

Instructions

- These notes are valid as of **April 2016**. Office 365 products are updated frequently so please make sure to verify this content for validity.
- This information should contain 60-70% of the material quizzed in the exam. But should only be used as a quick review aid.
For example,
 - You should know how to apply each PowerShell command and its output
 - For each screenshot you should know how to navigate there and what each option in the screens achieve.

Study hard and good luck!!

90% of the information contained in this document has been extracted from internet posts. All copyright belongs to the original creators

Office 365

Features Office 365 Services	E1	E3	E5
Business Class Email and Calendars Exchange Online	50 GB	Unlimited	Unlimited
Social, Video, Sites Yammer, O365 Video, SharePoint Online	●	●	●
IM, Online Meetings, Meeting Broadcast Skype for Business	New ●	New ●	●
File Storage, Sharing, Information Discovery OneDrive for Business, Delve	●	●	●
Office Online	●	●	●
Office Client Apps Office 365 ProPlus		●	●
Archiving, Rights Management, Data Loss Prevention, Encryption		New ●	●
Predictive eDiscovery, Secure Attachments and URLs, Access Control			●
End User and Organizational Analytics Power BI Pro, Delve Org Analytics			●
Cloud PBX Skype for Business			●
PSTN Conferencing Skype for Business			●
PSTN Calling Skype for Business			Add-on

Office 365 Plans

		Business			Enterprise		
		Business	Business Essentials	Business Premium	ProPlus	E1	E3
Core Details	Seat Cap	300 (for each plan)			Unlimited		
	24/7 phone support from Microsoft	Critical issues			All issues		
Office	Word, PowerPoint, Excel, Outlook, OneNote, Publisher	●		●	● ²		● ²
	iPad, Windows RT & smartphone apps	●		●	●		●
	Office Online	●	●	●	●	●	●
	Access				●		●
Standard services	1TB cloud storage (OneDrive for Business)	●	●	●	●	●	●
	Email, calendar (Exchange)		●	●		●	●
	Online meetings, IM (Lync)		●	●		●	●
	Team sites, internal portals (SharePoint)		●	●		●	●
	Enterprise social (Yammer)		●	●		●	●
	Content discovery and search (Delve) ³		●	●		●	●
Advanced services	Active Directory integration	●	●	●	●	●	●
	Licensed for hybrid deployment				●	●	●
	Support for shared computer activation				●		●
	Video content management					●	●
	Compliance – Archiving, eDiscovery, mailbox hold						●
	Information protection – message encryption, RMS, DLP						●

Document collaboration and co-authoring

Semiformal co-authoring : Multiple authors edit simultaneously anywhere in the document. Examples include: recurring minutes, brainstorming sessions, and reference material for OneNote; and team-developed financial models, budgets, and asset tracking lists for Excel.

Formal co-authoring: Multiple authors edit simultaneously in a controlled way by saving content when ready to be revealed. Examples include: business plans, newsletters, and legal briefs for Word; and marketing and conference presentations for PowerPoint.

Comment and review: A primary author solicits edits and comments (which can be threaded discussions) by routing the document in a workflow, but controls final document publishing. Examples include online Help, white papers, and specifications.

Document sets: Authors start workflows on an entire document set or individual items within the Document Set to manage common tasks such as review and approval.

Co-authoring and the checking out of documents

Co-authoring is not compatible with the process of checking out and checking in documents in a SharePoint library. Checking out a document means you want to exclusively write to it, and then eventually check it back in so others can see the changes or do further work on the document. Therefore, when you check out a file, other users cannot co-author the document with you. By default SharePoint libraries do not require checking out files, and should not be enabled where co-authoring will be used. You should also not explicitly check out a document if you want to co-author the document.

Co-authoring documents and versioning

Because several co-authors might keep a document open for a long period of time, versioning for co-authored documents is performed at specific time intervals and not necessarily when the document is saved. By default, versioning is not enabled in a SharePoint library.

When you co-author Word and PowerPoint documents, it's a good idea to use versioning, both major and minor, so that users can retrieve changes made by other users when necessary. Furthermore, the versioning period determines how often SharePoint creates a new version of a document that is being co-authored. The default value of 30 minutes probably works for most environments, but this value can be adjusted by an administrator as necessary.

For libraries containing OneNote notebooks, it's a good idea to only do major versioning, because minor versions might cause synchronization errors that could prevent changes from being saved.

Co-authoring documents in a mixed Office version environment

Although you can upload files via Word and PowerPoint 2007 or earlier to a SharePoint library, you cannot co-author these documents with those legacy applications. Furthermore, when a user opens a Word or PowerPoint OOXML document with Word or PowerPoint 2007, SharePoint creates a lock on the document and prevents other users of Office from using co-authoring to edit that document. To take best advantage of co-authoring in Word or PowerPoint, it is recommended that all users work with at least Microsoft Office 2010 or 2012. Excel workbooks can only be coauthored via at least the Excel 2010 or Excel 2012 Web App. Using the Excel 2012 or earlier client application will always create an exclusive lock on the server document which will prevent coauthoring.

ADFS Build	Notes
ADFS 1.0	Released with Windows 2003 R2. Built into OS.
ADFS 1.1	Released with Windows 2008 and 2008 R2. Built into OS.
ADFS 2.0	Released After Windows 2008 / 2008 R2. Separate download
ADFS 2.1	Windows 2012
ADFS 3.0	Windows 2012 R2

ADFS:

enabling forms-based authentication on the AD FS federation server farm. To do this, follow these steps:

Step 1: Edit the web.config file on each server in the AD FS federation server farm

1. In Windows Explorer, locate the C:\inetpub\adfs\ls\ folder, and then make a backup copy of the web.config file.
2. Click **Start**, click **All Programs**, click **Accessories**, right-click **Notepad**, and then click **Run as administrator**.
3. On the **File** menu, click **Open**. In the **File Name** box, type C:\inetpub\adfs\ls\web.config, and then click **Open**.
4. In the web.config file, follow these steps:
 1. Locate the line that contains **<authentication mode=**, and then change it to **<authentication mode="Forms"/>**.
 2. Locate the section that begins with **<localAuthenticationTypes>**, and then change the section so that the **<add name="Forms"** entry is listed first, as follows:

```
<localAuthenticationTypes>
<add name="Forms" page="FormsSignIn.aspx" />
<add name="Integrated" page="auth/integrated/" />
<add name="TlsClient" page="auth/sslclient/" />
<add name="Basic" page="auth/basic/" />
```
5. On the **File** menu, click **Save**.
6. At an elevated command prompt, restart IIS by using the iisreset command.

View Office 365 admin permissions by role

This table shows the Office 365 admin roles and their associated permissions.

Permission	Billing admin	Global admin	Password admin	Service admin	User management admin	Exchange administrator	SharePoint administrator	Skype for Business administrator
View organization and user information	Yes	Yes	Yes	Yes	Yes	Yes	Yes (but can't edit)	Yes (but can't edit)
Manage support tickets	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reset user passwords	No	Yes	Yes; with limitations. This admin can only reset passwords for non-admins.	No	Yes; with limitations. This admin can't reset passwords for billing, global, and service admins.	No	No	No
Perform billing and purchasing operations	Yes	Yes	No	No	No	No	No	No
View users and roles	No	Yes	No	No	Yes	Yes	Yes	Yes
Create, edit, and delete users and groups	No	Yes	No	No	Yes; with limitations. This admin can't delete a global admin or create other admins.	No	No	No

Manage user licenses	No	Yes	No	No	Yes; with limitations. This admin can't delete a global admin or create other admins.	No	No	No
View user licenses	No	Yes	No	Yes	Yes; with limitations. This admin can't delete a global admin or create other admins.	Yes	Yes	Yes
Manage domains	No	Yes	No	No	No	No	No	No
Manage organization information	No	Yes	No	No	No	No	No	No
View service health and message center posts	No	Yes	No	No	No	Yes	Yes	Yes
Delegate administrative roles to others	No	Yes	No	No	No	No	No	No
Use directory synchronization	No	Yes	No	No	No	No	No	No
Manage reporting	No	Yes	No	No	No	Yes	Yes	Yes
Manage mobile devices	No	Yes	No	No	No	No	No	No

Your default directory service quota is calculated according to the following guidelines:

- If you don't have any verified domains

The current directory service quota in Azure AD is 50,000 objects.

- If your organization was created before October 5, 2011, your default directory service quota is 10,000 objects.
- If your organization was created after October 5, 2011 and before May 2012, your default directory service quota is 20,000 objects.
- If your organization was created after May 2012, your default directory service quota is 50,000 objects.

- If you have at least one verified domain

The default directory service quota in Azure AD is 300,000 objects.

Office 365 system requirements

Operating system

PC: Windows 10, Windows 8, Windows 7 Service Pack 1, Windows 10 Server, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2

Mac: Mac OS X 10.10

For the best experience, use the latest version of any operating system.

Browser

The current or immediately previous version of Internet Explorer; the current version of Microsoft Edge, Safari, Chrome, or Firefox

Your Office clients are compatible with Office 365. Office 365 works with any version of Office in mainstream support:

Office 2016, 2013

Outlook 2010 with Service Pack 1 or later

Outlook 2007 with Service Pack 3

Office 365 office suit requirements:

Windows 7 and later

Purpose	Source Credentials	Destination	Destination Port
Required: Authentication and identity	See Office 365 authentication and identity		
Required: This url is needed to renew the product key approximately every 30 days	Office client only Local system	activation.sls.microsoft.com	TCP 443
Required: This URL is the Office Licensing Service, which is used during activation and subscription maintenance	Office client only Local system	ols.officeapps.live.com	TCP 443
Required: Client SMTP Relay	Client Computer Logged on user	smtp.office365.com	TCP 587
Optional: Exchange Online IMAP4 migration	IMAP4 Service N/A	outlook.office365.com *.outlook.office.com	TCP 143/993
Optional: Exchange Online POP3 migration	POP3 Service N/A	outlook.office365.com *.outlook.office.com	TCP 995

Office365 Download settings:

Office 365 admin center <<

DASHBOARD | USER SOFTWARE

Search users, admin tasks and...

DOMAINS

PUBLIC WEBSITE

BILLING

EXTERNAL SHARING

MOBILE MANAGEMENT

SERVICE SETTINGS

Mail

Sites

Skype for Business

Updates

User purchasing

Sway

User software

Passwords

Community

Rights Management

Mobile

Cortana

Office Online

REPORTS

SERVICE HEALTH

SUPPORT

PURCHASE SERVICES

MESSAGE CENTER

TOOLS

ADMIN

Exchange

Skype for Business

Manage user software through Office 365

Choose which software your users can download and install directly from Office 365.
[How do I manage user software?](#)

Software for PC

Which versions of Office desktop apps do you want to make available for download?

☒ **2016 version**

- ☒ Office (includes Skype for Business)
- ☒ Skype for Business (Standalone)

Additional Office desktop apps that need to be downloaded separately

- ☒ SharePoint Designer 2013
- ☒ InfoPath 2013

How often do you want users to get updates for Office 2016 apps?

☐ Every month (Current channel)

☒ Every 4 months (Deferred channel)

☒ **2013 version**

- ☒ Office (includes Skype for Business)
- ☒ Skype for Business (Standalone)
- ☒ SharePoint Designer

Software for Mac

Which versions of Office for Mac do you want to make available for download?

☒ **2016 version**

- ☒ Office

Additional Office desktop apps that need to be downloaded separately

- ☒ Lync for Mac 2011 (OS X 10.6 or higher)

☒ **2011 version**

- ☒ Office
- ☒ Lync for Mac 2011 (OS X 10.6 or higher)

[Cancel](#)

Your changes to the user software settings will take effect on February 23, 2016.

Office 365 portal page

The screenshot shows the Office 365 portal page. At the top right, there are buttons for "Trial version" and "Purchase". Below this, the main heading is "Install Office 2016 on your PC". To the right of this heading, there are two checked boxes: "Make Bing your search engine" and "Make MSN your browser homepage", with a note that they apply to Internet Explorer, Firefox, Chrome, and Safari. Below these are icons for Word, Excel, PowerPoint, Outlook, OneNote, and Skype for Business. A prominent red "Install now" button is visible. Below the icons, there is a link for "Other installs" and a link for "Troubleshoot installation".

Got a Mac? Sign in to Office 365 on your Mac to install.

How do I get Office 2013?
Smartphone or tablet? Get Office on your devices
Learn how to set up email and Office 365 apps on your device

Collaborate with Office Online

Below the heading, there is a grid of icons for various Office Online services: Mail, Calendar, People, Yammer, Newsfeed, OneDrive, Sites, Tasks, Delve, Video, Word Online, Excel Online, PowerPoint Online, OneNote Online, Sway, and Admin.

The **Microsoft Office Configuration Analyzer Tool (OffCAT)** 2.1 provides a quick and easy way to analyze Microsoft Office programs for known configurations that cause problems

The screenshot shows the Microsoft Office Configuration Analyzer Tool (OffCAT) 2.1 interface. The top menu bar includes "NEW SCAN", "REPORT", "MANAGE SCANS", "OPTIONS", "ADVANCED TOOLS", and "HELP/FEEDBACK". The main area is divided into two panels. The left panel, titled "I want to scan", shows icons for Excel, Outlook, PowerPoint, Word, Access, InfoPath, OneDrive for Business, and OneNote. A "Scan" button is at the bottom. The right panel, titled "OffCAT_Results.outl", shows the results of a scan. It includes a summary of issues: Critical: 1, Warning: 15, Informational: >99. Below this, there is a list of issues, including "Missing feature", "Publish to WebDAV Server", "The OneNote icon is missing from the Outlook ribbon", "Modern Authentication for Office", "Office 365", "Office Update", "Offline Address Book (OAB)", "OneNote-Outlook integration", "Outlook profile", "Search", and "Slowness".

Command line Options:

<p>-dat <fullfilepath> Write the output data to <fullfilepath>. The default is Offcat_Results.<label>.<timestamp>.offx saved to the 'Default location for scans' directory that is configured in OffCAT.</p> <p>-l <label> Specify an optional <label> for the output.</p> <p>-r <option> Specify the type of scan for Outlook. The default is "" (full scan), for an offline scan use "Offline Scan".</p>	<p>-cfg <application> Specify the Office application to scan.</p> <p>-gs MAJORVERSION <version> INSTALLTYPE <installation type> Specify the version of the Office application to scan (12 for 2007, 14 for 2010, 15 for 2013, etc.) and the installation type (MSI or ClickToRun).</p> <p>-NoRTS Do not start the OffCAT_RTS.exe background process. This is recommended for computers where you are using OffCATcmd.exe but you did not actually run OffCAT.msi to install OffCAT.</p> <p>-? Display this information.</p>
---	---

Example: OffCATcmd.exe -dat C:\data\output.offx -l "New Offline Scan" -r "offline scan" -cfg outlook -gs MAJORVERSION 15 INSTALLTYPE MSI

Example: OffCATcmd.exe -cfg word -gs MAJORVERSION 14 INSTALLTYPE MSI -NoRTS

Example: OffCATcmd.exe -dat "\\Server\Share\user files\output.offx" -l "New Excel 2013 C2R Scan" -cfg excel -gs MAJORVERSION 15 INSTALLTYPE ClickToRun

Reference for Click-to-Run configuration.xml file

<p>Configuration element Top-level element. This element is required, and all other elements must appear within this element.</p> <p>Syntax <Configuration> {0 or 1 Add element} {0 or 1 Remove element} {0 or 1 Updates element} {0 or 1 Display element} {0 or 1 Logging element} </Configuration></p> <p>Add element Specifies the products and languages to install.</p> <p>Syntax <Add SourcePath=""\\server\share\" Version="15.1.2.3" OfficeClientEdition=32 64 Branch= "Business" > {0 or N Product elements} </Add></p>	<p>Product element Specifies the Click-to-Run product to install.</p> <p>Syntax <Product ID="O365ProPlusRetail" PIDKEY="12345-12345-12345-12345-12345" > {1 or N Language elements} </Product></p> <p>Property element Supports generic properties as described below.</p> <p>Syntax <Property Name=string Value=string /> where:</p> <ul style="list-style-type: none"> Name is a required attribute. It indicates the name of the Property. Value is an optional attribute. The default is an empty string. <table> <tr> <th>Attribute</th><th>Value</th></tr> <tr> <td>AUTOACTIVATE</td><td>1 0</td></tr> <tr> <td>FORCEAPPSHUTDOWN</td><td>TRUE FALSE</td></tr> </table>	Attribute	Value	AUTOACTIVATE	1 0	FORCEAPPSHUTDOWN	TRUE FALSE
Attribute	Value						
AUTOACTIVATE	1 0						
FORCEAPPSHUTDOWN	TRUE FALSE						

Display element

Specifies the level of user interface to display to users.

Syntax

<Display

Level=None | Full

AcceptEULA=TRUE | FALSE

/>

ExcludeApp element

Specifies which Office programs not to install.

Syntax

<ExcludeApp ID= "Access" **/>**

Language element

Specifies the languages to install.

Syntax

<Language ID= "ll-cc" **/>**

Logging element

Specifies the type of logging that Click-to-Run performs.

Syntax

<Logging

Level=Off | Standard

Path=UNC or local path

/>

PACKAGEGUID

12345678-ABCD-1234-ABCD-

1234567890AB

SharedComputerLicensing

1

0

Updates element

Specifies attributes for configuring updates.

