netwrix

Office 365

Administrator's Guide

Jonathan Hassell

Table of Contents

I. Provisioning Office 365 Accounts

All users who consume Office 365 services need their own user accounts. In this chapter, I'll cover how to set up these accounts quickly and efficiently, assign the appropriate licenses to them, block accounts temporarily (for instance, when users are on leave), and deprovision accounts when the users no longer require access to your Office 365 tenant.

Connecting to Office 365

The first step in any of these tasks is to open a PowerShell session to Office 365 from your local machine. I've created the script below to simplify this process; just copy it into a text file and save the file with the extension .PS1. When you're ready to connect, go to the PowerShell console window and run the script by entering ***.\scriptname.ps1*** (that's period, backslash, name of file), and enter your Office 365 administrative credentials when prompted. Here's the script:

How to open a PowerShell session to Office 365 from your local machine

```
$URL = "https://ps.outlook.com/powershell"
$Credentials = Get-Credential -Message "Enter your Exchange
Online or Office\
 365 administrator credentials"
$CloudSession = New-PSSession -ConfigurationName Microsoft.
Exchange -Connect\
ionUri $URL -Credential $Credentials -Authentication Basic
-AllowRedirection\
 -Name "Office 365/Exchange Online"
Import-PSSession $CloudSession -Prefix "365"
```

The ***–Prefix*** parameter in the last line of this script is important in hybrid deployments; if you want to run this script in a purely cloud environment, you can remove the ***-Prefix 365*** part. The reason it's needed in a hybrid environment is that sometimes namespaces for cmdlets collide. For instance, if you were to run the New-Mailbox command when you had Exchange Server running both locally and in Office 365, PowerShell would not know whether to create the new mailbox locally or in the cloud. To fix this, this script loads the Office 365 namespace of cmdlets with the prefix *"365"*. Therefore, you should name all your Exchange cmdlets that should run in the cloud using the prefix *"365"* (such as *"New-365Mailbox"* or *"Get-365DistributionGroup"*) and leave all Exchange cmdlets that should run on your local deployment as they are by default.This makes it very easy to tell them apart.

Creating New Users

Once you have connected to Office 365, you can create accounts either one at a time or in batches.

To provision a single new Office 365 user, use the following script:

How to provision a single new Office 365 user

```
New-MsolUser -DisplayName "Employee Name Here" -FirstName
FirstName -LastName LastName -UserPrincipalName alias@
yourtenant.onmicrosoft.com –UsageLocation US
```

If the user is outside the United States, replace *"US"* with the appropriate two-letter ISO country code. This is a required field; you can't assign licenses, which we cover in the next section, until Office 365 knows which country your users will access their services from. The user account will automatically be assigned a password, which will be displayed on the screen.

To provision multiple new Office 365 user accounts at the same time, first create a CSV file with the following structure:

```
UserPrincipalName,FirstName,LastName,DisplayName,UsageLocation
```

For example, here are three entries:

```
newuser1@yourtenant.onmicrosoft.com,John,Smith,John Smith,US
newuser2@yourtenant.onmicrosoft.com,Greg,Jones,Greg Jones,US
newuser3@yourtenant.onmicrosoft.com,Jacob,Rogers,Jacob Rogers,UK
```

Then use PowerShell to import the CSV file and pipe the contents to the New-Msoluser command, like this:

How to provision multiple new Office 365 user accounts at the same time

```
Import-Csv -Path "C:\newusers.csv" | foreach {New-MsolUser
-DisplayName $_.DisplayName -FirstName $_.FirstName -LastName
$_.LastName -UserPrincipalName $_.UserPrincipalName} -
UsageLocation $_.UsageLocation | Export-Csv -Path "C:\
newuserresults.csv"
```

The script will create the user accounts and also write a new CSV file that lists the new users along with the passwords that were automatically generated for them, which you can then share with your users.

Assigning Licenses

It's not enough to create an account in Office 365; to be able to do anything, the account needs to have a license assigned to it. Different types of licenses *"light up"* different features of the service. You have 30 days after creating an account to assign a license to it. You can generally mix and match licenses within a family, so some of your users could have E3 plans, for example, while others have E1 and still others have E5.

Use the `Get-MsolAccountSku` cmdlet to view the available licensing plans and licenses in your organization, and use `Get-Msoluser` to see the licensing status of all users in your tenant.

To assign licenses, use the `Set-MsolUserLicense` cmdlet. For example, to assign the Office 365 Enterprise E3 plan (which shows up in PowerShell as ***"ENTERPRISEPACK"***) to a user, use this command:

How to assign licenses to a user

```
Set-MsolUserLicense -UserPrincipalName "newuser1@yourtenant.
onmicrosoft.com" -AddLicenses "yourorgname:ENTERPRISEPACK"
```

To assign E3 licenses to all users who currently do not have a license assigned to them, use the following two commands:

How to assign licenses to all users who don't have a license assigned to them

```
$UsersWithoutALicense = Get-MsolUser -All -UnlicensedUsersOnly
$UsersWithoutALicense | foreach {Set-MsolUserLicense
-AddLicenses "yourorgname:ENTERPRISEPACK"}
```

Where to Buy Licenses

You can acquire licenses for your organization in a few ways:

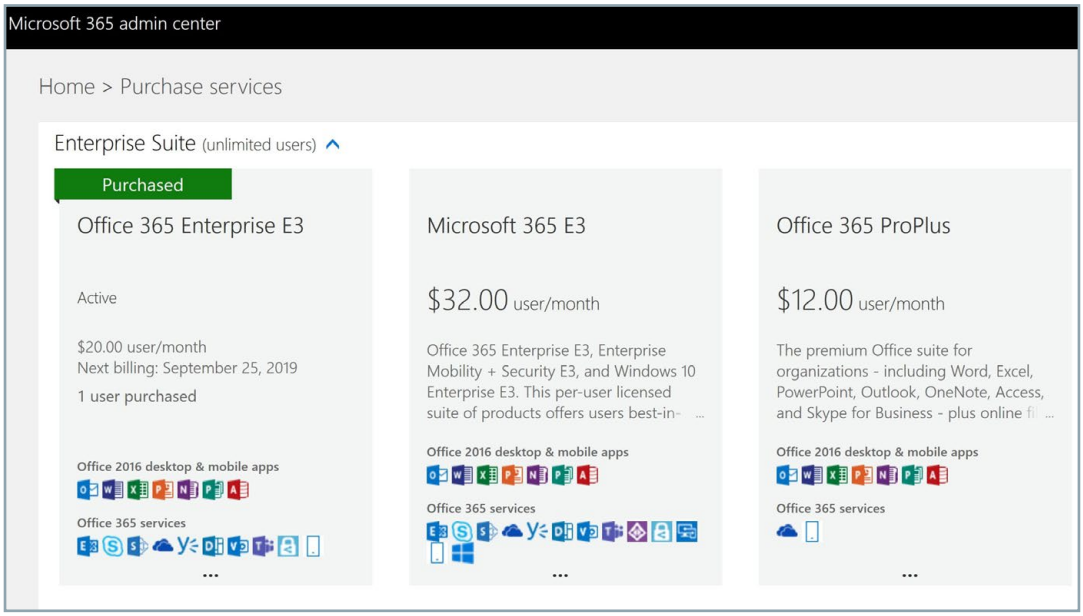
Directly from Microsoft in the Office 365 web portal. For most organizations, this is the most direct way of purchasing services: You simply add a quantity of licenses to your cart and buy them with a credit card, and then they're generally immediately available for use.

Through a volume licensing agreement. This method enables you to take advantage of organizational discounts, but it will take some time before you receive a code for your licenses. Then you redeem the code on the web portal (there is no way to use PowerShell to redeem licenses).

From a reseller. Sometimes it can be more cost-effective to purchase Office 365 through a reseller, who might offer additional services like online backup or enhanced spam filtering bundled with the core Office 365 offering. In this case, redemption of licenses varies, but the reseller will walk you through the process.

You can change and add licenses from the admin center GUI — just hover over *"Billing"* and click *"Purchase Services"* and you'll see the following screen (Fig. 1.1):

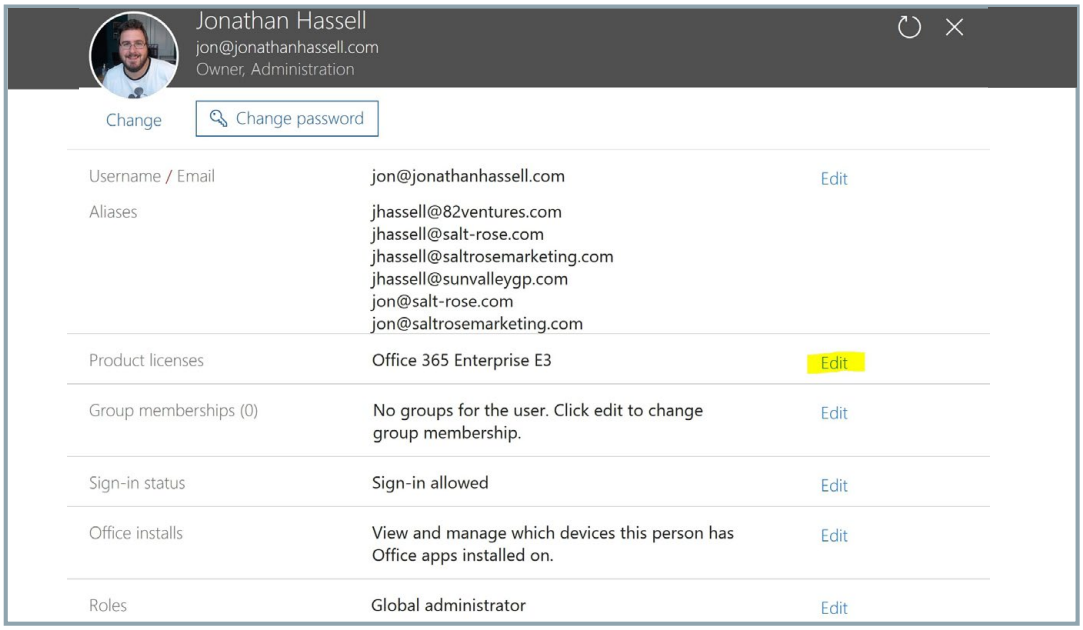
Figure 1.1
Purchasing additional licenses



In this guide, I'll note which features require more advanced licenses. Some features might well be sufficiently compelling to convince you to upgrade to those licenses, at least for a few users.

Once you have purchased licenses, you can assign them to new users or existing users. To change the license for an existing user, go to Users in the admin portal and click the user's name. Then, in the flyout menu, under Product licenses, click the Edit hyperlink, as shown in the Figure 1.2.

Figure 1.2
Changing the product license for a user



Blocking Users

If a user is on leave or otherwise temporarily away, you can block their account so no one can use it. This is a good security precaution if you don't want to delete a user account but the user won't need it for an extended period of time. One PowerShell command will take care of it:

How to block a user account

```
Set-MsolUser -UserPrincipalName newuser2@yourtenant.
onmicrosoft.com -BlockCredential $true
```

To disable the block, use this command:

How to disable the block

```
Set-MsolUser -UserPrincipalName newuser2@yourtenant.
onmicrosoft.com -BlockCredential $false
```

Deleting Users

When a user leaves your company or no longer needs to use Office 365, you'll want to delete their account. PowerShell makes this easy, too:

How to delete a user account

```
Remove-MsolUser -UserPrincipalName newuser2@yourtenant.
onmicrosoft.com
```

In addition to removing the user account, this command automatically removes the license assignment and puts the license back in your general pool so you can assign it to another account in the future.

II. Managing Exchange Online

Exchange Online offers enterprise-class email, calendaring, and collaboration features. Administrators can manage Exchange Online either using the graphical user interface or using PowerShell and the command line. I'll review both options.

Administering Exchange Online using the Graphical User Interface

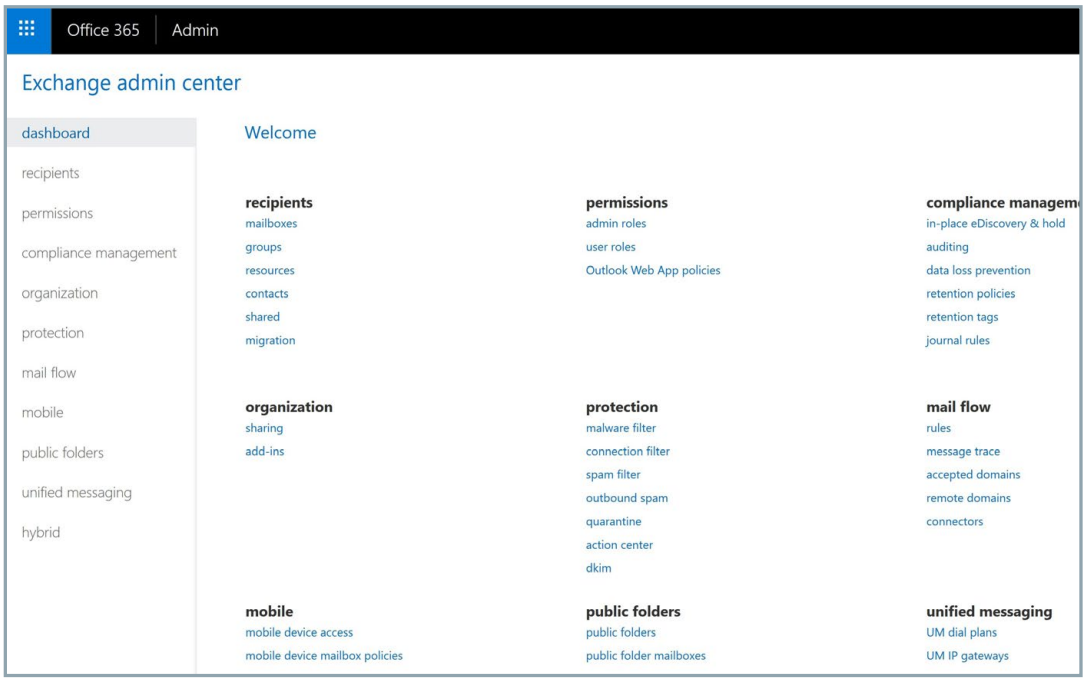
The web interface for Exchange Online is nearly identical to the web-based Exchange Management Console (EMC) included in the on-premises product since Exchange 2013. While some parts of the Exchange Online EMC are specific to Office 365, most parts work exactly as you expect — for instance, you can create transport rules, edit recipient settings to add new SMTP addresses, and establish and configure archive mailboxes.

To access the Office 365 EMC, take the following steps:

1. Log in to ***portal.office.com***.
2. Click the waffle item in the top left corner.
3. Click ***Admin***.
4. Click the **...** icon in the left-hand pane of the resulting page.
5. Look for the icon with the ***A*** on it, and hover over it.
6. From the resulting Admin Centers pop-out menu, click ***Exchange***.

This will get you to the Exchange admin center dashboard, as shown in Figure 2.1:

Figure 2.1
The Exchange admin center dashboard



Creating a Shared Mailbox

Shared mailboxes are commonly used to allow multiple employees to access mail, contacts, calendar items and related information stored in a single mailbox. For instance, you might have a Customer Support mailbox associated with the support@yourcompany.com address, which three employees are responsible for monitoring.

To create a shared mailbox:

1. Go to the EMC.
2. On the Dashboard page, under the Recipients link, click ***Shared***.
3. Click the **+** icon, as shown in Figure 2.2.
4. Fill out the resulting form (Fig. 2.3), specifying the email address for the shared mailbox and which users are allowed to view and send mail on behalf of the mailbox.

Figure 2.2
Adding a shared mailbox

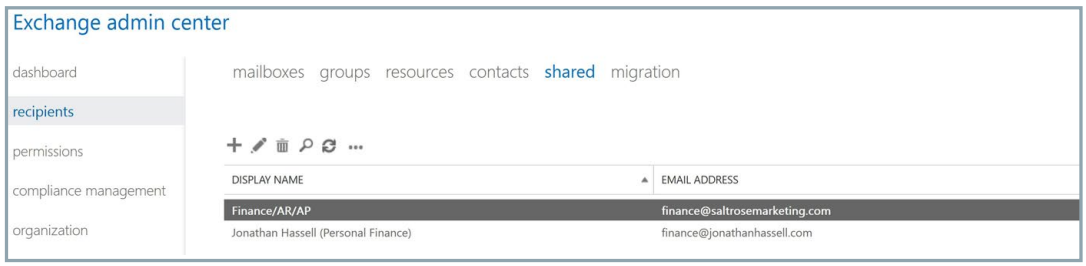
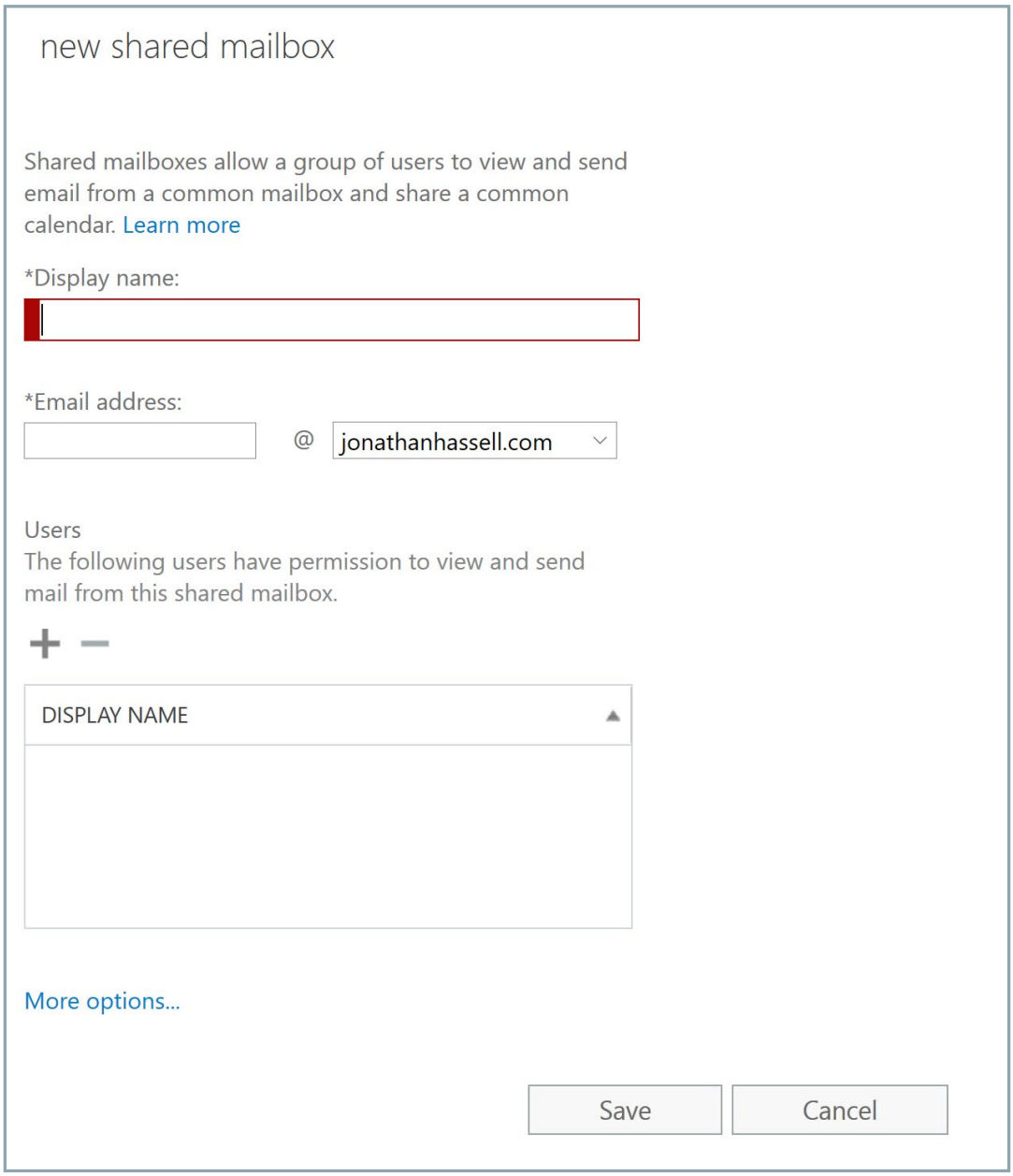


Figure 2.3
Specifying the details of a shared mailbox



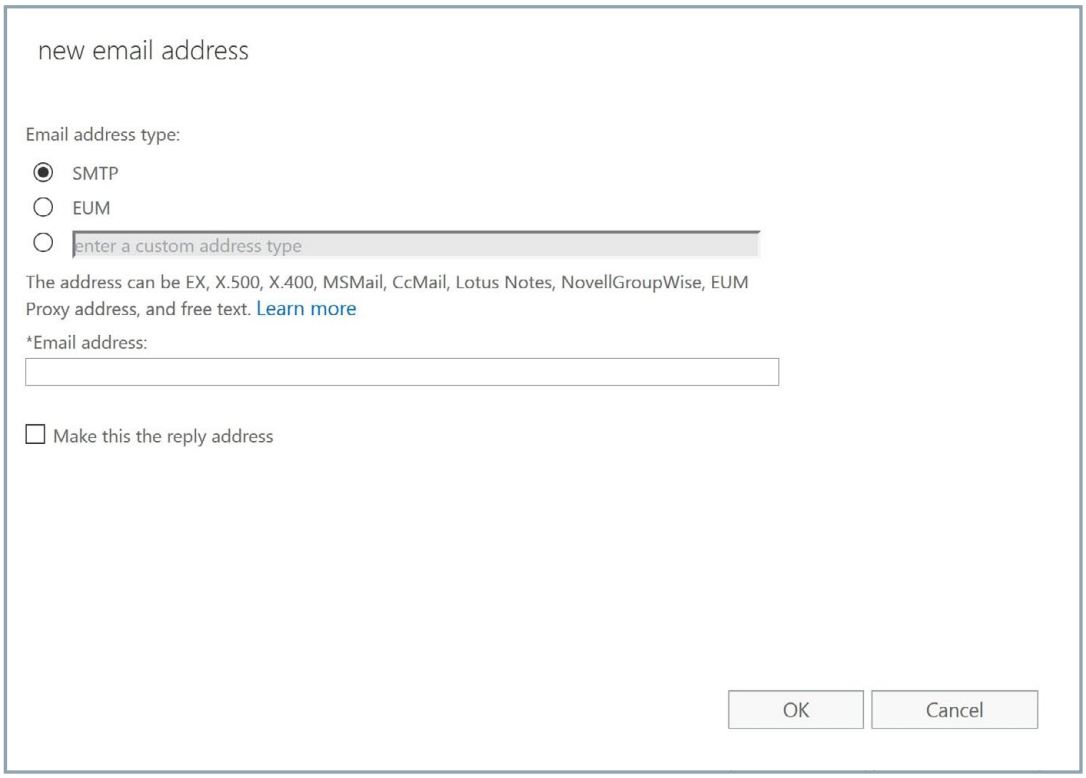
Specifying SMTP Addresses for a Recipient

Most organizations have multiple DNS domains for which they accept inbound email. For example, you might have yourorganization.com, yourorganization.net and so on. In order to get all of your domains working with Office 365, you need to set them up in the service. There is a comprehensive wizard that walks you through identifying your domains, verifying your ownership of those domains, and then setting up the proper DNS records that will get other internet users to send traffic to your Office 365 tenant. For that wizard, go to https://admin.microsoft.com/AdminPortal/Home#/Domains and then click the ***Add Domain*** button.

