your user account.
2. On the list of apps, click OneDrive.
3. In the OneDrive for Business site, select the Folder you want to share. Figure 2-64 shows the Hovercraft folder selected.

![FIGURE 2-64 Share a folder](image)

4. On the toolbar, click Share.

5. On the Invite People page, enter the email addresses of people who you want to invite to the folder and specify their permissions, either Read Only or Edit. Figure 2-65 shows sharing with an external user granted the Edit permission to items in the folder.

![FIGURE 2-65 Share folder](image)

You can’t create links for anonymous users to folders. Anonymous links can only be created for documents.
Administering OneDrive for Business

Administrators are able to view files and folders stored in OneDrive for Business. To access a user’s OneDrive for Business content, perform the following steps:

1. In the Admin area of the Office 365 Admin Center, click SharePoint.
2. In the SharePoint Admin Center, click User Profiles.
3. In the User Profiles setting, click Manage User Profiles, as shown in Figure 2-66.

4. In the Find User Profiles box, enter part of the account name. Figure 2-67 shows a search for the name Don.

5. Select the user whose OneDrive for Business content you want to examine, and then click Manage Site Collection Owners, as shown in Figure 2-68.
6. Add an administrator account to the list of Site Collection Administrators, and then click OK.

![Add Site Collection Administrator](image)

**FIGURE 2-69** Add Site Collection Administrator

7. Select the user again, and this time select Manage Personal Site.

8. On the Site Settings page, click Documents.

9. The user’s OneDrive for Business content will be displayed, as shown in Figure 2-70.

![Administrator viewing documents](image)

**FIGURE 2-70** Administrator viewing documents

---

**MORE INFO ONE DRIVE FOR BUSINESS**

You can learn more about OneDrive for Business at [https://support.office.com/en-us/article/What-is-OneDrive-for-Business--187f90af-056f-47c0-9656-cc0ddca7f0c2](https://support.office.com/en-us/article/What-is-OneDrive-for-Business--187f90af-056f-47c0-9656-cc0ddca7f0c2).
Understanding the App Store

The SharePoint App Store provides organizations with a collection of SharePoint apps that can be used with SharePoint 2013 and SharePoint Online. A SharePoint app is a stand-alone application that can add functionality to a SharePoint deployment. You can add apps to a SharePoint Online tenancy from the apps section of the SharePoint Admin Center, as shown in Figure 2-71.

From the Apps section of the SharePoint Admin Center, you can perform the following tasks:

- **App Catalog**  Allows you to make purchased apps available to people in your organization. You need an app catalog if you want to disable Store purchases for end users.
- **Purchase Apps**  Allows administrators to purchase apps from third-party developers, as well as Microsoft, from the SharePoint store.
- **Manage Licenses**  Allows you to manage licensing for apps purchased from the SharePoint Store.
- **Configure Store Settings**  Allows you to manage how apps are acquired by users from the SharePoint Store.
- **Monitor Apps**  Allows you to track how SharePoint apps are being used across the SharePoint Online tenancy.
- **App Permissions**  Allows you to manage how Apps interact with the SharePoint Online tenancy.
Understanding Enterprise eDiscovery

Enterprise eDiscovery is the process of locating content that will serve as evidence in litigation or an official investigation. SharePoint Online has a special site collection called the eDiscovery Center. This site collection allows you to create special SharePoint sites named cases that you can use to locate, hold, search, and export content from Exchange online, SharePoint Online, and OneDrive for Business.

Creating a case

To create an eDiscovery case, perform the following steps:

1. In the Admin area of the Office 365 Admin Center, click Compliance.
2. In the Compliance Center, click eDiscovery.
3. In the list of eDiscovery Cases, shown in Figure 2-72, click the Plus icon to create a new case.

![Figure 2-72 eDiscovery Cases](image)

4. On the Site Contents, New SharePoint Site page, provide the following information, as shown in Figure 2-73, ensuring that you select the eDiscovery Case template:
   - Title: Title for the eDiscovery case
   - Description: Description for the case
   - URL name: Address of the site related to the case

MORE INFO  SHAREPOINT STORE APPS

You can learn more about SharePoint Store Apps at [https://support.office.com/en-us/article/Buy-an-app-from-the-SharePoint-Store-dd98e50e-d3db-4ecb-9bb7-82b189822d43](https://support.office.com/en-us/article/Buy-an-app-from-the-SharePoint-Store-dd98e50e-d3db-4ecb-9bb7-82b189822d43).
5. You can specify whether the site will use the same permissions as the parent site or unique permissions. If you need to allow specific people access to one case, but not other eDiscovery cases stored within your SharePoint Online tenancy, choose unique permissions.

Add sources and place them on hold

Adding sources to an eDiscovery case allows information to be added to the case. To add sources to an eDiscovery case, perform the following steps:

1. In the Admin area of the Office 365 Admin Center, click Compliance.
2. In the Compliance Center, click eDiscovery.
3. In the list of eDiscovery Cases, shown in Figure 2-74, click the case that you want to add a source to and then click the pencil icon, which allows you to edit the case.
4. On the eDiscovery case page, shown in Figure 2-75, click New Item.