Syntax

<Updates

Enabled=TRUE | FALSE

UpdatePath=UNC | local | http path

TargetVersion=X.Y.Z.W

Deadline=MM/DD/YYYY HH:MM

Branch= "Business"

/>

<Configuration>

<Add SourcePath="\\Server\Share" **OfficeClientEdition=**"32" **>**

<Product ID="O365ProPlusRetail">

<Language ID="en-us" **/>**

</Product>

<Product ID="VisioProRetail">

<Language ID="en-us" **/>**

</Product>

</Add>

<Updates Enabled="TRUE" **UpdatePath=**"\\Server\Share" **/>**

<Display Level="None" **AcceptEULA=**"TRUE" **/>**

<Logging Level="Standard" **Path=**"%temp%" **/>**

<Property Name="AUTOACTIVATE" **Value=**"1" **/>**

</Configuration>

Download:

C:\PATH to setup>setup.exe /download "Path to configuration file\configuration.xml"

Install:

C:\<PATH to setup>setup.exe /configure "<Path to configuration file>\configuration.xml"

Overview of Office Telemetry



Telemetry Dashboard

Telemetry Dashboard:

- Shows IT Pros a consolidated view of inventory and telemetry data
- Requires Excel 2013
- Is installed with Office Professional Plus 2013 and Office 365 ProPlus
- Connects to the telemetry database
- Can be viewed by multiple IT Pros



Telemetry Log

Telemetry Log:

- Helps developers and experienced users diagnose compatibility issues on an Office 2013 client
- Requires Excel 2013
- Is installed with Office Professional Plus 2013 and Office 365 ProPlus
- Connects to the local data store on the client

OFFICE TELEMETRY COMPONENTS



Telemetry logging

Telemetry logging:

- Monitors events for (and is built into) Word 2013, Excel 2013, PowerPoint 2013, and Outlook 2013
- Is disabled by default
- Is enabled by using Group Policy, registry settings, or from within Telemetry Log



Telemetry agent

Telemetry agent:

- Monitors document and add-in usage for all Office applications in the 2003, 2007, 2010, and 2013 versions of Office
- Is supported on Windows XP and later versions
- Must be deployed to Office 2003, Office 2007, and Office 2010 clients
- Is built into Office 2013 clients
- Must be enabled using Group Policy or the registry
- Runs as a scheduled task (except on Windows XP)
- Requires domain membership
- Periodically uploads data to a shared folder



Group Policy settings

Group Policy settings:

- Configure the telemetry agent on each client
- Are part of Office15.admx and Office15.adml
- Are located under User Configuration\Administrative Templates\Microsoft Office 2013\Telemetry Dashboard



Shared folder

Shared folder:

- Stores telemetry data that is uploaded by telemetry agents
- Must be on premises (no cloud support)
- Can be located on the same computer as other telemetry components
- Is configured when you install the telemetry processor



Telemetry processor

Telemetry processor:

- Uploads data from the shared folder to the telemetry database
- Runs as a Windows service named "Office Telemetry Processor"
- Runs on Windows Server 2008 and later versions
- Can be run on Windows 7 and Windows 8 in test or small environments
- Can be run on the same computer as other telemetry components
- Can be installed on multiple computers for large deployments
- Requires domain membership (unless a workaround is used)

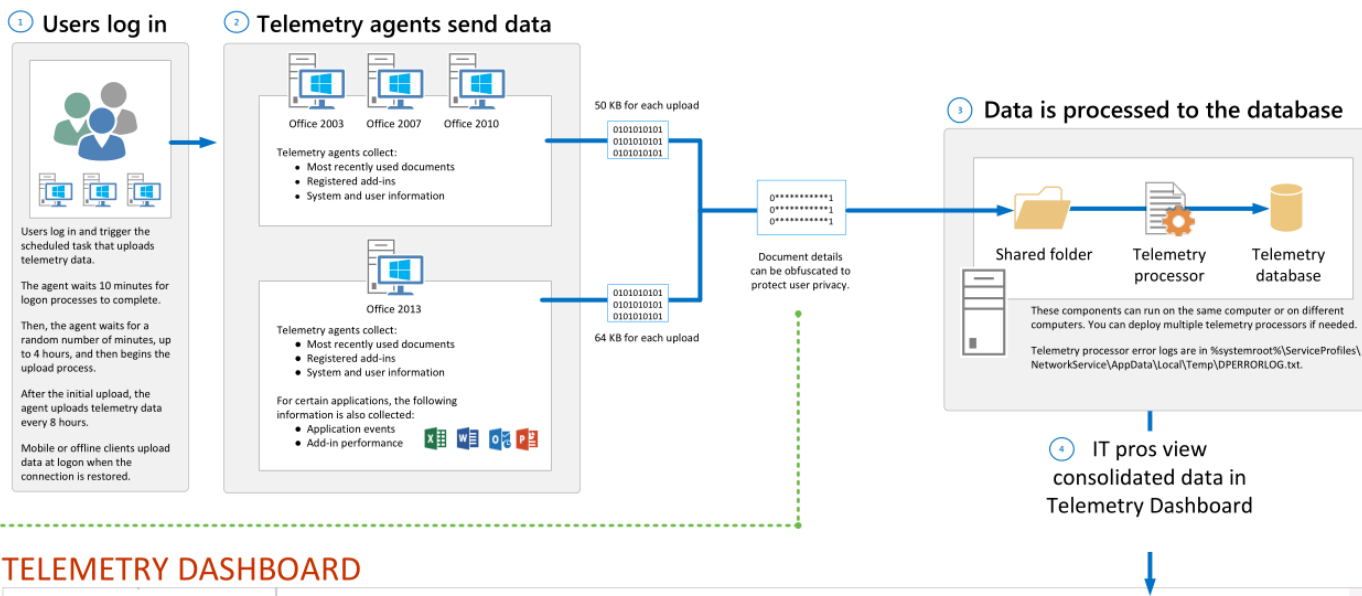


Telemetry database

Telemetry database:

- Provides a data source for Telemetry Dashboard
- Requires SQL Server 2005 and later versions
- Can be run on SQL Express editions in test or small environments
- Can be run on the same computer as other telemetry components

HOW TELEMETRY DATA IS COLLECTED



TELEMETRY DASHBOARD

PROTECTING USER PRIVACY

Telemetry Dashboard offers three methods that help you protect user privacy.

Obfuscate

Obfuscate the document name, title, and path

Re*****.xlsx

Exclude

Exclude applications and solution types from reporting



apps for Office
Application add-ins
COM add-ins

Document files
Template files

Set threshold

Only show files that are used by *N* or more users

Corporate Scorecard.xlsx

Total users: 10

resume.xlsx

Total users: 1

Office Telemetry agents for all versions of Microsoft Office 2003 and above collect the following data and upload it to the shared folder:

- Most recently used documents
- Registered add-ins
- System and user information

The Office Telemetry agents running in Microsoft Office 2013 or Microsoft Office 365 ProPlus will also collect the following data for certain Microsoft Office 2013 applications:

- Application events
- Add-in performance

Use the registry to enable and configure Telemetry Agent

The easiest way to update the registry on a single client is to run a .reg file that sets the registry values that enable Telemetry Agent to collect and upload data. You can create this .reg file by copying one of the following examples

20/04/2016

to a text file, updating the required fields, saving the file as **agent.reg**, and running it from an elevated command prompt. In the .reg file, make sure that you specify the UNC path of the shared folder to which the agent uploads the data. Optionally, you can update the <TAG> fields so you can easily identify the collected data in your organization, such as by department, location, or deployment group.

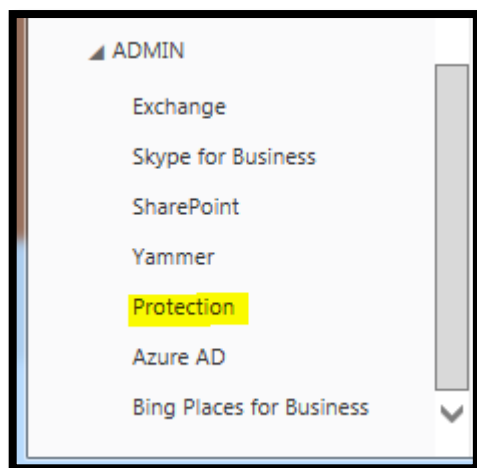
The following example sets the default settings that are needed to enable Telemetry Agent. AgentInitWait and AgentRandomDelay are set to their default values, which are appropriate for production deployments.

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\15.0\osm]
"CommonFileShare"="\\<SERVERNAME>\<SHARENAME>"
"Tag1"="<TAG1>"
"Tag2"="<TAG2>"
"Tag3"="<TAG3>"
"Tag4"="<TAG4>"
"AgentInitWait"=dword:00000258
"Enablelogging"=dword:00000001
"EnableUpload"=dword:00000001
"EnableFileObfuscation"=dword:00000000
"AgentRandomDelay"=dword:000000F0
```

You can also use Group Policy to enable and configure Telemetry Agents. Download the Group Policy administrative template files from the [Microsoft Download Center](#). The policy settings that are listed in the following table are available in the path **User Configuration\Administrative Templates\Microsoft Office 2013\Telemetry Dashboard**.

Compliance and eDiscovery

The Compliance Center is becoming the Protection Center



Compliance Center

Home

Archiving

Data loss prevention

eDiscovery

Reports

Retention

Import

Permissions

Search

eDiscovery cases

Use eDiscovery cases to identify, manage, and hold content in Exchange, SharePoint, and OneDrive for Business. Use this page to create cases, manage existing cases, and close cases that you no longer need. To access the eDiscovery Center or an eDiscovery case, you have to be a site collection administrator or a member of the Owners group. [Learn more](#)

[Go to the eDiscovery Center in SharePoint](#)

[Go to Advanced eDiscovery](#)



Case name	Date created	
No cases found		

BROWSE PAGE

SHARE FOLLOW



Home

eDiscovery Center

Search this site

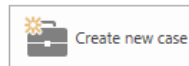
Cases

Site Contents



Welcome to the eDiscovery Center

- Use eDiscovery cases to manage the identification and in-place hold of Exchange mailboxes, SharePoint sites, and other sources of content. You can create and manage queries to identify relevant content and then export the search results.



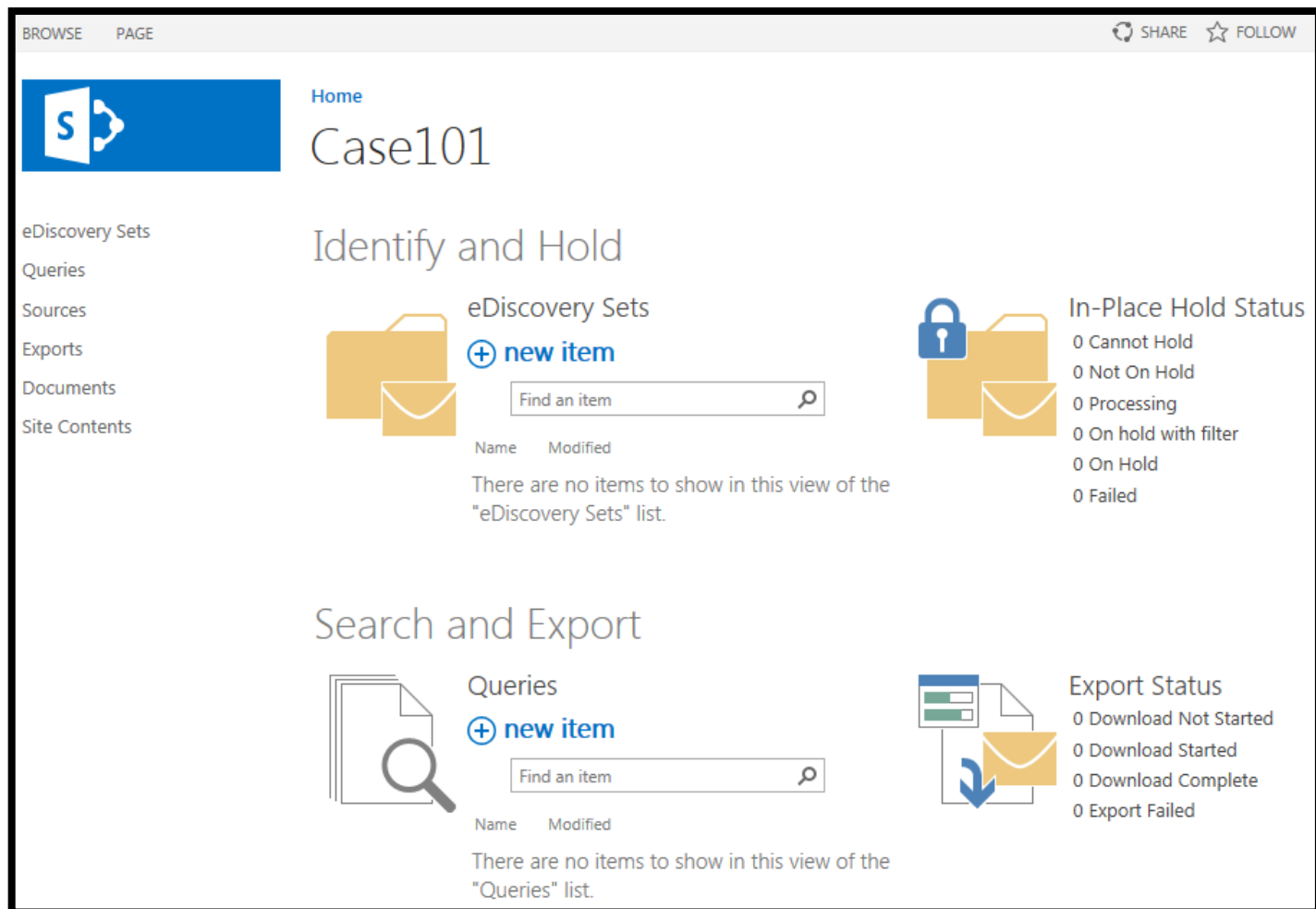
Get Started

1. Grant your legal users permissions to access content across your SharePoint deployment. We recommend creating a security group that contains your legal team members.
2. To discover Exchange mailboxes, ensure your administrator has installed the Exchange Web Services Managed Client on all SharePoint servers and have your administrator configure authentication between Exchange and SharePoint.
3. Give your legal team security group user policy permissions to all appropriate SharePoint Web Applications that contain content you need to perform eDiscovery on.
4. Grant your legal users eDiscovery permissions for the Exchange mailboxes you must perform eDiscovery actions on.

In-Place Hold, Search, & Export

- With in-place holds you can specify SharePoint sites and mailboxes to place on hold. When content is modified or deleted it will be stored in-place until you need to export it.
- In-place eDiscovery search allows you to search across SharePoint sites, file shares, and Exchange mailboxes. Use proximity, wildcards, Boolean logic, and refiners to scope the results to the content you need. Because the search is in-place, your results are live and up to date just like if you were doing a normal Outlook Web Access or SharePoint site search.
- Once you have identified the content you need, you can download it to your local hard drive or file share in a portable native format. Easily download SharePoint pages, documents, lists, and Exchange mailbox data.

https://o347.sharepoint.com/Sites/eDiscoveryCenter/_layouts/15/viewcases.aspx



Planning and creating cases

If you anticipate managing multiple cases in your eDiscovery Center, consider whether you want to define consistent processes for people in your organization to follow.

- Naming conventions for cases – Could matter if you anticipate a larger number of cases, or different types or classifications of cases, for different departments,
- Additional data to describe cases
- Defining and communicating permissions for managing cases.
- Guidelines on creating queries
- Standard procedures for communicating when content is placed on hold
- Standard procedure for retaining and closing cases

Example lifecycle of an eDiscovery case

- Create the site to manage a case
- Add sources
- Place sources on hold
- Create queries
- Export case content
- Close case

Create a case

1. In an eDiscovery Center, click **Create new case**.
2. Type a title and description for your case.
3. In the **Web Site Address** box, type the last part of the URL you want for the case, such as ContosovsFabrikam.
4. Under **Select a template**, make sure that **eDiscovery Case** is selected.
5. Under **User Permissions**, select whether or not to keep the same permissions as the parent site or use unique permissions. If specific people will need access to this case, but not to other cases, you should choose **Use unique permissions**.

Add sources and place them on hold

1. In the eDiscovery Center, open the case that you want to add a source to.
2. Click **eDiscovery Sets**.
3. Type a name for the eDiscovery Set, such as **Executive Correspondence**.
4. Next to **Sources**, click **Add & Manage Sources**.
5. In the dialog box that appears, under **Mailboxes**, type the account names or e-mail addresses for the Exchange mailboxes.
6. Under **Locations**, type the URL or file share address for the content you want to use as the source. Any content you include must be indexed by search.
7. Click **Save**.
8. In the box under **Filter**, type any keywords you want to use to narrow down the source.
9. To narrow down content by a date range, enter the **Start Date** and **End Date**.
10. To limit results to the author of a document or list item, or to a specific sender of e-mail messages, type the names or e-mail addresses in the **Author/Sender** box.
11. To limit results to a specific Exchange domain, type its name in the **Domain** box.
12. Click the **Apply Filter** button.
13. Click **Enable In-Place** hold.
14. To verify that you've selected the right content, click **Preview Results**.
15. Click **Save**.


Run queries and export content

Once you have defined your sources, and placed them on hold if necessary, you can run queries to narrow down and extract exactly the content you need for a particular case. SharePoint has some tools that can help you refine your queries.

You export content from a case when you are ready to deliver it to an authority or want to work on it with another legal program. The content is exported in a format that is compatible with the Electronic Discovery Reference Model standard.

Close cases

When you close a case, in-place holds will be released for all of its sources, and you will no longer be able to put sources on hold for this case.

1. Click **Settings**
 , and then click **Case Closure**.
2. Click **Close this case**.

Verify that a federation server is operational

Procedure 1:

1. To verify that Internet Information Services (IIS) is configured correctly on the federation server, log on to a client computer that is located in the same forest as the federation server.
2. Open a browser window, in the address bar type the federation server's DNS host name, and then append /adfs/fs/federationserverservice.asmx to it for the new federation server, for example:
<https://fs1.fabrikam.com/adfs/fs/federationserverservice.asmx>
3. Press ENTER, and then complete the next procedure on the federation server computer. If you see the message **There is a problem with this website's security certificate**, click **Continue to this website**.
The expected output is a display of XML with the service description document. If this page appears, IIS on the federation server is operational and serving pages successfully.

Membership in Administrators, or equivalent, on the local computer is the minimum required to complete this procedure.

Procedure 2:

1. Log on to the new federation server as an administrator.
2. On the **Start** screen, type **Event Viewer**, and then press ENTER.
3. In the details pane, double-click **Applications and Services Logs**, double-click **AD FS Eventing**, and then click **Admin**.

4. In the **Event ID** column, look for event ID 100. If the federation server is configured properly, you see a new event—in the Application log of Event Viewer—with the event ID 100. This event verifies that the federation server was able to successfully communicate with the Federation Service.

Powershell:

Set-MsolUserPrincipalName cmdlet is used to change the User Principal Name (user ID) of a user. This cmdlet can be used to move a user between a federated and standard domain, which will result in their authentication type changing to that of the target domain.

The following command renames user1@contoso.com to CCole@contoso.com.