Once your domains are properly set up on your tenant, you can then add the additional email addresses to each user.

1. In the EMC, go to the Dashboard page and click either ***Recipients*** (for an individual user) or ***Shared*** (for a shared mailbox).
2. On the resulting page, double-click the mailbox you want to modify.
3. Select ***Email address*** from the options in the left pane of the pop-up menu.
4. Click the **+** icon to add a new email address, and enter the new email address in the next window, as shown in Figure 2.4.

Figure 2.4
Adding an email address to a mailbox



Granting Send on Behalf and Full Access Permissions for a Mailbox

In many organizations, principals and management have assistants or chiefs of staff to help manage their inboxes. In these cases, you need to grant other users permissions to access the mailbox and/or send and receive mail on behalf of that user.

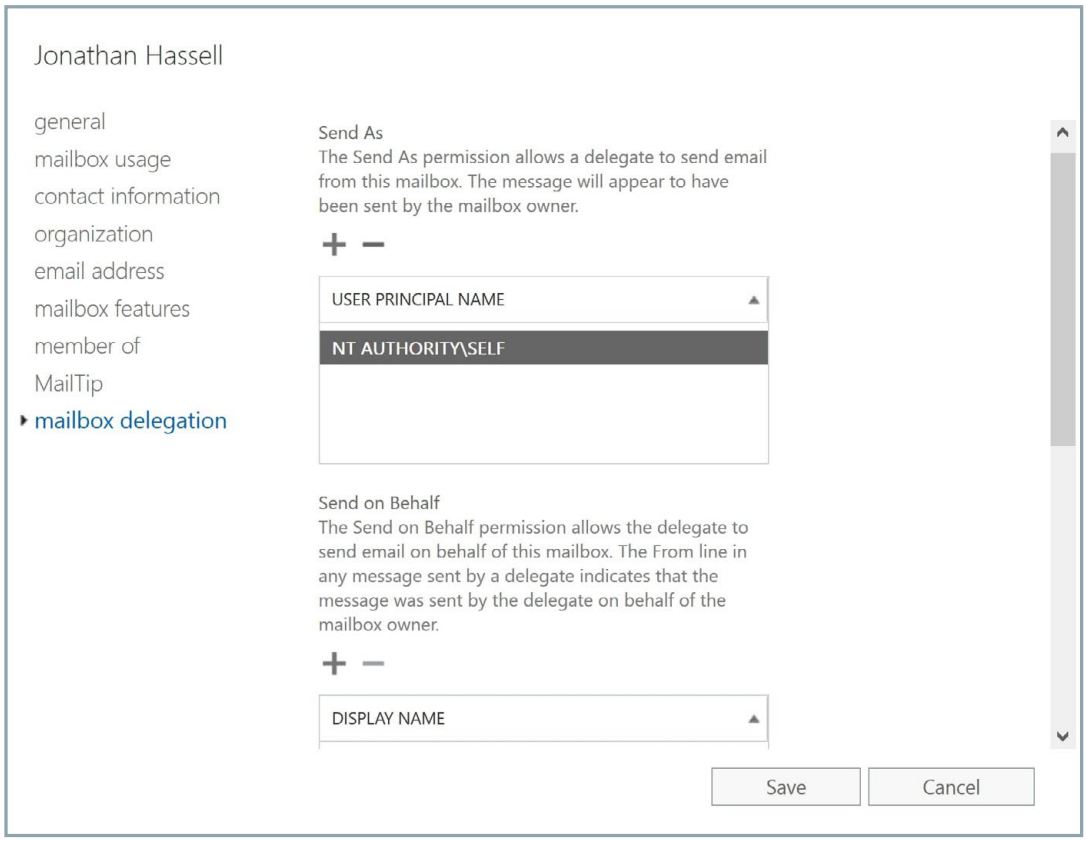
Here are the steps to take:

1. In the EMC, go to the Dashboard page and click either ***Recipients*** (for an individual user) or ***Shared*** (for a shared mailbox).
2. On the resulting page, double-click the mailbox you want to modify.

3. Select ***Mailbox delegation*** from the options in the left pane of the pop-up menu.

4. Click the **+** button under *"Send As"* or *"Send on Behalf"* to add users with those capabilities for the mailbox (Fig. 2.5).

Figure 2.5
Adding Send As and Send on Behalf permissions to a mailbox



Creating Distribution Lists

A distribution list is a single point of contact for a group of users. You might have a distribution list that includes all of a manager's direct reports, another that includes all employees in a company, and yet another with all users involved in a particular project. Anyone can send email to the whole group by simply sending it to the distribution list.

Distribution lists are different than Office 365 groups because they function only within the context of email. Groups include a distribution list but also enable other functionality in applications like SharePoint, Microsoft Teams and so on.

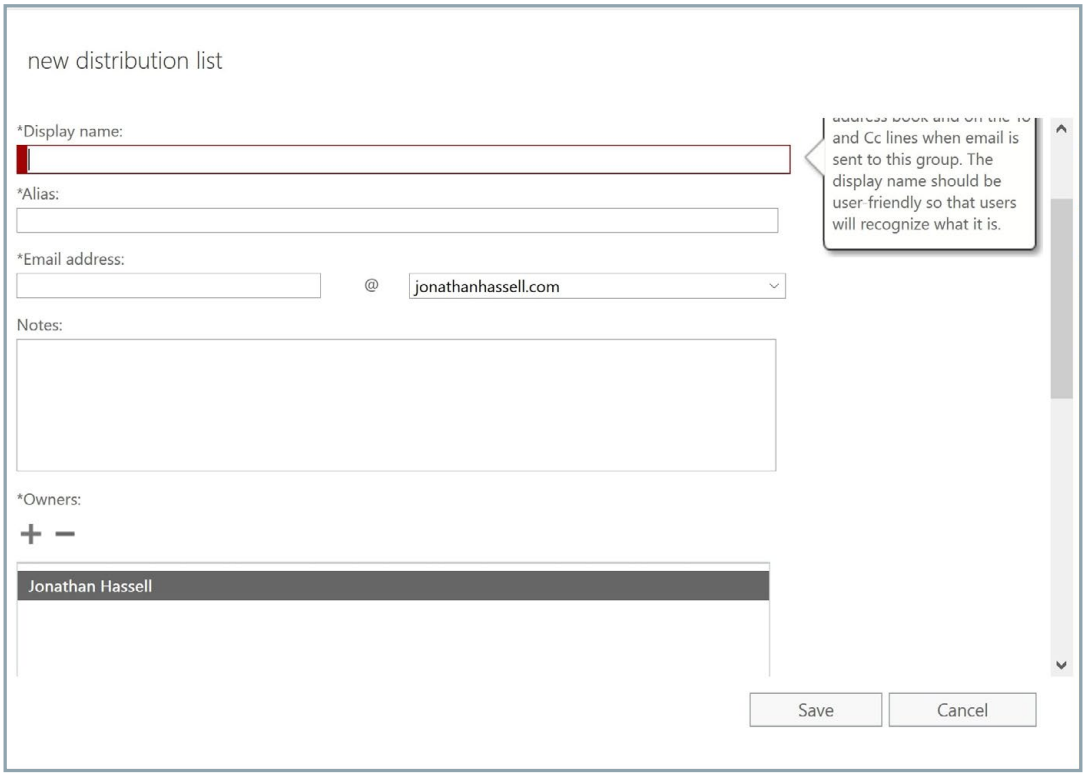
To create a distribution list:

1. In the EMC, go to the Dashboard page and click ***Groups***.

2. On the resulting page, in the drop-down menu beside *"+ New Office 365 Group,"* select ***Distribution List***.

3. Fill in the page that pops up, specifying the name of the distribution list and the users to be added to it.

Figure 2.6
Creating a distribution list



Creating a Mail Flow (Transport) Rule

Mail flow (transport) rules are similar to the Inbox rules in Outlook; you can use them to identify and take action on messages flowing through your Office 365 organization. For example, mail claiming to be from executives and managers is often spoofed, so it can be helpful to identify mail that originated outside of your organization. That way, you can train your users to double-check that mail with sensitive instructions (like to make a wire transfer or pay an invoice) comes from the real user and not some poser outside the company.

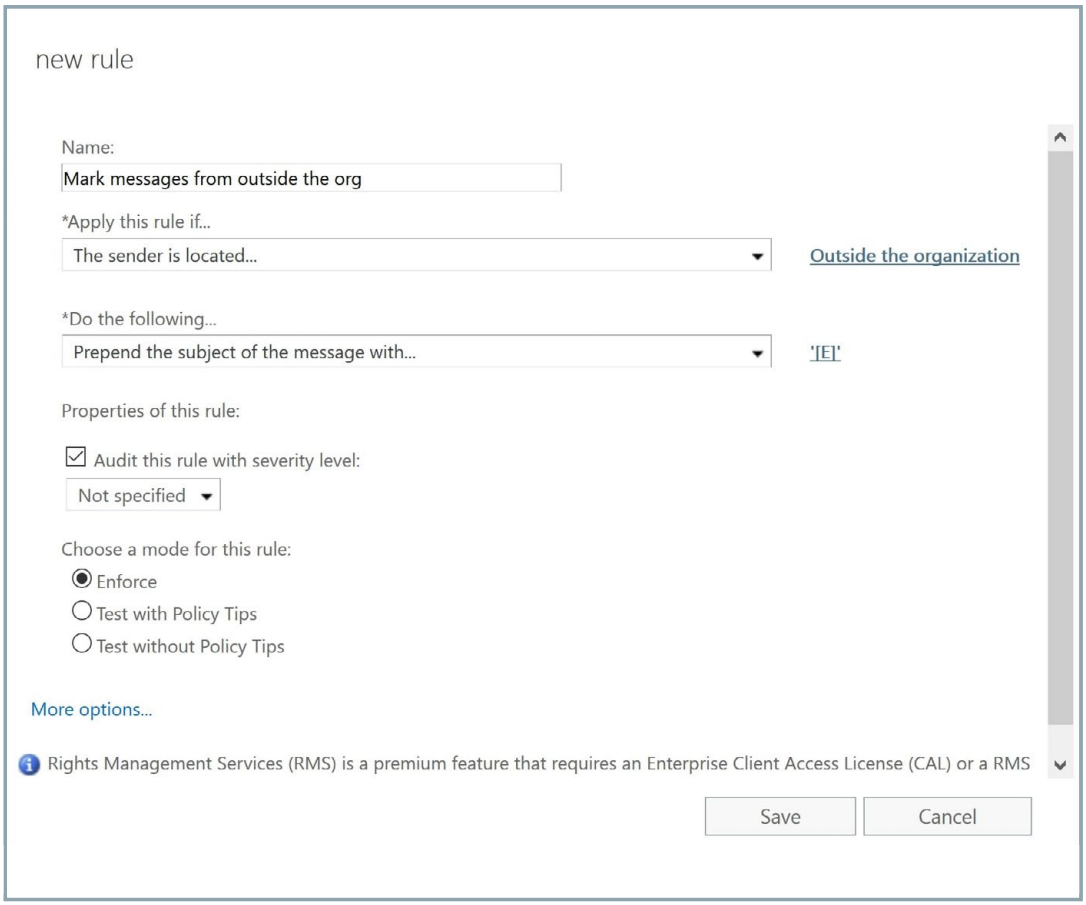
To create a rule that stamps any message that originates from outside your organization:

1. In the EMC, go to the Dashboard page. Under *"Mail Flow,"* click Rules.

2. Click the down arrow beside the **+** sign and choose Modify Messages from the menu. (You can see here the other types of transport rules you can create.)

3. Fill out the resulting pop-up, as shown in Figure 2.7.

Figure 2.7
Configuring a rule to mark messages that originate from outside the organization



Blocking Senders

There are a number of reasons, such as spam and user harassment, that users might ask you to block certain outside senders from sending email to your organization.

To put folks on a tenant-wide block list, take the following steps:

1. In the EMC, in the *"Mail Flow"* section, click ***Rules***.
2. Click the **+** icon and then choose ***Create a new rule***.
3. Name the rule, and then click ***More options***.
4. Under *"Apply this rule if,"* choose ***The Sender***.
5. Add the email addresses you want to block and then click ***Check Names*** to put them on the list.
6. Under *"Do the following,"* choose ***Block the message*** and then click ***Delete the message*** without notifying anyone.

7. Click ***More options***, and then for the *"Match sender address in message"* option, select ***Header or envelope***.

8. Click ***Save*** to finish.

Enabling Archive Mailboxes

Archive mailboxes were introduced a couple of versions of Exchange ago to solve the problem of tons of PSTs with old mail lying around in your network. Each mailbox has an archive mailbox attached to it, where older mail can be retained on cheaper storage. That way, older mail is available for e-discovery, while the size of the primary mailbox is kept under control to improve performance.

To enable an archive mailbox in Office 365:

1. In the EMC, go to the Dashboard page and click either ***Recipients*** (for an individual user) or ***Shared*** (for a shared mailbox).

2. Select the mailbox for which you want to enable an archive mailbox.

3. On the right, under *"In-Place Archive,"* click ***Enable***.

Administering Exchange Online using PowerShell and the Command Line

Now I'll show you how to use PowerShell to perform the same tasks we just saw how to do using the Office 365 web interface. Be sure you're connected to Exchange Online PowerShell (as explained in Chapter I) and your session is ready.

Creating a Shared Mailbox

The following command will create a new shared mailbox and give the account User1 access and Send on Behalf rights for that mailbox:

```
New-Mailbox -Shared -Name "Customer Support" -DisplayName
"Customer Support" -Alias support | Set-Mailbox
-GrantSendOnBehalfTo User1 | Add-MailboxPermission -User User1
-AccessRights FullAccess -InheritanceType All
```

Specifying SMTP Addresses for a Recipient

The following command adds three email addresses to a mailbox and makes user1@yourdomain.com the default reply address for all mail sent out from that mailbox:

```
Set-Mailbox user1 -EmailAddresses "SMTP:user1@yourdomain.
com","user1@yourdomain.net","user1@yourdomain.org"
```

Granting Send on Behalf and Full Access Permissions for a Mailbox

To grant George Caldwell access to Rita Bailey's mailbox, use this command:

```
Add-MailboxPermission -Identity "Rita Bailey" -User "George
Caldwell" -AccessRights FullAccess -InheritanceType All
```

Creating Distribution Lists

To allow George to send email on behalf of Rita (as if the email were coming from Rita), use this command:

```
Add-RecipientPermission -Identity "George Caldwell"
-Accessrights SendAs -Trustee "Rita Bailey"
```

The following command creates a new distribution list with three members:

```
New-DistributionGroup -Name "Jon's Direct Reports" -Members
edward@yourdomain.com,louann@yourdomain.com,rogelio@yourdomain.
com
```

To add or remove employees from a distribution list, use the following commands:

```
Add-DistributionGroupMember -Identity
"NameOfDistributionGroup\" -Member "usertoadd@yourorganization.
```

```
Remove-DistributionGroupMember -Identity "NameOfDistribution\
Group" -Member "usertodelete@yourorganization.org"
```

What if you need to create a new distribution group and then add a list of users to that group? Perhaps there has been a reorganization and you need to recreate lists of direct reports, or there's a new cross-departmental project with a lot of members and you need to add 50 people to a list really quickly. PowerShell makes this easy indeed.

First, you need a list of the email addresses in a CSV file that looks like this:

```
Emailaddress
user1@yourorganization.org
user2@yourorganization.org
```

The email addresses must already exist in your Office 365 tenant in order for this command to work.

First, we'll establish a variable to hold the list of email addresses:

```
$UsersToAdd = Import-CSV listofusers.csv
```

Then we'll write a simple routine that iterates through that list and pipes each email address to the Add-DistributionGroupMember command:

```
ForEach ($User in $UsersToAdd)
{
Add-365DistributionGroupMember -Identity "Test DG" -Member \
$User.emailaddress
}
```

Creating a Mail Flow (Transport) Rule

Sometimes your legal team will require you to add a disclaimer to all outbound mail, especially if your organization operates in a heavily regulated industry. Here's how to create the mail flow rule you need:

```
New-TransportRule -Name ExternalDisclaimer -SentToScope
'NotInOrganization' -ApplyHtmlDisclaimerText "<h3>This is the
disclaimer heading</h3><p>Here is the text of the disclaimer.</
p><img alt='Corporate logo' src='http://www.yourdomain.com/
images/logo.png'>"
```

Enabling Archive Mailboxes

The following command will enable an archive mailbox for user1:

```
Enable-Mailbox user1 -Archive
```

The following command will enable an archive mailbox for each user mailbox in your Office 365 tenant:

```
Get-Mailbox -Filter {ArchiveStatus -Eq "None" -AND
RecipientTypeDetails -eq "UserMailbox"} | Enable-Mailbox -
Archive
```

III. Managing SharePoint Online

SharePoint Online is designed to facilitate collaboration. Users can share documents, calendars, lists, pictures, discussion boards and more with users both within your network and, in some cases, users outside of your network, such as partners or vendors.

Understanding the Default Site Structure

The basic unit of SharePoint content is the site collection — a group of sites with similar characteristics that can be managed as a whole. By default, your Office 365 subscription includes two site collections:

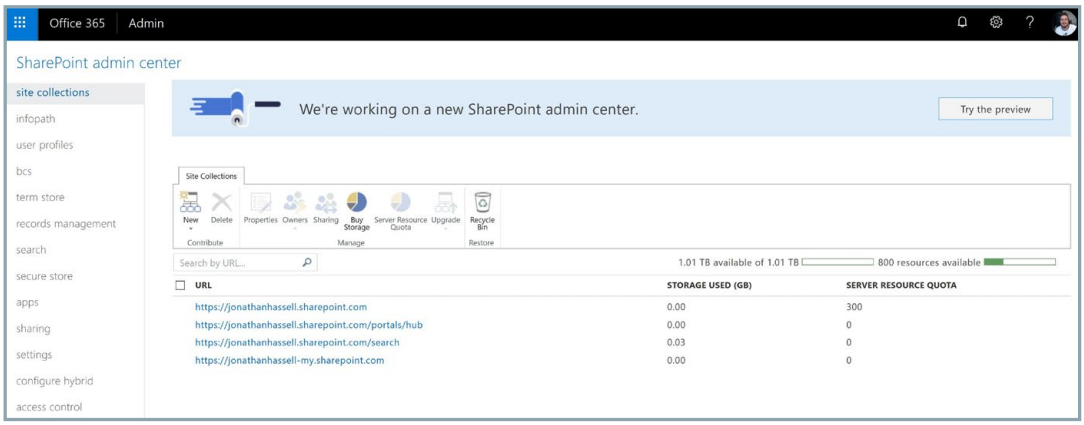
- A default team site collection, https://yourtenantname.sharepoint.com, which is a basic SharePoint site designed for collaboration. You can create additional sites in this site collection for individual teams, projects, meetings or whatever makes sense for your organization.
- A default public website collection, https://yourtenantname-public.sharepoint.com, which was originally designed to host the public-facing website for your company. This functionality is being deprecated, so I recommend ignoring this site collection.

In addition to those two tenant-wide sites, you also get individual *"My"* sites for each user in your tenant who has a SharePoint Online license. My site is essentially a front end to the OneDrive for Business service and is where each user's one terabyte of storage space is found. This storage space can be synchronized to desktops and laptops so that a person's documents are always on whatever device they are using. We will talk more about OneDrive for Business later in this guide.

Administering SharePoint Online

You can access the SharePoint admin center by heading to https://yourtenantname-admin.sharepoint.com. You'll be prompted to log in, and then you will see

Figure 3.1
The SharePoint admin center



Types of SharePoint Online Site Content

SharePoint Online has a defined list of content types that you can create on a given site.

They include:

A page. A page is exactly what it sounds like — a page that is edited in the browser using the editor functionality in SharePoint. Pages primarily contain text, but you can embed images, links, lists, and web parts (little bits of code) in them.

A document library. A document library is a set of Word and other files. You can create folders to structure the documents logically within the library. To modify a file, a user must check it out and back in; this ensures that only one person edits a file at any given time and enables you to keep past versions so you can see the revision history of a given document.

Other kinds of libraries. There are form libraries that store XML forms which your business can use to route information through Microsoft InfoPath; picture libraries that store image files; and wiki page libraries, which basically create a quick way to edit text and have it remain on the web as well as link that text to other pages — a poor man's shareable text editor, you might say.

A site itself. Sites are basically collections of content, so you can create sites underneath your main SharePoint site (kind of like large folders on your file system) to collect related materials that deserve their own focus. Meetings, blogs, documents, and teams might have their own sites. If the hierarchy is confusing, think of it like this: A site is a file drawer in a file cabinet, and the libraries, lists and other types of content are the individual folders in that file drawer.

A list. Lists are collections of like items. You can create a list of links, a list of announcements, a calendar, a list of contacts, a custom list in either list form or editable datasheet form, a discussion board, an issue tracking list, a list of project tasks (with a Gantt-like chart), a survey, a task list, or an imported spreadsheet.

Best Practices for Structuring SharePoint Online

When you are first starting with Office 365, it's important to give some thought to how you will structure your SharePoint sites. Most SharePoint experts recommend creating site collections based on the types of permissions that users and creators will need.