5. On the New: eDiscovery Set page, provide a name for the set and then click Add & Manage sources, as shown in Figure 2-76.
6. On the Add & Manage Sources page, provide the names of mailboxes and the locations of SharePoint Sites and File Shares that are indexed by Search and click Save. All subsites and sub-folders will be included as sources. Figure 2-77 shows the Contoso347er Team Site selected.

7. As shown in Figure 2-78, you can use the filter box to provide keywords; provide a start date and an end date; the name of an author; an email domain; and also enable in-place hold, stopping the deletion of objects that match the search criteria.

8. Click Save to save the eDiscovery Set.
Objective 2.3: Plan a collaboration solution

EXAM TIP
Remember that document Check Out should be disabled if coauthoring is to take place with documents stored in SharePoint Online.

Thought experiment
SharePoint apps and Contoso’s Office 365 deployment
In this thought experiment, apply what you learned about this objective. You can find answers to these questions in the “Answers” section at the end of this chapter.

Your organization has purchased several SharePoint apps to increase user productivity. You are in the process of training an assistant to manage how these apps are used. Which part of the apps section of the SharePoint Admin Center should be used to perform the following tasks?

1. Determine application usage and errors
2. View license utilization
3. Control which SharePoint apps interact with the tenant

Objective summary
- Newsfeeds in SharePoint Online function as an organizational blog where members of the organization can post and reply to posts.
- A newsfeed exists at the SharePoint Online tenancy level. Newsfeeds also exist at the team site level.
- Yammer is a private social network that has features similar to many of the larger social networks.
- To use Yammer with SharePoint Online, you need to configure Yammer as the SharePoint social collaboration option.
- Every user who will coauthor a document needs to have appropriate permissions to edit the document.
- If a document is checked out by an author, the document is locked until the check out is released, which blocks coauthoring.
- Project Online is a stand-alone web service that provides browser-based portfolio and project management tools.
- Excel Services is used when a file hosted in an on-premises SharePoint deployment is opened in a browser.
- Visio Services allows Visio diagrams stored SharePoint Online to be viewed in a browser without requiring a full Visio client or Visio Viewer.
- OneDrive for Business allows users to store, sync, and share work files.
- Whether users can share OneDrive for Business documents with external users depends on the settings in the SharePoint Online tenancy.
- eDiscovery allows you to configure search and hold for the purposes of litigation and investigation.

**Objective review**

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. Which of the following can block collaboration when configured for a SharePoint Online document library?
   - A. Disabling major versions
   - B. Enabling major versions
   - C. Disabling minor versions
   - D. Enabling check out

2. You want to block users of OneDrive for Business from sharing documents with people external to the organization. Users should still be able to share documents with other users who have accounts in your organization's Office 365 tenancy. Which of the following steps can you take to accomplish this goal with a minimum of administrative effort?
   - A. Configure the Don’t Allow Sharing Outside Your Organization option at the site collection level
   - B. Configure the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users option at the site collection level
   - C. Configure the Don’t Allow Sharing Outside Your Organization option at the SharePoint Online tenancy level
   - D. Configure the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users option at the site collection level
3. You want to block OneDrive for Business users from sending links that allow anonymous users to access documents stored in SharePoint Online. Users should still be able to share documents with external users that have Microsoft or Office 365 accounts. Which of the following steps could you take to accomplish this goal?

A. Configure the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users option at the site collection level

B. Configure the Don’t Allow Sharing Outside Your Organization option at the SharePoint Online tenancy level

C. Configure the Allow External Users Who Accept Sharing Invitations And Sign In As Authenticated Users option at the site collection level

D. Configure the Don’t Allow Sharing Outside Your Organization option at the site collection level
Answers

This section contains the solutions to the thought experiments and answers to the objective review questions in this chapter.

Objective 2.1: Thought experiment

1. Change the sharing settings at the SharePoint Online tenancy level.
2. It will be necessary to modify the sharing settings of each site collection to remove the external user’s access.

Objective 2.1: Review

1. Correct answer: A
   A. Correct: An invitation to access shared content sent to an external user from an Office 365 SharePoint site collection remains valid for 7 days.
   B. Incorrect: An invitation to access shared content sent to an external user from an Office 365 SharePoint site collection remains valid for 7 rather than 14 days.
   C. Incorrect: An invitation to access shared content sent to an external user from an Office 365 SharePoint site collection remains valid for 7 rather than 21 days.
   D. Incorrect: An invitation to access shared content sent to an external user from an Office 365 SharePoint site collection remains valid for 7 rather than 28 days.

2. Correct answer: B
   A. Incorrect: This will block all sharing in all site collections in the tenancy.
   B. Correct: This will only allow sharing to be performed with authenticated users in all site collections.
   C. Incorrect: While this will accomplish the overall goal of requiring all external users to authenticate to access shared content, it will not do so with a minimum amount of administrative effort.
   D. Incorrect: This will block sharing of all content in each site collection.

3. Correct answers: A and D
   A. Correct: You must enable the ability to use anonymous guest links at both the tenancy level and the site collection level to allow anonymous access to documents hosted within that site collection.
   B. Incorrect: Configuring this option at the site collection level would block users from sending anonymous links.
   C. Incorrect: Configuring this option at the tenancy level will block the option for allowing anonymous links at the site collection level.
   D. Correct: You must enable the ability to use anonymous guest links at both the tenancy level and the site collection level to allow anonymous access to documents hosted within that site collection.
4. Correct answers: A and C
   A. Correct: To allow users to send anonymous links in other site collections, this option needs to be configured.
   B. Incorrect: This option will block anonymous links in other site collections.
   C. Correct: This option will block anonymous links for the specific site collection.
   D. Incorrect: This option will allow anonymous links for the specific site collection.

