



Microsoft Exchange Online for Enterprises

Service Description

Published: June 28, 2011

Updated: July 29, 2011

For the latest information, please see [Microsoft Office 365](#).

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication and is subject to change at any time without notice to you. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. This document is confidential and proprietary to Microsoft. It is disclosed and can be used only pursuant to a non-disclosure agreement.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

All trademarks are the property of their respective companies.

©2011 Microsoft Corporation. All rights reserved.

Microsoft, Access, Active Directory, Backstage, Excel, InfoPath, Internet Explorer, Lync, OneNote, Outlook, PowerPoint, PowerShell, SharePoint, Silverlight, Windows Live, Windows Mobile, Windows Server, Windows Vista, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	6
Features of Microsoft Office 365	7
Office Desktop Setup	7
Federated Identity and Single Sign-On	8
Operating System and Software Requirements	8
International Availability	9
Data Center Locations.....	9
Localization.....	10
Exchange Online Service Details	11
Exchange Online Client Languages	11
Exchange Online Administration Languages	11
Subscription Plans	11
Mailbox Size Limits.....	13
Mailbox Capacity Alerts.....	13
Message Size Limits.....	14
Recipient Limits.....	14
Message Rate Limits	14
Other Limits.....	15
Deleted Item Recovery	15
Deleted Mailbox Recovery	15
Mailbox Backup	16
Service Continuity Management	16
Access to Exchange Online	17
Microsoft Outlook	17
Outlook Web App.....	18
Microsoft Outlook for Mac 2011	20
Microsoft Office Entourage 2008 Web Services Edition.....	20
IMAP.....	21
POP	21
SMTP	21
Exchange ActiveSync (Mobile Devices).....	21
Email Features and Configurations	24
Delegate Access (Send on Behalf Permissions)	24
Send As Permissions.....	24
Shared Mailboxes	24
Catch-all Mailbox.....	24
Inbox Rules.....	25
MailTips.....	25

Connected Accounts.....	25
Contacts and Distribution Groups.....	26
Distribution Groups.....	26
Global Address List.....	27
Custom Address Lists	27
External Contacts	27
Calendar Features	28
Out-of-Office Replies	28
Federated Calendar Sharing	28
Calendar Sharing through iCal	28
Conference Rooms and Resource Mailboxes	28
Voicemail and Fax Features	30
Hosted Voicemail (Unified Messaging).....	30
Interoperability with On-Premises Voicemail Systems	31
Fax Interoperability	31
Security Features.....	32
Anti-Spam and Antivirus Filtering	32
Safe and Blocked Senders	32
Junk Mail and Spam Quarantine.....	32
Use of Other Filtering Services for Inbound Email	32
Custom Routing of Outbound Email.....	33
Transport Layer Security (TLS)	33
Encryption Between Clients and Exchange Online	33
Information Rights Management	34
Archiving and Compliance Features	36
Disclaimers.....	36
Transport Rules.....	36
Personal Archive.....	37
Journaling	38
Retention Policies	38
Legal Hold.....	38
Rolling Legal Hold (Single Item Recovery)	39
Multi-Mailbox Search	39
Administration Features	41
Microsoft Online Services Portal.....	41
Exchange Control Panel	41
Forefront Online Protection for Exchange Administration Center	41
Remote PowerShell	41
Role-Based Access Control	42

Message Tracking	43
Usage Reporting	43
Auditing	43
Application Interoperability Features.....	44
Exchange Web Services	44
SMTP Relay.....	44
Outlook Web App Web Parts.....	44
Outlook Add-Ins and Outlook MAPI.....	44
Exchange Server MAPI/CDO.....	45
WebDAV	45
Lync Server 2010 or Office Communications Server 2007 R2.....	45
Other Information.....	46
Public Folders	46
Directory Synchronization	46
Migration and Hybrid Deployments	46
Exporting Data from Exchange Online.....	49
Appendix A: Exchange Online and Exchange Server Feature Comparison.....	50

Introduction

Microsoft® Exchange Online is a hosted messaging solution that delivers the capabilities of Microsoft Exchange Server as a cloud-based service. It gives users rich and familiar access to email, calendar, contacts, and tasks across PCs, the web, and mobile devices. With Exchange Online, organizations can take advantage of sophisticated messaging capabilities without the operational burden of on-premises server software.