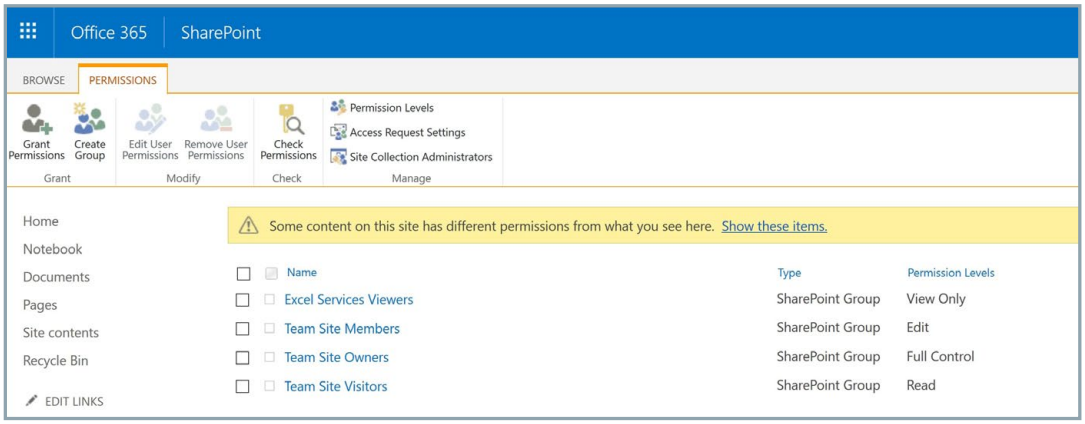
For example, you might want to have separate site collections for sales and marketing, customer support, research and development, and operations. Within each of those site collections, you might give users permission to create subsites at will, so that teams can manage their own sites and IT isn't a bottleneck.

Understanding Groups and Permissions

Some of the most common administrative tasks are granting, modifying and removing permissions from Office 365 users. The easiest way to understand SharePoint permissions is to compare them to standard NTFS permissions like you have in Windows — groups of SharePoint users can have read and write (and some other SharePoint-specific) permissions granted to them.

You can see what permissions are available to grant on the ribbon of each SharePoint site, on the Permissions tab:

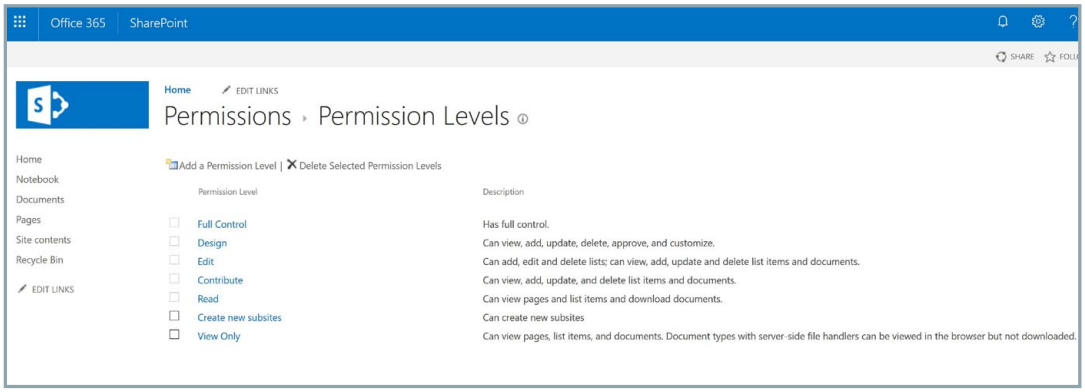
Figure 3.2
Viewing permissions and groups for the default SharePoint team site in a tenant



On this page, you can create a new group; grant, edit or revoke permissions for the default groups (Team Site Members, Team Site Owners, and Team Site Visitors), or check permissions on a specific user or object.

If you click ***Permission Levels*** in the Manage section of the ribbon, you can see all of the permission levels available, as well as create or delete permission levels:

Figure 3.3
Viewing and managing permission levels



If you want to create new groups of users so that you can assign them SharePoint permissions more granularly, the easiest option is to use the regular Office 365 admin center. Since the entire service is based on Azure Active Directory, the groups you create in one application are available for use in other applications, just as you would expect if you created security groups in your on-premises Active Directory.

To create a new group:

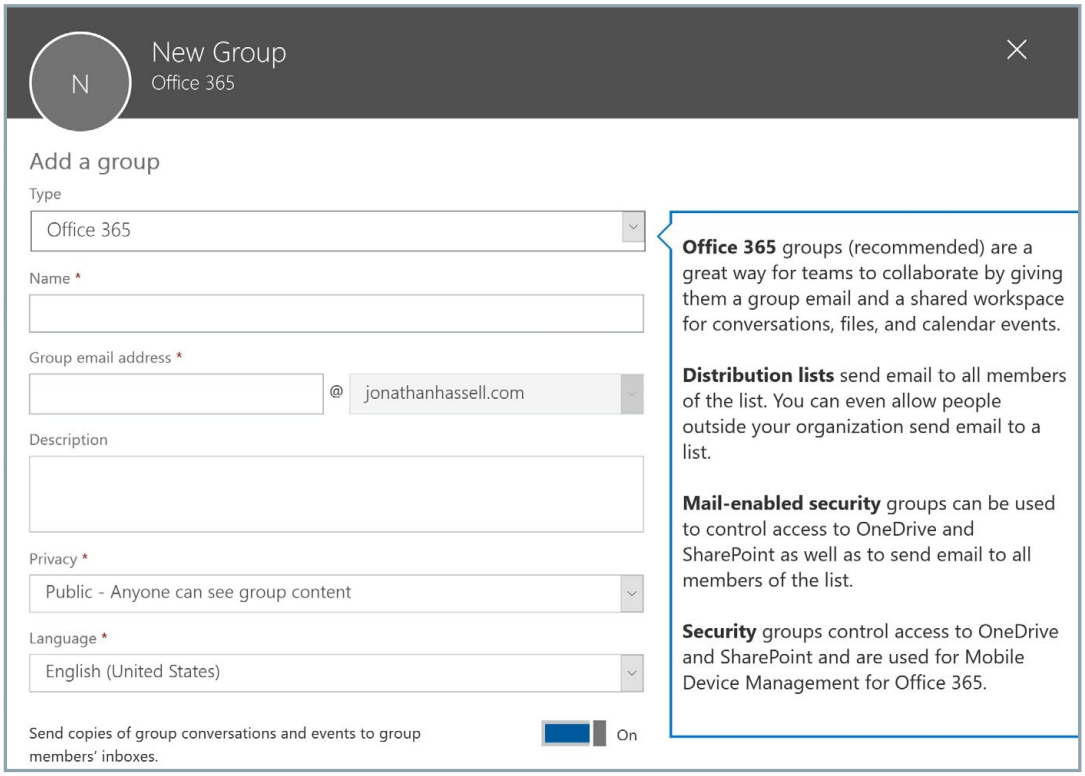
1. Go to the administrative portal at https://admin.microsoft.com/AdminPortal/Home#/homepage.

2. In the menu at the left, hover over the icon with multiple people. From the pop-out menu, click ***Groups***.

3. Click ***+ Add a Group***.

4. Fill out the form to create a new mail-enabled security group. At this time, do not create an Office 365 group — that is a different type of group that is irrelevant to our purposes right now. A mail-enabled security group is a group of users that can be assigned permissions in various sites and services but that can also be addressed through a single alias like an Exchange distribution group could.

Figure 3.4
Creating a new group

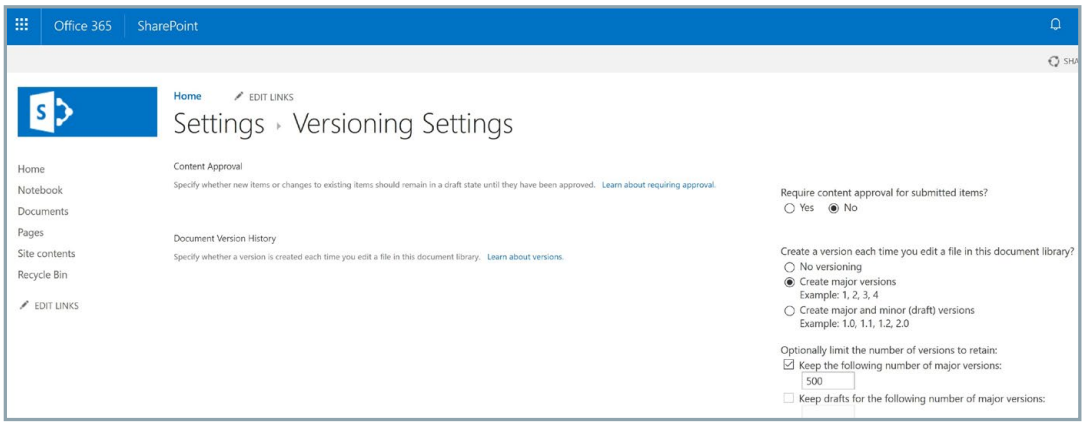


Enabling Versioning

One of the neat features of SharePoint Online is the service's built-in support for versioning of documents. When versioning is enabled, SharePoint will create a new version of a file each time it is saved. This makes it easy to create an audit trail, see who made what changes and back out unwanted revisions. Most businesses that work on sets of documents for long periods of time will find versioning helpful.

You enable versioning on document libraries. On a team site, for example, click ***Documents***, click the settings wheel at the top right of the window (within the black bar) and then click ***Library Settings***. On the resulting page, under General Settings, click ***Versioning settings***. You'll see this page:

Figure 3.5
Versioning settings for a document library

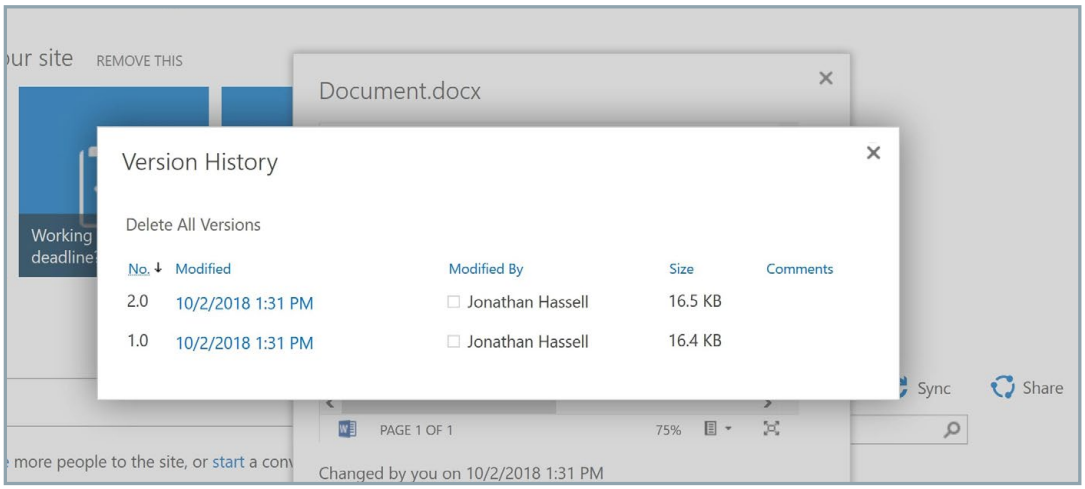


Make sure one of the versioning options — either *"create major versions"* or *"create major and minor (draft) versions"* — is enabled and click Save. Then, when your users are creating, modifying and saving documents to that library, they'll be able to see and use different versions in the history of the documents.

I recommend against enabling minor versions because every small change will generate a new version of the file. While SharePoint is relatively efficient at storing files, you can quickly find your storage allotment eaten up with files that add little value to the versioning history. Unless you have a specific need, stay with the *"Create major versions"* option.

SharePoint automatically tracks the different versions. Users can access them from the web, but not directly from Microsoft Word, so instruct your users to head to the team site document library when they need to see older versions. To see and edit different versions, click ... next to a file in a document library, and from the pop-up menu, select Version history. You'll see a screen like in Figure 3.6:

Figure 3.6
Accessing an older version of a file in a SharePoint Online document library



To edit a particular version, simply click the hyperlink.

Managing SharePoint Online using PowerShell

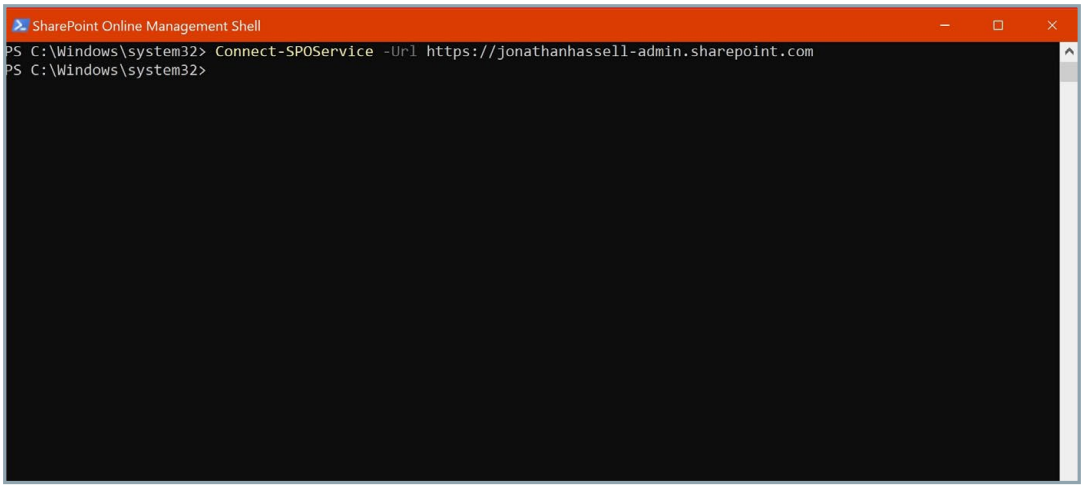
You can manage the settings for most Office 365 applications using PowerShell. For SharePoint Online, you need to download the SharePoint Online Management Shell from the Microsoft website (https://www.microsoft.com/en-us/download/details.aspx?id=35588) and then install it. If you're running Windows 8.1 or Windows 10 on your management workstation, that's all you need. But if you're still running Windows 7, you must also download and install the Windows Management Framework version 3.0 or later.

Run the SharePoint Online Management Shell and open a session to the admin site in your tenant by entering:

```
Connect-SPOService -URL https://yourtenant-admin.sharepoint.com
```

You'll be prompted for your tenant administrator credentials and then your session will be loaded, like this:

Figure 3.7
Starting a new SharePoint Online Management Shell session



Creating and Populating Sites

To create a new SharePoint Online site, use the New-SPOSite command, specifying a web address for the site, the user who will own the site and the storage quota in gigabyes:

```
New-SPOSite -Url https://yourtenant.sharepoint.com/Sites/newsitename -Owner you@yourtenant.com -StorageQuota 100
```

To find out what groups are available on a site, use this command:

```
Get-SPOSiteGroup https://yourtenant.sharepoint.com/sites/
yoursitename
```

You can add a user to a site, but when you do, you need to add the user to one of the existing site groups at the same time:

```
Add-SPOUser https://yourtenant.sharepoint.com/sites/
yoursitename -Loginname you@yourtenant.com -Group Visitors
```

Configuring Sharing

One of the biggest draws of SharePoint Online is the ability to create extranet-like functionality with a couple of clicks. For example, you can select to share a document, document library, or even whole site with users external to your organization without worrying (at least from the end user's perspective) about federation, identity management, mapping credentials and all that jazz.

But some companies, especially those with more stringent or sensitive regulatory and compliance requirements, want to completely disable the ability for external users to access or even receive invitations to the content stored in their tenant. Luckily, one command in PowerShell turns this ability on and off.

To completely disable external sharing, use this command:

```
Set-SPOSite -Identity https://yoursite.sharepoint.com/sites\
/thesiteyouwant -SharingCapability Disabled
```

To enable both external user and guest (i.e., unauthenticated) access, use this command:

```
Set-SPOSite -Identity https://yoursite.sharepoint.com/sites\
/thesiteyouwant -SharingCapability ExternalUserAndGuestSharing\
```

To enable only authenticated external users (no guests) to have content shared with them, use this command:

```
Set-SPOSite -Identity https://yoursite.sharepoint.com/sites\
/thesiteyouwant -SharingCapability ExternalUserSharingOnly
```

Auditing Who Has External Access to a SharePoint Online Site

You will likely want to periodically review the current state of sharing on your tenant. The following script will spit out sharing status and also who has received invitations outside your organization for each site in your tenant:

```
$SitesToAudit = Get-SPOSite | Where-Object {$_.SharingCapab\
ility -ne "Disabled}

ForEach-Object ($Site in $SitesToAudit)
{
Write-Host $Site.URL " has " $Site.SharingCapability " conf\
igured"
Get-SPOExternalUser -SiteUrl $Site.URL | Select DisplayName\
, Email, InvitedBy, WhenCreated | Format-Table -AutoSize
}
```

IV. Managing OneDrive for Business

OneDrive for Business is a file storage and synchronization service that's similar to Dropbox: It makes all of an individual's files and folders available to them no matter where they are or what device they are using.

Understanding the Differences between SharePoint and OneDrive for Business

Both SharePoint and OneDrive for Business enable users to store and share files, and access them from multiple devices. So when should users choose each solution?

OneDrive. OneDrive is like a home directory or personal mapped drive where you can save documents and retrieve them. While you can share files from OneDrive with others, it's really meant to be a personal repository of files that can simply be synced over many different devices.

SharePoint. SharePoint, on the other hand, is ideal for projects that require collaboration with coworkers or people outside your organization. Having the project in a SharePoint site makes it trivial to share information with colleagues and work on the project together in real time. Essentially, if you own files as a team and not as an individual, it generally makes sense to put them in a SharePoint site. Moreover, SharePoint can handle additional types of content that OneDrive doesn't support, such as calendars, wikis and meeting workspaces.

Administering OneDrive for Business

To customize how OneDrive for Business works in your Office 365 tenant, use the OneDrive admin center at https://admin.onedrive.com/?v=SharingSettings.

There you can configure:

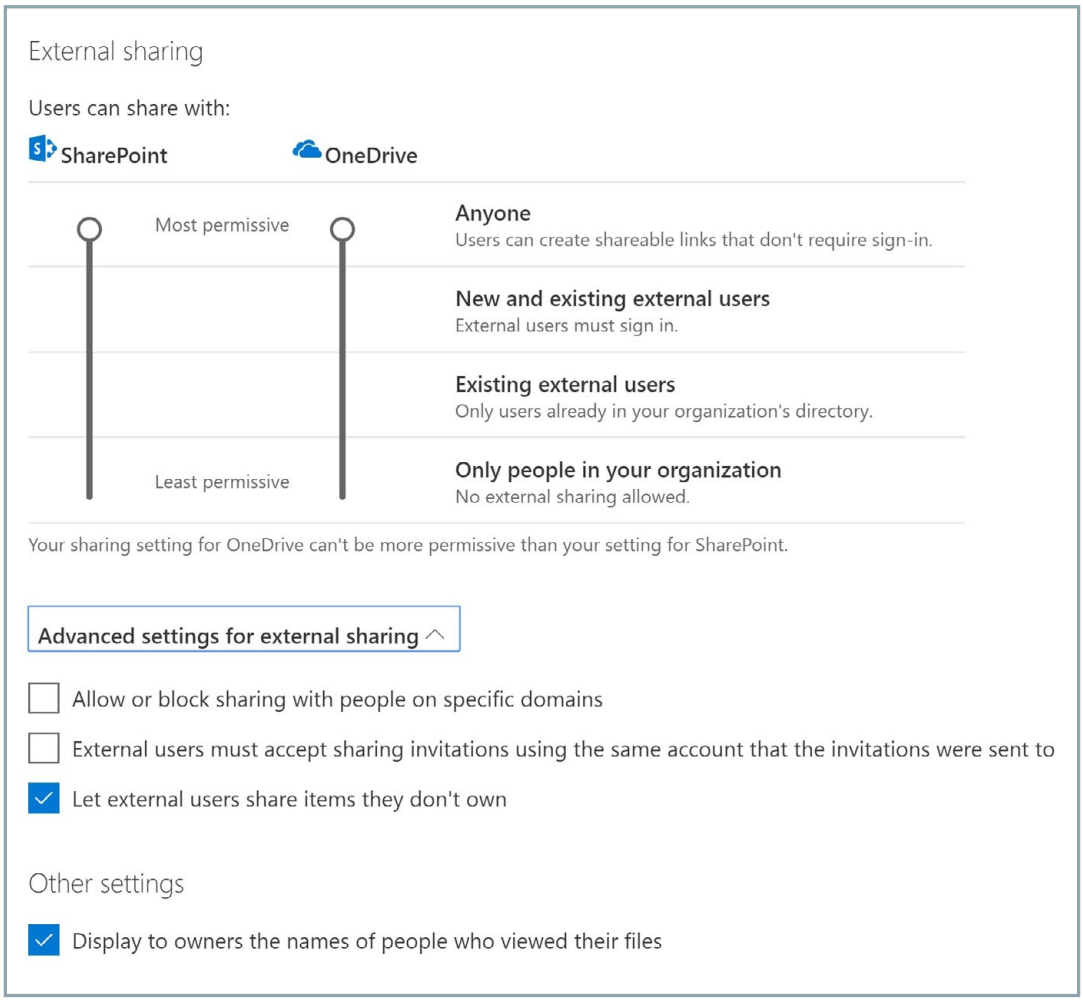
- Sharing
- Storage
- Compliance
- Sync
- Device access
- Notifications

Sharing

On the Sharing page, you can choose the type of link that is generated when a user shares a document. You can also configure the number of days until a link expires and whether links for files have different permissions than links that share the contents of entire folders.

Pay particular attention to the external sharing options. You can control which, if any, external users can access your OneDrive data. You can also set up a list of domains with which sharing will be prevented; require users outside the organization accept an invitation from the same account that the invitation was sent to (which prevents forwarding of invitations); and prevent external users from sharing items they don't own.