```
Set-MsolUserPrincipalName -UserPrincipalName User1@contoso.com -NewUserPrincipalName  
CCole@contoso.com
```

To view summary information about your current licensing plans and the available licenses for each plan, run the following command in Office 365

Get-MsolAccountSku

To view details about the Office 365 services that are available in a specific licensing plan, use the following syntax.

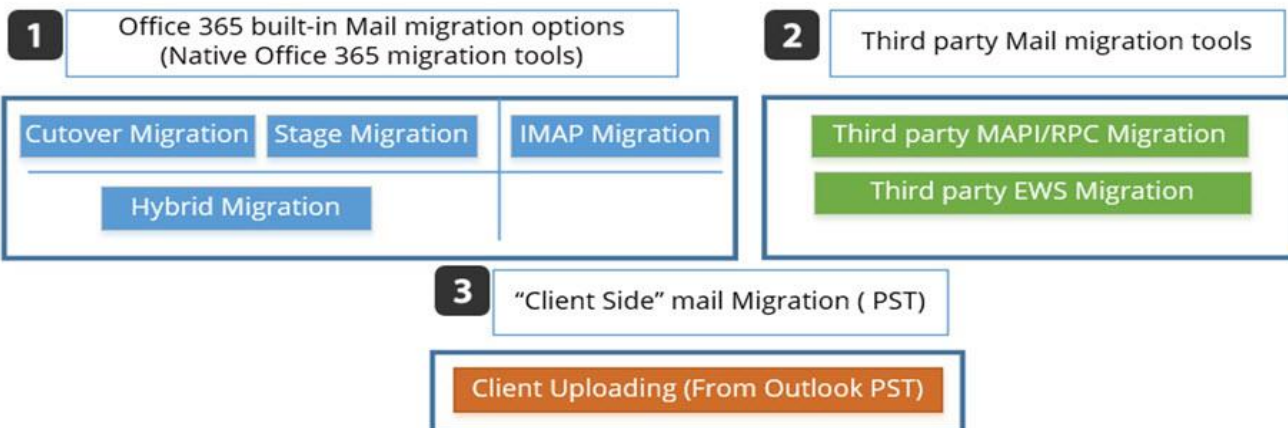
```
(Get-MsolAccountSku | where {$_.AccountSkuld -eq '<AccountSkuld>'}).ServiceStatus
```

Exchange online:

There are three types of email migrations that can be made from an Exchange Server:

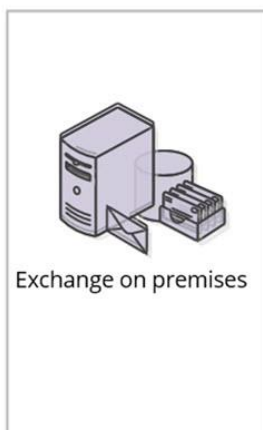
- **Migrate all mailboxes at once (cutover migration)**
Use this type of migration if you're running Exchange 2003, Exchange 2007, Exchange 2010, or Exchange 2013, and if there are fewer than 2000 mailboxes. For an overview of cutover migration, see [What you need to know about a cutover email migration to Office 365](#). You can perform a cutover migration by using the Setup wizard, or by starting from the Exchange admin center (EAC). If you want to use the EAC, see [Perform a cutover migration to Office 365](#). See [Use the Office 365 Setup wizard to perform a cutover migration](#) to migrate during the setup.
Important The Setup wizard is limited to migrating 150 mailboxes only.
If you start the cutover migration from the EAC, you can move up to 2000 mailboxes, but due to length of time it takes to create and migrate 2000 users, it is more reasonable to migrate 150 users or less.
- **Migrate mailboxes in batches (staged migration)**
Use this type of migration if you're running Exchange 2003 or Exchange 2007, and there are more than 2,000 mailboxes. For an overview of staged migration, see [What you need to know about a staged email migration to Office 365](#). To perform the migration tasks, see [Perform a staged migration of Exchange Server 2003 and Exchange 2007 to Office 365](#).
- **Migrate using an integrated Exchange Server and Office 365 environment (hybrid)**
Use this type of migration to maintain both on-premises and online mailboxes for your organization and to gradually migrate users and email to Office 365. Use this type of migration if:
 - You have Exchange 2010 and more than 150-2,000 mailboxes.
 - You have Exchange 2010 and want to migrate mailboxes in small batches over time.
 - You have Exchange 2013.

Mail migration to Office 365 | Methods and classifications



O365INFO.COM COPYRIGHT ©

Pre requirements for Exchange On-Premises server



Exchange on premises

On-Premises

- 1** Public Certificate
The certificate should include reference to the Exchange On-Premises server public SMTP domain name and reference to the AutoDiscover host name.
- 2** Public IP
- 3** Public name (FQDN)
- 4** Outlook AnyWhere
Exchange On-Premises server configure to use Outlook AnyWhere settings.



O365INFO.COM COPYRIGHT ©

Migration options

tech 2013
days

Migration	IMAP migration Supports wide range of email platforms Email only (no calendar, contacts, or tasks)
	Cutover Exchange migration Good for fast, cutover migrations No Exchange upgrade required on-premises
	Staged Exchange migration No Exchange upgrade required on-premises Identity federation with on-premises directory
Hybrid	Hybrid deployment Manage users on-premises and online Enables cross-premises calendaring, smooth migration, and easy off-boarding

	IMAP migration	Cutover migration	Staged migration	Hybrid
Exchange 5.5	X			
Exchange 2000	X			
Exchange 2003	X	X	X	
Exchange 2007	X	X	X	X
Exchange 2010	X	X		X
Exchange 2013	X	X		X
Notes/Domino	X			
GroupWise	X			
Other	X			



IMAP migration

Exchange Online offers a web-based tool for migrating mailbox data from email systems that support IMAP. It guides administrators through the following migration steps:

1. Create empty mailboxes in the cloud for users in the organization (typically this is done by uploading a .csv file or using remote Windows PowerShell).
2. Enter the remote server connection settings.
3. Use a CSV file to specify the mailboxes whose data will be migrated to Exchange Online mailboxes.
4. After this information is entered, Exchange Online begins to migrate mailbox content via IMAP (calendar items, contacts, tasks, and other non-mail items are not migrated).

For more information about IMAP migration, see [Migrate Email from an IMAP Server to Exchange Online Mailboxes](#) and [Migrate other types of IMAP mailboxes](#).

Important:

To avoid overusing the remote server's resources and bandwidth during the migration, Exchange Online creates fewer than 10 connections to the IMAP server.

Cutover Exchange migration

Exchange Online offers a web-based tool for migrating data from on-premises [Exchange Server 2003](#), [Exchange Server 2007](#), or [Exchange Server 2010](#) environments. It guides an administrator through the following migration steps:

1. Using the email address and credentials for an on-premises administrator account, Exchange Online connects to the on-premises email organization by using the Autodiscover service.
2. Exchange Online uses an RPC/HTTP connection to read directory information from the remote server and create mailboxes in Exchange Online.
3. Exchange Online synchronizes the mailbox content to the cloud mailboxes. Users remain connected to their original mailboxes while their data is being migrated to Exchange Online.
4. After the initial migration is complete, any changes are synchronized to the cloud every 24 hours until the administrator stops or deletes the migration batch.

To switch users to their cloud mailboxes, administrators configure their MX record to point to Office 365 and reconfigure the users' profiles in Outlook. When users switch to their cloud mailboxes, [their local offline folders \(.ost files\) will resynchronize](#), resulting in the download of migrated mail to the client workstation. Users can reply to old messages in their mailboxes after migration.

For more information about a cutover Exchange migration, see [What you need to know about a cutover email migration to Office 365](#).

Important:

An organization can migrate a maximum of 2,000 Exchange 2003, Exchange 2007, Exchange 2010, or Exchange 2013 mailboxes to the cloud using a cutover Exchange migration.

Exchange Online must connect to an on-premises Exchange Server, so the on-premises server must have a certificate issued by a trusted certificate authority and a public IP address.

Staged Exchange migration

With a staged migration, users can be migrated to the cloud using the web-based Exchange migration tool and the **Directory Synchronization tool**. Instead of migrating all users at once, like a cutover Exchange migration, administrators **migrate users in batches**. This is accomplished by uploading a .csv file to specify a partial list of users to migrate. In a staged migration, all of the users in an organization can share the same email domain name. Staged Exchange migration requires administrators to use the Online Services Directory Synchronization tool. This provides users with a **unified Global Address List (GAL)** where the online environment is continuously synchronized with the on-premises environment.

For more information about staged Exchange migrations, see What you need to know about a staged email migration.

Important:

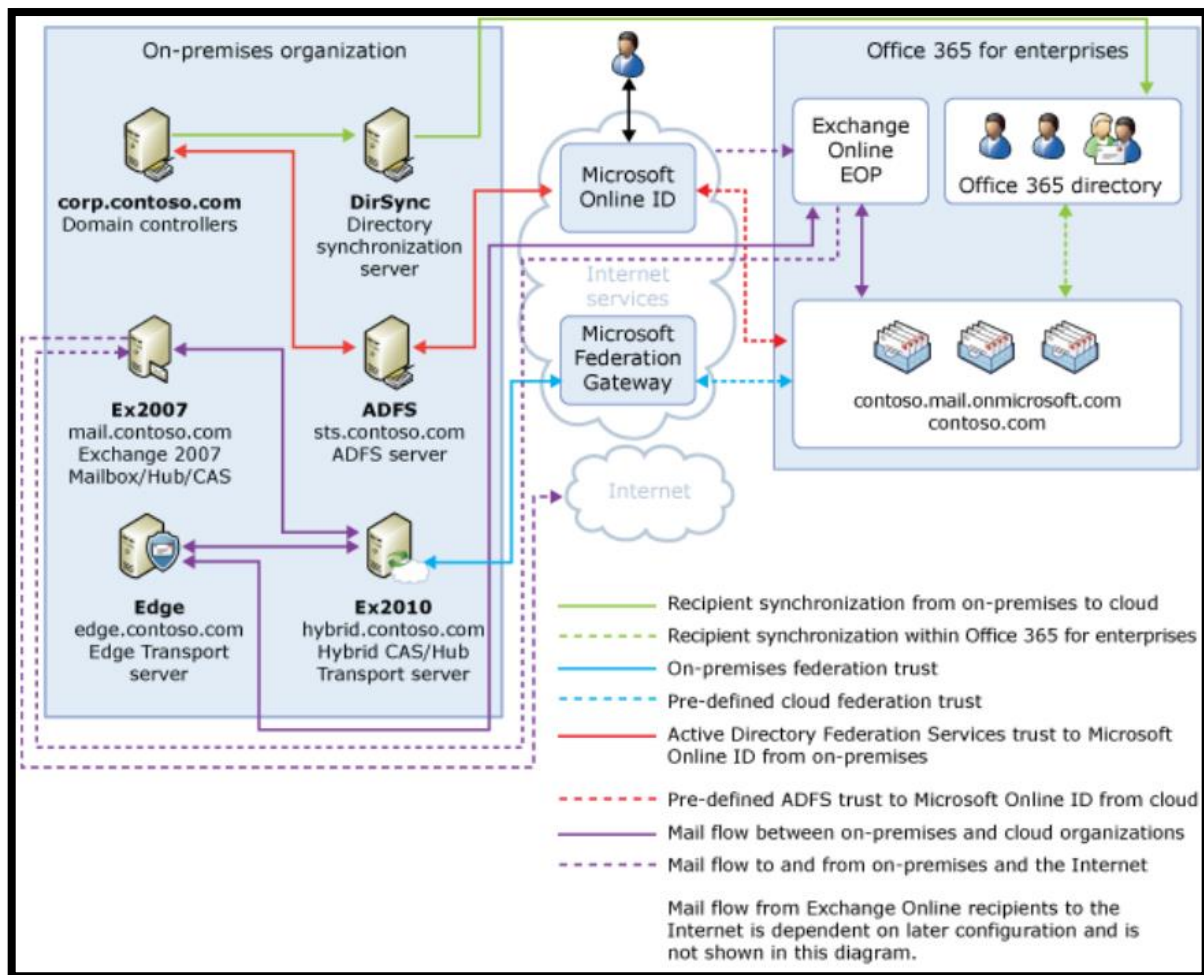
Organizations can't use a staged Exchange migration to migrate Exchange 2010 and Exchange 2013 mailboxes. If you have fewer than 2,000 Exchange 2010 or Exchange 2013 mailboxes in your organization, you can use a cutover Exchange migration. If you have more than 2,000 Exchange 2010 or Exchange 2013 mailboxes, you can implement a hybrid deployment.

During migration, administrators must use the Online Services Directory Synchronization tool to provide users with a unified Global Address List where the online environment is continuously synchronized with the on-premises environment.

Staged Migration vs. Hybrid

Private &
Public Cloud

Feature	Staged	Hybrid
Mail routing between on-premises and cloud (recipients on either side)	●	●
Mail routing with shared namespace (if desired) - @company.com on both sides	●	●
Unified GAL	●	●
Free/Busy and calendar sharing cross-premises		●
Mails tips, messaging tracking, and mailbox search work cross-premises		●
OWA Redirection cross-premise (single OWA URL for both on-premises and cloud)		●
Exchange Online Archive		●
Exchange Management Console used to manage cross-premises relationship & mailbox migrations		●
Native mailbox move supports both onboarding and offboarding		●
No outlook reconfiguration or OST resync required after mailbox migration		●
Online Mailbox Move allows users to start logged into their mailbox while it is being moved to the cloud		●
Secure Mail ensure emails cross-premises are encrypted, and the internal auth headers are preserved		●
Centralized mailflow control , ensures that all email routes inbound/outbound via On Premises		●



Limits across Office 365 options

Feature	Office 365 Business Premium	Office 365 Enterprise E1 Office 365 Government E1	Office 365 Enterprise E3 /Government
User mailboxes	50 GB	50 GB	50 GB
Archive mailboxes ^{8, 9}	50 GB	50 GB	No limit
Shared mailboxes	50 GB	50 GB	50 GB
Resource mailboxes	50 GB	50 GB	50 GB
Site mailboxes ⁶	50 GB	50 GB	50 GB
Public folder mailboxes	50 GB	50 GB	50 GB
Group mailboxes	50 GB	50 GB	50 GB
Warning [Capacity]	49 GB	49 GB	49 GB
Prohibit Send	49.5 GB	49.5 GB	49.5 GB
Prohibit Send/Receive	50GB	50GB	50GB
File attachment size - Outlook	150 MB	150 MB	150 MB
File attachment size limit - OWA	35 MB	35 MB	35 MB
File attachment size limit - ActiveSync	25 MB	25 MB	25 MB
Recipient rate limit	10,000 recipients P/D	10,000 recipients P/D	10,000 recipients P/D
Recipient limit	500 recipients	500 recipients	500 recipients
Deleted Items folder /del retention	14 days	14 days	14 days

Built-in role groups

Role group	Description
Company Administrators (TenantAdmins_<unique value>)	The Company Administrators role group is a special role group that ties together the Global administrators Office 365 role and the Organization Management Role Exchange Online role group. The Company Administrators role group doesn't have any roles assigned to it. However, it's a member of the Organization Management role group and inherits the permission provided by that role group. This role group can't be managed in Exchange Online. You can add members to this role group by adding users to the Global administrator Office 365 role.
Discovery Management	Administrators or users who are members of the Discovery Management role group can perform searches of mailboxes in the Exchange Online organization for data that meets specific criteria and can also configure legal holds on mailboxes.
Help Desk	The Help Desk role group, by default, enables members to view and modify the Microsoft Outlook Web App options of any user in the organization. These options might include modifying the user's display name, address, and phone number. They don't include options that aren't available in Outlook Web App options, such as modifying the size of a mailbox or configuring the mailbox database on which a mailbox is located.
Help Desk Administrators (HelpdeskAdmins_<unique value>)	The Help Desk Administrators role group doesn't have any roles assigned to it. However, it's a member of the View-Only Organization Management role group and inherits the permissions provided by that role group. This role group can't be managed in Exchange Online. You can add members to this role group by adding users to the Password administrator Office 365 role.
Organization Management	Administrators who are members of the Organization Management role group have administrative access to the entire Exchange Online organization and can perform almost any task against any Exchange Online object, with some exceptions, such as the Discovery Management role. Important: Because the Organization Management role group is a powerful role, only users that perform organizational-level administrative tasks that can potentially impact the entire Exchange Online organization should be members of this role group.
Recipient Management	Administrators who are members of the Recipient Management role group have administrative access to create or modify Exchange Online recipients within the Exchange Online organization.
Records Management	Users who are members of the Records Management role group can configure compliance features, such as retention policy tags, message classifications, and transport rules.
UM Management	Administrators who are members of the UM Management role group can manage features in the Exchange Online organization such as UM properties on mailboxes, UM prompts, and UM auto attendant configuration.
View-Only Organization Management	Administrators who are members of the View Only Organization Management role group can view the properties of any object in the Exchange Online organization.

Import PST files to Office 365

You have to perform Step 1 and Step 2 only once to import PST files to Office 365 mailboxes. After you perform these steps, follow Step 3 through Step 6 each time you want to upload and import a batch of PST files.

Before you begin

- You have to be assigned the Mailbox Import Export role to import PST files to Office 365 mailboxes. By default, this role isn't assigned to any role group in Exchange Online. Additionally, you have to be a global administrator in your Office 365 organization to access the **Import** page (under **Data management**) in the Office 365 Compliance Center.
- You need to store the PST files that you want to import to Office 365 on a file server or shared folder in your organization. In Step 3, you'll run the Azure AzCopy tool that will upload the PST files that are stored on this file server or shared folder to Office 365.

Step 1: Download the PST Import tools

The first step is to download and install the tools that you will run in Step 3 to upload PST files to Office 365.

1. Go to <https://protection.office.com>.
2. In the left pane, click **Data management** and then click **Import**.
3. On the **Import** page, click **Go to the Import service**.
4. On the **Import files to Office 365** page, click **New job**
+, and then click **Upload files over the network**.
5. On the **Upload files over the network** page, click **Download the Azure AzCopy tool**.
6. In the pop-up window, click **Run** to install the Azure AzCopy tool.

Important:

Be sure to install the Azure AzCopy tool in the default location (%ProgramFiles(x86)%\Microsoft SDKs\Azure\ on a computer running 64-bit Windows). That's because if you want to encrypt the PST files before they're uploaded to Office 365, the O365ImportTool.exe tool that you run to encrypt them looks for the AzCopy tool in this location.

Step 2: Obtain the SAS key and network upload URL for PST Import

The next step is to copy and save the Shared Access Signature (SAS) key and the network upload URL to a file. The SAS key provides you with the necessary permissions to upload PST files to the Azure storage location in the Microsoft cloud. As previously stated, be sure to take precautions to protect this file. They are unique to your organization and will be used in Step 3.

1. On the **Upload files over the network** page, under **Copy secure network upload SAS key**, click **Copy network upload SAS key**.
2. Under **Copy the secure network upload URL**, click **Show URL for PST files**.
This URL is used to identify the location in Office 365 where the PST files that you upload in Step 3 will be stored.

Step 3: Upload your PST files to Office 365

Now you're ready to use the AzCopy.exe tool to upload PST files to Office 365. This tool uploads and stores them in an Azure storage location in the Microsoft cloud. To complete this step, the PST files have to be located in a file share or file server in your organization. This is known as the *source directory* in the following procedure. Each time you run the AzCopy.exe tool, you'll can specify a different source directory.

1. Open a Command Prompt on your local computer.
2. Go to the directory where you installed the AzCopy.exe tool in Step 1. If you installed the tool in the default location, go to %ProgramFiles(x86)%\Microsoft SDKs\Azure.
3. Run the following command to upload the PST files to Office 365.
AzCopy.exe /Source:<Location of PST files> /Dest:<Network upload URL + PST file path> /DestSAS:<SAS key> /V:<Log file location>

Here's an example of the syntax for the AzCopy.exe tool using actual values for each parameter:

```
AzCopy.exe /Source:\\FILESERVER1\PSTs  
/Dest:"https://3c3e5952a2764023ad14984.blob.core.windows.net/ingestiondata/FILESERVER01/PSTs  
" /DestSAS:"?sv=2012-02-12&se=9999-12-
```

31T23%3A59%3A59Z&sr=c&si=IngestionSasForAzCopy201601121920498117&sig=Vt5S4hVzlzMcBkuH8bH711atBffdrOS72TIV1mNdORg%3D" /V:C:\Users\Admin\Desktop\AzCopy1.log

After you run the command, status messages are displayed that show the progress of uploading the PST files. A final status message shows the total number of files that were successfully uploaded.

Step 4: Create the PST Import mapping file

After the PST files have been uploaded to the Azure storage location for your Office 365 organization, the next step is to create a comma separated value (CSV) file that specifies which user mailboxes the PST files will be imported to. You will submit this CSV file in the next step when you create a PST Import job.


1. Download a copy of the PST Import mapping file.
2. Open or save the CSV file to your local computer. The following example shows a completed PST Import mapping file (opened in NotePad). It's much easier to use Microsoft Excel to edit the CSV file.
Workload,FilePath,Name,Mailbox,IsArchive,TargetRootFolder,SPFileContainer,SPManifestContainer,SPSiteURL
Exchange,FILESERVER01/PSTs,annb.pst,annb@contoso.onmicrosoft.com,FALSE,/Inbox,,,
Exchange,FILESERVER01/PSTs,annb_archive.pst,annb@contoso.onmicrosoft.com,TRUE,/Inbox,,,

Note:

Don't change anything in the header row, including the SharePoint parameters; they will be ignored during the PST Import process.




3. Use the information in the following table to populate the CSV file with the required information.

Parameter	Description	Example
Workload	Specifies the Office 365 service that data will be imported to. To import PST files to user mailboxes, use Exchange.	Exchange
FilePath	Specifies the folder location in the Azure storage location that you uploaded the PST files to in Step 3. Important: This in the same path name that you used for the source directory component of the /Dest: parameter in the previous step. If you didn't include the optional pathname in the /Dest: parameter, leave this parameter blank in the CSV file.	FILESERVER01/PSTs
Name	Specifies the name of the PST file that will be imported to the user mailbox.	annb.pst
Mailbox	Specifies the email address of the mailbox that the PST file will be imported to.	annb@contoso.onmicrosoft.com
IsArchive	Specifies whether or not to import the PST file to the user's archive mailbox. There are two options: <ul style="list-style-type: none"> • FALSE Imports the PST file to the user's primary mailbox. • TRUE Imports the PST file to the user's archive mailbox. 	FALSE
TargetRootFolder	Specifies the folder that the PST file is imported to. If you leave this parameter blank, the PST will be imported to a new folder named Imported located at the root level of the mailbox (the same level as the Inbox and the other default mailbox	Inbox

	folders). If you specify "/" the PST file will be imported to the root level.	
	 Tip: Consider running a few test batches to experiment with this parameter so you can determine the best folder location to import PSTs files to.	
SPFileContainer	For PST Import, leave this parameter blank.	Not applicable
SPManifestContainer	For PST Import, leave this parameter blank.	Not applicable
SPSiteUrl	For PST Import, leave this parameter blank.	Not applicable

Step 5: Create a PST Import job in Office 365

The last step is to create the PST Import job in the Import service in Office 365. As previously explained, you will submit the PST Import mapping file that you created in Step 4. After you create the new job, the Import service will use the information in the mapping file to import the PST files (that you uploaded to Office 365 in Step 3) to the specified user mailbox.

1. Go to <https://protection.office.com>.
2. In the left pane, click **Data management** and then click **Import**.
3. On the **Import** page, click **Go to the Import service**.
4. On the **Import files to Office 365** page, click **New job**

 , and then click **Upload files over the network**.
5. On the **Upload files over the network** page, click the **I'm done uploading my files and I have access to the mapping file** check boxes, and then click **Next**.
6. Type a name for the PST Import job, and then click **Next**.
7. Click **Add**

 to select the PST Mapping file that you created in Step 4.
8. After the name of the CSV file appears in the list, select it and then click **Validate** to check your CSV file for errors.
 The CSV file has to be successfully validated to create a PST Import job. If the validation fails, click the **Invalid** link in the **Status** column. A copy of your PST Import mapping file is opened, with a error message for each row in the file that failed.
9. When the PST mapping file is successfully validated, read the terms and conditions document, and then click the checkbox.
10. Click **Finish** to submit the job.
 The job is displayed in the list of PST Import jobs on the **Import files to Office 365** page.
11. Select the job and click **Refresh**

 to update the status information that's displayed in the details pane.
12. In the details pane, click **View details** to get the latest status for the selected job.

Parameter	Description	Example
/Source:	Specifies the source directory in your organization that contains the PST files that will be uploaded to Office 365.	/Source:\\FILESERVER01\\PSTs
/Dest:	<p>Specifies the destination in Office 365 where your PST files will be uploaded to; this is the location of the Azure storage directory. The value for this parameter consists of the following:</p> <ul style="list-style-type: none"> The network upload URL that you obtained in Step 2. (Optional) You can also include the path of the source directory that contains the PST files (the source directory that is specified by the /Source: parameter). If you include this path, the path name has to be converted to a URL format. For example, <u>\\FILESERVER01\\PSTs</u> is changed to FILESERVER01/PSTs. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note:</p> <p>If you include the optional pathname, the namespace for a PST file after it's uploaded to the Azure storage area will include the pathname and the name of the PST file; for example, FILESERVER01/PSTs/annb.pst. If you don't include a pathname, the namespace is only the PST filename; for example annb.pst.</p> </div> <p>Be sure to surround the value of this parameter with double-quotation marks ("").</p>	<p>/Dest:"https://3c3e5952a023.blob.core.windows.net/ingestiondata/"</p> <p>Or</p> <p>/Dest:"https://3c3e5952a023.blob.core.windows.net/ingestiondata/FILESERVER01/PSTs"</p>
/DestSAS:	Specifies the SAS key that you obtained in Step 2. Be sure to surround the value of this parameter with double-quotation marks ("").	/DestSAS:"?sv=2012-02-12&se=9999-12-31T23%3A59%3A59Z&sr=c&si=IngestionSasForAzCopy201601121920498117&sig=Vt5S4hVzIzMcBkH711OS72TIV1mNdORg%3D"
/V:	Outputs verbose status messages into a log file. By default, the verbose log file is named AzCopyVerbose.log in %LocalAppData%\Microsoft\Azure\AzCopy. If you specify an existing file location for this option, the verbose log will be appended to that file.	/V:C:\Users\Admin\Desktop\Uploadlog.log
/S	<p>This optional switch specifies the recursive mode so that the AzCopy.exe tool will copy PSTs files that are located in subfolders in the source directory in /Source: parameter.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note:</p> <p>If you include this switch, PST files in subfolders will have a different file pathname in the Azure storage location after they're uploaded. You'll have to specify the exact file pathname in the CSV file that you create in Step 4.</p> </div>	/S

Compliance Center

- Home
- Archiving
- Device management
- Data loss prevention
- eDiscovery
- Reports
- Retention
- Import**
- Permissions

Import data to Office 365

Use the Import service to transfer data from your organizations's servers to Office 365. You can ship hard drives to Microsoft or upload the data directly over the network. [Learn more](#)

[Go to the Import service](#)

Import Service

Import data to Office 365

The Import Service for SharePoint has temporarily been suspended until further notice. We apologize for any inconvenience caused.

Use the Import service to move email (PST files) or SharePoint data from your organization's servers to Office 365. You can ship hard drives to Microsoft or upload the files directly over the network. This feature is currently in preview.

[Learn more about importing data to Office 365](#)

[Learn how to move SharePoint or OneDrive for Business data](#)

Name	Type	Status last changed	Status
There are no items to show in this view.			

New Job

Upload files over the network

New job

1. Open the companion guide that's associated with the type of data you want to import. The detailed instructions in these guides will help you complete the steps in this wizard:

[Guide for importing email \(PST files\)](#)[Guide for importing SharePoint or OneDrive for Business data](#)

2. Upload files using the Azure AzCopy tool | [Download tool](#)

Copy the secure network upload SAS key

[Copy network upload SAS key](#)

Copy the secure network upload URL

[Show URL for PST files](#)[Show URL for SharePoint or OneDrive for Business files](#)☐ * I'm done uploading my files

3. Prepare the mapping file.

☐ * I have access to the mapping file

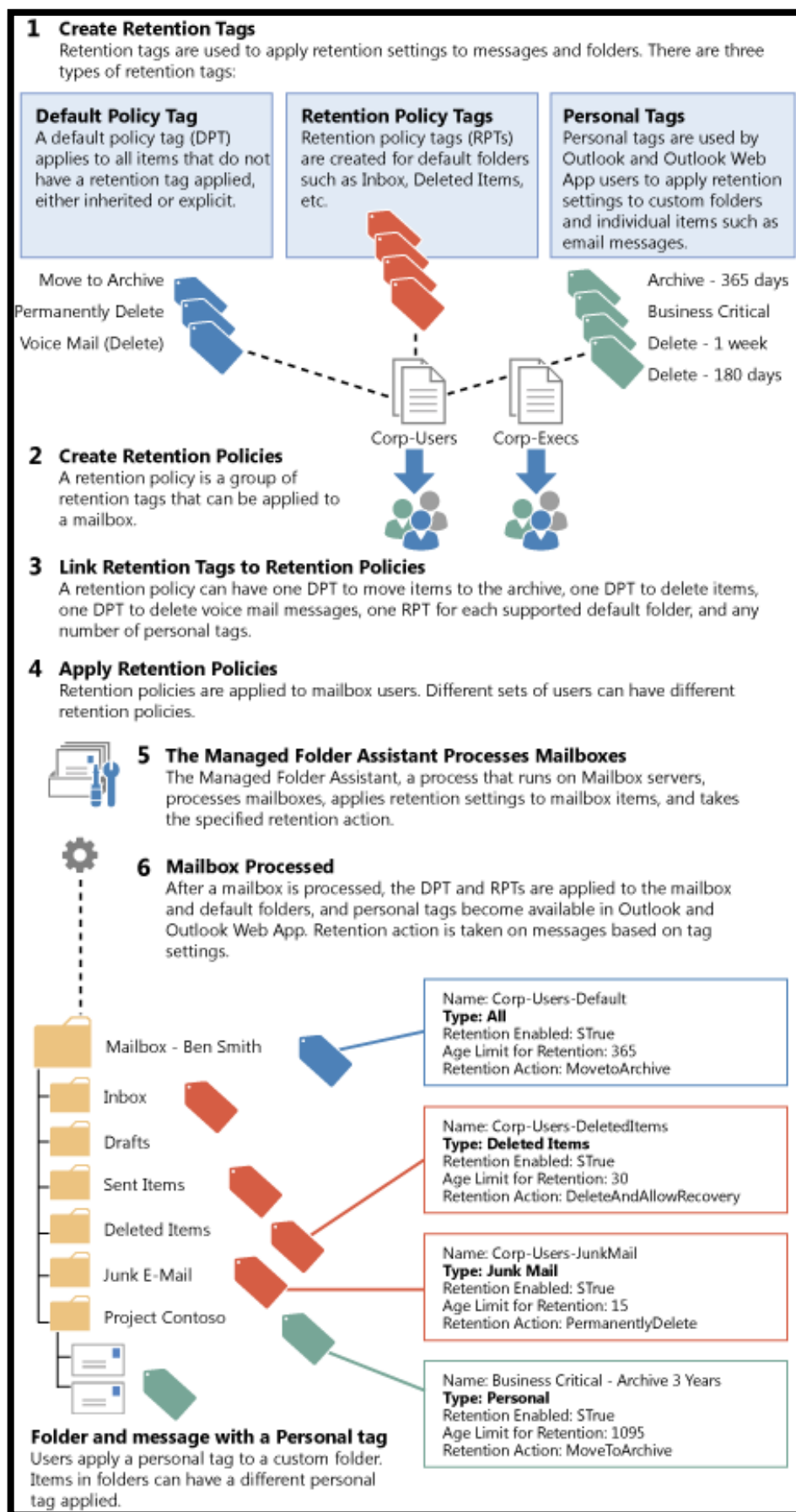
4. Click Next and complete the remaining steps in this wizard.

Next

[Cancel](#)

Messaging records management (MRM)

MRM in Exchange 2013 and Exchange Online is accomplished by using retention tags and retention policies



Exchange admin center

dashboard in-place eDiscovery & hold auditing data loss prevention retention policies **retention tags** journal rules

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

hybrid

Retention tags are visible to end users and can be used to specify when items in users' mailboxes will be moved to the archive or removed from the mailbox.

+ - ✎ 🗑️ ↺

NAME	TYPE ▲	RETENTION PERI...	RETENTION ACTION	
Default 2 year move to arch...	Default	730 days	Archive	Default 2 year move to archive
Deleted Items	Deleted Items	30 days	Delete	Retention tag type
Junk Email	Junk Email	30 days	Delete	Default
1 Month Delete	Personal	30 days	Delete	Retention period
1 Week Delete	Personal	7 days	Delete	730 days
1 Year Delete	Personal	365 days	Delete	After retention period
6 Month Delete	Personal	180 days	Delete	Move To Archive
Never Delete	Personal	Unlimited	Delete	Comment
Personal 1 year move to arc...	Personal	365 days	Archive	
Personal 5 year move to arc...	Personal	1825 days	Archive	
Personal never move to arch...	Personal	Unlimited	Archive	

Exchange Online Archiving Requirements and Setup

The following are general requirements required to configure Exchange Online Archiving.

- User's primary mailboxes must be hosted on on-premises Exchange 2010 SP1 or later Mailbox servers.
- Users must use Outlook 2013, Outlook 2010, Outlook 2007 SP2, or Outlook Web App to access the cloud-based archive mailbox.

PowerShell

Create NEW Retention Policy Tags

This example creates the retention policy tag Finance-DeletedItems for the Deleted Items default folder. When applied to a mailbox as a part of a retention policy, the tag permanently deletes items of all types in the Deleted Items folder in 30 days.

New-RetentionPolicyTag "Finance-DeletedItems" -Type DeletedItems -RetentionEnabled \$true -AgeLimitForRetention 30 -RetentionAction PermanentlyDelete

Parameter	Required	Description
<i>Name</i>	Required	The <i>Name</i> parameter specifies the name of the tag.
<i>AgeLimitForRetention</i>	Optional	The <i>AgeLimitForRetention</i> parameter specifies the age at which retention is enforced on an item. The age limit corresponds to the number of days from the date the item was delivered, or the date an item was created if it wasn't delivered. If this parameter isn't present and the <i>RetentionEnabled</i> parameter is set to \$true, an error is returned.
<i>RetentionAction</i>	Optional	The <i>RetentionAction</i> parameter specifies one of the following actions: <ul style="list-style-type: none"> • MarkAsPastRetentionLimit If you specify this action for a retention tag, messages that have the tag applied are marked as past the retention limit. • MoveToFolder This action isn't available for retention tags. • MoveToDeletedItems This action isn't available for retention tags. • DeleteAndAllowRecovery This action deletes a message and allows recovery from the Recoverable Items folder.

		<ul style="list-style-type: none"> PermanentlyDelete This action permanently deletes a message. A message that has been permanently deleted can't be recovered using the Recoverable Items folder. Permanently deleted messages aren't returned in a Discovery search, unless litigation hold is enabled for the mailbox. MoveToArchive This action moves a message to the user's archive mailbox. You can use this action for retention tags of type All, Personal, and RecoverableItems. <p>If this parameter isn't present and the <i>RetentionEnabled</i> parameter is set to \$true, an error is returned.</p>			
<i>RetentionEnabled</i>	Optional	<p>The <i>RetentionEnabled</i> parameter specifies whether the tag is enabled. When set to \$false, the tag is disabled, and no retention action is taken on messages that have the tag applied.</p> <div> <p>Note:</p> <p>Messages with a disabled tag are still considered tagged, so any default policy tags in the user's retention policy aren't applied to such messages.</p> </div> <p>When you set the <i>RetentionEnabled</i> parameter to \$false, the retention period for the tag is shown as Never. Users may apply this tag to items they want to indicate should never be deleted or should never be moved to the archive. Enabling the tag later may result in unintentional deletion or archiving of items. To avoid this situation, if a retention policy is disabled temporarily, it may be advisable to change the name of that tag so that users are discouraged from using it, such as DISABLED_<Original Name>.</p>			
<i>Type</i>	Optional	<p>The <i>Type</i> parameter specifies the type of retention tag being created. Valid values include:</p> <table> <tr> <td> <ul style="list-style-type: none"> Calendar Clutter Available in Exchange Online only. Contacts DeletedItems Drafts Inbox </td><td> <ul style="list-style-type: none"> JunkEmail Journal Notes Outbox SentItems Tasks </td><td> <ul style="list-style-type: none"> All RecoverableItems RssSubscriptions SyncIssues ConversationHistory Personal </td></tr> </table> <div> <p>Note:</p> <p>To create a default policy tag (DPT), specify type All. For tags of type RecoverableItems, the only valid retention action is MoveToArchive.</p> </div>	<ul style="list-style-type: none"> Calendar Clutter Available in Exchange Online only. Contacts DeletedItems Drafts Inbox 	<ul style="list-style-type: none"> JunkEmail Journal Notes Outbox SentItems Tasks 	<ul style="list-style-type: none"> All RecoverableItems RssSubscriptions SyncIssues ConversationHistory Personal
<ul style="list-style-type: none"> Calendar Clutter Available in Exchange Online only. Contacts DeletedItems Drafts Inbox 	<ul style="list-style-type: none"> JunkEmail Journal Notes Outbox SentItems Tasks 	<ul style="list-style-type: none"> All RecoverableItems RssSubscriptions SyncIssues ConversationHistory Personal 			

Use the **New-RetentionPolicy** cmdlet to create a retention policy

This example creates the retention policy Business General and uses the *RetentionPolicyTagLinks* parameter to associate two retention policy tags with this policy. You can enter multiple retention policy tags, separated by commas. If a tag name includes a space, enclose the name in quotation marks.