This document provides information technology (IT) professionals with an overview of the capabilities of the Exchange Online service. To obtain detailed technical information about Exchange Online, please refer to the documentation available at <http://help.outlook.com>, especially the resources found on the help page [Manage Your Organization - Office 365 for enterprises](#).

Features of Microsoft Office 365

Exchange Online is one of several cloud services offered by Microsoft Office 365 for enterprises. These Internet-based services are designed to help meet the need for robust security, 24/7 reliability, and user productivity.

Each service is designed for reliability, availability, and performance with a financially backed service level agreement (SLA) for a guaranteed 99.9-percent scheduled uptime. Microsoft deploys patches, security updates, and back-end upgrades, helping to eliminate the time and effort organizations spend managing their servers.

Subscribers to Exchange Online benefit from a set of features that are common to all of the Microsoft business-class cloud services:

- **Secure access:** Each offering from Microsoft Office 365 is accessed through 128-bit Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption. Anyone who intercepts a communication sees only encrypted text.
- **Intrusion monitoring:** Microsoft continuously monitors the Office 365 systems for any unusual or suspicious activity. If Microsoft detects such activity, it investigates and responds appropriately. In the unlikely event that a significant incident occurs, the customer is notified.
- **Security audits:** Microsoft regularly assesses the Office 365 infrastructure to ensure that the latest antivirus signatures and required security updates are installed, and that high-level configuration settings are in compliance with Microsoft security policies. For details, refer to the [Security and Service Continuity for Enterprises Service Description](#).
- **High availability:** Microsoft Office 365 services have a 99.9-percent scheduled uptime. If a customer's service is affected, Office 365 offers financial remedies subject to the terms and conditions of the SLA. For details, refer to the [Service Level Agreement for Microsoft Online Services](#).
- **Service continuity:** Redundant network architecture is hosted at geographically dispersed Microsoft data centers to handle unscheduled service outages. Data centers act as backups for each other: If one fails, the affected customers are transferred to another data center with limited interruption of service.
- **Microsoft Online Services Portal:** This easy-to-use website is the center for activities related to Microsoft Office 365. The portal provides services based on each organization's specific needs. Prospective subscribers can use the portal to sign up for a free trial. End users accessing the portal can find online help, open Microsoft SharePoint site collections, and launch Microsoft Outlook® Web App. Administrators can manage users, administer services, download tools, and learn about service administration from online help.
- **Directory Synchronization tool:** For subscribers with Active Directory® directory services deployed on-premises, this tool helps keep the on-premises Active Directory and the Microsoft Office 365 directory synchronized.
- **Remote administration:** With Microsoft Windows PowerShell™, administrators can perform many tasks using a script or automated process. For example, tasks such as creating users, resetting passwords, assigning licenses, and obtaining service-use data can be fully automated.

Office Desktop Setup

For the best experience with Office 365, a set of required components and updates must be applied to each workstation. To simplify the installation and maintenance of these components and updates, Microsoft provides an installable piece of software—called Office desktop setup—at no charge. These updates are required for all workstations that use rich clients (such as Microsoft Office 2010) and connect to Microsoft Office 365.

Office desktop setup provides multiple benefits, including:

- Automatically detecting necessary updates.
- Installing updates and components upon approval or silently from a command line.
- Automatically configuring Outlook and Microsoft Lync for use with Microsoft Office 365.
- Uninstalling itself from the client computer after running.

A list of these update requirements are available for companies that want to use an alternative method of deploying the updates. See the help topic [Manually update and configure desktops for Office 365](#) for details.

 **Note**

Office desktop setup is not an authentication or sign-in service and should not be confused with single sign-on.

Federated Identity and Single Sign-On

With on-premises Active Directory, administrators can use a single sign-on approach to Office 365 authentication. To achieve this, administrators can configure on-premises Active Directory federation Services—a Microsoft Windows Server® 2008 service—to federate with the Microsoft Federation Gateway. After Active Directory Federation Services is configured, all Office 365 users whose identities are based on the federated domain can use their existing corporate logon to automatically authenticate to Office 365.

Operating System and Software Requirements

Table 1 shows the operating system and browser combinations that are required to access Microsoft Office 365 services—including Exchange Online.