5. Correct answer: D
   A. Incorrect: While this will accomplish the goal, it will not do so with a minimum amount of administrative effort. Performing this task at the tenancy level will apply this setting across all site collections.
   B. Incorrect: This will allow sharing of content to people external to your organization who have Microsoft accounts.
   C. Incorrect: This will allow sharing of content to people external to your organization who have Microsoft accounts as well as to anonymous people.
   D. Correct: Configuring this setting at the SharePoint Online tenancy level will block sharing at the site collection and document levels.

Objective 2.2: Thought experiment

1. Microsoft support can recover site collections up to 14 days after being removed from the Recycle Bin.
2. You need to remove the site from the Recycle Bin, as site collection URLs must be unique.

Objective 2.2: Review

1. Correct answer: C
   A. Incorrect: The amount of storage space allocated uses the formula 10 GB plus 500 MB per user. This would mean that 30 GB, rather than 10 GB, will be available.
   B. Incorrect: The amount of storage space allocated uses the formula 10 GB plus 500 MB per user. This would mean that 30 GB, rather than 20 GB, will be available.
   C. Correct: The amount of storage space allocated uses the formula 10 GB plus 500 MB per user. This would mean that 30 GB will be available.
   D. Incorrect: The amount of storage space allocated uses the formula 10 GB plus 500 MB per user. This would mean that 30 GB, rather than 40 GB, will be available.

2. Correct answer: C
   A. Incorrect: The maximum amount of storage that can be allocated to an individual SharePoint Online site collection is 1 TB, not 100 GB.
   B. Incorrect: The maximum amount of storage that can be allocated to an individual SharePoint Online site collection is 1 TB, not 500 GB.
C. **Correct:** The maximum amount of storage that can be allocated to an individual SharePoint Online site collection is 1 TB.

D. **Incorrect:** The maximum amount of storage that can be allocated to an individual SharePoint Online site collection is 1 TB, not 5 TB.

3. **Correct answer:** D

A. **Incorrect:** You should configure the quota warning email threshold. Setting the quota to 48 GB will not notify you that 48 GB of a 50 GB quota has been consumed. It will simply limit the site collection storage to 48 GB.

B. **Incorrect:** You should configure the quota warning email threshold. Setting the quota to 52 GB will not notify you that 48 GB of a 50 GB quota has been consumed. It will simply limit the site collection storage to 52 GB.

C. **Incorrect:** Setting the email warning threshold to 48 percent will mean a notification will be sent when 24 GB of space is consumed, rather than 48 GB.

D. **Correct:** You should set the quota alert email threshold to 96 percent. The quota is already set to 50 GB, so this will send an email when 48 GB has been consumed.

4. **Correct answer:** D

A. **Incorrect:** You can alter which users are assigned site collection administrator privileges after site collection creation.

B. **Incorrect:** Storage Quota can be altered after site collection creation.

C. **Incorrect:** Server Resource Quota can be altered after site collection creation.

D. **Correct:** You cannot alter the primary language setting of a site collection after site collection creation.

5. **Correct answer:** B

A. **Incorrect:** Site collections remain in the Recycle Bin for 30 days, not 15 days.

B. **Correct:** Site collections remain in the Recycle Bin for 30 days.

C. **Incorrect:** Site collections remain in the Recycle Bin for 30 days, not 60 days.

D. **Incorrect:** While some older documentation might suggest that site collections remain in the Recycle Bin for 90 days, the figure listed in current documentation and in the actual SharePoint Online interface is 30 days.

6. **Correct answers:** A, B, and C

A. **Correct:** You cannot recover a site collection from the Recycle Bin if the resource quota has been exceeded.

B. **Correct:** You cannot recover a site collection from the Recycle Bin if the storage quota has been exceeded.

C. **Correct:** You will be unable to recover a site collection from the Recycle Bin that was deleted more than 50 days ago.

D. **Incorrect:** You will be able to recover a site collection that was deleted less than 20 days ago assuming that usage quotas and storage quotas have not been exceeded.
7. **Correct answer:** B
   
   A. **Incorrect:** Only 1 primary site collection administrator, rather than 5, can be assigned to a site collection.
   
   B. **Correct:** Only 1 primary site collection administrator can be assigned to a site collection.
   
   C. **Incorrect:** Only 1 primary site collection administrator, rather than 2, can be assigned to a site collection.
   
   D. **Incorrect:** Only 1 primary site collection administrator, rather than 10, can be assigned to a site collection.

8. **Correct answer:** B
   
   A. **Incorrect:** A storage quota restricts how much storage space a site collection can consume, not how much of the server resources in terms of RAM and CPU it can consume.
   
   B. **Correct:** A resource quota allows you to restrict how much RAM and CPU resources a specific site collection can consume.
   
   C. **Incorrect:** Assigning a user as a site collection administrator will not ensure that a specific site collection does not consume all of the RAM and CPU resources available to the tenancy.
   
   D. **Incorrect:** While purchasing additional user licenses will increase the overall server resource quota, it will not stop a specific site collection from consuming all those resources.