```
New-RetentionPolicy "Business General" -RetentionPolicyTagLinks "General Business","Legal"
```

Apply Retention policy for a single Mailbox

```
Set-Mailbox John -RetentionPolicy "My Policy"
```

Apply Retention Policy to ALL Office 365 Mailbox's (Bulk Mode)

```
$UserMailboxes = Get-Mailbox -Filter {(RecipientTypeDetails -eq 'UserMailbox')}}
$UserMailboxes | Set-Mailbox -RetentionPolicy "My Policy"
```

Remove Retention Policy from a single a Mailbox (set to Null)

```
Set-Mailbox John -RetentionPolicy $Null
```

Run the Managed Folder Assistant for a specific Mailbox

```
Start-ManagedFolderAssistant John
```

Use the **Set-RetentionPolicy** cmdlet to change the properties of an existing retention policy.

This example modifies the policy MyPolicy to link the retention policy tag MyRetentionPolicyTag with it.
Set-RetentionPolicy "MyPolicy" -RetentionPolicyTagLinks "MyRetentionPolicyTag"

Use the **Set-RetentionPolicyTag** cmdlet to modify the properties of a retention tag

This example changes the comment for the AllUsers-DeletedItems retention policy tag.

Set-RetentionPolicyTag "AllUsers-DeletedItems" -Comment "Items in the Deleted Items folder will be automatically deleted in 120 days"

Use the **Write-AdminAuditLog** cmdlet to write a comment to the administrator audit log.

This example adds a comment to the administrator audit log.

Write-AdminAuditLog -Comment "Ran custom script."

Use the **New-MailboxAuditLogSearch** cmdlet to search mailbox audit logs and have search results sent via email to specified recipients

This example creates a mailbox audit log search to search Ken Kwok and April Stewart's mailboxes for administrator and delegate logons from 1/1/2015 to 12/31/2015. Search results are sent to auditors@contoso.com by email.

New-MailboxAuditLogSearch "Admin and Delegate Access" -Mailboxes "Ken Kwok","April Stewart" -LogonTypes Admin,Delegate -StartDate 1/1/2015 -EndDate 12/31/2015 -StatusMailRecipients auditors@contoso.com

Use the **New-MoveRequest** cmdlet to begin the process of an asynchronous mailbox or personal archive move. You can also check mailbox readiness to be moved by using the *WhatIf* parameter.

New-MoveRequest -Identity "**INSERT_USER_ALIAS_HERE**" -Remote -RemoteHostName **hybridserver.domainname.com** -TargetDeliveryDomain **domainname**.mail.onmicrosoft.com -RemoteCredential \$ONPREMCREDS -BadItemLimit 1000

To **monitor move requests**, run this command...

Get-MoveRequest | Get-MoveRequestStatistics

To **remove move requests**, run this command...

Get-MoveRequest | Remove-MoveRequest

Use the **Search-AdminAuditLog** cmdlet to search the contents of the administrator audit log.

This example finds all the administrator audit log entries that contain either the **New-RoleGroup** or the **New-ManagementRoleAssignment** cmdlet.

Search-AdminAuditLog -Cmdlets New-RoleGroup, New-ManagementRoleAssignment

This example returns entries in the administrator audit log of an Exchange Online organization for cmdlets run by Microsoft datacenter administrators between September 17, 2013 and October 2, 2013.

Search-AdminAuditLog -ExternalAccess \$true -StartDate 09/17/2013 -EndDate 10/02/2013

Use the **Get-OrganizationRelationship** cmdlet to retrieve settings for an organization relationship that has been created for federated sharing with other federated Exchange organizations or for hybrid deployments with Exchange Online

This example retrieves the organization relationship settings for Contoso using the *Identity* parameter.

Get-OrganizationRelationship -Identity Contoso

Use the **Get-FederationInformation** cmdlet to get federation information, including federated domain names and target URLs, from an external Exchange organization.

This example gets federation information from the domain contoso.com.

Get-FederationInformation -DomainName contoso.com

Use the **Get-SharingPolicy** cmdlet to view existing sharing policies that control how users inside your organization can share free/busy and contact information with users outside your organization..

Users can only share free/busy and contact information after federation has been configured between Exchange organizations. After that, users can send sharing invitations to the external recipients as long as those invitations

comply with the sharing policy. A sharing policy needs to be assigned to a mailbox to be effective. If a mailbox doesn't have a specific sharing policy assigned, a default policy enforces the sharing settings for the mailbox.

This example retrieves the full information for the sharing policy Fabrikam.

```
Get-SharingPolicy Fabrikam | Format List
```

Use the **Test-FederationTrust** cmdlet to verify that the federation trust is properly configured and functioning as expected.

The **Test-FederationTrust** cmdlet runs the following series of tests to ensure that federation is working as expected:

- A connection to the Microsoft Federation Gateway is established. This test ensures that communication between the local Exchange server and the Microsoft Federation Gateway is working correctly.
- Certificates are checked to ensure they're valid and can be used with the Microsoft Federation Gateway.
- A security token is requested from the Microsoft Federation Gateway. This test ensures that a token can be properly retrieved and used.

Add additional email addresses to a user in Office 365

This example shows how to add multiple SMTP addresses to a mailbox.

```
Set-Mailbox "Dan Jump" -EmailAddresses
```

```
@{add="dan.jump@northamerica.contoso.com","danj@tailspintoys.com"}
```

This example shows how to remove an email address from the mailbox of Janet Schorr.

```
Set-Mailbox "Janet Schorr" -EmailAddresses @{remove="janets@corp.contoso.com"}
```

```
Set-Mailbox "username" -WindowsEmailAddress username@domain.com
```

- In on-premises environments where the recipient is subject to email address policies (the **EmailAddressPolicyEnabled** property is set to the value True for the recipient), the *WindowsEmailAddress* parameter has no effect on the **WindowsEmailAddress** property or the primary email address value.
- In cloud environments or in on-premises environments where the recipient isn't subject to email address policies (the **EmailAddressPolicyEnabled** property is set to the value False for the recipient), the *WindowsEmailAddress* parameter updates the **WindowsEmailAddress** property and the primary email address to the same value.

Hide Mail Contact from Global Address List

```
Set-MailContact <contact alias> -HiddenFromAddressListsEnabled $true
```

This example **creates an Exchange Online mailbox** and Office 365 user account for Holly Holt. The optional parameter *ResetPasswordOnNextLogon* will require the user to reset their password the first time they sign in to Office 365.

```
New-Mailbox -Alias hollyh -Name hollyh -FirstName Holly -LastName Holt -
DisplayName "Holly Holt" -MicrosoftOnlineServicesID hollyh@corp.contoso.com -
Password (ConvertTo-SecureString -String 'P@ssw0rd' -AsPlainText -Force) -
ResetPasswordOnNextLogon $true
```

After you create a mailbox by running the previous command, an Office 365 user account is also created. You have to activate this user account by assigning a license. To assign a license in the Office 365 admin center,

Use the **New-DistributionGroup** cmdlet to create distribution groups and mail-enabled security groups.

This example creates a distribution group named ITDepartment and specifies the members.

```
New-DistributionGroup -Name "ITDepartment" -Members
```

```
chris@contoso.com,michelle@contoso.com,laura@contoso.com,julia@contoso.com
```

This example creates a mail-enabled security group named Managers without specifying any members.

```
New-DistributionGroup -Name Managers"Managers" -Type "Security"
```

Use the **New-DynamicDistributionGroup** cmdlet to create dynamic distribution groups. A dynamic distribution group queries mail-enabled objects and builds the group membership based on the results. The group membership is recalculated whenever an email message is sent to the group.

This example creates a dynamic distribution group named Marketing Group that contains all recipients who have a **Department** field that equals the strings "Marketing" or "Sales".

New-DynamicDistributionGroup -Name "Marketing Group" -IncludedRecipients "MailboxUsers,MailContacts" -ConditionalDepartment "Marketing","Sales"

This example creates a dynamic distribution group named Washington Management Team that contains all users in Washington State whose titles start with "Director" or "Manager".

New-DynamicDistributionGroup -Name "Washington Management Team" -RecipientFilter {(RecipientType -eq 'UserMailbox') -and (Title -like 'Director*' -or Title -like 'Manager*') -and (StateOrProvince -eq 'WA')}

Parameter	Description
<i>IncludedRecipients</i>	<p>The <i>IncludedRecipients</i> parameter specifies a filter that's based on the recipient type. Valid values are:</p> <ul style="list-style-type: none"> • AllRecipients This value can be used only by itself. • MailboxUsers • MailContacts • MailGroups • MailUsers • Resources This value indicates room or equipment mailboxes. <p>You can specify multiple values separated by commas. When you use multiple values, the OR Boolean operator is applied.</p> <p>You need to use this parameter when you use any of the <i>Conditional</i> parameters. You can't use this parameter with the <i>RecipientFilter</i> parameter.</p>
<i>RecipientFilter</i>	<p>The <i>RecipientFilter</i> parameter specifies an OPath filter that's based on the value of any available recipient property. You can use any available Windows PowerShell operator, and wildcards and partial matches are supported. When you use this parameter, remember the following OPath filter rules:</p> <ul style="list-style-type: none"> • Use braces { } around the whole OPath syntax string. • Include a hyphen before all operators. • In cloud-based environments, you can't use a wildcard as the the first character. For example, Sales* is allowed, but *Sales isn't allowed. <p>You can't use this parameter with the <i>IncludedRecipients</i> parameter or any of the <i>Conditional</i> parameters.</p>
<i>ConditionalCompany</i>	<p>The <i>ConditionalCompany</i> parameter specifies a filter that's based on the value of the recipient's Company property. You can specify multiple values separated by commas.</p> <p>When you use multiple values for this parameter, the OR Boolean operator is applied. You can't use this parameter with the <i>RecipientFilter</i> parameter. You need to use the <i>IncludedRecipients</i> parameter with a <i>Conditional</i> parameter.</p>
<i>ConditionalDepartment</i>	<p>The <i>ConditionalDepartment</i> parameter specifies a filter that's based on the value of the recipient's Department property. You can specify multiple values separated by commas.</p> <p>When you use multiple values for this parameter, the OR Boolean operator is applied. You can't use this parameter with the <i>RecipientFilter</i> parameter. You need to use the <i>IncludedRecipients</i> parameter with a <i>Conditional</i> parameter.</p>
<i>ConditionalStateOrProvince</i>	<p>The <i>ConditionalStateOrProvince</i> parameter specifies a filter that's based on the value of the recipient's StateOrProvince property. You can specify multiple values separated by commas.</p> <p>When you use multiple values for this parameter, the OR Boolean operator is applied. You can't use this parameter with the <i>RecipientFilter</i> parameter. You need to use the <i>IncludedRecipients</i> parameter with a <i>Conditional</i> parameter.</p>
<i>RecipientContainer</i>	<p>The <i>RecipientContainer</i> parameter specifies a filter that's based on the recipient's location in Active Directory. Valid input for this parameter is an organizational unit (OU) or domain that's visible using the Get-OrganizationalUnit cmdlet. You can use any value that uniquely identifies the OU or domain. For example:</p> <ul style="list-style-type: none"> • Name • Canonical name • Distinguished name (DN)

- GUID

If you don't use this parameter, the default value is the OU where the object was created.

Use the **Add-DistributionGroupMember** cmdlet to add a single recipient to distribution groups and mail-enabled security groups. To replace all members, use the **Update-DistributionGroupMember** cmdlet.

This example adds John Evans to the distribution group named Staff.

```
Add-DistributionGroupMember -Identity "Staff" -Member "JohnEvans@contoso.com"
```

Use the **Add-RecipientPermission** cmdlet to add SendAs permission to users in a cloud-based organization.

This example gives the user Ayla Kol SendAs permission for the mailbox Help Desk. Ayla can send messages that appear to come directly from the Help Desk mailbox.

```
Add-RecipientPermission "Help Desk" -AccessRights SendAs -Trustee "Ayla Kol"
```

This example **creates the shared mailbox** "Sales Department" and grants *Full Access* and *Send on Behalf* permissions for the security group "MarketingSG". Users who are members of the security group will be granted the permissions to the mailbox.

```
New-Mailbox -Shared -Name "Sales Department" -DisplayName "Sales Department" -
Alias Sales
Set-Mailbox -Identity Sales -GrantSendOnBehalfTo MarketingSG
Add-MailboxPermission -Identity Sales -User MarketingSG -AccessRights FullAccess
-InheritanceType All
```

This example delivers John Woods's email messages to John's mailbox and also forwards them to Manuel Oliveira's (manuel@contoso.com) mailbox.

```
Set-Mailbox -Identity "John Woods" -DeliverToMailboxAndForward $true -
ForwardingSMTPAddress manuel@contoso.com
```

Use the **Add-MailboxPermission** cmdlet to add permissions to a mailbox

This example grants Kevin Kelly full access to Terry Adams's mailbox.

```
Add-MailboxPermission -Identity "Terry Adams" -User KevinKelly -AccessRights
FullAccess -InheritanceType All
```

This example sets Tony Smith as the owner of the resource mailbox Room 222.

```
Add-MailboxPermission -Identity "Room 222" -Owner "Tony Smith"
```

This example grants the user Mark Steele Full Access permission to Jeroen Cool's mailbox and disables the auto-mapping feature.

```
Add-MailboxPermission -Identity JeroenC -User 'Mark Steele' -AccessRights
FullAccess -InheritanceType All -AutoMapping $false
```

This example **enables the archive** for Tony Smith's mailbox.

```
Enable-Mailbox "Tony Smith" -Archive
```

This example enables an archive for all user mailboxes in your organization.

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

When you run this command, the **archive mailbox name** is set to "Personal Archive – <display name>" by default.

You can also configure a different archive name when you use Windows PowerShell to enable archive mailboxes.

For example, to name archive mailboxes "In-Place Archive - <display name>" when you enable archive mailboxes for all users in your organization, run the following commands:

```
$users = Get-Mailbox -ResultSize unlimited -Filter { ArchiveStatus -Eq "None" -AND RecipientTypeDetails -eq
'UserMailbox'}
```

```
ForEach ($a in $users) {$a.ArchiveName.Add("In-Place Archive - $a")}
```

```
$users | %{Enable-Mailbox $_.Identity -Archive -ArchiveName $_.ArchiveName}
```

In the Shell, run the following command to display information about the new archive.