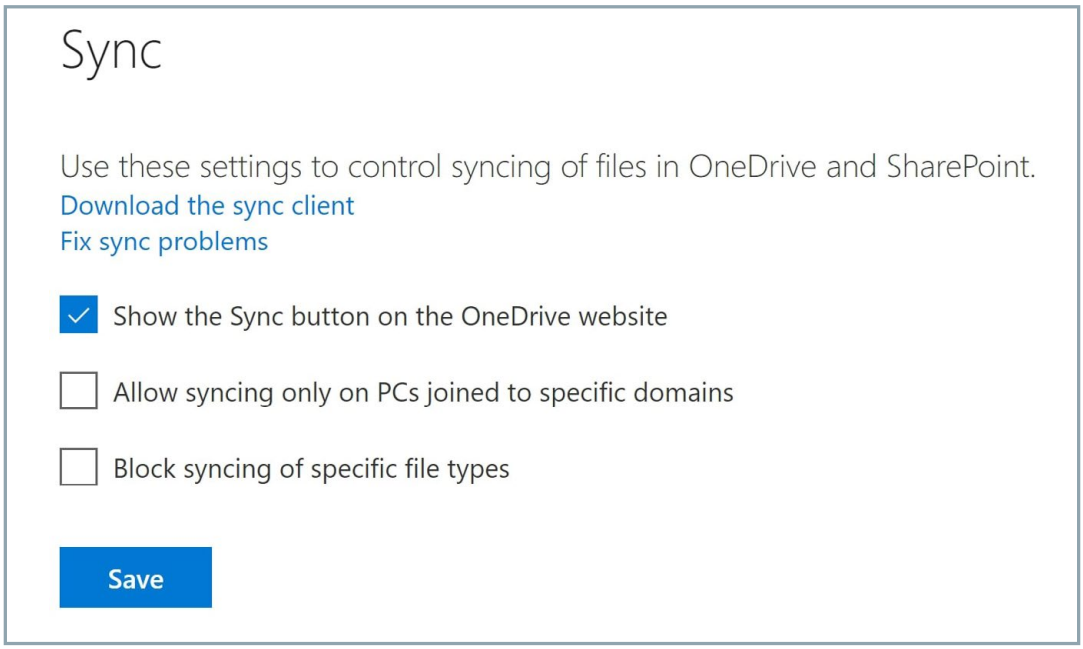
Figure 4.1
Configuring external sharing



Sync

From the Sync page, you can download the latest OneDrive sync client, which is recommended for Windows 7, Windows 8.1 and Mac clients — sync is built into Windows 10 and the Windows Update function will handle updating the client on those machines. You can also prevent syncing of documents to users' home PCs and blocking syncing of specific file types, such as databases that might not sync well.

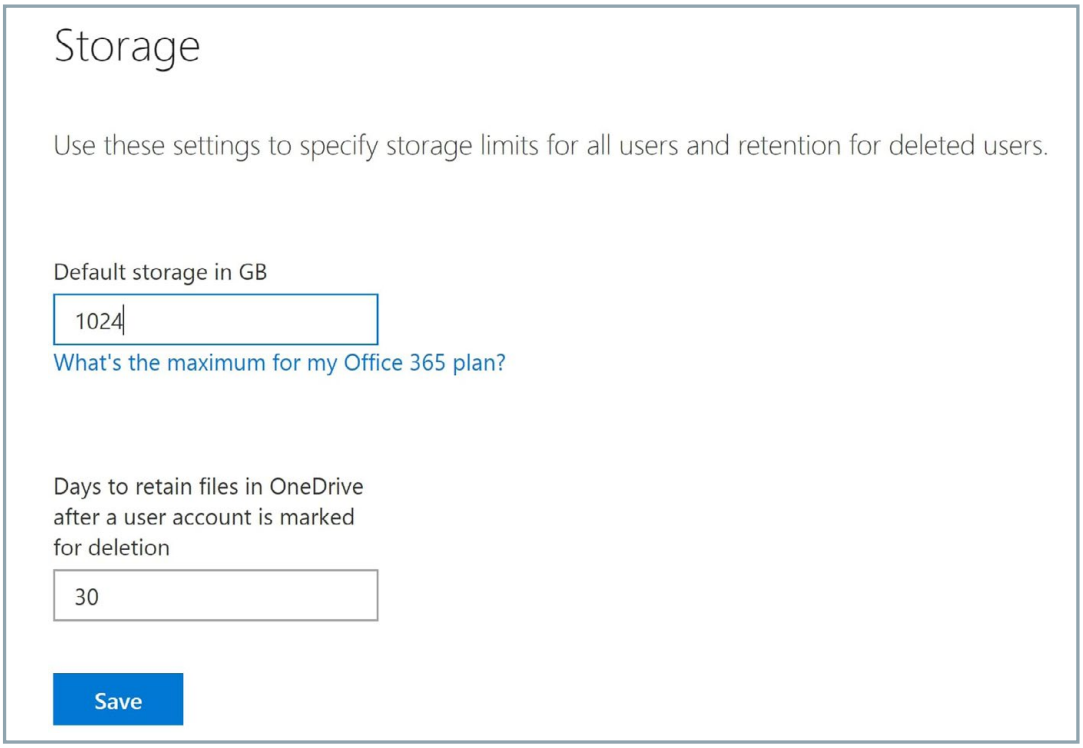
Figure 4.2
Managing sync settings



Storage

On the Storage page, you can configure the default quota for all users (from 1 to 5 terabytes), and also configure the retention policy for documents that belong to deleted users.

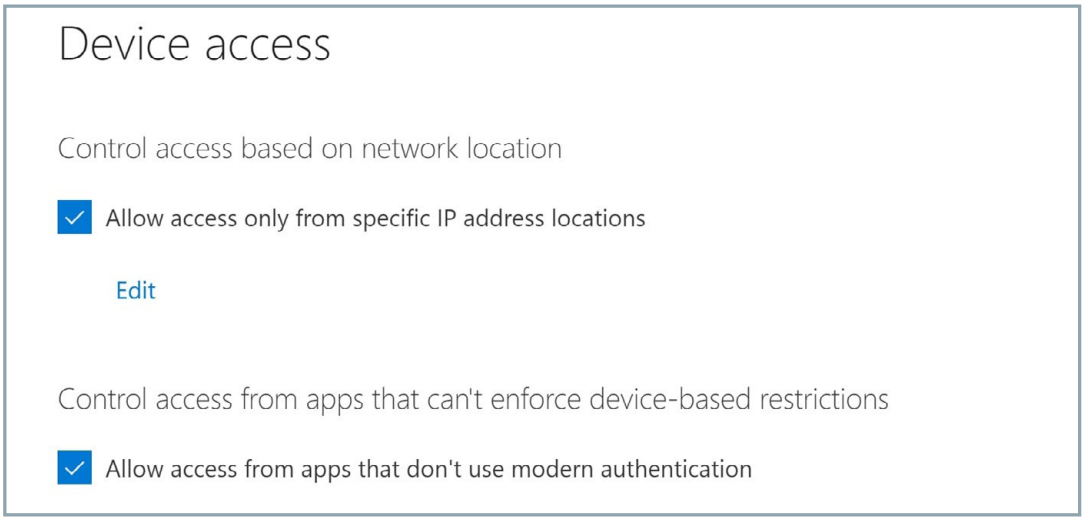
Figure 4.3
Managing storage quotas



Device Access

On the Device access page, you can restrict access to certain IP ranges (for example, so that only devices on your office network can sync) or restrict access to devices that support the latest authentication methods.

Figure 4.4
Managing device access restrictions



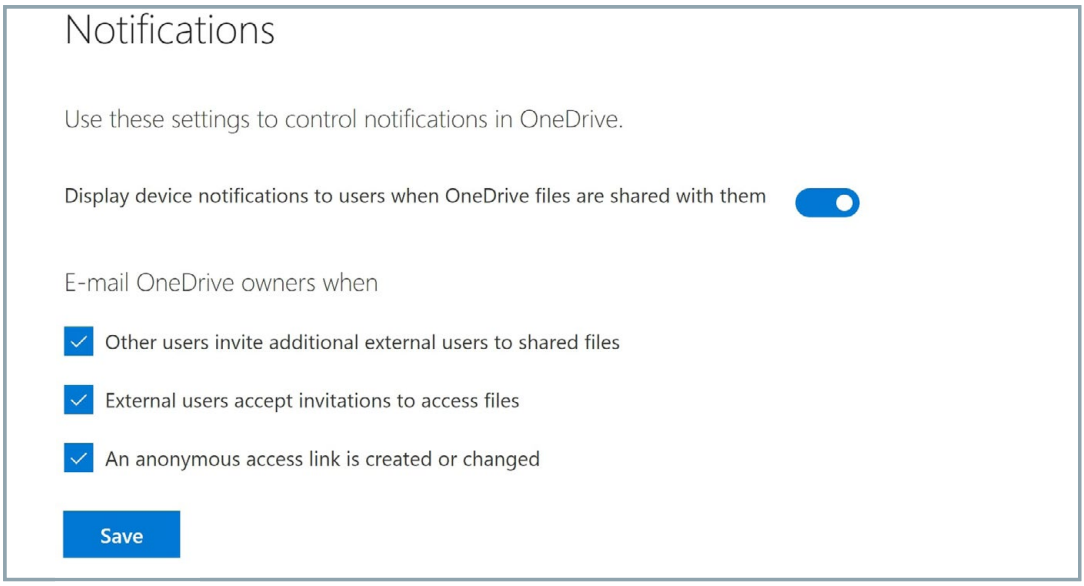
Compliance

The compliance page is simply a shortcut to the Security & Compliance Center, which I'll cover later in this guide.

Notifications

On the notifications page, you can configure how OneDrive notifies users and file owners when things happen to their files.

Figure 4.5
Configuring OneDrive for Business notifications



Configuring Storage Quotas

Each user with an Office 365 E type plan gets at least one terabyte of OneDrive for Business storage. For E3 plans and higher with at least five users, you get *"unlimited"* storage, but of course that's not entirely true — you initially get one terabyte of space per user, and the administrator can increase that quota to five terabytes per user. Once a user reaches the five terabyte limit, you can file a ticket with Microsoft support to increase the quota to 25 terabytes per person. Once that limit is reached, further space is apportioned to individual users as SharePoint team sites limited to a single person.

You configure storage quotas using the SharePoint Online Management Shell. To set the default storage quota to 1TB, enter the following command:

How to set the default storage quota

```
Set-SPOTenant -OneDriveStorageQuota 1048576
```

For 5TB, I'll save you the math; it's 5242880. There is no free lunch here, though: If any individual user's license doesn't allow for the value you specify here, their quota will be set to the maximum value permitted by their license.

To reset an existing user's OneDrive to the new default storage limit, run the following command:

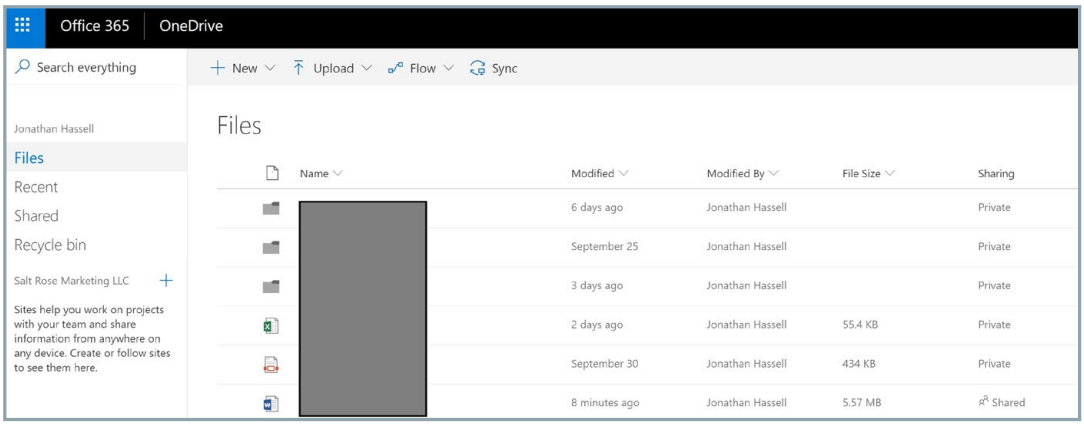
How to reset an existing user's OneDrive to the new default storage limit

```
Set-SPOSite -Identity /personal/jon_jonathanhassell_com
-StorageQuotaReset
```

Guiding Users through the OneDrive for Business User Experience

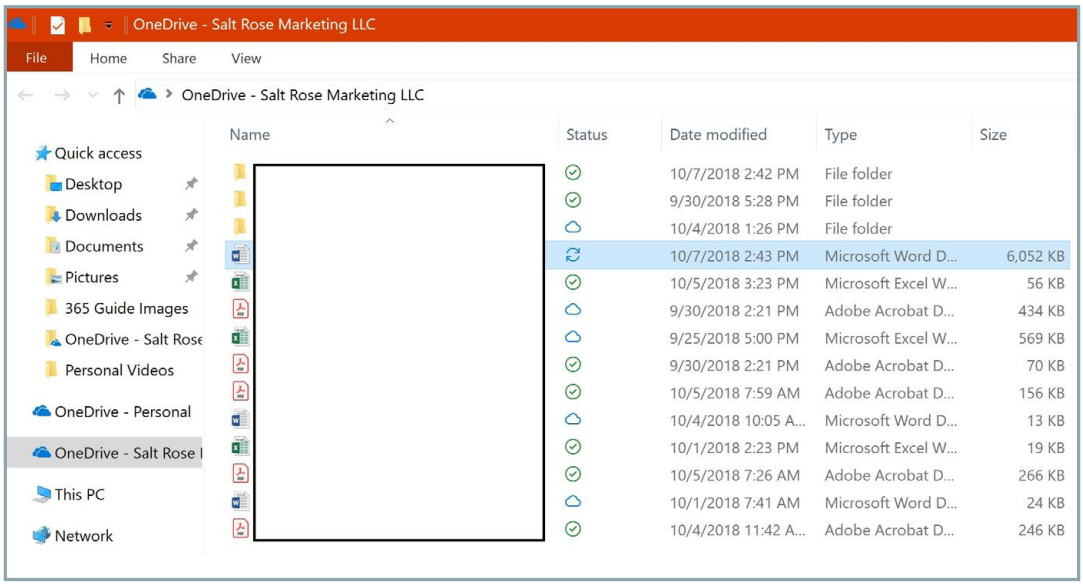
It's easy for users to get started with OneDrive for Business — they simply log in to the Office 365 portal at https://portal.office.com and click the OneDrive button. The resulting page looks like this:

Figure 4.6
OneDrive for Business web user interface



Essentially, OneDrive for Business becomes another file folder on the user's system — users can save files, documents, spreadsheets, and everything else to the folder.

Figure 4.7
The OneDrive user experience



The Status column for each file will have either:

- A circle with a green check mark, which means the file exists both in the cloud and on the local device.
- Two arrows in a circle pattern, which means the file is currently being synched.
- A cloud icon, which means the file exists only in the OneDrive cloud. To download a permanent copy of a cloud file to your local device, right-click the file and choose ***Always keep on this device***.

V. Setting up a Hybrid Environment

Many organizations that use Office 365 have a hybrid deployment — that is, they also have an on-premises Active Directory, which is the primary storage for identity information. To enable you to synchronize identity data from your on-prem AD to Azure AD, Microsoft provides Azure Active Directory Connect, a fairly lightweight service that runs on a server in your office or datacenter. You can select which objects to sync and which objects to leave local.

There are two key facts that you should absolutely understand:

- When you use Azure AD Connect to sync directories, you are creating what amounts to an irrevocable relationship between your Office 365 tenant and your local directory. You must create new users and make changes to your existing users in your on-premises directory; you won't be able to use the Office 365 GUI or PowerShell to do it. While there are various hacks and unsupported ways of breaking a sync relationship between an on-premises directory and Office 365, you won't be able to call for help when things go wrong. Expect that your tenant will be forever bound to a local domain controller and that you will always have to have that domain controller unless you migrate to a brand new tenant.

- You don't have to have a local Exchange Server to have Office 365 in directory sync mode. But once you do create an Exchange hybrid relationship (this is another step beyond directory sync; you'll know it if you do it), you will have to leave a single Exchange Server machine on your local network forever. This is because of the way Office 365 defers some things to on-premises Exchange Server machines; some roles that the on-prem machine holds cannot be moved up to Office 365 in a supported way. Microsoft is working on changing this, so that when all of your mailboxes are migrated to Office 365, you will decommission that last Exchange Server on your network, but at this time, it remains a requirement.

Installing and Configuring Azure AD Connect

To use Azure AD Connect, take the following steps:

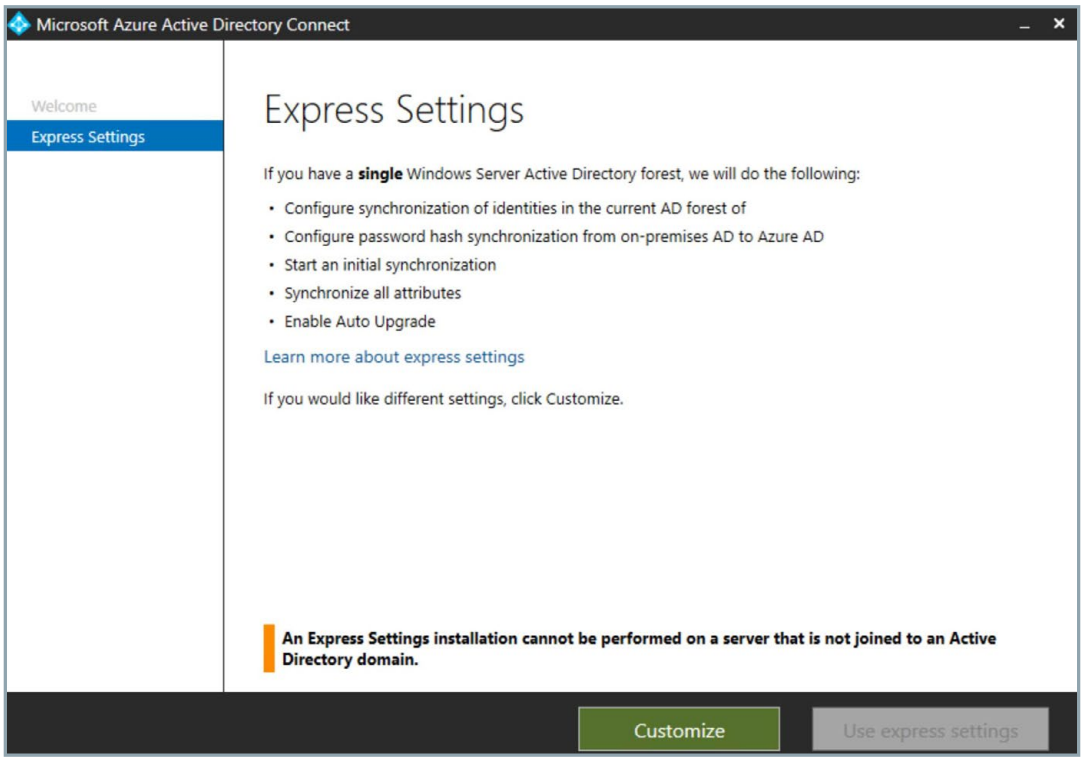
1. Download the Azure AD Connect installer from http://go.microsoft.com/fwlink/?LinkId=615771.

2. Copy the installer to the server that you want to designate as the sync server and run the installer.

3. Agree to the license terms and click ***Continue***.

4. The Express Settings screen appears. Read the details of what the wizard will do, and then, for the purposes of our walkthrough, click ***Use express settings***.

Figure 5.1
The Azure AD Connect Express Settings screen



5. The Connect screen appears. Enter your Office 365 administrator's username and password and then click ***Next***.

6. The wizard will do some computations and then show the Ready to configure screen. On this screen:

   - I recommend deselecting the *"Start the synchronization process as soon as configuration completes"* checkbox. You'll want to do some filtering of the directory parts that get synchronized anyway, and when you uncheck this box, the wizard configures the sync service itself but disables the scheduler. Once you have completed your filtering, you'll re-run the installation wizard in order to enable the schedule.

   - If you are running Exchange locally, check the box to enable a hybrid Exchange deployment. This will enable a few more directory attributes to sync, which will serve you well when it's time to run the Exchange Hybrid Configuration Wizard, as explained in the next section.

7. Click ***Install***.

8. Once the installation completes, exit the wizard and reboot the machine.

Customizing What Gets Synchronized

It makes sense to sync only those directory objects that can be used in Office 365; you don't want a bunch of service accounts and other objects littering your Azure AD when there is literally nothing you can do with them in the cloud.

To customize which organizational units (OUs) are synchronized, take the following steps:

1. Launch the Synchronization Service Manager.

2. Select ***Connectors***.

3. Open the properties of the Active Directory Domain Services connector.

4. In Configure Directory Partitions, go to Containers. Enter your credentials to proceed.

5. Select the OUs you want to sync and then click ***OK***.

6. Last, you just need to enable the scheduler, which is just a standard Windows scheduled task that has been disabled. To enable it, simply open Task Scheduler, find the *"Azure AD Sync Scheduler"* task, and then in the right pane under Selected item, click ***Enable***. Wait until it runs (or run it immediately from the Task Scheduler interface) and you'll see a bunch of new user accounts populating in Azure AD. That's how you know the sync is working. You can also try logging on with one of the accounts.

Setting Up a Hybrid Exchange Environment

If you are running Exchange on-premises, the next step is the fully enable the hybrid relationship by configuring coexistence between your on-prem Exchange and Exchange Online.

Take the following steps:

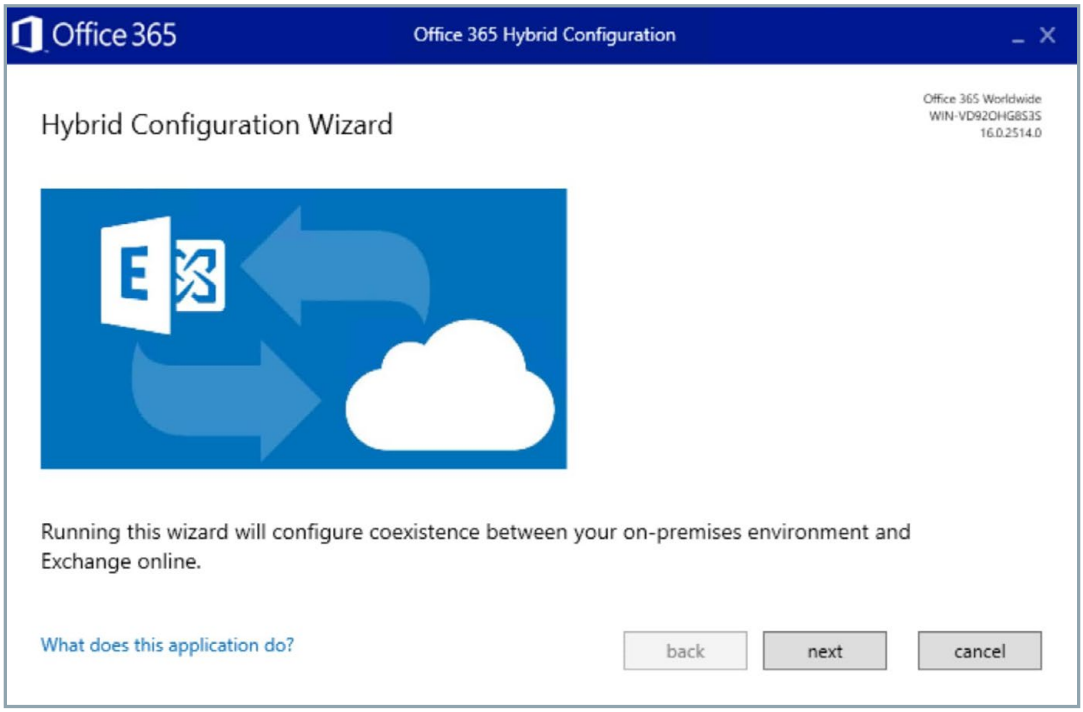
1. From the Exchange Admin Center, launch the Hybrid Configuration Wizard. In the left pane, navigate to Hybrid and click ***Enable***.