**Objective 2.3: Thought experiment**

1. You use the Monitor Apps section to determine application usage and review errors.
2. You use the Manage Licenses section to view SharePoint app license utilization.
3. You use the App Permissions section to configure which apps can access the SharePoint Online tenant.

**Objective 2.3: Review**

1. **Correct answer:** D
   
   A. **Incorrect:** Collaboration can function when the major versions versioning functionality is disabled.
   
   B. **Incorrect:** Collaboration can function when the major versions versioning functionality is enabled.
   
   C. **Incorrect:** Minor versioning allows previous versions of documents to be restored, but does not block collaboration.
   
   D. **Correct:** If users check out files when opened, other users will not be able to collaborate on that file until the file is closed.
2. **Correct answer: C**

   A. **Incorrect:** While this will function, it would take an extraordinary amount of effort to perform this task for each user’s OneDrive for Business site collection.

   B. **Incorrect:** This would allow sharing with external users with Microsoft or Office 365 accounts. It would also require extraordinary effort to perform this task for each user’s OneDrive for Business site collection.

   C. **Correct:** Configuring this option at the SharePoint Online tenancy level would accomplish your goal with a minimum of administrative effort.

   D. **Incorrect:** This would allow sharing with external users with Microsoft or Office 365 accounts.

3. **Correct answer: A**

   A. **Correct:** This would allow sharing with external users with Microsoft or Office 365 accounts.

   B. **Incorrect:** Configuring this option at the SharePoint Online tenancy level would block users from sharing documents with users that had Microsoft or Office 365 accounts.

   C. **Incorrect:** While this would work, it would also require extraordinary effort to perform this task for each user’s OneDrive for Business site collection.

   D. **Incorrect:** This option would block sharing with external users. It would also take an extraordinary amount of effort to perform this task for each user’s OneDrive for Business site collection.
### Index

#### A

ACEs. See Access Control Entries (ACEs)

activation management

- Office 365 ProPlus 8–13
- Office for Mac 19–23

ActiveSync

- configuration of 295–298
- disabling 295–298

Add A Domain page 217

Add Allowed Domain dialog box 248

Add Blocked Domain dialog box 246–247

Add-MailboxPermission cmdlet 175

Add-RecipientPermission cmdlet 170

address books

- adding external contacts to 183–184

administrator privileges 5

administrators

- OneDrive for Business 132–134
- site collection 99–101

Agents worksheet 58

Allow Anonymous Attendees To Dial-Out option 221

allowed mailbox list 302–303

Allowed IP Address WebPage Dialog 240–241

anonymous sharing 129

anti-malware notifications 231–233

anti-malware policies 229–239

anti-malware notifications 231–233

creating 235–238

default 233–235

Enable-MalwareFilterRule cmdlet 239

Get-MalwareFilterPolicy cmdlet 238

malware detection response settings 230–231

New-MalwareFilterPolicy cmdlet 238

New-MalwareFilterRule cmdlet 238

Remove-MalwareFilterPolicy cmdlet 238

Set-MalwareFilterPolicy cmdlet 238

Set-MalwareFilterRule cmdlet 239

Windows PowerShell cmdlets 238–239

anti-spam policies

- advanced policy options 250–252
- allow lists 246–247
- applying 253–254
- block lists 244–246
- bulk actions 243–244
- connection filter policies 239–242
- international spam 248–251

Outbound Spam policy 254–256

Quarantine 256–257

spam confidence levels 252–253

spam filter policies 242–254

Windows PowerShell cmdlets 254

Apple App Store 6–7

Applied To setting 235, 253

Apply Sensitive Word List 252

App Store 134–135

App-V package 30

Archive Mailbox dialog 199–200

archives

- accessing 273
- client requirements for 273–277
- enabling personal 196–201
- importing PST files 275–278
- transferring items to 273–274

Auto Account Setup page 65

#### B

blocked domain list 303–304

BlockedDomains parameter 303

blocked IP address ranges 240

Blocked IP Address webpage dialog box 240

blocked sender list 245
Bring Your Own Device (BYOD) scenarios

self-provisioning software in 5

bulk add

of email addresses 157–158

Bulk Assign Retention Policy page 212

bulk email 243–244

Business clients

Click-to-Run for 70–72

configuring Office 365 for 64–75

MSI for 70–72

Office Web Apps for 69–70

Skype for Business Online for 67–69

central deployment

of Office 365 ProPlus 29

CIDR notation 239

Click-to-Run 30, 70–73

Click-to-Run installation source 30

Client Access servers 263

client requirements

for archives 273–277

collaboration 118–139. See also sharing

App Store 134–135

collaborating 122–125

Excel Services 125

newsfeeds 119–122

OneDrive for Business 126–133

Project Online 125

Visio Services 125

Yammer 121–122

communication settings

configuring end-user 215–222

managing external 302–310

Skype consumer connectivity 304–305

Conditional Sender ID Filtering: Hard Fail 252

correlation

ActiveSync 295–298

additional email addresses 147–168

connection filters 239–242

email account 64–67

Exchange Online 147–168

external user sharing 81–98

Office 365 ProPlus 28–29

of telemetry and reporting 36–47

OWA access 293–295

personal archive policies 196–201

primary email address 155–156

site collection administrators 99–100

site collections 110

Skype for Business Online

end-user communication settings 215–222

external communication settings 216–220

presence settings 215–216

user options 220–222

spam filter policies 242–254

Telemetry Agent 59–60

Telemetry Processor 41–45

Configuration.xml 32–36

attributes 33–35

connection filter policies 239–242

Get-HostedConnectionFilterPolicy cmdlet 242

Set-HostedConnectionFilterPolicy cmdlet 242

connectors. See also receive connectors;