```
Get-Mailbox <Name> | FL Name,*Archive*
```

Use the **Add-RecipientPermission** cmdlet to add SendAs permission to users in a cloud-based organization.

This example gives the user Ayla Kol SendAs permission for the mailbox Help Desk. Ayla can send messages that appear to come directly from the Help Desk mailbox.

Add-RecipientPermission "Help Desk" -AccessRights SendAs -Trustee "Ayla Kol"

Use the **Get-CASMailbox** cmdlet to view the client access settings that are configured on mailboxes

This example returns the values of the following client access settings for the user named Jeff Hay.

- *ActiveSyncEnabled*
- *OWAEnabled*
- *PopEnabled*
- *ImapEnabled*
- *MapiEnabled*

Get-CASMailbox "Jeff Hay"

Use the **Get-MobileDeviceStatistics** cmdlet to retrieve the list of mobile devices configured to synchronize with a specified user's mailbox and return a list of statistics about the mobile devices.

This example retrieves the statistics for the mobile phone configured to synchronize with the mailbox that belongs to the user Tony Smith.

Get-MobileDeviceStatistics -Identity TonySmith

Use the **Get-ActiveSyncDevice** cmdlet to retrieve the list of devices in your organization that have active Exchange ActiveSync partnerships.

Get-ActiveSyncDevice -Identity "TonySmith"

The **Get-ActiveSyncDevice** cmdlet will be removed in a future version of Exchange. Use the **Get-MobileDevice** cmdlet instead

retrieves mailboxes with **ActiveSync partnerships** using Get-CASMailbox, and gets the full information via piping the output to Get-Mailbox.

```
$EASMailboxes = Get-CASMailbox -Filter {HasActiveSyncDevicePartnership -eq $True  
-and DisplayName -notlike "CAS_*"} | Get-Mailbox
```

In the example line below, we can see the **number of devices each user has**:

```
$EASMailboxes | Select-Object SamAccountName, DisplayName, PrimarySMTPAddress,  
@{Name="EASDeviceCount";Expression=((Get-ActiveSyncDevice -Mailbox $_.Identity).Count)} | Export-CSV  
.\EASMailboxes.csv -NoTypeInformation
```

Use the Shell to place a mailbox on Litigation Hold indefinitely

This example places the mailbox bsuneja@contoso.com on Litigation Hold. Items in the mailbox are held indefinitely or until the hold is removed.

Set-Mailbox bsuneja@contoso.com -LitigationHoldEnabled \$true

Set-Mailbox bsuneja@contoso.com -LitigationHoldEnabled \$true -LitigationHoldDuration 2555

Note:

When you place a mailbox on Litigation Hold indefinitely (by not specifying a duration period), the value for the *LitigationHoldDuration* property mailbox is set to Unlimited.

There are two types of holds available in Exchange 2016: **Litigation Hold** and **In-Place Hold**. Litigation Hold uses the LitigationHoldEnabled property of a mailbox. When Litigation Hold is enabled, all mailbox all items are placed on hold. In contrast, you can use an In-Place Hold to preserve only those items that meet that the criteria of a search query that you define by using the In-Place eDiscovery tool. You can place multiple In-Place Holds on a mailbox, but Litigation Hold is either enabled or disabled for a mailbox.

Use the **Get-HostedContentFilterPolicy** cmdlet to view the settings of content filter policies in your cloud-based organization

Use the **Set-HostedContentFilterPolicy** cmdlet to modify the settings of content filter policies in your cloud-based organization.

Use the **New-HostedContentFilterPolicy** cmdlet to create content filter policies in your cloud-based organization.

Use the **Remove-HostedContentFilterPolicy** cmdlet to remove content filter policies from your cloud-based organization

<i>EnableEndUserSpamNotifications</i>	<i>LanguageBlockList</i>	<i>MarkAsSpamNdrBackscatter</i>	<i>QuarantineRetentionPeriod</i>
<i>EnableLanguageBlockList</i>	<i>MarkAsSpamBulkMail</i>	<i>MarkAsSpamObjectTagsInHtml</i>	<i>RedirectToRecipients</i>
<i>EnableRegionBlockList</i>	<i>MarkAsSpamEmbedTagsInHtml</i>	<i>MarkAsSpamSensitiveWordList</i>	<i>RegionBlockList</i>
<i>HighConfidenceSpamAction</i>	<i>MarkAsSpamEmptyMessages</i>	<i>MarkAsSpamSpfRecordHardFail</i>	<i>AllowedSenderDomains</i>
<i>IncreaseScoreWithBizOrInfoURLs</i>	<i>MarkAsSpamFormTagsInHtml</i>	<i>MarkAsSpamWebBugsInHtml</i>	<i>AllowedSenders</i>
<i>IncreaseScoreWithImageLinks</i>	<i>MarkAsSpamFramesInHtml</i>	<i>MatchSubDomains</i>	<i>BlockedSenderDomains</i>
<i>IncreaseScoreWithNumericclps</i>	<i>MarkAsSpamFromAddressAuthFail</i>	<i>ModifySubjectValue</i>	<i>BlockedSenders</i>
<i>IncreaseScoreWithRedirectToOtherPort</i>	<i>MarkAsSpamJavaScriptInHtml</i>		

Use the **Get-MalwareFilterPolicy** cmdlet to view the malware filter policies in your organization.

Use the **Set-MalwareFilterPolicy** cmdlet to modify malware filter policies in your organization

```
Set-MalwareFilterPolicy -Identity "Contoso Malware Filter Policy" -Action DeleteMessage -
EnableInternalSenderAdminNotifications $true -InternalSenderAdminAddress admin@contoso.com
```

<i>AdminDisplayName</i>	<i>CustomFromAddress</i>	<i>EnableExternalSenderNotifications</i>
<i>BypassInboundMessages</i>	<i>CustomFromName</i>	<i>EnableInternalSenderAdminNotifications</i>
<i>BypassOutboundMessages</i>	<i>CustomInternalBody</i>	<i>EnableInternalSenderNotifications</i>
<i>CustomAlertText</i>	<i>CustomInternalSubject</i>	<i>ExternalSenderAdminAddress</i>
<i>CustomExternalBody</i>	<i>CustomNotifications</i>	<i>InternalSenderAdminAddress</i>
<i>CustomExternalSubject</i>	<i>EnableExternalSenderAdminNotifications</i>	

Use the **Set-HostedConnectionFilterPolicy** cmdlet to modify the settings of connection filter policies in your cloud-based organization

```
Set-HostedConnectionFilterPolicy "Contoso Connection Filter Policy" -IPAllowList 192.168.1.10,192.168.1.23
-IPBlockList 10.10.10.10/24,172.17.17.0/16
```

Use the **Set-MailboxJunkEmailConfiguration** cmdlet to configure the junk email rule for specific mailboxes. This example makes the following configuration changes to the junk email rule for the user named Michele Martin:

```
Set-MailboxJunkEmailConfiguration "Michele Martin" -TrustedSendersAndDomains
@{Add="contoso.com","fabrikam.com"} -BlockedSendersAndDomains @{Add="jane@fourthcoffee.com"}
```

Use the **Enable-JournalRule** cmdlet to enable an existing journal rule on a Mailbox server

Journaling can help your organization respond to legal, regulatory, and organizational compliance requirements by recording inbound and outbound email communications

This example enables the existing journal rule Brokerage Communications.

```
Enable-JournalRule "Brokerage Communications"
```

Use the **New-JournalRule** cmdlet to create a journal rule in your organization

This example creates and enables a journal rule. The rule applies to all email messages that pass through the Transport service and contain at least one recipient or sender who is a member of the brokers@contoso.com distribution list.

```
New-JournalRule -Name "Brokerage Communications" -JournalEmailAddress "Brokers Journal Mailbox" -
Scope Global -Recipient brokers@contoso.com -Enabled $true
```

By default, new journal rules are disabled unless the *Enabled* parameter is set to \$true

20/04/2016

To disable Offline OWA completely for the mailboxes using the Default OWA Policy use the following:

```
Set-OwaMailboxPolicy -Identity Default -AllowOfflineOn NoComputers
```

To disable Offline OWA for all currently present OWA policies use:

```
Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -AllowOfflineOn NoComputers
```

Exchange Online Distribution Groups

Notice

general

ownership

membership

► **membership approval**

delivery management

message approval

email options

MailTip

group delegation

Choose whether owner approval is required to join the group.

- ☒ Open: Anyone can join this group without being approved by the group owners.
- ☐ Closed: Members can be added only by the group owners. All requests to join will be rejected automatically.
- ☐ Owner approval: All requests are approved or rejected by the group owners.

Choose whether the group is open to leave.

- ☒ Open: Anyone can leave this group without being approved by the group owners.
- ☐ Closed: Members can be removed only by the group owners. All requests to leave will be rejected automatically.

Notice

general

ownership

membership

membership approval

► **delivery management**

message approval

email options

MailTip

group delegation

By default, only senders inside your organization can send messages to this group. You can also allow people outside the organization to send to this group. Choose one of the options below.

- ☒ Only senders inside my organization
- ☐ Senders inside and outside of my organization

If you want to restrict who can send messages to the group, add users or groups to the list below. Only the specified senders will be able to send to the group and mail sent by anyone else will be rejected.

+ -

All senders can send messages to this group.

Notice

general

ownership

membership

membership approval

delivery management

message approval

email options

MailTip

group delegation

☐ Messages sent to this group have to be approved by a moderator

Group moderators:

+ -

If you don't select a moderator, the group owner will review and approve messages.

Senders who don't require message approval:

+ -

You can select senders who can send messages to the group without message approval.

Notice

general

ownership

membership

membership approval

delivery management

message approval

email options

MailTip

▶ group delegation

Send As

The Send As permission allows the delegate to send email from this group. From the recipient's perspective, the email is sent by this group.

+ -

DISPLAY NAME ▲

Send on Behalf

The Send on Behalf permission allows the delegate to send email on behalf of this group.

+ -





DISPLAY NAME ▲

Exchange admin center

- dashboard
- recipients
- permissions
- compliance management
- organization
- protection

malware filter connection filter spam filter outbound spam quarantine dkim

Review items in your quarantine. You can release one or more messages to either selected users or to all users. If an item was incorrectly detected as spam, you can also report it as a false positive.
Tip: To select multiple messages for release, you can hold down CTRL and click multiple messages or use the [CTRL + A] to select all.

SENDER	SUBJECT	RECEIV...	EXPIRES
--------	---------	-----------	---------

Malware Filter:

Default

Enabled

Relative priority: Lowest

Summary

Malware detection response:
Delete the entire message

Sender notifications:
Notify internal senders
Notify external senders




Administrator notifications:
Undelivered messages from internal senders
Undelivered messages from external senders

Customized notification text:
Configured

Connection filter:




connection filtering

IP Allow list
Always accept messages from the following IP addresses.

Allowed IP Address
192.168.180.2/26

IP Block list
Always block messages from the following IP addresses.

Blocked IP Address
10.23.45.78

SPAM Filter:

Default

▶ general

spam and bulk actions

block lists

allow lists

international spam

advanced options

spam and bulk actions

Select the action to take for incoming spam and bulk email. [Learn more](#)

Spam:

Move message to Junk Email folder

High confidence spam:

Move message to Junk Email folder

Bulk email:

☒ Mark bulk email as spam

Select the threshold. 1 marks the most bulk email as spam and 9 allows the most bulk email to be delivered.

7 (Default) ▼

Quarantine

Retain spam for (days):

15

*Add this X-header text:

*Prepend subject line with this text:

*Redirect to this email address:

block lists

Sender block list

Always mark email from the following senders as spam.

+  -

BLOCKED SENDER

Domain block list

Always mark email from the following domains as spam.

+  -

BLOCKED DOMAIN

allow lists

Sender allow list

Always deliver email from the following senders to the inbox.

+  -

ALLOWED SENDER

Domain allow list

Always deliver email from the following domains to the inbox.

+  -

ALLOWED DOMAIN

international spam

☒ Filter email messages written in the following languages

+ -

CODE	LANGUAGE
AF	Afrikaans

☒ Filter email messages sent from the following countries or regions

+ -

CODE	REGION
UA	Ukraine

advanced options

Increase Spam Score

Specify whether to increase the spam score for messages that include these types of links or URLs.

Image links to remote sites:

Off ▼

Numeric IP address in URL:

Off ▼

URL redirect to other port:

Off ▼

URL to .biz or .info websites:

Off ▼

Mark as Spam

Specify whether to mark messages that include these properties as spam.

Empty messages:

Off ▼

JavaScript or VBScript in HTML:

Off ▼

Frame or IFrame tags in HTML:

Off ▼

Object tags in HTML:

Off ▼

Embed tags in HTML:

Off ▼

Form tags in HTML:
 ▼

Web bugs in HTML:
 ▼

Apply sensitive word list:
 ▼

SPF record: hard fail:
 ▼

Conditional Sender ID filtering: hard fail:
 ▼

NDR backscatter:
 ▼

Test Mode Options
 Configure the test mode options for when a match is made to a test-enabled advanced option.

☒ None
☐ Add the default test X-header text
☐ Send a Bcc message to this address:

SPF record: hard fail	<p>When this setting is enabled, messages that fail an SPF check (meaning they were sent from an IP address not specified in the SPF record) will be marked as spam. Turning this setting on is recommended for organizations who are concerned about receiving phishing messages.</p> <p>Note: Test mode is not available for this option.</p>
Conditional Sender ID filtering: hard fail	<p>When this setting is enabled, any message that hard fails a conditional Sender ID check is marked as spam. This option combines an SPF check with a Sender ID check to help protect against message headers that contain forged senders.</p> <p>Note: Test mode is not available for this option.</p>
NDR backscatter	<p>If you're using EOP to protect on-premises mailboxes, when this setting is enabled, all legitimate non-delivery report (NDR) messages are delivered to the original sender, and all backscatter (illegitimate NDR) messages will be marked as spam. If you don't enable this setting, then all NDRs still go through spam filtering. In this case, most legitimate messages will get delivered to the original sender while some, but not all, backscatter messages will get marked as spam. However, backscatter messages that aren't marked as spam won't go to the original sender because it will go to the spoofed sender.</p> <p>If you're using the service to protect Exchange Online cloud-hosted mailboxes, you don't need to configure this setting.</p>

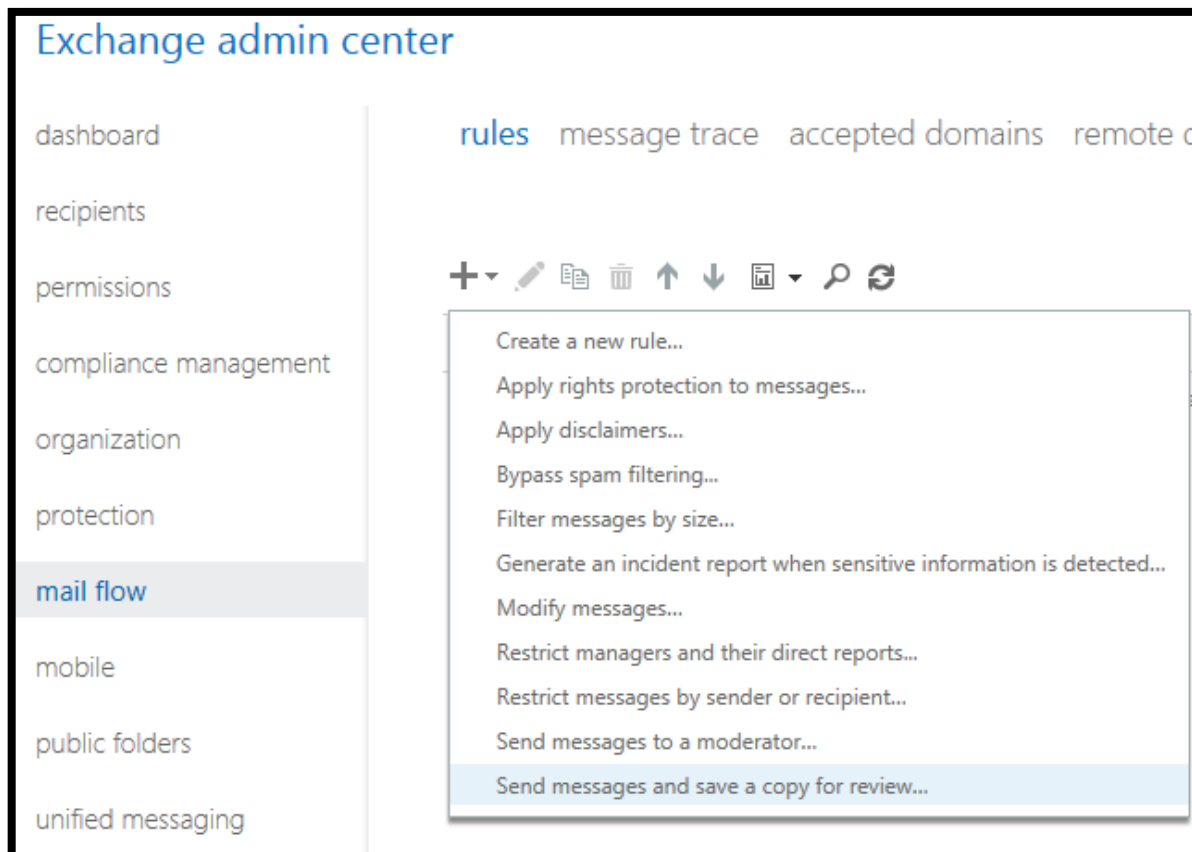
Outbound SPAM

outbound spam preferences

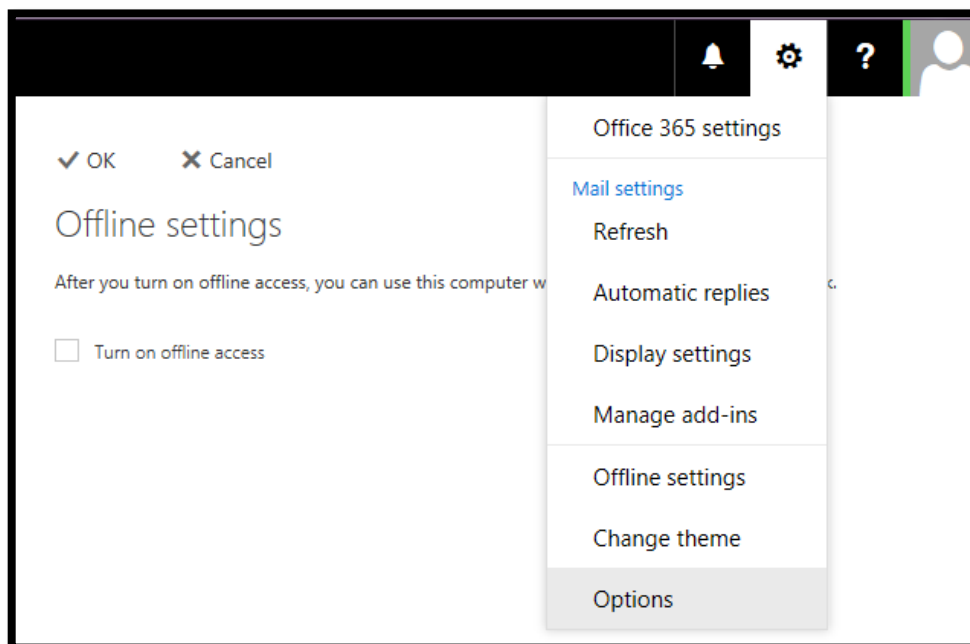
☒ Send a copy of all suspicious outbound email messages to the following email address or addresses.

☒ Send a notification to the following email address or addresses when a sender is blocked for sending outbound spam.

Exchange mail flow rules



OWA Offline settings:



Offline access in Outlook Web App for Exchange 2013 lets users use Outlook Web App even when not connected to a network.

Offline access is newly available in Outlook Web App on the following web browsers.:

- Internet Explorer 10
- Safari 5 or greater (supported on Mac desktops only)
- Chrome

What data is available offline?**Mail**

- Users will be able to see all their folders, and content in all offline-supported folders.
- Offline-supported folders include:

- Inbox
- Drafts
- Any folder viewed from the browser in the last week
- For each offline-supported folder, users will have 3 days of content or 150 items, whichever is larger.
- Attachments are not available when offline.

Calendar

- Reminders will pop-up for meetings and appointments
- Current month and upcoming year of calendar
- Multiple calendars are not available when offline

People

- All Contacts
- Anyone the user emails often or has emailed recently
- The Auto-Complete cache (the list of matching names that appear as someone is added to a message)

Skype for Business

Meeting limits across Office 365 options

Feature	Office 365 Enterprise
File upload limit [Meetings]	500 MB
File transfer limit [P2P]	No limit
Participants in a Skype for Business meeting	250
Presenters in a Skype for Business meeting	250
Skype for Business web app meeting participants	250
Skype for Business web app anonymous participants	250
Guests joining by phone	250
Individuals in a team-call group	25
Meeting content retention	15 Days
Meeting expiration	14 Days

Server Options:

Skype for Business admin center

dashboard

users

organization

dial-in conferencing

meeting invitation

tools

general external communications

presence privacy mode

By default, anyone who can communicate with one of your users can also see that user's presence information. You can make presence information for all users available only to their contacts. Individual users can later change this setting themselves using Skype for Business. [Learn more](#)

☒ Automatically display presence information
☐ Display presence information only to a user's contacts

mobile phone notifications

You can turn on alerts for incoming instant messages (IMs), voice mail messages, and missed IMs or missed calls for Skype for Business Mobile users by using a push notification service instead of Microsoft Office 365 to send those alerts. Depending on your supported mobile devices, you can use the Microsoft Push Notification Service, the Apple Push Notification Service, or both. [Learn more](#)

☒ Microsoft Push Notification Service
☒ Apple Push Notification Service

save

cancel

Skype External communications options:

The screenshot shows the 'Skype for Business admin center' with the 'external communications' tab selected. The left sidebar lists navigation options: dashboard, users, organization (selected), dial-in conferencing, meeting invitation, and tools. The main content area is titled 'external access' and includes a dropdown menu set to 'On only for allowed domains'. Below this is a section for 'public IM connectivity' with a checkbox 'Let people use Skype for Business to communicate with Skype users outside your organization.' which is unchecked. At the bottom, there is a table for 'blocked or allowed domains' with columns for DOMAIN and STATUS. The table contains one entry: 'test.com' with status 'Allowed'.

Office 365 | Admin

Skype for Business admin center

dashboard
users
organization
dial-in conferencing
meeting invitation
tools

general external communications

external access

You can control access to Skype for Business users in other organizations in two ways: 1) block specific domains, 2) allow access for everyone else. [Learn more](#)

On only for allowed domains

public IM connectivity

☐ Let people use Skype for Business to communicate with Skype users outside your organization.

blocked or allowed domains

DOMAIN	STATUS
test.com	Allowed

This close-up shows the 'external access' dropdown menu. The text above the menu reads: 'You can control access to Skype for Business users in other organizations in two ways: 1) block specific domains, 2) allow access for everyone else. [Learn more](#)'. The dropdown menu is open, showing four options: 'On only for allowed domains' (selected), 'Off completely', 'On except for blocked domains', and 'On only for allowed domains'.

external access

You can control access to Skype for Business users in other organizations in two ways: 1) block specific domains, 2) allow access for everyone else. [Learn more](#)

On only for allowed domains
Off completely
On except for blocked domains
On only for allowed domains

The screenshot shows the 'Skype for Business admin center' with the 'dial-in conferencing' tab selected. The left sidebar lists navigation options: dashboard, users, organization, dial-in conferencing (selected), meeting invitation, and tools. The main content area is titled 'Microsoft bridge' and includes links for 'Microsoft bridge settings' and 'third-party provider'. Below this is a section titled 'How to give users a Microsoft conferencing bridge' with a message stating 'Your organization is not currently enabled for Skype for Business Dial-in Conferencing.' It then explains that when enabled, users will have a Microsoft conferencing bridge for dialing into meetings. A list of features for the Microsoft conferencing bridge is provided: Consolidated billing, Fast-and-easy setup, and Local and international dial-in conferencing numbers. A final paragraph states that the Microsoft conferencing bridge is a great solution for dial-in conferencing needs, followed by a 'Learn more' link.

Skype for Business admin center

dashboard
users
organization
dial-in conferencing
meeting invitation
tools

Microsoft bridge Microsoft bridge settings third-party provider dial-in users

How to give users a Microsoft conferencing bridge

Your organization is not currently enabled for Skype for Business Dial-in Conferencing.

When you're enabled for Skype for Business Dial-in conferencing, you will have a Microsoft conferencing bridge that can be used by participants to dial in to a meeting using either their mobile or wired phone.

A Microsoft conferencing bridge offers:

- Consolidated billing
- Fast-and-easy setup
- Local and international dial-in conferencing numbers

A Microsoft conferencing bridge is a great solution for your organization's dial-in conferencing needs.

[Learn more](#)

Skype for Business admin center

dashboard

users

organization

dial-in conferencing

meeting invitation

tools

You can customize Skype for Business meeting invitations to meet your organization's needs. You can add your own logo. You can replace the default URL for Skype for Business meeting support with the URL of your organization's support website if you have one. You can also add legal disclaimers by providing the link to a website with this information or by including the text directly in the meeting invitation. [Learn more](#)

Logo URL:

Help URL:

Legal URL:

Footer text:

save

cancel

Skype for Business admin center

dashboard

users

organization

dial-in conferencing

meeting invitation

tools

You can use the tools to manage or troubleshoot the Skype for Business Online service for your organization.

[Troubleshooting Skype for Business Online sign-in for administrators](#)

Diagnoses and resolves Skype for Business Online sign-in issues.

[Skype for Business Connectivity Analyzer tool](#)

Determines whether your Office 365 setup meets the requirements to make connections from mobile devices that have Skype for Business apps installed.

[Microsoft Remote Connectivity Analyzer](#)

Tests connectivity to the Office 365 DNS servers.

[Setting up Skype for Business Online external communications](#)

Sets up Skype for Business Online external communications to let your Skype for Business users IM and talk with Skype users and Skype for Business contacts in other organizations.

[Skype for Business Online Call Quality Dashboard](#)

Displays call quality information for troubleshooting network issues that can impact call quality.

User Options:

pas bad

general
external
communications
dial-in conferencing

Options

Select the Skype for Business features you would like this user to have. [Learn more](#)

Audio and video:

Audio and HD video

☒ Record conversations and meetings

☐ For compliance, turn off non-archived features

save cancel

pas bad

general
external
communications
dial-in conferencing

Options

Choose people outside your organization that the user can communicate with. [Learn more](#)

☒ External Skype for Business users

☒ External Skype users

save cancel

pas bad

general
external
communications
dial-in conferencing

Properties

Provider name:

None

save cancel

Set up your network for Skype for Business Online

Purpose	Source IP	Destination IP	Source Port	Destination Port
SIP signaling	Client	Office 365	Ephemeral TCP ports	TCP 443
Persistent Shared Object Model (PSOM) connections web conferencing	Client	Office 365	Ephemeral TCP ports	TCP 443
HTTPS downloads	Client	Office 365	Ephemeral TCP ports	TCP 443
Audio	Client	Office 365	TCP/UDP 50,000-50019	TCP 443, UDP 3478, TCP/UDP 50,000-59,999
Video	Client	Office 365	TCP/UDP 50,020-50039	TCP 443, UDP 3478, TCP/UDP 50,000-59,999
Desktop sharing	Client	Office 365	TCP/UDP 50,040-50059	TCP 443, TCP 50,000-59,999
Skype for Business push notifications for Lync Mobile 2010 on iOS devices. You don't need this for Android, Nokia Symbian or Windows Phone mobile devices.	Client	Office 365	Ephemeral TCP ports	TCP 5223

What is Skype for Business Web App?

Skype for Business Web App is a browser-based meeting client that you use to join Skype for Business meetings. You can't schedule a meeting from Skype for Business Web App but can join a meeting that was scheduled using either Microsoft Outlook or Skype for Business Web Scheduler.

Tip: If your organization is using Microsoft Lync 2010 and you want information about using Lync Web App for 2010, see Quick Start: Participate in online meetings with Lync Web App.

You don't need to download or install any apps to join a meeting with Skype for Business Web App. Just select **Join Skype Meeting** in the email or calendar meeting request you received. If the computer you're using doesn't have Skype for Business installed, a browser window opens and you can join the meeting.

Comparison with other Skype for Business clients

Skype for Business Web App is intended to provide only a rich meeting experience. It doesn't offer any other Skype for Business features, such as instant messaging, presence, and contact information.

Skype For Business PowerShell

Enables or disables **push notification**. Push notifications enable people using Apple iPhones or Windows Phones to receive notifications about events even when Lync is suspended or running in the background.

Get-CsPushNotificationConfiguration

Set-CsPushNotificationConfiguration

The command shown in Example 1 disables push notifications from the Apple Push Notification Service for the Redmond site.

Set-CsPushNotificationConfiguration -Identity "site:Redmond" -EnableApplePushNotificationService \$False

Get-CsTenant

Returns information about your tenant account. Tenants are groups of users who have accounts homed on Skype for Business Online. Most organizations will have only a single tenant in which to house all their user accounts, although, in some cases, an organization manages multiple tenants.

Get-CsTenantLicensingConfiguration

Indicates whether licensing information is displayed in the Skype for Business Online admin center.

Get-CsOnlineUser

Returns information about users who have accounts homed with your Skype for Business Online tenant.

Information is returned for a single online user: the user with the SIP address "sip:kenmyer@litwareinc.com".

```
Get-CsOnlineUser -Identity "sip:kenmyer@litwareinc.com"
```

Set-CsUserAcp

cmdlet is used to assign a new audio conferencing provider to the user Ken Myer. To do this, the Identity parameter is used to indicate the user account to be modified. In addition, the required parameters TollNumber, ParticipantPassCode, Domain, and Name are included, along with the appropriate parameter values.

```
Set-CsUserAcp -Identity "Ken Myer" -TollNumber "14255551298" -ParticipantPassCode 13761 -Domain "fabrikam.com" -Name "Fabrikam ACP"
```

Set-CsUser

Modifies Skype for Business Server 2015 properties for an existing user account

AudioVideoDisabled is the only parameter that you can use together with the **Set-CsUser** cmdlet in **Skype for Business Online**. Depending on what you were trying to do, you may be able to complete the same task by using other available cmdlets.

Client policies are used to determine the Lync client features that are available to users. For example, you might give the capability to transfer files to some users, but not to others.

```
Get-CsClientPolicy
```

```
Set-CsClientPolicy
```

```
Grant-CsClientPolicy
```

the client policy SalesPolicy is assigned to the user with the Identity Ken Myer.

```
Grant-CsClientPolicy -Identity "Ken Myer" -PolicyName SalesPolicy
```

three different property values are modified for the client policy RedmondClientPolicy: the properties DisableEmoticons, DisableHtmlIm, and DisableRTFIm are all set to True.

```
Set-CsClientPolicy -Identity RedmondClientPolicy -DisableEmoticons $True -DisableHtmlIm $True -DisableRTFIm $True
```

Conferencing policies determine the features and capabilities that can be used in a conference. This includes everything from whether the conference can include IP audio and video to the maximum number of people who can attend a meeting.

```
Get-CsConferencingPolicy
```

```
Grant-CsConferencingPolicy
```

In Example 1, the **Grant-CsConferencingPolicy** cmdlet is used to assign the policy SalesConferencingPolicy to the user with the Identity "Ken Myer".

```
Grant-CsConferencingPolicy -identity "Ken Myer" -PolicyName SalesConferencingPolicy
```

modifies a property value of the conferencing policy SalesConferencingPolicy; in particular, the command sets the value of the AllowConferenceRecording property to False. To do this, the **Set-CsConferencingPolicy** cmdlet is called along with the Identity parameter and the AllowConferenceRecording parameter.

```
Set-CsConferencingPolicy -Identity SalesConferencingPolicy -AllowConferenceRecording $False
```

External access policies are used to determine whether your users are allowed to communicate with users from federated domains, and/or whether your users are allowed to communicate with users who have accounts on public IM providers, such as Windows Live or AOL.