Table 1: Operating systems and browser combinations supported by Microsoft Office 365

Operating system	Supported browsers
Windows 7 (32-bit)	<ul style="list-style-type: none">• Windows Internet Explorer 8 and later versions• Firefox 3 and later versions• Chrome 6 and later versions
Windows 7 (64-bit)	<ul style="list-style-type: none">• Internet Explorer 8 and later versions• Firefox 3 and later versions• Chrome 6 and later versions
Windows Vista with Service Pack 2 (32-bit)	<ul style="list-style-type: none">• Internet Explorer 7 and later versions• Firefox 3 and later versions• Chrome 6 and later versions
Windows Vista with Service Pack 2 (64-bit)	<ul style="list-style-type: none">• Internet Explorer 8• Internet Explorer 7• Firefox 5
Windows XP with Service Pack 3 (32-bit)	<ul style="list-style-type: none">• Internet Explorer 7 and later versions• Firefox 3 and later versions• Chrome 6 and later versions
Windows XP with Service Pack 2 (64-bit)	<ul style="list-style-type: none">• Internet Explorer 8• Internet Explorer 7• Firefox 5

Operating system	Supported browsers
Windows Server 2008 and Windows Server 2008 R2	<ul style="list-style-type: none"> Internet Explorer 8 and later versions Firefox 3 and later versions Chrome 6 and later versions
Mac OS X 10.5 or Mac OS X 10.6	<ul style="list-style-type: none"> Firefox 3 and later versions Safari 4 and later versions

Table 2 identifies other software required for using Office 365 services.

Table 2: Software supported by Microsoft Office 365

Software	Supported Version
System software	<ul style="list-style-type: none"> Microsoft .NET Framework 3.0 (for Windows XP) Java client 1.4.2 (for Macintosh OS X)*
Office clients	<ul style="list-style-type: none"> Microsoft Office 2010 or Office 2007 Service Pack 2 Office 2008 for Mac and Microsoft Entourage® 2008 Web Services Edition Office 2011 for Mac and Outlook 2011 for Mac Microsoft Lync 2010 client .NET Framework 2.0 or later
Client applications	Office desktop set up
Browser software for Microsoft Online Services Portal	<ul style="list-style-type: none"> Internet Explorer 7 or later Mozilla Firefox 3.x Apple Safari 3.x
Browser software for Outlook Web App	<ul style="list-style-type: none"> Internet Explorer 7 or later Firefox 3 or later Safari 3 or later on Macintosh OS X 10.5 Chrome 3 and later versions <p>Outlook Web App also has a "light" version that supports a reduced set of features across almost any browser</p>

International Availability

Office 365 is available in Austria, Belgium, Canada, Colombia, Costa Rica, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Greece, Hong Kong, Hungary, India, Ireland, Israel, Italy, Japan, Luxembourg, Malaysia, Mexico, Netherlands, New Zealand, Norway, Peru, Poland, Portugal, Puerto Rico, Romania, Singapore, Spain, Sweden, Switzerland, Trinidad and Tobago, United Kingdom, and United States.

Multinational customers that purchase services in an approved country may enable use by their end users that reside anywhere in the world, except for Argentina and countries currently embargoed by the U.S. government. Features availability may vary by location. See the help topic [License restrictions for Office 365](#) for details.

Data Center Locations

Microsoft Office 365 maintains primary and backup data centers distributed around the world. When a company signs up for a Microsoft Office 365 service, its hosted environment is automatically provisioned in the appropriate data center based on the company's address. All users for the company are hosted from the same data center.

Localization

Table 3 summarizes the languages supported the Microsoft Office 365 platform and related components.

Table 3: Supported languages for components related to Microsoft Office 365

Component	Supported languages
Microsoft Online Services Portal	Brazilian Portuguese, Chinese Traditional, Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hungarian, Italian ¹ , Japanese, Norwegian (Bokmal), Polish, Romanian, Spanish, Swedish
Help content—for end users and IT professionals	Brazilian Portuguese, Chinese Traditional, Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Norwegian (Bokmal), Polish, Romanian, Spanish, Swedish
Directory Synchronization Tool	Brazilian Portuguese, Chinese Traditional, Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Norwegian (Bokmal), Polish, Romanian, Spanish, Swedish

Technical Support

The Microsoft Office 365 technical support team provides support services to people with administrator permissions for their company's Office 365 services. Those with administrator permissions provide support services to their company's Office 365 end users. For contact information, see Online Help in the services Administration Center.