See also send connectors

contacts

external 183–184

Customer Experience Improvement Program 22, 44

Custom report worksheet 58

cutover migration 266–268

Data Connection Settings dialog box 45

deactivation

of Office 365 ProPlus 10–13

Deadline attribute 34

default anti-malware policy 233–235

default email address 148

Default MRM Policy 206–208

default retention policy 206–208

Delete All Attachments And Use Custom Alert Text option 230

Delete All Attachments And Use Default Alert Text option 230

Delete Entire Message option 230

Delete Message option 244

deployment

activation management 8–13

central 29

Configurations 32–36

IT, of Office 365 ProPlus 24–36

manual 25–30
Enable Safe List option

Office 365 ProPlus
   central deployment 29
   manual deployment 25–30
Office Deployment Tool 5, 30–32
restricting software 2–5
Telemetry Agent 55–57
Telemetry Dashboard 37–47
Telemetry Processor 39–47
user-driven 1–26
Deployments worksheet 58
Disable-MalwareFilterRule cmdlet 239
Display attribute 33
distribution groups
dynamic 185, 191–194
join settings 186
leave settings 187
mail-enabled security groups 188–190
managing 185–194
New-DistributionGroup Windows PowerShell cmdlet 190
Set-DistributionGroup Windows PowerShell cmdlet 188
Document details worksheet 57
Document issues worksheet 57
documents
   anonymous sharing of 129
   check out of 122–123
coauthoring 122–125
   permissions for sharing 130
   sharing with external users 91–93
   versioning 122, 123–124
   viewing who is sharing 129–130
Document sessions worksheet 58
Documents worksheet 57
Domain Allow List 246, 247
domain controller 47
domains
   Add a Domain page 217
   Add Blocked Domain dialog box 246
   allowed 302–303
   blocked 246–247, 303–304
   Domain Allow List 246–247
   Get-CsTenantFederationConfiguration cmdlet 302, 303–304
   New-CsEdgeAllowAllKnownDomains cmdlet 302
   New-CsEdgeAllowList cmdlet 302
   New-CsEdgeDomainPattern cmdlet 302
   removing allowed 303
dynamic distribution groups 185, 191–194

eDiscover
   in-place holds 286–292
eDiscovery 278–291
   in-place holds 278
   litigation holds 278–286
eDiscovery requests 196
email account
   adding 64–67
email addresses
   adding additional 149–154
   adding to mail contact 184
   bulk add of 157–158
   configuring additional 147–168
   managing 148–158
   managing reply-to address 154–157
   primary 148
      changing 154–155
      configuring 155–156
   secondary 154
SIP addresses
   adding 158–162
   changing 161–164
   managing 158–167
   removing 165–166
email messages
   allow lists 246–247
   anti-malware policies 229–239
   archiving 196–201
   block lists 244–246
   connection filter policies 239–242
   Delete All Attachments And Use Custom Alert Text 230
   Delete All Attachments And Use Default Alert Text 230
   Delete Entire Message 230
   importing from PST files 274–277
   inbox rules for 274
   in-place holds 278, 286–292
   litigation holds 278–286
   moving to archives 273–274
   quarantine of 256–257
   retention of 201–214, 274
   spam filter policies 242–254
   Embed Tags In HTML 252
   Empty Messages 251
   Enable-MalwareFilterRule cmdlet 239
   Enable Safe List option 241
end-user communication settings

end-user communication settings for Skype for Business Online 215–222
Enterprise eDiscovery 135–138
adding sources 136–138
case creation 135–136
equipment mailboxes 178–181
Equipment parameter 181
ESRA. See EdgeSync replication account (ESRA)
Excel
installing on mobile devices 6–8
Excel Services 125
Exchange hybrid deployment 262–263
Exchange Online
adding additional email addresses 149–154
anti-malware policies 229–239
anti-spam policies 239–258
configuration of 147–168
default configuration of 229
delegating permissions in 167–175
hybrid deployment 262–263
managing reply-to address 154–157
managing SIP addresses 158–167
personal archive policies 196–201
planning for 272–297
ActiveSync 295–298
client requirements for archives 273–277
eDiscovery 278–291
OWA access 293–295
Exchange Online mailbox
configuring access to 64–67
ExcludeApp attribute 33
external communications 301–304
global 301–309
Skype for Business Online 301–309
external communication settings
Skype for Business Online 216–220
external contacts
managing 183–184
external users 81–98
removing access for 93–96
sharing with 88–93
documents 91–93
enabling globally 83–85
enabling per site collection 86–89
links 93–94
sites 89–91
understanding 82
use rights of 82

F
First Things First page 27
folders
sharing 130–131
For Compliance, Turn Off Non-Archived Features option 221
Form Tags In HTML 252
Frame Or IFrame Tags In HTML 251
From Address setting 232
From Name setting 232
Full Access permission 173–175