```
Get-CsExternalAccessPolicy
```

```
Grant-CsExternalAccessPolicy
```

modifies the per-user external access policy that has the Identity RedmondExternalAccessPolicy. In this example, the command changes the value of the EnableFederationAccess property to True.

Set-CsExternalAccessPolicy -Identity RedmondExternalAccessPolicy -EnableFederationAccess \$True

<i>EnableFederationAccess</i>	Indicates whether the user is allowed to communicate with people who have SIP accounts with a federated organization. The default value is False.
<i>EnableOutsideAccess</i>	Indicates whether the user is allowed to connect to Lync Server over the Internet, without logging on to the organization's internal network. The default value is False.
<i>EnablePublicCloudAccess</i>	Indicates whether the user is allowed to communicate with people who have SIP accounts with a public Internet connectivity provider such as MSN. The default value is False.
<i>EnablePublicCloudAudioVideoAccess</i>	Indicates whether the user is allowed to conduct audio/video conversations with people who have SIP accounts with a public Internet connectivity provider such as MSN. When set to False, audio and video options in Lync will be disabled any time a user is communicating with a public Internet connectivity contact. The default value is False.

Voice policies are used to manage Enterprise Voice features, as simultaneous ringing (the ability to have a second phone ring each time someone calls your office phone) and call forwarding.

Get-CsVoicePolicy

Grant-CsVoicePolicy

Remove-CsVoicePolicy

Cmdlet	Description
Get-CsImFilterConfiguration	Retrieves information about the URI restrictions in use in your organization. When sending instant messages, users can embed a URI within the text of that message that refers other participants in the conversation to a particular website or share. Skype for Business Online can be configured so that hyperlinks with certain prefixes are blocked or are not active. This helps to ensure that participants can't click the link and go to the site the URI refers to. Instead, they must copy and paste the link manually into a browser.
Get-CsPresencePolicy	Returns information about two important aspects of presence subscriptions: prompted subscribers and category subscriptions. When you are added to someone's Contact list, the default behavior is for you to receive a pop-up notification informing you that you've been added to that list. Until you dismiss the pop-up, each notification counts as a prompted subscriber. Category subscriptions represent a request for a specific category of information—for example, an application that requests calendar data.
Get-CsPrivacyConfiguration Set-CsPrivacyConfiguration	Configures default privacy values in Skype for Business Online, while still giving users the option to change these values. Skype for Business Online gives users the opportunity to share a wealth of presence information with other people. Users can publish a photograph of themselves, provide detailed location information, and have presence information automatically available to everyone in the organization (instead of only to people on their Contacts list). CsPrivacyConfiguration cmdlets enable administrators to configure default privacy values in Skype for Business Online, while still allowing users the option to change these values.
Cmdlet	Description
Get-CsExUmContact New-CsExUmContact	Creates and manages contact objects used for Auto Attendant and Subscriber Access services, when Exchange UM is a hosted service.

Remove-CsExUmContact Set-CsExUmContact	Skype for Business Online works with Exchange UM to provide several voice-related capabilities, including Auto Attendant and Subscriber Access. Auto Attendant provides a way for calls to automatically be answered and routed to the correct person. Subscriber Access enables users to connect to Exchange UM and retrieve email, voice messages, contacts, and calendar information. When Exchange UM is provided as a hosted service, contact objects used for the Auto Attendant and Subscriber Access services must be created by using Windows PowerShell. These objects are created and managed by using the CsExUmContact cmdlets.
Get-CsHostedVoicemailPolicy Grant-CsHostedVoicemailPolicy	Manages hosted voicemail policies used in the organization. Hosted voicemail policies specify how unanswered calls are routed to the Exchange UM service. These policies affect only users who have been enabled for Exchange UM hosted voicemail. To verify whether a user is enabled for hosted voicemail, run a command similar to this from the Windows PowerShell prompt: Get-CsOnlineUser -Identity "kenmyer@litwareinc.com" Select-Object HostedVoiceMail
Cmdlet	Description
New-CsEdgeAllowAllKnownDomains	Allows users to communicate with all domains except for those specified on the blocked domains list. Federation is a service that enables users to exchange IM and presence information with users from other domains. Typically, administrators use allowed and blocked lists to specify the outside domains that users can communicate with.
New-CsEdgeAllowList	Limits user communication to a specified collection of domains. Users will be allowed to communicate only with domains that appear on the allowed domains list.
New-CsEdgeDomainPattern	Modifies the allowed or blocked domain lists.
Get-CsTenantFederationConfiguration Set-CsTenantFederationConfiguration	Enables and disables federation with other domains and federation with public providers.
Get-CsTenantHybridConfiguration Set-CsTenantHybridConfiguration	Assigns the appropriate values to hybrid configuration settings. In a hybrid or "split domain" deployment, an organization has some users with accounts homed on Skype for Business Online while simultaneously having other users with accounts homed on Lync Server 2013. By default, users homed on Skype for Business Online do not have access to the complete range of capabilities offered by Enterprise Voice. To provide Skype for Business Online users with access to these Enterprise Voice capabilities, administrators need to assign the appropriate values to hybrid configuration settings. These values can be managed only by using the CsTenantHybridConfiguration cmdlets.
Get-CsTenantPublicProvider Set-CsTenantPublicProvider	Manages federation with public providers. Public providers are organizations that provide SIP communication services for the general public. When you establish a federation relationship with a public provider, you effectively establish federation with any user who has an account hosted by that provider.
Cmdlet	Description
Disable-CsMeetingRoom Enable-CsMeetingRoom Get-CsMeetingRoom Set-CsMeetingRoom	Manages endpoint devices for meeting rooms. In Skype for Business Online, meeting rooms are self-contained computer appliances that are installed in conference rooms and supply advanced meeting capabilities. To manage these new endpoint devices you must, among other things, create and enable an Exchange resource mailbox

	account for the device, and then enable that resource account for Skype for Business Online.
Get-CsAudioConferencingProvider	Returns information about the audio conferencing providers that your organization is contracted with. An audio conferencing provider is a third-party company that provides organizations with conferencing services, including high-end services such as live translation, transcription, and live per-conference operator assistance.

Set-CsMeetingConfiguration enables you to modify the meeting configuration settings currently in use in your organization. Meeting configuration settings help dictate the type of meetings (also called conferences) that users can create, and also control how (or even if) anonymous users and dial-in conferencing users can join these meetings. Note that these settings only affect scheduled meetings; they do not affect ad-hoc meetings created by clicking the Meet Now option in Skype for Business

Set-CsMeetingConfiguration -Identity site:Redmond -DesignateAsPresenter Everyone

Get-CsMeetingConfiguration | Where-Object {\$_.AdmitAnonymousUsersByDefault -eq \$False} | Set-CsMeetingConfiguration -PstnCallersBypassLobby \$True

Parameter	Description
<i>AdmitAnonymousUsersByDefault</i>	Determines whether meetings will, by default, allow attendance by anonymous users (that is, by unauthenticated users). Set this value to True if you would like new meetings to allow for attendance by anonymous users by default. Set this value to False if you would prefer that, by default, new meetings do not allow for attendance by anonymous users. The default value is True.
<i>AssignedConferenceTypeByDefault</i>	Determines whether new meetings will be configured, by default, as public meetings. Set this value to True to use public meetings by default; set this value to False to use private meetings by default. The default value is True.
<i>CustomFooterText</i>	Text to be used on custom meeting invitations.
<i>DesignateAsPresenter</i>	Indicates which users (besides the meeting organizer) are automatically designated as presenters when they join a meeting. Valid choices are: None; Company; and Everyone. By default, DesignateAsPresenter is set to Company, meaning everyone in your organization will have presenter rights the moment they join a meeting.
<i>EnableAssignedConferenceType</i>	Indicates whether users are allowed to schedule public meetings. With a public meeting, the conference ID and the meeting link remain consistent each time the meeting is held. With a private meeting, the conference ID and meeting link change from meeting to meeting. The default value is True.
<i>HelpURL</i>	URL to a website where users can obtain assistance on joining the meeting.
<i>Identity</i>	Indicates the unique identifier for the collection of meeting configuration settings you want to modify. To refer to the global settings, use this syntax: -Identity global. To refer to a collection configured at the site scope, use syntax similar to this: -Identity "site:Redmond". Settings configured at the service scope can be referenced using syntax like this: -Identity "service:UserServer:atl-cs-001.litwareinc.com". If this parameter is not specified, then the Set-CsMeetingConfiguration cmdlet will modify the global settings.
<i>LegalURL</i>	URL to a website containing legal information and meeting disclaimers.

<i>LogoURL</i>	URL for the image to be used on custom meeting invitations.
<i>PstnCallersBypassLobby</i>	Indicates whether users dialing in over a public switched telephone network (PSTN) phone line should automatically be admitted to a meeting. If set to True (\$True), PSTN callers will automatically be admitted to the meeting. If set to False (\$False), then PSTN callers will initially be routed to the conference lobby. At that point, they will have to wait, on hold, until a conference presenter grants them access to the meeting. The default value is True.
<i>RequireRoomSystemsAuthorization</i>	When set to True (\$True) all users must be authenticated before they can join a meeting using the Skype for Business Room System. The default value is False (\$False).

Update-CsTenantMeetingUrl Updates the meeting URL for the specified Lync Online tenant. The updated URL uses a simpler, more standardized format that makes it easier for clients to locate and connect to meetings. suppose the organization undergoes some changes and decides to use the “vanity” URL litwareinc.com instead of the onmicrosoft.com URL. The organization modifies their user email addresses to use the litwareinc.com domain. However, meeting URLs will still use the old domain name:https://meet.lync.com/contoso/user1/45GZFH99 To fix this problem, administrators should run the Update-CsTenantMeetingUrl cmdlet. That will replace the old meeting URL with a new one that features the vanity URL
instead:https://meet.lync.com/litwareinc.com/user1/37JYLP71
Update-CsTenantMeetingUrl -Tenant "38aad667-af54-4397-aaa7-e94c79ec2308" -Force

Change Skype for Business SIP address

Set-mailbox <user name> -EmailAddress @("SMTP: zzz@domain.com";"SIP: zzz@domain.com")

	SharePoint Server		SharePoint Online	
	Standard	Enterprise	Plan 1	Plan 2
	Licensing options	Try now Licensing options	\$5.00 user/month Buy now	\$10.00 user/month Buy now
Apps				
App Catalog and Marketplace				
Collaboration				
Team Sites				
Work Management				
External Sharing				
Search				
Basic Search				
Standard Search				
Enterprise Search				
Content Management				
Content Management				
Records Management				
E-discovery, ACM, Compliance				
Business Intelligence				
Excel Services, PowerPivot, PowerView				
Scorecards & Dashboards				
Business Solutions				
Access Services				
Visio Services				
Form Based Application				
SharePoint 2013 Workflow				
Business Connectivity Services				
New capability: Included:				

SharePoint 2013 Social and Yammer – Feature Overview

SharePoint 2013 Social

Personal Context

- **User Profiles** - Privacy Settings and Organization Browser
- **My News Feed** – Microblogging – Posts, Replies, Likes, Follow Up, Mentions, Hashtags, Company Feed
- **Following & Suggestions** – Documents, Tags, People, and Sites
- **My Documents** – Sky Drive Pro, Windows 8 Mobile & Desktop App
- **My Tasks** – Aggregated View
- **Mobility** - No Mobile Apps for On-Premises, Windows 8 Phone available for Office 365

Business Context

- **Community Sites** - for dedicated Knowledge Groups, Security Trimmed
- **Discussion Forums** - Categories, Best Reply, Q/A, Moderation
- **Site Feed** – Site specific Microblogging
- **Basic Gamification Features** – Reputation Points, Badging, and Top Contributors

- Integrated with SharePoint Search
- Extensibility Points – SSOM, CSOM, REST API

Yammer.com

- **Yammer Groups Feed** – Structured Microblogging & default company feed - Posts, Attachments, Replies, Likes, Q/A, Polls, Praises, Mentions
- **External Networks**
- **Following** – People, Groups
- **Suggestions** – People (Groups coming soon)
- **Extensibility Points** - Open Graph, Yammer Embed, and REST API
- **Mobile Apps** – iOS, Android, and Windows Platform
- **Corporate Communication** - Direct Message, Instance Messaging
- **Missing Features** - No Personal Feed, No Gamification, and No Moderation

SharePoint Admin centre

SharePoint admin center

site collections

infopath

user profiles

bcs

term store

records management

search

secure store

apps

settings

Site Collections

New Delete Properties Owners Sharing Buy Storage Server Resource Quota Upgrade Recycle Bin Restore

Contribute Manage

Search by URL...

5600 resources available

1.01 TB available of 1.01 TB

<input type="checkbox"/>	URL	STORAGE USED (GB)	SERVER RESOURCE QUOTA	VERSION
<input checked="" type="checkbox"/>	https://o347.sharepoint.com	0.00	300	2013
	https://o347.sharepoint.com/portals/hub	0.00	0	2013
	https://o347.sharepoint.com/search	0.03	0	2013
	https://o347.sharepoint.com/sites/CompliancePolicyCenter	0.00	0	2013
	https://o347-my.sharepoint.com	0.00	0	2013

Manage Site collection administrators

manage administrators

Primary Site Collection Administrator
Specify the administrator for this site collection. Only one user login can be provided; security groups are not supported.

User name:

Site Collection Administrators
Site Collection Administrators are given full control over all Web sites in the site collection. They may also receive site use confirmation mail. Enter users separated by semicolons.

Site Sharing settings

SharePoint admin center

site collections

sharing

Sharing outside your company
Control how users invite people outside your organization to access content

☐ Don't allow sharing outside your organization

☐ Allow external users who accept sharing invitations and sign in as authenticated users

☒ Allow sharing with all external users, and by using anonymous access links

Allowing non-owners to invite new users

Status: Allowed. This is the default setting for new sites.

Some sites in this site collection allow non-owners to grant permission to files, folders, or sites and sub-sites without requiring owner approval. [Learn more](#)

[Turn off sharing for non-owners on all sites in this site collection.](#)

Document library sharing

Home EDIT LINK

DocLibrar

+ New Upload

All Documents ...

✓	File Name
✓	test1
	test2

Share 'test1'

Shared with lots of people

Open to anyone with a guest link

Invite people

Get a link

Shared with

Enter names or email addresses...

Can edit

Include a personal message with this invitation (Optional).

☒ Require sign-in

HIDE OPTIONS

☒ Send an email invitation

Share Cancel

DocLibrar

+ New Upload

All Documents ...

✓	File Name
✓	test1
	test2

Share 'test1'

Shared with lots of people

Open to anyone with a guest link

Invite people

Get a link

Shared with

Edit link - no sign-in required

Restricted link - Only specific people can open this link (created)

View link - lucas account required (created)

Edit link - lucas account required (created)

View link - no sign-in required

Edit link - no sign-in required (created)

REMOVE

Close

[BROWSE](#)
[ACCESS REQUESTS](#)

Resend
 Withdraw

Approve
 Decline

Check Permissions

[Invitations](#)
[Requests](#)
[Check](#)

[Home](#)
[Notebook](#)
[Documents](#)
[Recent](#)
[DocLibrary](#)
[Site Contents](#)
[Recycle Bin](#)

[EDIT LINKS](#)

PENDING REQUESTS

[Modify this View](#)
[Create View](#)

☒ Person
 ☐ Request for
 ☐ Requested on
 ☐ Approve/Decline

You are all up to date! There are no requests pending.

EXTERNAL USER INVITATIONS

[Modify this View](#)
[Create View](#)

<input checked="" type="checkbox"/>	Person	Permission	Requested on	Status	Request for
<input checked="" type="checkbox"/>	pasan_@gmail.com	Contribute	11 minutes ago	Pending(Expires in 90 days)	test2

20/04/2016

Limits in SharePoint Online in Office 365 plans

FEATURE	OFFICE 365 ENTERPRISE PLANS (INCLUDING E1-E4, E2-E4, G1-G4, AND SHAREPOINT ONLINE PLAN 1 AND PLAN 2
Storage per user (contributes to total storage base of tenant)	0.5 GB per subscribed user.
Storage base per tenant	1 TB + .5 GB per subscribed user + additional storage purchased. You can purchase an unlimited amount of additional storage.
Additional storage (per GB per month); no minimum purchase	To buy storage, see Change storage space for your subscription .
List view threshold limit in site libraries or lists	You can view up to 5,000 items in site document libraries or lists. To view anything more than this, see Manage large lists and libraries in Office 365 .
Site collection storage limit	Up to 1 TB per site collection.
Site collections (#) per tenant	500,000 site collections (other than personal sites).
Subsites	Recommended up to 2,000 subsites per site collection
Office 365 Groups file storage	Group files storage has the same storage and upload limits as a site collection storage limit above.
Public Website storage default	5 GB A SharePoint admin can allocate up to 1 TB (the limit for a site collection).
File upload limit	10 GB per file.
Sync limits	5,000 items in site libraries, including files and folders.
Maximum number of users per tenant	1 – 500,000+ Note: If you have more than 500,000 users, please contact a Microsoft representative to discuss detailed requirements.
Number of external user invitees	There is no limit to number of external users you can invite to your SharePoint Online site Collections.

Suggested uses for SharePoint groups

The following table describes the SharePoint groups that are created when you use a standard site template to create a site. The table also provides suggested uses for each group.

Group Name	Permission level)	Use this group for:
Approvers	Approve	Members of this group can edit and approve pages, list items, and documents.
Designers	Design	Members of this group can edit lists, document libraries, and pages in the site. Designers can create Master Pages and Page Layouts in the Master Page Gallery and can change the behavior and appearance of each site in the site collection by using master pages and CSS files..
Hierarchy Managers	Manage Hierarchy	Members of this group can create sites, lists, list items, and documents.
Owners	Full Control	People who must be able to manage site permissions, settings, and appearance.
Members	Edit or Contribute	People who must be able to edit site content. Permission level depends on the site template that was used to create the site
Visitors	Read	People who must be able to see site content, but not edit it.

Restricted Readers	Restricted Read	People who should be able to view pages and documents but not view versions or permissions.
Style Resource Readers	Restricted Read	People in this group have Limited Access to the Style Library and Master Page Gallery.
Quick Deploy Users	Contribute	These users can schedule Quick Deploy jobs (Content Deployment).
Viewers	View Only	These users see content, but can't edit or download it.

PowerShell

Connect to management shell

Connect-SPOService -Url <https://contoso-admin.sharepoint.com> -credential admin@contoso.com

returns all user or security group accounts from the site collection <http://contoso.sharepoint.com/sites/finance>.

Get-SPOUser -Site <https://contoso.sharepoint.com/sites/finance>

This example removes a specific external user who has the address "someone@example.com". Organization members may still see the external user name displayed in the **Shared With** dialog, but the external user will not be able to sign in and will not be able to access any tenant resources.

\$user = Get-SPOExternalUser -Filter someone@example.com

Remove-SPOExternalUser -UniqueIDs @(\$user.UniqueId)

The **New-SPOSite** cmdlet creates a new site collection for the current company. However, creating a new SharePoint Online site collection fails if a deleted site with the same URL exists in the Recycle Bin. You must be a SharePoint Online global administrator to run the cmdlet

Example creates a new site collection for the current company with specified site URL, title, owner, and template. The storage quota is set to 1000 megabytes and the resource quota is set to 300 megabytes. The template compatibility level is set to 15 which means that the site collection only supports the SharePoint 2013 template. The language is set to English - United States (LocaleID = 1033) and the time zone is set to (GMT-08:00) Pacific Time (US and Canada) (TimeZone = 13).

New-SPOSite -Url <http://contoso.sharepoint.com/sites/mynewsite> -Owner joe.healy@contoso.com -

StorageQuota 1000 -CompatibilityLevel 15 -LocaleID 1033 -ResourceQuota 300 -Template "STS#0" -TimeZoneId 13 -Title "My new site collection"

Use the **Set-SPOUser** cmdlet to configure properties of an existing user. That is, to add or remove a user as a SharePoint Online site collection administrator.

This example makes melissa.kerr@contoso.com a SharePoint Online site collection administrator on

<https://contoso.sharepoint.com/sites/marketing>.

Set-SPOUser -Site <https://contoso.sharepoint.com/sites/marketing> -LoginName melissa.kerr@contoso.com -IsSiteCollectionAdmin \$true

Set-SPOSite Sets or updates one or more properties' values for a site collection.

Example 1 updates the owner of site collection <https://contoso.sharepoint.com/sites/site1> to the person whose email address is joe.healy@contoso.com. This cmdlet is executed immediately without delay.

Set-SPOSite -Identity <https://contoso.sharepoint.com/sites/site1> -Owner joe.healy@contoso.com -NoWait

Example 2 updates the settings of site collection <https://contoso.sharepoint.com/sites/site1>. The storage quota is updated to 15000 megabytes and the resource quota is updated to 0 megabytes.

Set-SPOSite -Identity <https://contoso.sharepoint.com/sites/site1> -ResourceQuota 0 -StorageQuota 15000

Example 4 prevents non-owners of a site from inviting new users to the site.

Set-SpoSite -Identity <https://contoso.sharepoint.com> -DisableSharingForNonOwners

Set-SPOSiteGroup cmdlet Updates the SharePoint Online owner and permission levels on a group inside a site collection.

Example 1 changes permission level of the ProjectViewers group inside site collection

<http://contoso.sharepoint.com/sites/siteA> from Full Control to View Only.

Set-SPOSiteGroup -Site <http://contoso.sharepoint.com/sites/siteA> -Identity "ProjectViewers" -PermissionLevelsToRemove "Full Control" -PermissionLevelsToAdd "View Only"

Example 2 sets Melissa.kerr@contoso.com as the owner of the ProjectViewers group.

Set-SPOSiteGroup -Site <https://contoso.sharepoint.com> -Identity "ProjectViewers" -Owner Melissa.kerr@contoso.com

Set-SPOTenant Sets properties on the SharePoint Online organization.

This example enables the use of special persisted cookie for Open with Explorer.

Set-SPOTenant -UsePersistentCookiesForExplorerView \$true

This example blocks access to <https://contoso.sharepoint.com/sites/team1> and redirects traffic to <http://www.contoso.com>.

Set-SPOSite -Identity <https://contoso.sharepoint.com/sites/team1> -LockState NoAccess

Set-SPOTenant -NoAccessRedirectUrl '<http://www.contoso.com>'