Exchange Online Service Details

This section describes features included with the Microsoft Exchange Online service.

Exchange Online Client Languages

The client languages supported by Exchange Online are the same as those supported in Exchange Server 2010 Service Pack 1.

- For languages supported by Microsoft Outlook Web App, see the TechNet article [Client Languages for Outlook Web App](#).
- For languages supported by Outlook, see the TechNet article [Client Language Support for Outlook](#).
- For languages supported by Exchange Unified Messaging, see the TechNet article [Client Language Support for Unified Messaging](#).

Exchange Online Administration Languages

The administration interfaces for Exchange Online are the same as those supported in Exchange Server 2010 Service Pack 1:

- For languages supported by Windows Remote PowerShell (also called the "Exchange Management Shell"), see the TechNet article [Language Support for Exchange Management Interfaces](#).
- The languages supported by Exchange Control Panel are the same as those supported in Outlook Web App, see the TechNet article [Client Languages for Outlook Web App](#).

Note

The Microsoft Online Services Portal supports a different set of languages, as described earlier in this document.

Subscription Plans

Each user who accesses the Exchange Online service requires must be assigned to a subscription plan. Exchange Online offers three types of plans: **Exchange Online Kiosk**, **Exchange Online (Plan 1)**, and **Exchange Online (Plan 2)**.

Table 4 summarizes differences between the types of subscriptions.

Table 4: Overview of user subscriptions

Feature	Exchange Online Kiosk	Exchange Online (Plan 1)	Exchange Online (Plan 2)
Mailbox size	500 megabytes (MB)	25 gigabytes (GB)*	Unlimited**
Outlook Web App (regular and light versions)	Yes	Yes	Yes
POP	Yes	Yes	Yes
IMAP	No	Yes	Yes
Outlook Anywhere (MAPI)	No	Yes	Yes

Feature	Exchange Online Kiosk	Exchange Online (Plan 1)	Exchange Online (Plan 2)
Microsoft Exchange ActiveSync®	No	Yes	Yes
Exchange Web Services	No***	Yes	Yes
Inbox rules	No	Yes	Yes
Delegate access	No (cannot access other users' mailboxes, shared mailboxes, or resource mailboxes)	Yes	Yes
Instant messaging interoperability in OWA	No	Yes (requires Lync Online or Microsoft Lync Server 2010)	Yes (requires Lync Online or Microsoft Lync Server 2010)
SMS notifications	No	Yes	Yes
Custom retention policies	Yes	Yes	Yes
Multi-mailbox search	Yes	Yes	Yes
Personal archive	No	Yes	Yes
Voicemail	No	No	Yes
Legal hold	No	No	Yes

*25 GB of storage apportioned across the user's primary mailbox and personal archive

**25 GB of storage in the user's primary mailbox, plus unlimited storage in the user's personal archive. Refer to the personal archive section of this document for further information regarding unlimited storage in the archive

***Direct access to Kiosk user mailboxes via Exchange Web Services is not permitted. However, line of business applications can use Exchange Web Services impersonation to access Kiosk user mailboxes

All subscriptions include organization-wide capabilities such as journaling, transport rules, and premier anti-spam and antivirus filtering via Forefront Online Protection for Exchange.

User subscriptions are not required for conference rooms and shared mailboxes. These special mailbox types do not have login credentials—instead, licensed users with the appropriate permissions manage them via delegation.

Office 365 Suite Subscription Plans Exchange Online plans can be purchased on a standalone basis or as part of an Office 365 suite. Each Office 365 plan contains one of the Exchange Online plans. Tables 5 and 6 summarize the relationship between Exchange Online plans and Office 365 plans. To determine which plan is right for you, visit the [Office 365 home page](#).