G
Get-CsTenantFederationConfiguration cmdlet 302, 303, 303–304
Get-HostedConnectionFilterPolicy cmdlet 242
Get-HostedContentFilterPolicy cmdlet 254
Get-Mailbox cmdlet 286, 295, 298
Get-MalwareFilterPolicy cmdlet 238
Get-QuarantineMessage cmdlet 257
global external sharing options 83–85
Group Policy
configuration of telemetry 36–47
enabling telemetry through 46–54
groups
distribution 185–194
creating 185–187
New-DistributionGroup Windows PowerShell cmdlet 190
Set-DistributionGroup Windows PowerShell cmdlet 188
security 185
joint settings 190
leave settings 190
mail-enabled 188–190

H
holds
in-place 278
litigation 278–286
hybrid deployment 262–263
hygiene. See message hygiene
I
Image Links To Remote Sites 251
IMAP migration 268–270
Import a File page 276
Import And Export Wizard 275
Import Outlook Data File page 277–278
inbox rules 274
in-place archives 196–201
In-Place eDiscovery & Hold wizard 287–291
in-place hold 278, 286–291
installation
  Office 365 ProPlus 25–30
  Office Deployment Tool 30–32
  Office for Mac 14–19
  Telemetry Processor 40–41
International Spam settings 248–251
IP addresses
  adding IP address list 239
  Allowed IP Address WebPage Dialog 240
  blocked 240
  Blocked IP Address webpage dialog box 240
  specifying safe 239–240
IP Allow list 239, 242
IP block list 239, 242
IT deployments
  Office Deployment Tool 30–32
  of Office 365 ProPlus 24–36
  central deployment 29
  manual deployment 25–30

J
JavaScript Or VBScript In HTML 251

K
Key Management Services (KMS) 29

L
Language ID attribute 34
legal hold. See litigation hold
licenses 1, 5, 9–10, 13, 31, 47
links
  sharing with external users 93–94
litigation hold 278
  enabling 278–283
  in-place hold 286–291
  managing, with PowerShell 285–286
  removing 284–286
  Set-Mailbox Windows PowerShell cmdlet 285
LitigationHoldDuration parameter 286
local administrator privileges 5
Logging attribute 34
Lync Online. See Skype for Business

M
Mac OS X operating system
Office for Mac 13–24
mailboxes
  applying retention policies to 209–214
  archive
    accessing 273
    client requirements for 273–277
    enabling personal 175–180
    importing PST files 274–277
    transferring items to 273–274
  creating shared 175–178
  delegating permissions 167–175
    Full Access permission 173–175
    Send As permission 168–170
    Send on Behalf permission 170–173
  equipment 178–181
  inbox rules 274
  litigation holds on 278–290
  moving 263
  personal archive policies 196–201
  resource 177–182
  room 181–183
  shared 175–177
mailbox migration strategy 262–273
  comparison 270–271
  cutover migration 266–268
  IMAP migration 268–270
  remote move migration 262–263
  staged migration 264–266
mail-enabled security groups 188–190
malware
  anti-malware notifications 231
  anti-malware policies 229–239
  default anti-malware policy 233–235
Malware Filter list

detection response settings 230–231
Enable-MalwareFilterRule cmdlet 239
Get-MalwareFilterPolicy cmdlet 238
New-MalwareFilterPolicy cmdlet 238
New-MalwareFilterRule cmdlet 238
policy creation 235–238
Remove-MalwareFilterPolicy cmdlet 238
Set-MalwareFilterPolicy cmdlet 238
Set-MalwareFilterRule cmdlet 239
Malware Filter list 237
Manage Administrators dialog box 100–101
Manage Site Collection Owners 132
manual deployment
Office 365 ProPlus 25–30
meeting invitations 305–306
Meet OneDrive page 27–28
Messages From External Senders setting 232
Messages From Internal Senders setting 232
message transport. See transport
Messaging Records Management (MRM) 201
Microsoft Customer Experience Improvement Program 44
migration
batches 264, 265
comparison 270–271
cutover 266–268
endpoints 263
IMAP 268–270
mailboxes 262–274
remote move 262–263
staged 264–266
mobile devices
Office 365 and 6–8
Move Message To Junk Email Folder option 243
MRM. See Messaging Records Management
MRSProxy service 263
MSI 70–73

N
NAT. See network address translation (NAT)
NDR Backscatter 252
New Anti-Malware Policy page 237
New-CsEdgeAllowAllKnownDomains cmdlet 302
New-CsEdgeAllowList cmdlet 302
New-CsEdgeDomainPattern cmdlet 302
New Distribution Group dialog box 185, 188
New-DistributionGroup Windows PowerShell cmdlet 188, 190
New-DynamicDistributionGroup Windows PowerShell cmdlet 193
New-HostedContentFilterPolicy cmdlet 254
New-Mailbox cmdlet 181
New-MailboxSearch Windows PowerShell cmdlet 292
New-Mailbox Windows PowerShell cmdlet 177, 183
New-MailContact Windows PowerShell cmdlet 184
New-MalwareFilterPolicy cmdlet 238
New-MalwareFilterRule cmdlet 238
New Retention Policy dialog box 206
New-RetentionPolicyTag Windows PowerShell cmdlet 203
newsfeeds 119–122
New Shared Mailbox dialog box 176
New Shared Mailbox page 176
New Tag dialog box 202–203
NICs. See network interface cards (NICs)
notations
anti-malware 231–233
Notify Administrators About Undelivered Messages
From External Senders option 231
Notify Administrators About Undelivered Messages
From Internal Senders option 231
Notify External Senders option 231
Notify Internal Senders option 231
Numeric IP Address In URL 251