2. Sign in with your Office 365 account.

3. Click ***Accept***. The Hybrid Configuration Wizard tool will be downloaded and install itself automatically.

4. When the wizard has finished installing, it will open. Click ***Next*** to begin.

Figure 5.2
The Hybrid Configuration Wizard



5. Specify the Exchange Server machine you want to use or select the one that the wizard has identified automatically.

6. Enter credentials for your on-prem Active Directory deployment and for your Office 365 tenant.

7. The wizard will check the credentials. Once they've been verified, click ***Next*** to continue.

8. For our purposes, choose the ***Configure my Client Access and Mailbox servers for secure mail transport (typical)*** option and click ***Next***.

9. Choose the right SSL certificates and click ***Next***.

10. Review all of the information you've entered and click ***Update***.

The wizard will run a number of PowerShell commands behind the scenes to configure your local Exchange Server machine and Office 365 tenant, make connectors, and configure remote domains, encryption and so on.

Migrating Mailboxes from On-Premises Exchange to Office 365 in a Hybrid Environment

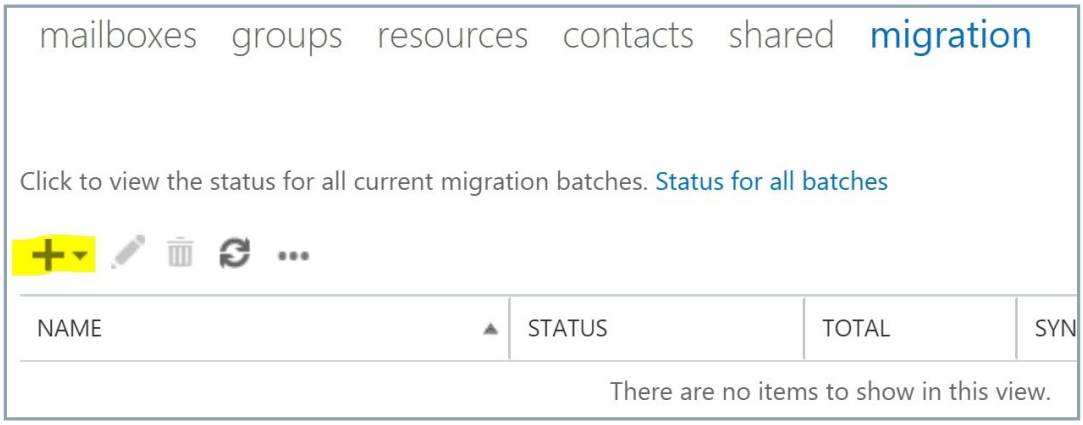
One of the benefits of a hybrid configuration is that you get a great way to migrate your mailboxes to the cloud without having to pay for a third-party solution or do it yourself manually over many long weekends.

To migrate mailboxes, take the following steps:

1. Open the Exchange Admin Center at https://outlook.office365.com/ecp and choose ***Migration*** in the recipients section.

2. Click the **+** icon, and then click ***Migrate to Exchange Online*** from the pop-up menu.

Figure 5.3
Migrating mailboxes in a hybrid relationship



3. Select the ***remote move*** migration, and then click through the wizard. You'll add a mailbox to a migration batch, create an endpoint if you need to and name the batch. Tell the wizard where to contact you when the migration is complete, and then wait for that email. Note that the migration could take hours, depending on the size of your mailbox, the bandwidth and latency on your Internet connection, and how busy Microsoft's Exchange Online servers are.

4. Launch Outlook on the migrated user's computer. Autodiscover should realize the mailbox has been moved and do some reconfiguration. Their phone or tablet should also work with no user action required.

VI. Configuring Email Encryption

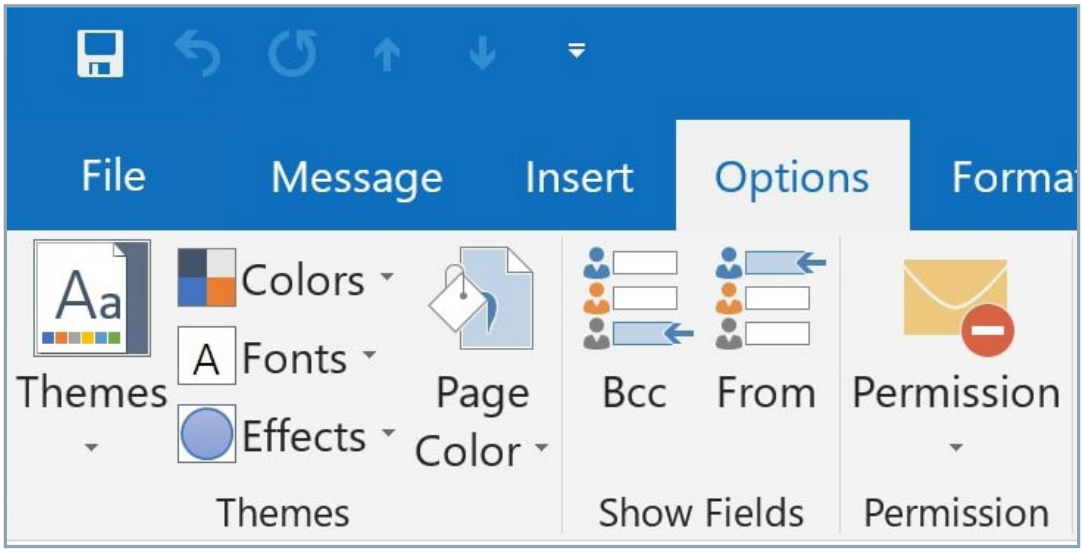
Office 365 includes powerful message encryption features that enable organizations to securely send sensitive information across a heretofore relatively insecure infrastructure — mail servers. The E3 and E5 plans of the Office 365 and Microsoft 365 suites are automatically licensed for encryption, and lower plans can use it if you add the Azure Information Protection add-on license to those users. If your Office 365 tenant was created after February 2018, then you automatically have the email encryption capabilities present and turned on. If your tenant was created prior to that date, Microsoft is slowly but surely rolling out the capabilities and enabling them for you; they began this process in August 2018, so it should not be long before your older tenant gets access.

Encrypting Messages

Users can encrypt any message they send. The procedure depends on which mail client they are using.

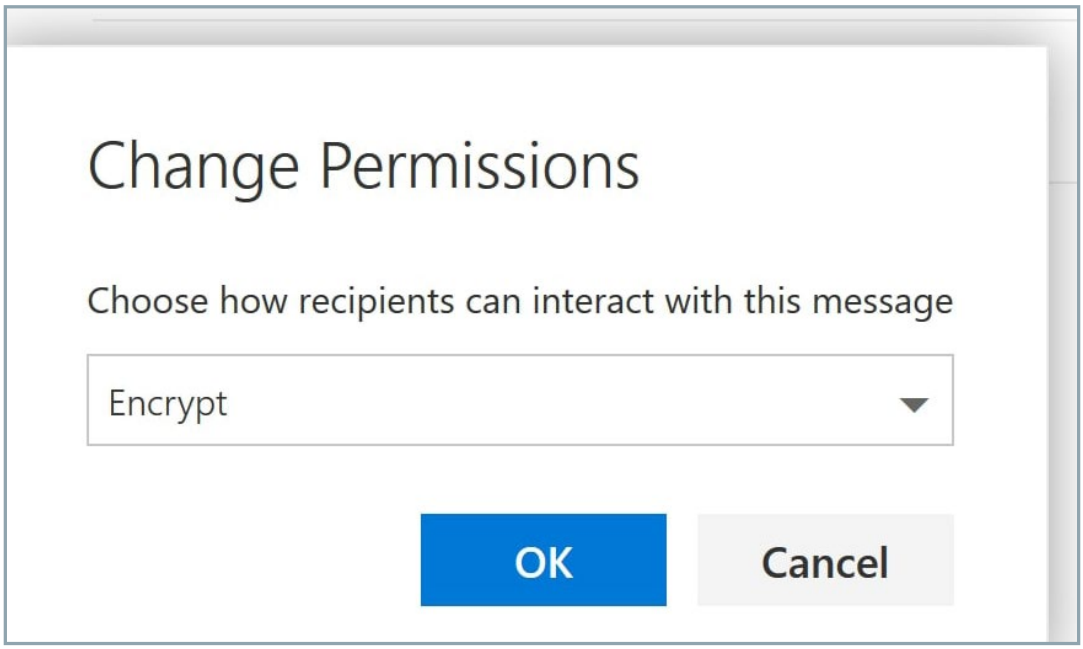
Using the Outlook client, from the message window, go to the Options tab, click ***Permission***, and choose from the list of protection options.

Figure 6.1
Encrypting a message in Outlook 2016



In Outlook on the Web, in a new message window, click ***Protect*** in the menu bar, and then click ***Change permissions***. In the window that pop ups, choose a protection option:

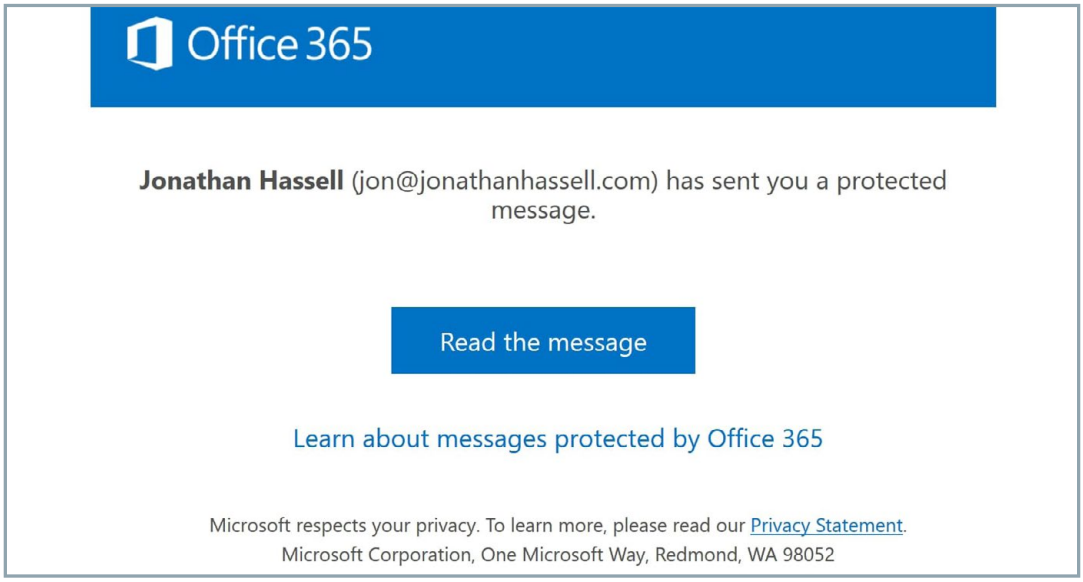
Figure 6.2
Encrypting a message in Outlook for the Web



Receiving and Responding to Encrypted Messages

When a user chooses to encrypt a message, the service will keep a copy of the message on its own servers and send a message to the outside recipient that looks like this:

Figure 6.3
Receiving an encrypted message sent outside the Office 365 tenant



When the outside user clicks the *"Read the message"* button, they can either sign in with an existing social account that uses the same email address as the message was sent to, or they can choose to have the service send a one-time passcode to the same email address. When either of those conditions is satisfied, the service will display the encrypted message in the web browser. The recipient can also reply securely to the original sender.

Managing Encryption through PowerShell

To verify that your tenant is set up for encryption, use the following command, making sure the Sender value is a valid account within your tenant:

How to verify that a tenant is set up for encryption

```
Test-IRMConfiguration -Sender someaccount@yourtenant.com
```

If you see ***"OVERALL RESULT: PASS"*** then you are ready to go.

When recipients of encrypted messages reply to those messages, you can set up a rule that automatically strips the encryption from the reply so that your internal users don't need to sign in to the encrypted message portal to view the reply. (Since the reply stays on the Microsoft servers, there is no risk of intercepting the message contents in SMTP transit.) Use the following command:

How to set up a rule that automatically strips the encryption from inbound emails

```
New-TransportRule - Name "Strip encryption from inbound
e-mail" -SentToScope "InOrganization" -RemoveOME $true
```

VII. Filtering Spam with Exchange Online Protection

Office 365 comes with an enterprise-class mail hygiene solution called Exchange Online Protection (EOP). Mail sent to your organization is directed by your DNS MX records to the EOP service, where it is scrubbed of spam, malware, unsolicited back-scatter, phishing attempts and more; only then does it go to the Exchange servers that make up the Exchange Online offering.

Configuring Exchange Online Protection

You can configure EOP from the Exchange admin center at https://outlook.office365.com/ecp/. From the left menu, click Protection, and you'll see the various options and areas that EOP lets you adjust and customize:

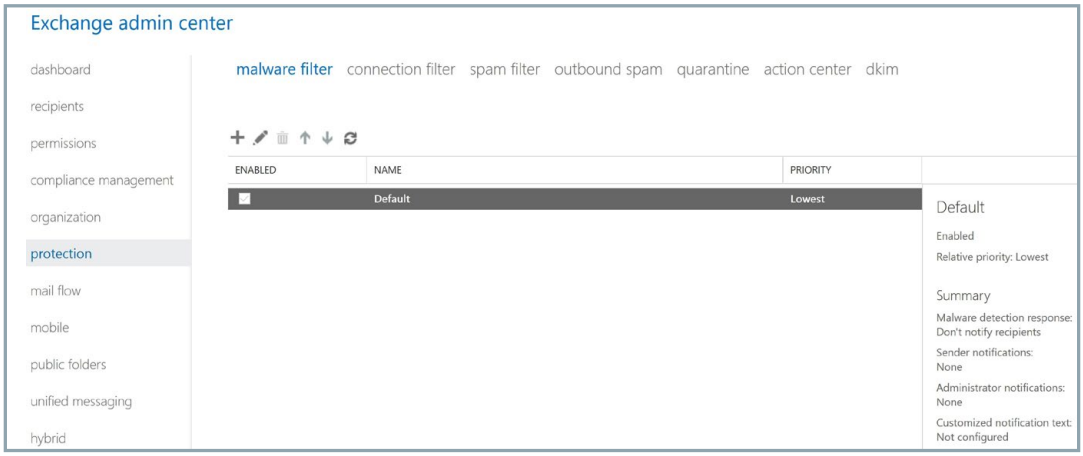


Figure 7.1
Configuring EOP options in the Exchange admin center

Each of the sections — malware filter, connection filter, spam filter, outbound spam, quarantine, action center and dkim — has a default policy for your tenant. You can either modify that policy or add new policies, some for a given set of recipients and others for other groups of recipients.

Malware Protection

The EOP service uses several different antivirus engines to scan each message to ensure that your inbound mail stream is as free of viruses as is practically possible. You likely don't want to turn this off, but you might want to adjust how notifications are provided to users when malware is detected. To adjust the settings, double-click the malware policy and go to the Settings tab of the pop-up window.

Connection Filter

If you have trusted systems sending email to your Office 365 tenant, you can add their IP addresses to the list of trusted IP hosts so that mail coming from those systems won't be subject to filtering. You might also be subject to real-time spam attacks on rare occasions, and sometimes you can configure filters on certain keys in those attack's message headers until the EOP system learns of the attack and is able to respond intelligently.

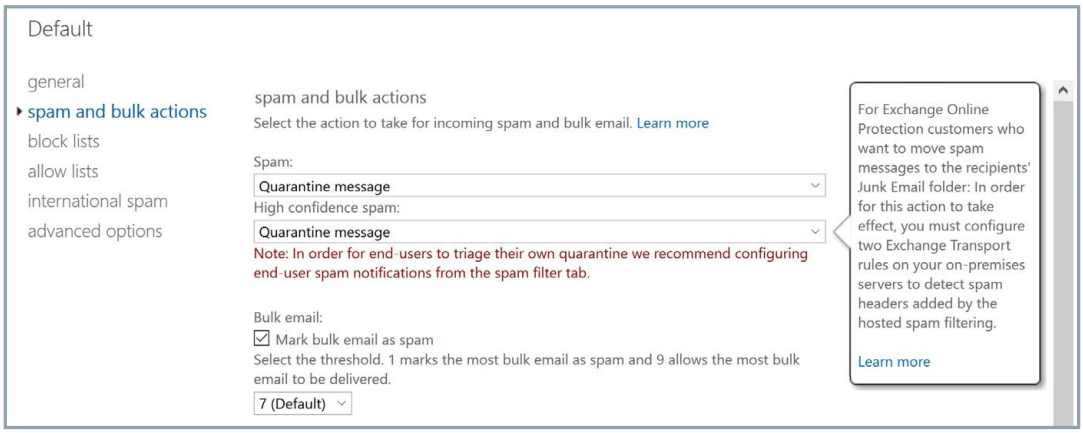
Spam Filter

This is probably where you will spend the most time configuring EOP. When EOP decides a message is spam, the default action is for it to send that spam to the user's Junk Email folder in Outlook. However, some organizations prefer a spam quarantine, where likely spam messages are held for a period of time for manual inspection until they expire and are deleted. If you prefer the quarantine approach, then it's a good idea to configure quarantine notifications for your users — the service will send daily emails to users listing all the messages it held back because the service considered them spam, and users can release any false positives and ignore the rest.

To set this up, take the following steps:

1. Double-click the default spam filter policy, choose ***spam and bulk actions*** from the left side of the pop-up menu, and then choose the ***Quarantine*** option for the first two items:

Figure 7.2
Configuring quarantine mode for EOP spam filtering



2. Return to the Exchange admin center page. In the right pane, select ***Configure end-user spam notifications***.

3. In the pop-up window that appears, check the ***Enable*** box, select how often to send quarantine notifications (I recommend 1 so users will get them every day), and then click ***OK***.

International Spam Notifications

Spam in foreign character sets is a notorious problem, and while there is obviously nothing wrong with receiving mail in another language per se, if none of your staff speaks a language, it doesn't do you much good to receive email in that language. The International Spam section of the spam filter dialog box lets you configure which languages to receive.

VIII. Data Loss Prevention

Data loss prevention (DLP) is an intelligent service that's part of Office 365. It looks for messages, files, and objects that contain sensitive information and applies the policies you configure about what can and cannot be done with that data. The most common types of sensitive information an organization would want DLP to look for are credit card numbers, Social Security or insurance numbers, and other personally identifiable information (PII).

DLP uses pattern matching to determine whether text is likely to be sensitive information. When users try to interact with that data, the service applies the policies you configured. For example, it might log an audit event for later review; display a warning to the user saying, in effect, *"hey, this looks sensitive; are you sure you want to be doing that?"*; or block the action completely.

Setting Up Office 365 DLP Policies

In an Office 365 setting, it is best to configure tenant-wide DLP policies that take into account not just email but files and text in SharePoint, OneDrive for Business and other services as well. If you configure DLP in the Exchange admin center, it will work for email only; but if you set up the DLP policy in the right place, you get protection across multiple services for no additional cost.

To set up tenant-wide DLP policies, take the following steps:

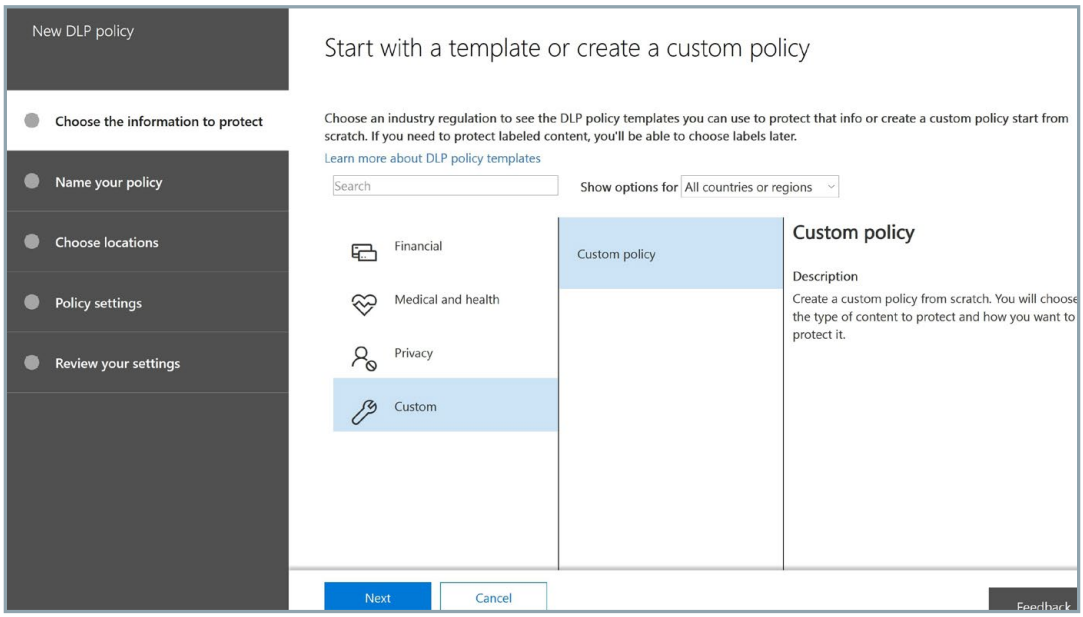
1. Go to the Security and Compliance center in the administrative portal at https://protection.office.com/?rfr=AdminCenter#/homepage.