Table 5: Office 365 subscription plans for kiosk workers

Office 365 (Plan K1)	Office 365 (Plan K2)
Exchange Online Kiosk	Exchange Online Kiosk
SharePoint Online Kiosk	SharePoint Online Kiosk
	Office Web Apps

Table 6: Office 365 subscription plans for information workers

Office 365 (Plan E1)	Office 365 (Plan E2)	Office 365 (Plan E3)	Office 365 (Plan E4)
Exchange Online (Plan 1)	Exchange Online (Plan 1)	Exchange Online (Plan 2)	Exchange Online (Plan 2)
SharePoint Online (Plan 1)	SharePoint Online (Plan 1)	SharePoint Online (Plan 2)	SharePoint Online (Plan 2)
Lync Online (Plan 2)	Lync Online (Plan 2)	Lync Online (Plan 2)	Lync Online (Plan 2)
	Office Web Apps	Office Web Apps	Office Web Apps
		Office Professional Plus	Office Professional Plus
			Lync Voice & PBX (Lync Plus CAL for Lync Server)*

* Lync Voice & PBX are only available with Lync Server 2010, deployed on-premises or hosted via a private cloud deployment. All Lync workloads (instant messaging, online meetings and Voice & PBX) must be deployed on Lync server in this case. It is not possible to split Lync workloads between Lync Server and Lync Online.

Mailbox Size Limits

The amount of mailbox storage available to a user is determined by his or her user subscription license:

- Each **Exchange Online Kiosk** user receives 500 MB of mailbox storage. The maximum mailbox size for a Kiosk user is 500 MB.
- Each **Exchange Online (Plan 1)** user receives 25 GB of mailbox storage, which can be split between the user's primary mailbox and the user's personal archive.
- Each **Exchange Online (Plan 2)** user receives 25 GB of storage in the user's primary mailbox. The maximum size of the primary mailbox is 25 GB. The user also receives unlimited storage in the user's personal archive (see the personal archive section of this document for details).

Administrators can use Remote PowerShell to reduce maximum mailbox sizes for some or all of their users. This is achieved by adjusting the mailbox capacity alerts described in the following paragraphs.

Special mailbox types, such as conference rooms and shared mailboxes, have different size limits. These limits are detailed in the relevant sections of this document.

Mailbox Capacity Alerts

Exchange Online provides three notifications to users as their primary mailboxes approach maximum size limits:

- **Warning:** Users receive email warnings when their mailboxes are approaching the maximum size limit. This warning is intended to encourage users to delete unwanted mail.
- **Prohibit Send:** Users receive email prohibit-send notifications when they reach their mailbox size limits. Users cannot send new messages until they delete enough messages so that their mailboxes are below the size limit.
- **Prohibit Send/Receive:** Exchange Online rejects any incoming mail when this limit is reached and then sends a non-delivery report (NDR) to senders. Sender can try resending the mail later. To receive messages, users must delete messages until the mailbox is below the size limit.

These values can be modified using Remote PowerShell, as described in the help topic [Set Mailbox Quotas in Office 365 using Windows PowerShell](#). Table 7 shows the default values.

Table 7: Mailbox size limits and notifications

Mailbox type	Warning	Prohibit Send	Prohibit Send/Receive
Exchange Online Kiosk	450 MB	475 MB	500 MB
Exchange Online (Plan 1)	24.5 GB	24.75 GB	25 GB
Exchange Online (Plan 2)	24.5 GB	24.75 GB	25 GB

These limits and notifications are for the user's primary mailbox. The personal archive has a separate, non-configurable quota.

Message Size Limits

Message size limits are necessary to prevent large messages from negatively affecting system performance and to ensure fast message delivery for all users. The message size limit for Exchange Online is 25 MB, including attachments. Messages larger than this limit will not be delivered, and the sender will receive a Non-Delivery Report (NDR). The message size limit is a global setting that applies to all messages (that is, inbound, outbound, and internal). This value cannot be adjusted up or down. However, administrators can create transport rules to limit the maximum size of any individual attachment.

Note

An email client may limit the size of an individual file attachment to a value less than the message size limit. For example, in Outlook Web App, the maximum individual file attachment size is 10 MB.

Recipient Limits

To discourage users from sending unsolicited bulk messages, Exchange Online has restrictions that prevent users and applications from sending large volumes of email. Each Exchange Online mailbox can send messages to a maximum of 1,500 recipients per day. An email message can be addressed to a maximum of 500 recipients. These limits apply to emails sent within an organization as well as to messages delivered to external organizations.

Note

For the purposes of these limits, a distribution group that is stored in the Global Address List counts as one recipient. In a personal distribution group, each recipient is counted separately.

See the help topic [Recipient and sender limits](#) for details.