O
Object Tags In HTML 252
Office 365
Business client configuration 64–75
console page 15
mobile devices and 6–8
signing in, on Mac 14
subscription types 4
user-driven client deployments 1–26
Office 365 ProPlus
activation management 8–13
central deployment of 29
configuration 28–29
deactivation 10–13
IT deployments of 24–36
licenses 1, 5, 9–10
manage user software 2–5
manual deployment 25–30
operating systems 5
reactivation 12–13
reduced functionality mode 9
restriction of self-provisioning of 2–5
software included with 2, 5
Office 2013 Group Policy administrative template 46–47
Office Applications To Exclude From Office Telemetry
Agent Reporting policy 53–54
OfficeClientEdition attribute 33
Office Deployment Tool 5, 30–32
  Configuration.xml 32–36
Office for Mac 13–24
  activation 19–23
  installation 14–19
Software License Agreement 16
Office on Demand 68–69
Office Solutions To Exclude From Telemetry Agent
Reporting policy 54–55
Office Telemetry. See telemetry
Office Telemetry Log 59–61
Office Web Apps 69–70
OneDrive for Business 126–133
  accessing 126–127
  administering 132–134
  collaborating with 127–131
OneNote
  installing on mobile devices 6–8
operating systems 5, 39
Outbound Spam policy 254–256
Outbound Spam Preferences page 255
Outlook client 64–67
Outlook Web App (OWA) 273
  access configuration 293–295
  disabling 293–295
  offline access for 264
Overview worksheet 57
OWA. See Outlook Web App (OWA)

P
permissions
  Add-MailboxPermission cmdlet 175
  delegating 167–175
  for accessing documents 130
  for coauthoring 122
  for shared mailboxes 175–176
Full Access 173–175, 175
hybrid deployment 262
Remove-MailboxPermission cmdlet 175
Send As 168–170, 176
Send on Behalf 170–173, 176
personal archives
  enabling 196–201
  policy configuration 196–201
personal store (.pst) files 196, 274–276
platform-as-a-service. See PaaS
pooled storage model 105–107
PowerPoint
  installing on mobile devices 6–8
presence settings 215–216
primary email address 148
  changing 148, 154–155
  configuring 155–156
  configuring new 153
Product ID attribute 34
Project Online 125
PST files 196
  importing messages from 274–277
public IM connectivity 304–305
Public Websites
  SharePoint Online 102
push notifications
  disabling 306–308

Q
Quarantine 256–257
Quarantine Message option 243

R
reactivation
  of Office 365 ProPlus 12–13
Record Conversations And Meetings option 221
Recycle Bin 113, 114
reduced functionality mode 9
registry
  configuration of Telemetry Agent through 59–60
Release-QuarantineMessage cmdlet 257
Release The Message And Report It As A False Positive
option 257
Release The Message Without Reporting It As A False
Positive option 257
remote move migration 262–263
Remove attribute 34
Remove-HostedContentFilterPolicy cmdlet 254
Remove-MailboxPermission cmdlet 175
RemovemailboxSearch cmdlet 292
Remove-MalwareFilterPolicy cmdlet 238
Remove-RecipientPermission cmdlet

Remove-RecipientPermission cmdlet 170
reply-to email address 148
managing 154–157
resource mailboxes
equipment mailboxes 178–181
managing 177–182
room mailboxes 181–183
resource quotas 100–102
Restore Site Collections page 115
retention period 201
retention policies
applying to mailboxes 209–214
creating custom 204–208
default 206–208
for moving messages 274
review and modify default 206–208
room mailboxes 181–183
Room parameter 183