2. On the left, click ***Data Loss Prevention***, and then in the right pane, click ***Create a new policy***.

   Office 365 provides a number of pre-populated templates. For example, for U.S. organizations, there are templates for detecting the following:

- Data subject to the Gramm-Leach-Bliley Act (GLBA)
- Data subject to the Payment Card Industry Data Security Standard (PCI-DSS)
- United States personally identifiable information (U.S. PII)
- Data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Figure 8.1
Starting a new DLP policy



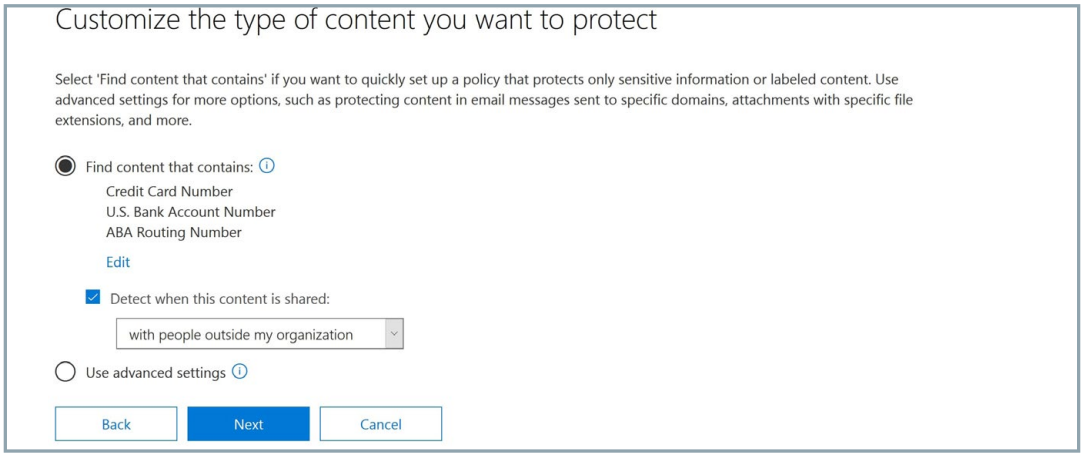
3. For our purposes, let's click ***Financial*** and then ***U.S. Financial Data***. Click ***Next***.

4. Give the policy a name and description. Click ***Next***.

5. On the *"Choose locations"* page, pick what parts of the Office 365 service this particular policy will be enforced in. For this walkthrough, let's choose ***All locations***. Then click ***Next***.

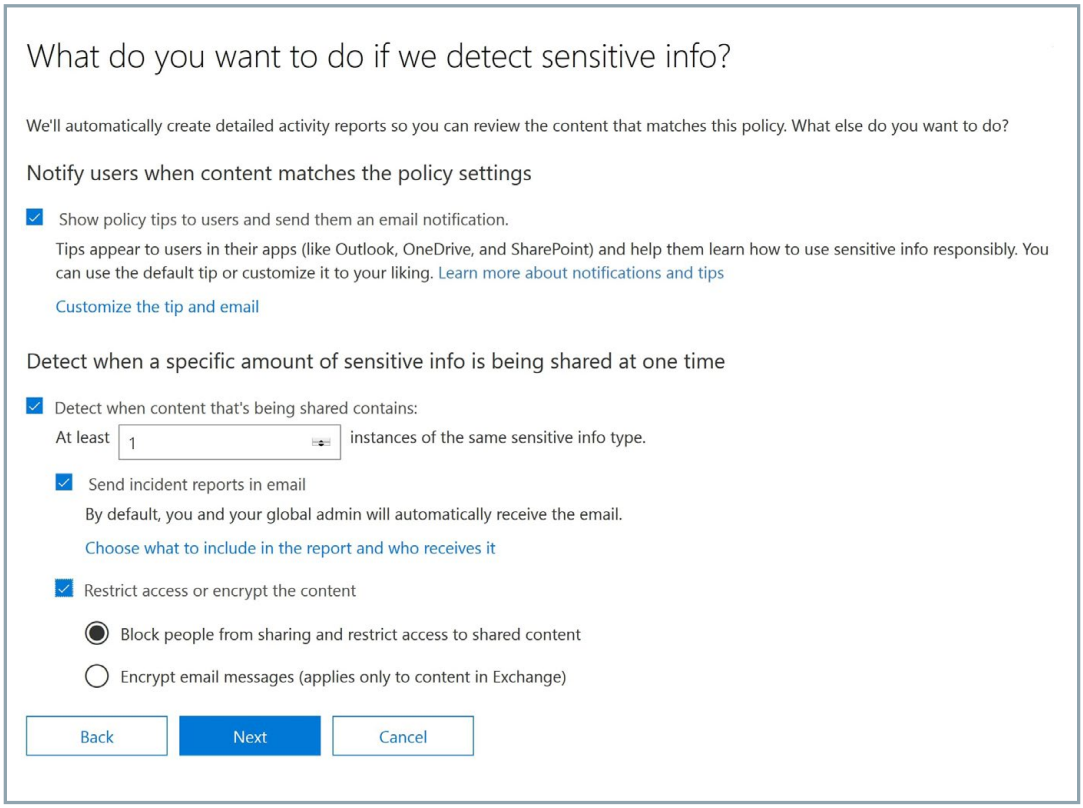
6. On the next screen, you can customize the types of information this policy will apply to. In most cases, you will want to accept the defaults, at least initially. In this case, we're looking for credit card numbers, U.S. bank account numbers and routing numbers, and for our protection we want to know when this content is attempted to be given to people external to our company. Click ***Next***.

Figure 8.2
Customizing the type of content to protect with a DLP policy



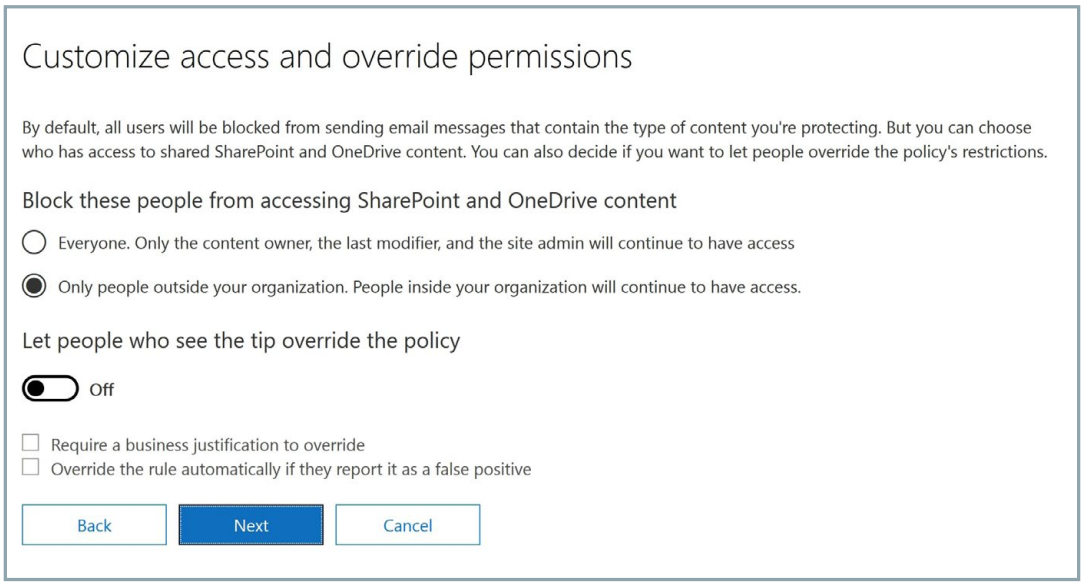
7. Next, you'll be asked what methods of enforcement you want to use. You can choose to simply show policy tips to the user, which will just inform the user that they're working with sensitive information, or you can select to notify different people or block actions. For our purposes, let's change the number of instances required to 1 — even one credit card number leaked is too many these days — and choose to block people from sharing the content. (If your business model requires sharing of this type of sensitive data, you could use the DLP policy to automatically encrypt it before it is sent out; you'd just check the last box on this page.) Click ***Next***.

Figure 8.3
Configuring actions upon triggering a DLP policy



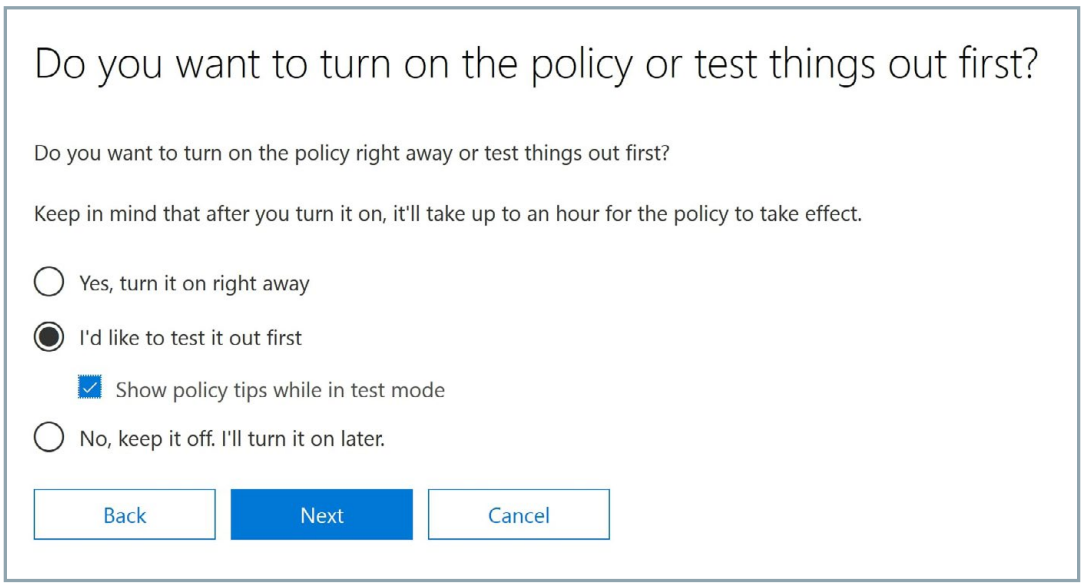
8. On the next page, you can choose to block certain people from accessing SharePoint and OneDrive for Business content and whether and how users can override the DLP policy.

Figure 8.4
Customizing access and override permissions



9. Finally, you can choose whether to run the policy in test mode or begin enforcement immediately. I recommend using test mode for a while to make sure you won't adversely affect user workflows. Test mode flags policy matches but doesn't actually prevent any content from being sent — it is like a *"what if"* mode that shows you what content would trigger a policy. You can also instruct Office to show tips with Outlook while in test mode for user edification.

Figure 8.5
Activating the policy

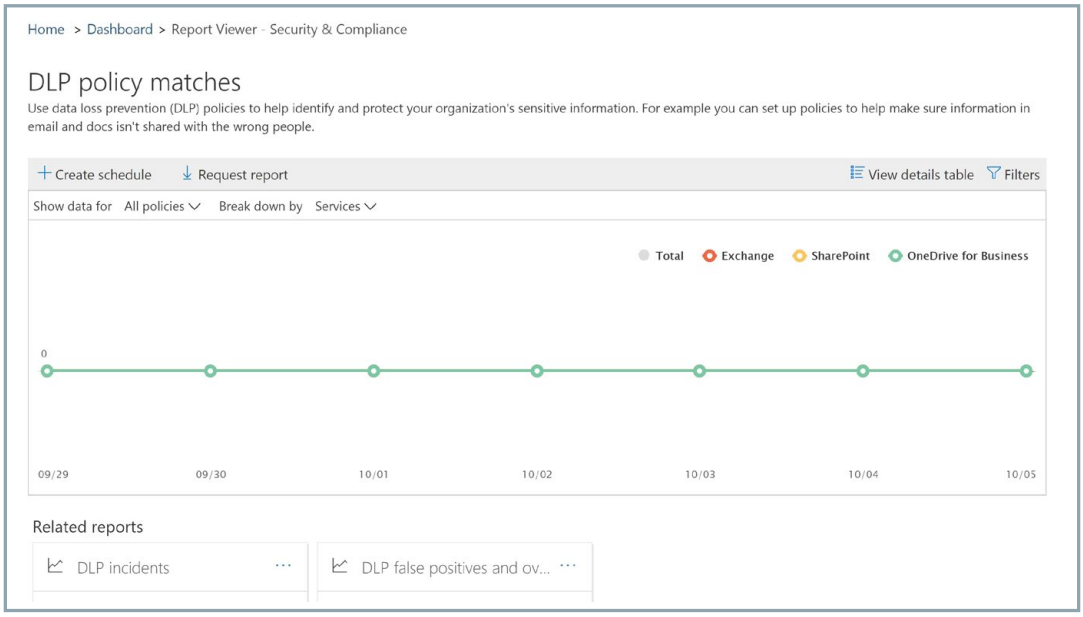


10. Review your settings and close the wizard.

Viewing DLP Reports

To understand how DLP affects your organization, you should review how often your users tried to send content that matched a DLP policy. The Security and Compliance center offers reports that show how often policies were matched over a period of time. You can filter on policy matches that hit in Exchange, OneDrive for Business and SharePoint, and you can also filter on severity, who the potential violator was and what action was taken.

Figure 8.6
Report on DLP policy matches



IX. Using Advanced Threat Protection

Viruses and malware use a variety of trajectories to infiltrate organizations these days. There is a premium service from Microsoft called Advanced Threat Protection (ATP) that offers five distinct features that add additional layers of security to your email and documents. However, ATP is included only for users who are licensed for Office 365 Enterprise E5 plans. If you don't want to upgrade everyone to an E5 package, you can purchase ATP as an add-on license for US $2 per user per month.

Safe Links

The Safe Links feature of ATP guards against malicious links in both emails and Office documents. It is similar to the *"unified threat management"* of older edge-protection and web-protection firewalls, in which the URLs users clicked on were intercepted by the firewall and run through a scanning and hygiene process before the content was allowed to come into the network. With Safe Links, email entering or leaving the organization goes through Exchange Online Protection (EOP), which filters spam and phishing messages it knows about, and scans each message through a variety of anti-malware detection engines.

When users click on links in messages that land in their inboxes, the ATP service checks the link and does one of the following:

- If the URL has been deemed by the ATP service to be safe, it is allowed to be opened.
- If the URL is on your organization's *"do not rewrite"* list, the website simply opens when the user clicks the link. A *"do not rewrite"* list is good for internal systems and line-of-business applications that take certain actions based on URLs, like one-click expense report approvals.
- If the URL is on a custom block list that your organization configured, a warning page is displayed to the user.
- If the URL has been deemed by the ATP service to be malicious in nature, a warning page is displayed to the user.
- If the URL goes to a downloadable file and your organization's ATP Safe Links policies are configured to scan such content, the ATP service will scan the file before downloading it.

To modify your Safe Links policy, take the following steps:

1. Navigate to https://protection.office.com. Under Threat management, choose ***Policy*** and then click ***Safe Links***.

2. In the *"Policies that apply to the entire organization"* section, select ***Default*** and then click the pencil button to edit the policy.

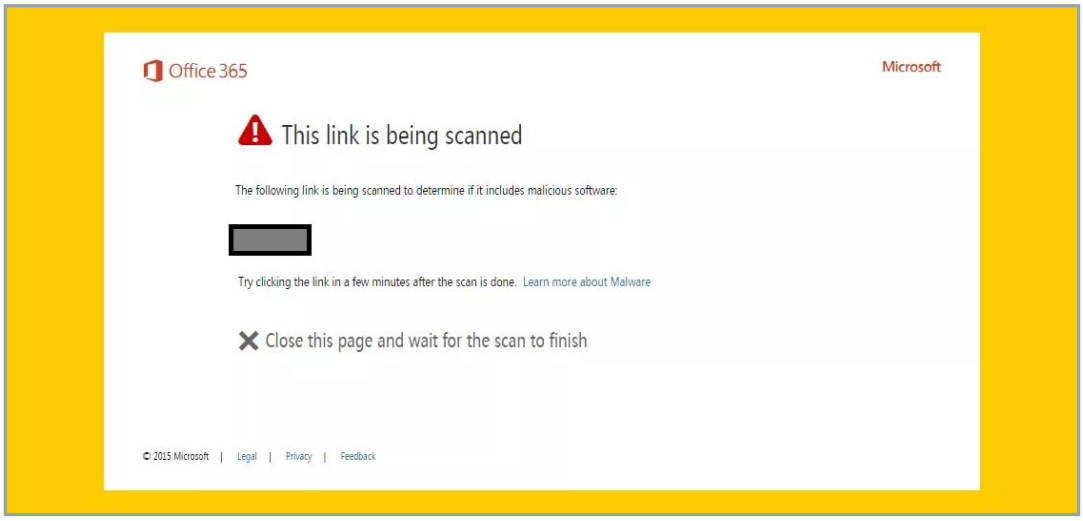
3. In the *"Block the following URLs"* section, you can add sites that no one in your organization ought to be able to visit. (This won't stop them from going to the site by directly entering its address into the address bar in their web browser, but it will prevent them from clicking a link in an email or document to visit it.)

4. In the *"Settings that apply to content except email"* section, leave everything checked.

5. Click ***Save***.

When a user clicks a link in an email or Office document, they will see a message like this:

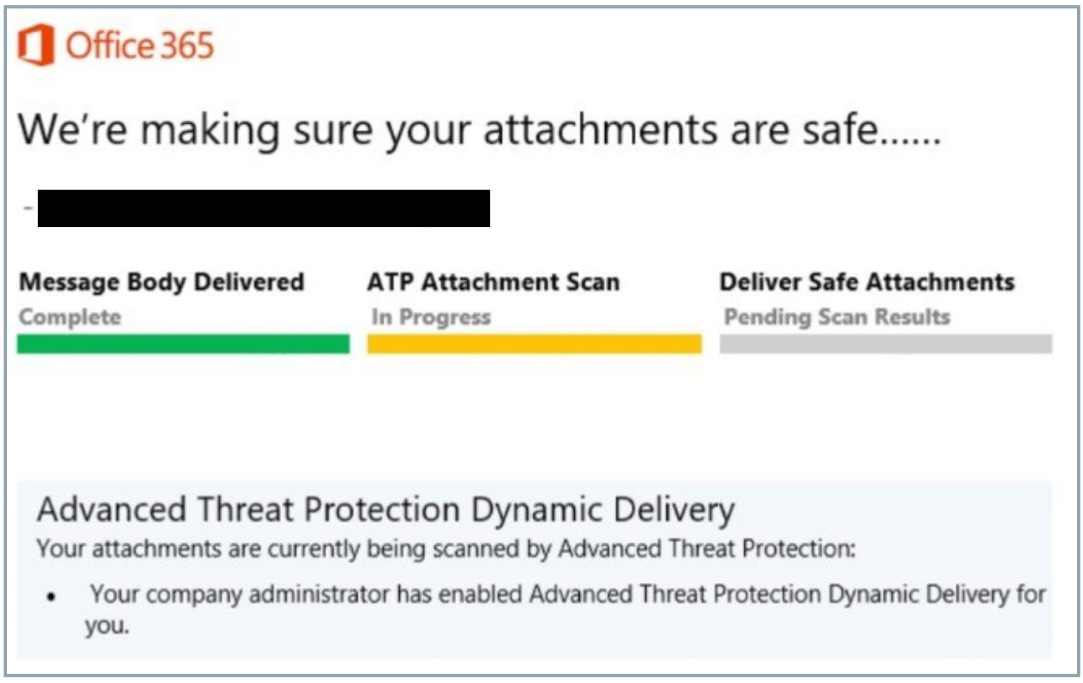
Figure 9.1
How Safe Links notifies a user that it is scanning a link



Safe Attachments

Scanning engines can miss new malware and viruses when they first break out, before they have been classified and the signatures have been updated. With Safe Attachments, messages with attachments that don't match known signatures are sent to a sandboxed virtual environment where they are securely opened. If the service detects suspicious activity like a virus or malware trying to execute, the message is rejected or quarantined. If no suspicious activity is detected, the message is released to the user.

Figure 9.2
Scanning attachments with the ATP safe attachments service



To configure Safe Attachments policies, take these steps:

1. Go to https://protection.office.com. In the left pane, under Threat management, choose ***Policy*** and then click ***Safe Attachments***. Make sure that if you're presented with the option to *"Turn on ATP for SharePoint, OneDrive, and Microsoft Teams,"* you do so. (You'll want to allow at least 30 minutes for this to take effect across all of Microsoft's global Office 365 datacenters.)

2. Click the **+** sign to create a Safe Attachments policy, and then enter a name and description for the policy. The table below explains the available settings. I recommend dynamic delivery for most recipients. It's the safest, it won't delay the body of an email, and it is virtually transparent to users who are not in front of their computer all the time.

Figure 9.3
Safe Attachments policy options (image courtesy Microsoft Corporation)

Off	Does not scan attachments for malware Does not delay message delivery	Turn scanning off for internal senders, scanners, faxes, or smart hosts that will only send known, good attachments Prevent unnecessary delays in routing internal mail **This option is not recommended for most users. It enables you to turn ATP Safe Attachments scanning off for a small group of internal senders.**
Monitor	Delivers messages with attachments and then tracks what happens with detected malware	See where detected malware goes in your organization
Block	Prevents messages with detected malware attachments from proceeding Sends messages with detected malware to quarantine in Office 365 where a security administrator or analyst can review and release (or delete) those messages Blocks future messages and attachments automatically	Safeguard your organization from repeated attacks using the same malware attachments
Replace	Removes detected malware attachments Notifies recipients that attachments have been removed Sends messages with detected malware to quarantine in Office 365 where a security administrator or analyst can review and release (or delete) those messages	Raise visibility to recipients that attachments were removed because of detected malware
Dynamic Delivery	Delivers messages immediately Replaces attachments with a placeholder file until scanning is complete, and then reattaches the attachments if no malware is detected Includes attachment previewing capabilities for most PDFs and Office files during scanning Sends messages with detected malware to Quarantine where a security administrator or analyst can review and release (or delete) those messages Learn about dynamic delivery and previewing with ATP Safe Attachments	Avoid message delays while protecting recipients from malicious files Enable recipients to preview attachments in safe mode while scanning is taking place
Enable redirect	Applies when the Monitor, Block, or Replace option is chosen Sends attachments to a specified email address where security administrators or analysts can investigate	Enable security administrators and analysts to research suspicious attachments

Spoof Intelligence

Spoof Intelligence spots mail with a From address (or with a sender field in the headers of a message) that matches one of the domains configured on your Office 365 tenant. Sometimes these messages can be legitimate — for example, you might send a marketing newsletter from a separate service like Aweber or Mailchimp, or your copier and scanner might send emails to your tenant and have a *"From"* address in your tenant. But other times it is someone impersonating an internal user in order to trick people into sending a check to pay a fake invoice, initiate a foreign wire transfer and so on.

Spoof Intelligence collects all the suspicious senders it detects in your mail flow and presents them in one convenient location, where you can decide which senders you'll allow to send mail into your tenant and which ones should be blocked. To review this list, go to the Security and Compliance page and click ***Anti-spam settings***.

X. Responding to Legal Requests

For legal reasons, your organization might be required to hold on to the contents of an employee's mailbox account or produce all documents related to a case. Office 365 provides both litigation hold and eDiscovery capabilities.