S
Safe List checkbox 239
secondary email addresses 154
security groups 185
join settings 190
leave settings 190
mail-enabled 188–190
Select Language dialog box 249–250
Select Region dialog box 249–250
Select Send As dialog box 169
self-service deployment. See user-driven client deployments
Send As permission 168–170, 176
Sender Allow List 246, 247
Send on Behalf permission 170–173, 176
Session Initiation Protocol (SIP) addresses
adding 158–162
changing 161–164
managing 158–167
removing 165–166
Set-CASMailbox Windows PowerShell cmdlet 295, 298
Set-CsPushNotificationConfiguration cmdlet 307
Set-CsTenantFederationConfiguration cmdlet 304
Set-CsTenantPublicProvider cmdlet 305
Set-DistributionGroup Windows PowerShell cmdlet 188, 190
Set-HostedConnectionFilterPolicy cmdlet 242
Set-HostedContentFilterPolicy cmdlet 254
Set-Mailbox cmdlet 154, 160, 164, 173
Set-MailboxSearch Windows PowerShell cmdlet 292
Set-Mailbox Windows PowerShell cmdlet 212, 285
Set-MailContact Windows PowerShell cmdlet 184
Set-MalwareFilterPolicy cmdlet 238
Set-MalwareFilterRule cmdlet 239
Set-RetentionPolicy Windows PowerShell cmdlet 208
shared mailboxes
creating 175–178, 176–179
permissions or 175
Shared parameter 177
SharePoint Admin Center 84
SharePoint Apps 134–135
SharePoint Online 81–146
collaboration 118–139
App Store 134–135
coauthoring 122–125
Excel Services 125
newsfeeds 119–122
OneDrive for Business 126–133
Project Online 125
Visio Services 125
Yammer 121–122
Enterprise eDiscovery 135–138
external user sharing configuration 81–98
pooled storage model 105–107
Public Websites 102
site collections
administrators 99–101
creating 98–118, 109–111
deleting 111–113
enabling external sharing per 86–89
managing 109–115
resource quotas 100–102
restoring deleted 113–115
storage quota for 103–108
tenancy level 87, 95
Share Site dialog box 89–90
sharing. See also collaboration
anonymous 129
external. See external users
folders 130–131
with OneDrive for Business 127–131
SIP addresses. See Session Initiation Protocol (SIP) addresses
site collections
administrators 99–101
creating 98–118, 109–111
deleting 111–113
external sharing of 86–89
managing 109–115
per-site storage management 106
resource quotas 100–102
restoring deleted 113–115
storage limits for 107–109
storage quota for 103–108
URLs for 114
Site Collection Storage Management 106
sites
sharing with external users 89–91
Skype for Business Admin Center 301–302, 304
Skype for Business Online
allowed domain list 302–303
audio and video settings 221
blocked domain list 303–304
consumer connectivity 304–305
default configuration of 229
end-user communication settings 215–222
presence 215–216
external communication settings 216–220
for Business client 67–69
global external communication settings 301–309
meeting invitations 305–306
presence settings 215–216
public IM connectivity 304–305
push notifications 306–308
SIP addresses for 158–167
user options 220–222
Slipstreamed Servicing 70
SMTP. See Single Mail Transfer Protocol (SMTP)
software deployment
on mobile devices 6–8
restricting 2–5
Software License Agreement
Office for Mac 16
software licenses 9–10, 13, 31, 47
Solution details worksheet 58
Solution issues worksheet 58
Solution sessions worksheet 58
Solutions worksheet 58
SourcePath attribute 33
spam confidence levels 252–253
Spam Confidence Level (SCL) rating 252–253
spam filter policies 242–254
advanced policy options 250–252
allow lists 246–247
applying 253–254
block lists 244–246
bulk actions 243–244
international spam 248–251
Outbound Spam policy 254–256
priority of 242–243
Quarantine 256–257
spam confidence levels 252–253
Windows PowerShell cmdlets 254
Spam Filter tab 242–243
Specify Custom Tags For Office Telemetry
Data policy 51–52
Specify The UNC Path To Store Office Telemetry
Data policy 51
SPF. See send policy framework (SPF) records
SPR Record: Hard Fail 252
SQL Server database 38–39
SQL Server Express 38
staged migration 264–266
Standard Operating Environment (SOE) 5
storage
per-site storage management 106
pooled storage model 105–107
purchasing additional 104–105
setting site collection limits 107–109
viewing allocated 103
storage quota
for site collection 103–108
System Info worksheet 61

T

TargetVersion attribute 34
telemetry
configuration of 36–47
enable through Group Policy 46–54
report user issues 59–61
Telemetry Agent 54–55
configuration, through registry 59–60
deployment 55–57
Telemetry Dashboard
deployment of 37–47
policies 48
search for 38
SQL server versions for 38–39
worksheets 57–58
Telemetry Log 59–61
Telemetry Processor 38
configuration 41–45
deployment 39–47
installation 40–41
operating systems for 39
Telemetry Processor worksheet

Telemetry Processor worksheet  58
Turn On Communication With Skype Users And Users Of Other Public IM Service Providers option  304
Turn On Data Uploading for Office Telemetry Agent policy 49–50
Turn On Privacy Settings In Office Telemetry Agent policy 53
Turn On Telemetry Data Collection policy 48

U
UpdatePath attribute 34
Updates attribute 34
URL Redirect To Other Port 251
URL To .Biz Or .Info Websites 251
User Account Control dialog box 26
user-based licensing 71
user-driven client deployments
  activation management 8–13
  management of 1–26
  on mobile devices 6–8
  restriction of self-provisioning of 2–5
User Mailbox dialog 200
User Mailbox properties page 151–152, 283–284
user options
  Skype for Business Online 220–222
Version attribute 33
versioning 122, 123–124
Visio Services 125

W
Web Bugs In HTML 252
Welcome to Office page 26
Windows Security dialog box 66
Windows Server 2012 R2 domain controller 47
Word
  installing on mobile devices 6–8
worksheets
  Telemetry Dashboard 57–58

Y
Yammer 119, 121–122
About the author

ORIN THOMAS is an MVP, a Microsoft Regional Director, an MCT and has a string of Microsoft MCSE and MCITP certifications. He has written more than 30 books for Microsoft Press on topics including Windows Server, Windows Client, Azure, System Center, Exchange Server, Security, and SQL Server. He is an author at PluralSight and is a contributing editor at Windows IT Pro magazine. He has been working in IT since the early 1990’s and regularly speaks at conferences in Australia and around the world. Orin founded and runs the Melbourne System Center, Security, and Infrastructure Group and is completing a Doctorate in Information Technology at Charles Sturt University. You can follow him on twitter at http://twitter.com/orinthomas.