Setting a Mailbox on Litigation Hold

A litigation hold suspends any retention policy or automatic deletion for a given mailbox so that no data can be removed from the mailbox. It preserves the original and all modified versions of each item, and even if a user deletes an item from their mailbox using any version of Outlook, Office 365 retains the item for discovery purposes. The user can continue to send and receive new mail. You can configure how long the litigation hold lasts. At the expiration of that period, the hold will automatically be removed and the existing retention policy (if any) that applies to the mailbox will be enforced.

If you've managed an Exchange on-premises installation, you might be familiar with another type of hold, called *"in-place holds."* These holds are being deprecated and removed from Exchange Online, so the only hold that will be supported after the fall of 2018 will be the litigation hold, which was introduced with Exchange Server 2010.

To set a mailbox on litigation hold using PowerShell, open a session to Exchange Online and then issue the following command:

How to set a mailbox on litigation hold

```
Set-Mailbox mailbox@yourtenant.com -LitigationHoldEnabled
$true -LitigationHoldDuration 365
```

To set a litigation hold on all mailboxes in your Office 365 tenant, use the following command:

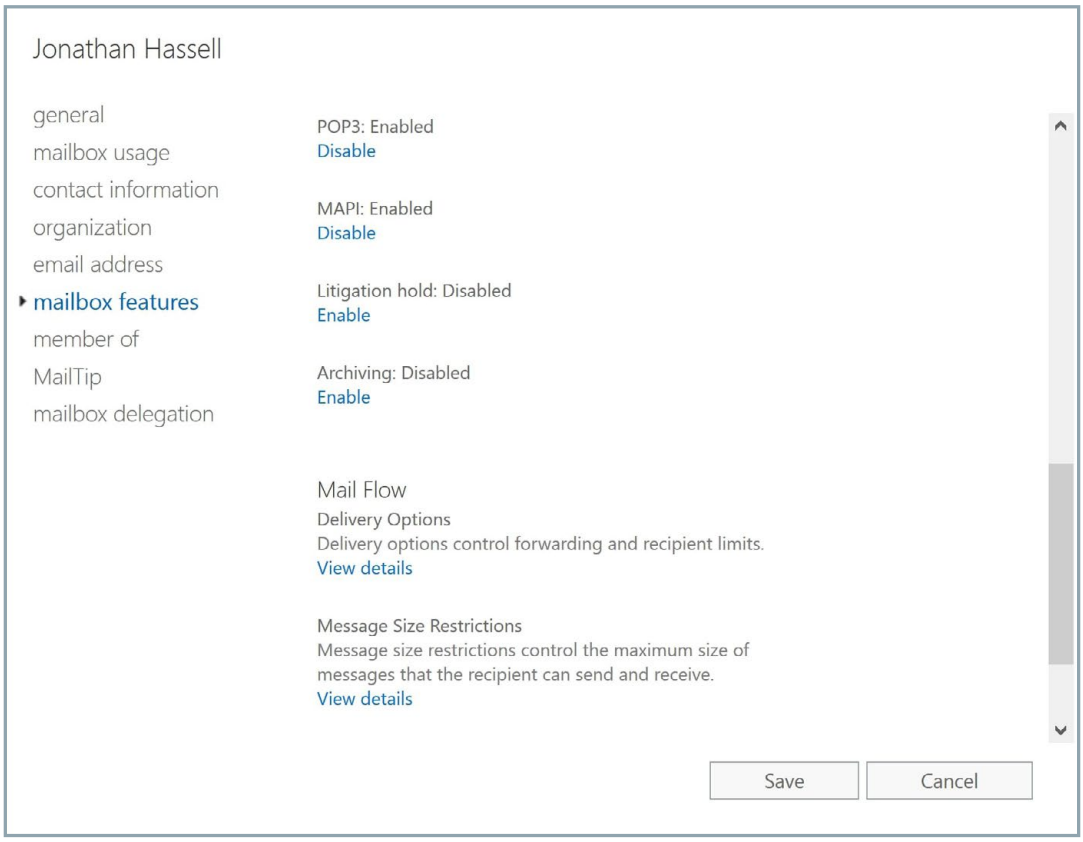
How to set a litigation hold on all mailboxes

```
Get-Mailbox -ResultSize Unlimited -Filter
{RecipientTypeDetails -eq "UserMailbox"} | Set-Mailbox
-LitigationHoldEnabled $true -LitigationHoldDuration 365
```

Alternatively, you can use the web interface, but it's obviously going to take a lot more time to enable a litigation hold on multiple mailboxes than it takes to issue one PowerShell command. But for one or two mailboxes, it is very simple:

1. Navigate to the Exchange admin center at https://outlook.office365.com/ecp. From the dashboard, select ***recipients*** and then double-click the mailbox you want to put on litigation hold. The following pop-up will appear:

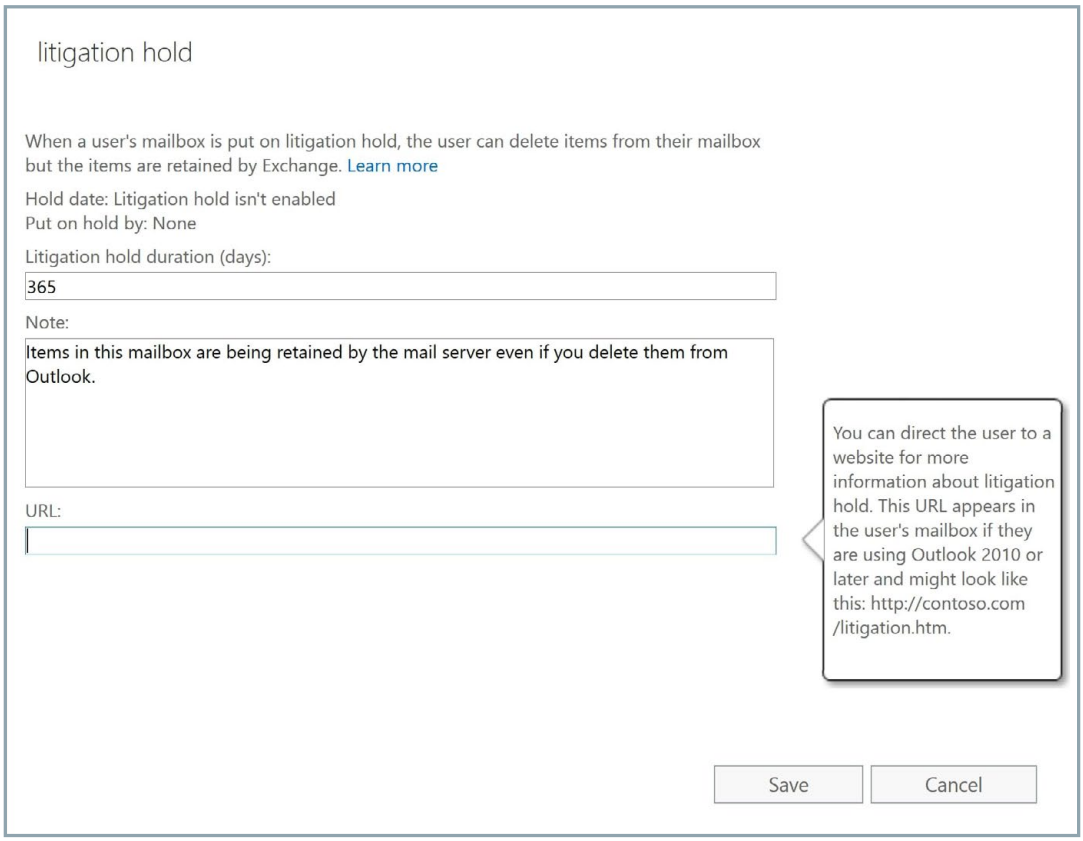
Figure 10.1
Putting a litigation hold on a mailbox



2. Click ***mailbox features*** on the left, and then scroll down to where it says *"Litigation hold: Disabled."*

3. Click the ***Enable*** hyperlink. The following screen will appear:

Figure 10.2
Enabling litigation hold on a mailbox through the Exchange admin center



4. In the first field, enter the number of days the litigation hold is to remain effective. In the Note section, you can enter text that will be displayed to the end user in a small display ribbon in the Microsoft Outlook client — it's a good way to explain to the user what's happening and let them know that deleting an item does not actually remove it. You can also enter a URL to an intranet or internet site that describes the hold, the reason behind it, details about the legal case or whatever your communications team might want to say.

5. Click ***Save*** and then ***Save*** again, and the litigation hold will take effect.

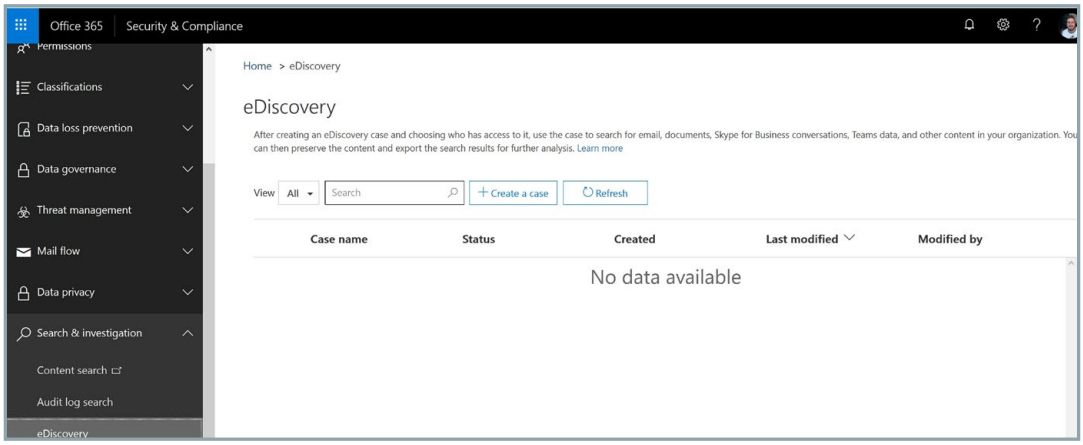
To disable the hold, follow steps 1 and 2, but in step 3, instead of clicking Enable, click ***Disable***. Then click ***Save***.

Performing eDiscovery

Sometimes, administrators will be asked to find all materials that deal with a certain keyword or keywords across your Exchange Online mailboxes, Office 365 groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, and Skype for Business conversations. To perform such a search, take the following steps:

1. In the Security and Compliance Center, from the left menu, choose ***Search & Investigation***, and then choose ***eDiscovery*** in the sub-menu. You'll be presented with the following screen:

Figure 10.3
The eDiscovery portal in the Security & Compliance Center



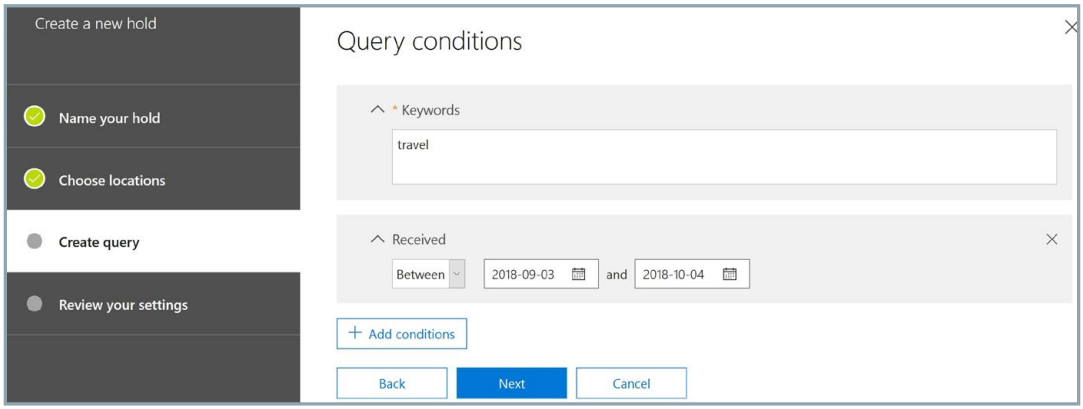
1. Click **+ *Create a case*** to create a new eDiscovery case. This is how you manage the holds, searches, and exports for each term; you separate them into cases so that you can easily turn things on and off, close cases that are complete, and track what is happening with each search term. Give your case a friendly name and description, and then click ***Save***.

2. Your case name will then appear in the list; click ***Open*** beside the case name to get started configuring discovery actions.

In the eDiscovery center, cases are split into three actions:

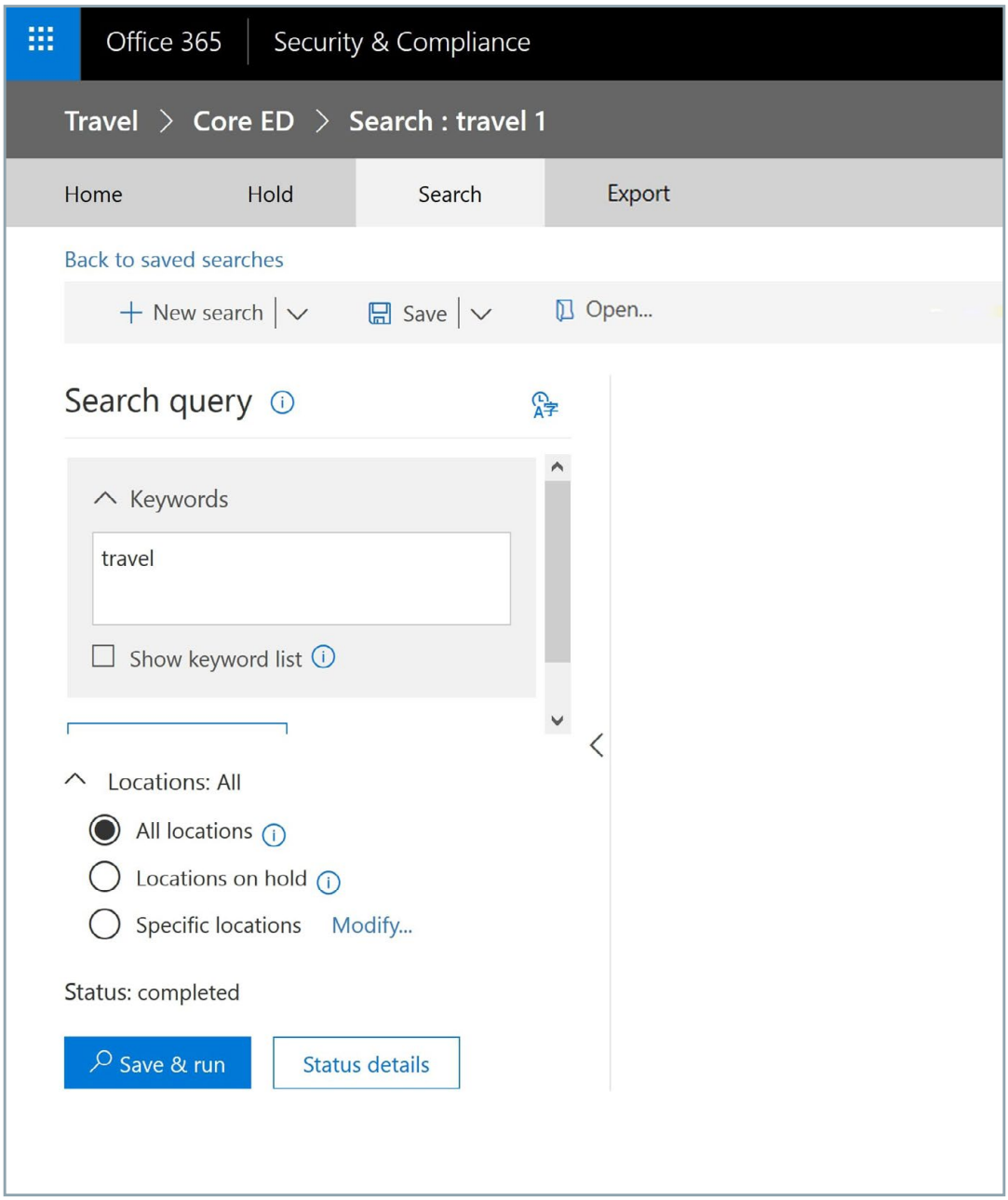
Hold. To have a litigation hold automatically placed on all mailboxes, SharePoint sites and public folders with content that matches certain keywords and conditions, click ***Create*** and follow the wizard; it is fairly self-explanatory. The key screen on the wizard is the one where you specify the query conditions. The figure below illustrates how to specify a keyword and a date filter to limit the scope of the search and resulting holds.

Figure 10.4
Specifying query conditions



Search. You can save and run searches for keywords and other content, and you can configure search to search only through held locations, all locations or some custom configuration. Since you can save these searches, you can start one, step away and come back after it is complete. This is a good option for larger tenants.

Figure 10.5
Searching



Export. The export area allows you to export the results of a search to a PST file, which you can then download and open on your own local computer or provide to counsel. You can choose to export to a single PST file or to one PST file per mailbox, and the output will be encrypted using a key that you choose. The wizard will walk you through the steps required to export data.

Assigning eDiscovery Permissions

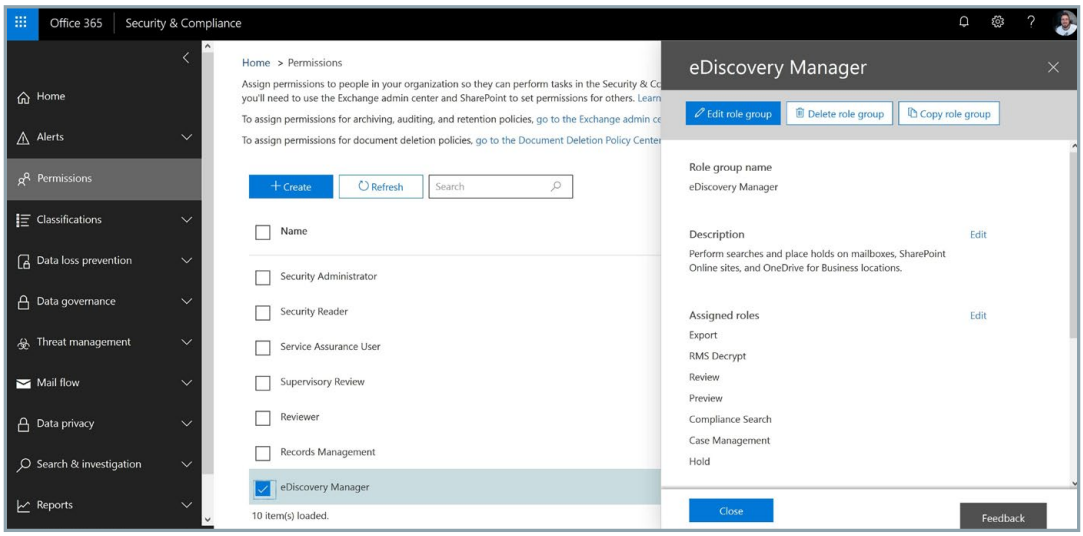
Being able to globally search on whatever keyword you specify across all of the mailboxes in your tenant is a sensitive privilege that requires discretion and respect. Therefore, you need to assign a designated eDiscovery manager who will have permissions to preview search results, export results and manage all aspects of the eDiscovery process. Choose this person wisely; they will have full access to every piece of data stored in your tenant, regardless of other permissions that are set.

To designate an eDiscovery manager, take the following steps:

1. In the administrator portal, go to Security & Compliance, and then click the only option in the left pane.

2. Scroll down to the eDiscovery Manager role and click the check box, and the pop-up window shown in Figure 10-6 will appear. Specify a user for the eDiscovery Manager role and a user for the eDiscovery Administrator role — the latter needs to have administrative privileges.

Figure 10.6
Designating an eDiscovery manager



XI. Troubleshooting Office 365 Issues

Issues with Office 365 can arise from problems with your local computers and connection, or problems with the Office 365 service itself. Microsoft offers tools to help you troubleshoot both.

Using Microsoft Support and Recovery Analyzer for Office 365

The Microsoft Support and Recovery Analyzer can run diagnostic tests to identif and, in some cases, automatically resolve issues with local application configurations. To use the Support and Recovery Analyzer, download it from https://diagnostics.outlook.com/#/. It will go through an installation process, prompt you to accept a license agreement, and then present you with the main screen below:

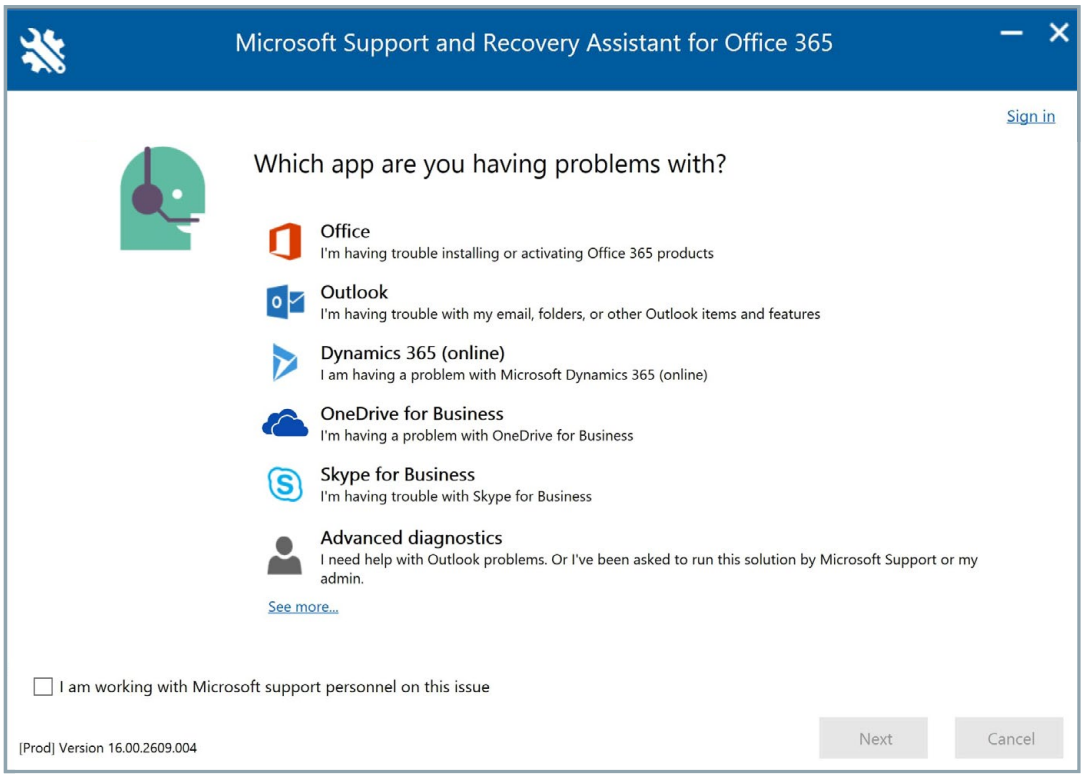


Figure 11.1
Microsoft Support and Recovery Assistant for Office 365

Understanding Bandwidth Requirements and Issues

One of the major pain points that some Office 365 users suffer from is a lack of bandwidth — more specifically, insufficient upstream bandwidth from the client site to the nearest Microsoft datacenter. Enterprises with fast, dedicated fiber connections can have a vastly different experience than a small office running over a 5 Mbps DSL circuit over copper, for several reasons:

Regular use of Outlook eats up a lot of bandwidth. Outlook is a very chatty program, and large attachments are still a preferred way of sharing documents and other files. Just two or three large attachments can saturate a 10 Mbps connection, which is a typical upload rate on business broadband connections these days.

Real-time audio and video conference demands a high-quality, low-latency connection. Skype for Business or Teams conferences both depend on enough bandwidth to handle an uninterrupted stream of video traffic and a connection with low latency. (Bandwidth and latency are different but related: Bandwidth is like how many lanes there are on a highway, while latency is how long it takes a car to get from point A to point B.) If your connection doesn't satisfy either of these demands, then your users' video and audio chats will be full of distortion and stutter.

Your initial migration of data to the service requires a lot of bandwidth. This is a one-time thing. When you sign up for Office 365, you will almost certainly want to bring your existing mail and calendar data into Exchange Online, or at least some subset of it. If you have 50 users and all of them have 4GB of mail, which would not be an unreasonable assumption these days, then you need to upload 200GB of mail. At 10 Mbps, you'll need nearly 49 hours of sustained upload. In reality, it'll take much longer due to connection overhead and the fact that, unless you manage the process well, all of your clients will attempt to upload all of their data at the same time, causing throttling.

Microsoft offers some calculators that will help you understand what type of connection you need:

- For Exchange, you can use the Exchange Client Network Bandwidth Calculator, available at https://gallery.technet.microsoft.com/Exchange-Client-Network-8af1bf00. This is an Excel spreadsheet that can help predict performance and suggest the bandwidth you need based on your organization's usage profile. You'll want to know statistics about your current usage, like your working hours, current bandwidth, number of mobile devices, number of calendar meetings, average mailbox size and size of your offline address book (OAB).

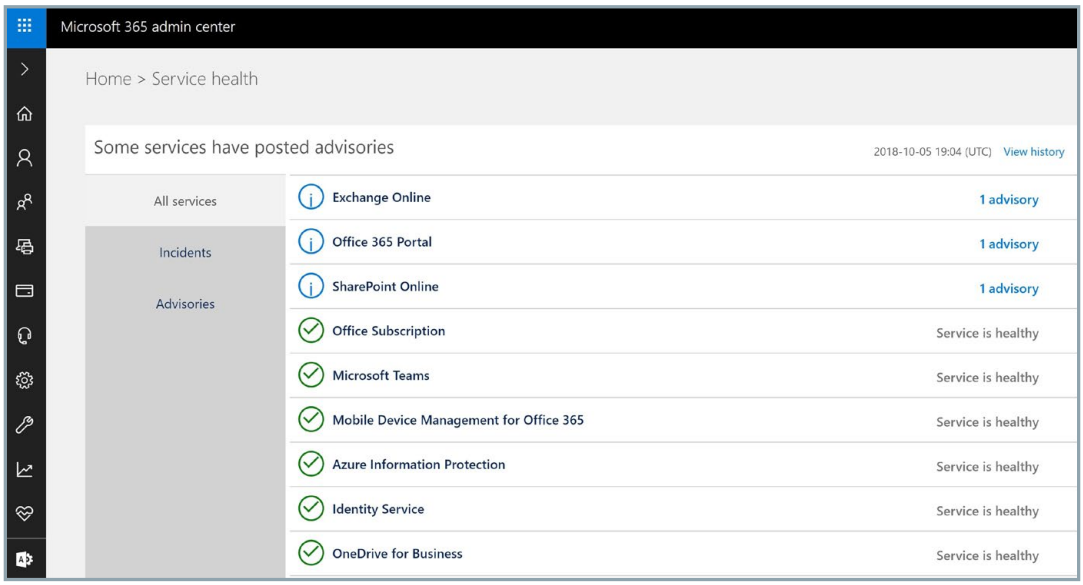
- For Microsoft teams and Skype for Business, you can use the Network Planner, available at https://myadvisor.fasttrack.microsoft.com/CloudVoice/NetworkPlanner, to understand the different sites and usage personas in your organization and receive recommendations about how your network will perform under load.

As a rule of thumb, if your entire infrastructure is hosted in Office 365, all but the smallest offices will want a connection with at least 50 Mbps downstream bandwidth and 10 Mbps upstream bandwidth.

Using the Service Health Dashboard

If you suspect a problem with any of the components of the Office 365 service itself, the first place you should look is the Service Health Dashboard, available at https://portal.office.com/adminportal/home#/servicehealth.

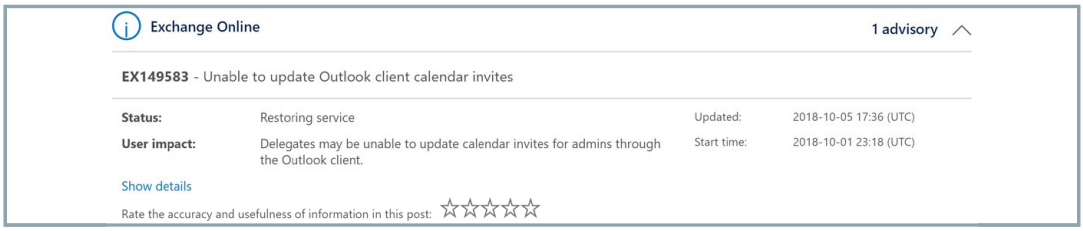
Figure 11.2
The Service Health Dashboard



If there are known issues with the servers that host your tenant (remember, Office 365 is a global service with millions of servers, so some users might see an issue while others do not), you should see a notice in the dashboard. This doesn't always happen, especially right as an outage begins or if an outage is particularly severe and lots of Microsoft hands are assigned to fix it, so it's not a completely accurate system, but it is a good place to start if you are experiencing service interruptions.

If you do see a relevant notice, you can click it to get more information. Here is an example:

Figure 11.3
Checking a known issue posted on the Service Health Dashboard

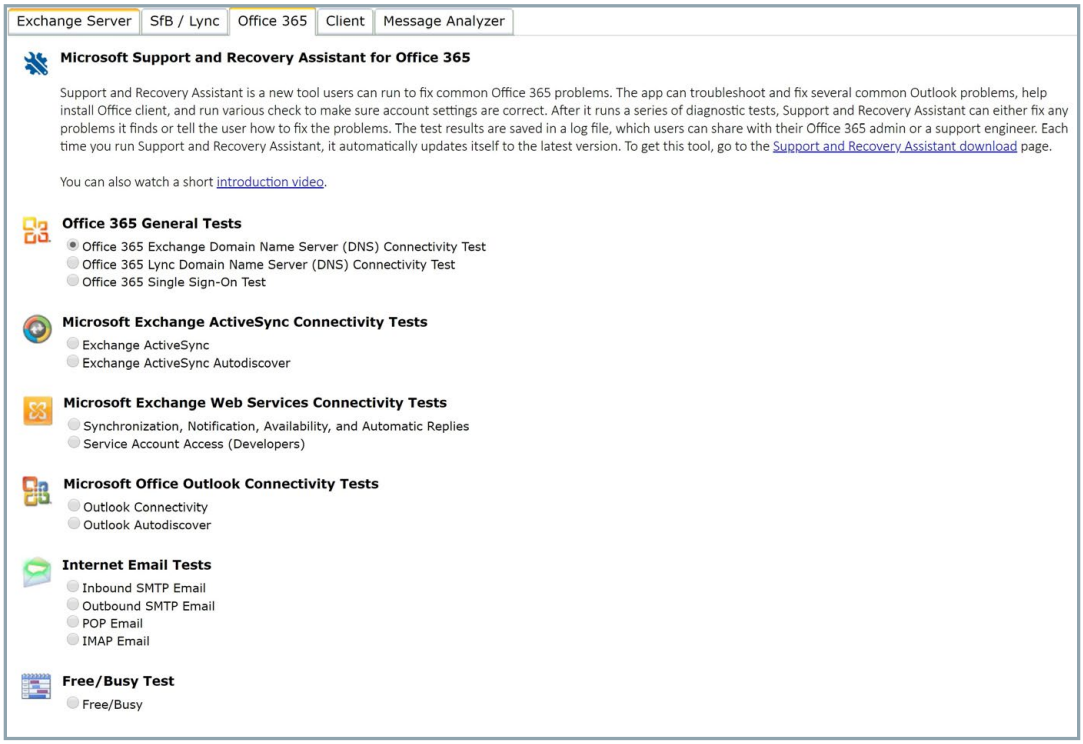


Using the Microsoft Remote Connectivity Analyzer

The Microsoft Remote Connectivity analyzer, available at https://testconnectivity.microsoft.com/, is a website hosted independently of the Microsoft datacenter network. It can attempt to connect to various Microsoft services (or your on-premises systems) in a variety of scenarios; a failure of any of these tests is a very strong indicator that an issue resides on the Microsoft side of the equation and not locally.

The Office 365 tab of the analyzer has a variety of tests, including tests to make sure Exchange and Skype for Business Online are responding. You can also test inbound and outbound email and, if you are operating in a hybrid environment, you can test whether calendar free/busy results are available on the Office 365 side. If you are in the initial stages of Office 365 adoption, you may also find it useful to try the Autodiscover tests to make sure your DNS records are properly entered and hosted so that late-model Outlook clients can automatically find their own configurations.

Figure 11.4
The Remote Connectivity Analyzer



XII. Using Office 365 Groups

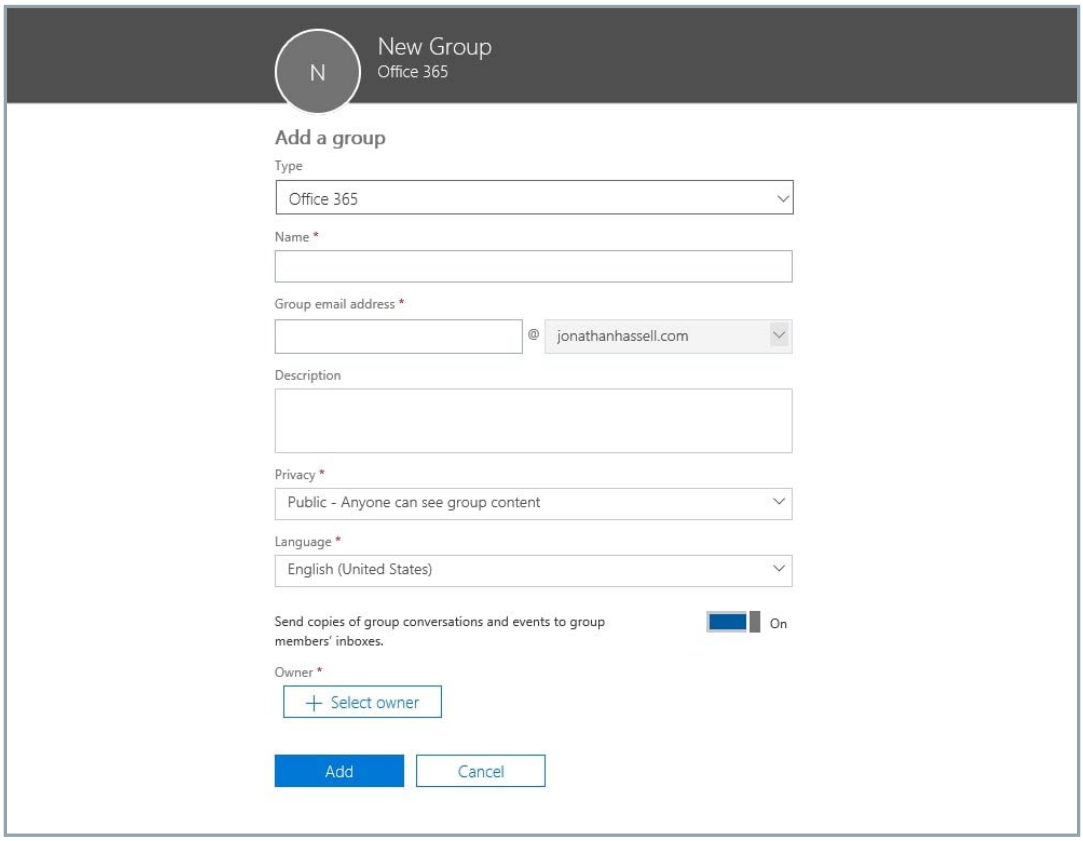
Office 365 groups enable users to access information in a variety of places, including a SharePoint or OneDrive for Business document library, a OneNote file, a shared mailbox or calendar on Exchange, Lync or Skype for Business meetings, and data in the Dynamics CRM database. Office 365 groups are objects in Azure Active Directory, so they are not available in your on-premises deployment. This group identity includes the users themselves, URLs for resources, who owns what groups, and what each group's membership list looks like.

Creating Groups

Both administrators and end users can create groups.

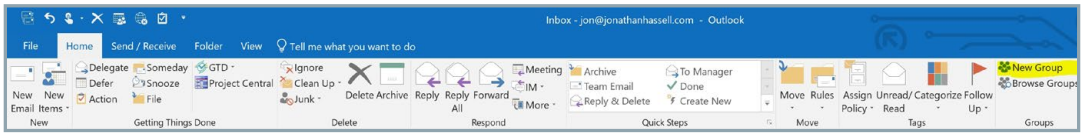
Office 365 administrators can log into the portal at https://portal.office.com, click the ***Admin*** link, hover over the people icon on the side, and then click ***Add Group***.

Figure 12.1
Creating a group from the Office 365 portal



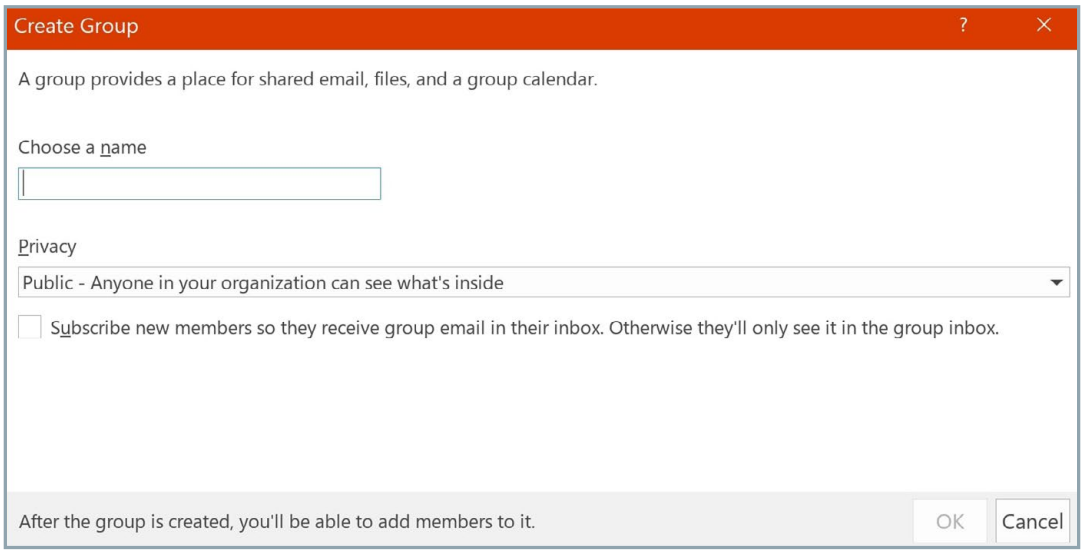
Users can create new groups directly from Outlook from the ribbon, as long as they are using Outlook from the Office 365 ProPlus package:

Figure 12.2
Adding a new group from Outlook



That will bring up a screen much like the portal's screen, where they can name the group and choose the privacy settings.

Figure 12.3
Creating a group from Outlook



Keep in mind that users can interact with Office 365 groups only from a web browser, not from an Office desktop client. The upcoming Office 2016 client will include support for groups, but that will require an upgrade of all of your clients.

Managing Office 365 Groups

Groups are intended to be largely self-service: Users can create their own groups and administer their membership using tools built into the web user interface or through the full applications in the Office 2016 suite. Users can also browse the list of groups and sign themselves up to be members. Therefore, groups tend to proliferate quickly, which leads to challenges for administrators, including the following:

- Who manages the lifecycle of all of these groups, some of which might have been created for week-long tasks and some of which are for long-term projects? Who decides what content is still live and what needs to be archived?

- What happens when the next iteration or version happens? How do accounts and resources move around? The process is less than clear, particularly for users that have a hybrid deployment of Exchange, SharePoint or both.

- What if the topic being discussed in a group is sensitive? This group should probably not be public, nor should just anyone be able to add themselves to the group.

Adding External Users to Groups

One of the big benefits of Office 365 groups is the ability to let users outside of the company collaborate on items in the group. Those capability centers around the concept of a guest user in Azure Active Directory, which is an account associated with an email address from outside the tenant.

Only an owner of a group owner can add a guest to the group. Open the group using Outlook Web Access on Office 365. From the three-dotted menu on the right, select ***Members*** and then ***Guests***. Click ***Add Members*** and then enter the guest's email address.

Behind the scenes, Office 365 checks whether a guest user object already exists for that email address; if it does not, Office 365 automatically creates one on the fly. Then it grants the guest user appropriate permissions to the group and sends an email to the guest user with a link to the object to be shared and information about how the guest user can remove himself or herself from the group.

If the guest user has a Microsoft account that matches the email address the Office 365 users adds, then the guest will just authenticate with that. If not, then the user will be pushed over to invitations.microsoft.com to begin the process of creating a special ad-hoc account in that Office 365 tenant (which is not a universal Microsoft account).

What can a guest user do in an Office 365 group? Here are some common scenarios:

- Join in a conversation in the group mailbox. This is through email only and not any sort of interface on the Office 365 system; the messages are emailed to the guest's email address. Therefore, they can also search the group conversations they have been a part of within their own mailbox.

- Send meeting requests to the shared calendar for the group,

- Interact with a single document in a SharePoint Online library that user has invited them to edit.

- Access the group's document libraries now and search through those documents in SharePoint Online using the Files view in Office 365.

- See attachments sent through the OneDrive for Business integration with Outlook and shared OneNote notebooks.

Mitigating the Risks of External Users in Office 365 Groups

Giving external users access to corporate access raises two key concerns:

Risk of data loss — How do you make sure that users keep private content in the site and don't forward it or download it?

Risk of continued access — How do you ensure that access rights of external users are consistently revoked when they are no longer needed?

Microsoft has built in some protections against these threats. For example:

- Guests can interact with Office 365 groups only through the browser (except for the individual email notifications described earlier).
- Guests can't see Global Address List information, such as organizational hierarchy.
- Guests can't view or interact with information saved with Information Rights Management (IRM) protection.
- Guests don't appear in the GAL.
- Guests cannot become owners of Office 365 groups.
- MailTips warn users of Outlook on the Web and the Outlook desktop client when they are mailing items to a group that includes guest users to help prevent the leak of confidential material.

To further mitigate these risks, you should educate your users about security best practices for Office 365 groups, and require owners to regularly attest to the continued usefulness and membership of their Office 365 groups.

netwrix

Useful Reference

Simplify management and streamline monitoring of your Office 365 environment with the following resources:

Manage

Blog post | Ten Most Useful Office 365 PowerShell Commands

SysAdmin Magazine | Office 365: A 360° Perspective

Blog post | IT Trick: View Azure AD Sign-in Activity

Blog post | Office 365: Configuring User Passwords to Never Expire

Blog post | Using AD to Add an Alias to an Office 365 Email Account

Monitor

Blog post | Best Tools for Management and Monitoring of Office 365

How-to | How to Detect Deleted User Accounts in Azure Active Directory

How-to | How to Stay on Top of Permissions Changes to Public Folders in Exchange Online

How-to | How to Detect Who Modified Mailbox Permissions in Exchange Online

How-to | How to Detect Who Was Accessing Shared Mailbox in Office 365

Webinar | Tracking Changes in Hybrid Identity Environments with Both AD and Azure AD

Webinar | Top 5 Critical Exchange Online Events You Need Visibility Into

Blog post | Why Isn't Native Office 365 and Azure AD Auditing Good Enough?

Quick reference guide | Azure AD Auditing

Quick reference guide | Exchange Online Auditing

Quick reference guide | Exchange Online Mailbox Auditing

Secure

SysAdmin Magazine | Danger in the Cloud

Research | 2018 Cloud Security Report

Webinar | A Hacker Explains: How Attackers Exploit Office 365 Vulnerabilities

Blog post | Security Tip: Enable Azure AD Self-Service Password Reset

Best practices | Password Policy

Netwrix Freeware Tools

Boost Your Productivity by Automating Auditing of Office 365 and Azure AD

Free Community Edition

Netwrix Auditor for Office 365

Reports on **access to data** in SharePoint Online and OneDrive for Business; **non-owner mailbox access** attempts in Exchange Online; and **configuration, security** and **file changes** in all these applications.

Free Download

Free Community Edition

Netwrix Auditor for Azure AD

Delivers daily reports on all **logon attempts** and **changes** to Azure AD during the past 24 hours right to your inbox.

Free Download

netwrix

About the Author

Jonathan Hassell is an expert in Microsoft products, including Azure AD and Office 365. He has written several books on Windows Server and related products, regularly contributes to leading industry publications, and has spoken worldwide on topics ranging from networking and security to Windows administration.

About Netwrix

Netwrix Corporation is a software company focused exclusively on providing IT security and operations teams with pervasive visibility into user behavior, system configurations and data sensitivity across hybrid IT infrastructures to protect data regardless of its location. Over 10,000 organizations worldwide rely on Netwrix to detect and proactively mitigate data security threats, pass compliance audits with less effort and expense, and increase the productivity of their IT teams.

Founded in 2006, Netwrix has earned more than 140 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information about Netwrix, visit https://www.netwrix.com/.

Contact Us

Corporate Headquarters

300 Spectrum Center

Drive Suite 200

Irvine, CA 92618

Phones

USA: 1-949-407-5125

Toll-free: 888-638-9749

EMEA: +44 (0) 203 588 3023

netwrix.com/social