Exchange Online customers who need to send legitimate bulk commercial email (for example, customer newsletters) should use third-party providers that specialize in these services.

Message Rate Limits

To prevent overconsumption of system resources and help guard against inappropriate use, users can send only 30 messages per minute. If a user submits messages at a faster rate, Exchange Online will deliver the messages but will queue the messages at the server and throttle the rate of delivery.

Other Limits

Additional limits relating to messages, mailboxes, and recipients help ensure the health and responsiveness of the Exchange Online service for all customers. To view these limits, go to the help topic [Message and Recipient Limits](#).

Deleted Item Recovery

Exchange Online enables users to restore items they have deleted from any email folder. When an item is deleted, it is kept in a user's Deleted Items folder. It remains there until it is manually removed by the user, or automatically removed by retention policies.

Note

By default, retention policies will automatically remove items from the Deleted Items folder after 30 days, but organizations can customize these retention policies if desired. See the help topic [Retention limits](#) for details.

After an item has been removed from the Deleted Items folder, the item is kept in a Recoverable Items folder for an additional 14 days before being permanently removed. Users can recover these items using the Recover Deleted Items feature in Outlook Web App or Outlook.

If a user has manually purged an item from the Recoverable Items folder, an administrator can recover the item within the same 14 day window, through a feature called Single Item Recovery. This feature allows administrators to conduct a multi-mailbox search to find purged items and then use the search-mailbox PowerShell commandlet to move the items from the discovery mailbox to users' mailboxes.

Note

The Single Item Recovery period is 14 days by default, but it can be customized in some circumstances. Refer to the [Rolling Hold \(Single Item Recovery\)](#) section of this document for details.

If an administrator has placed a user's mailbox on legal hold, purged items are retained indefinitely and the 14-day window does not apply.

See the help topic [Recover Deleted E-mail Messages in Exchange Online](#) for details.

Deleted Mailbox Recovery

When an Exchange Online mailbox is deleted, its contents are recoverable for 30 days. A recovered mailbox contains all of the data stored in it at the time it was deleted. After 30 days, the mailbox is not recoverable. Administrators can recover a deleted mailbox using the Exchange Control Panel.

If the mailbox was originally deleted from the Exchange Control Panel and the user's account still exists in the Microsoft Online Services Portal, the administrator can recover the mailbox without assistance. If the user's account was deleted from the Microsoft Online Services Portal, then a call to Office 365 support is required in order to restore the Microsoft Online account so it can be linked to the recovered mailbox.

See the help topic [Recover a Deleted Mailbox](#) for details.

Mailbox Backup

Exchange Online mailboxes are replicated to multiple database copies, in geographically dispersed Microsoft data centers, to provide data restoration capability in the event of a messaging infrastructure failure. For large-scale failures, service continuity management is initiated.

Service Continuity Management

Exchange Online is hosted in Microsoft-managed, enterprise-level data centers that are designed to operate highly available online services. Exchange Online provides a financially-backed Service Level Agreement (SLA) with a 99.9 percent uptime guarantee.

Hardware failures, natural disasters, and human error all have the potential to affect service availability. To address this, Exchange Online offers service continuity management, a process for managing risks to ensure that the Exchange Online infrastructure is capable of providing continuing services if unexpected events occur. Service continuity management for Exchange Online includes provisions to quickly recover from these events.

Two metrics commonly used in service continuity management to evaluate disaster recovery solutions are a *recovery time objective* (RTO), which measures the time between a system disaster and the time when the system is again operational, and a *recovery point objective* (RPO), which is a time representation of the possible data loss that occurred as a result of the recovery from the unexpected event .

Exchange Online has set an RPO and RTO for client messaging services in the event of a disaster:

- **Nearly instantaneous RPO:** Microsoft protects your Exchange Online data and makes a nearly instantaneous copy of your data.
- **1 hour RTO:** Organizations will be able to resume service within 60 minutes after service disruption if a disaster incapacitates a hosting data center.

The following conditions apply to service continuity management:

- Please see the *Office 365 Identity Service Description* for recovery times and other details related to sign-in and provisioning of new users and new tenants.
- Client access after recovery from a service disruption typically does not require reconfiguration on the part of Exchange Online subscribers.
- To achieve the stated recovery times, customer networking infrastructure must honor the DNS record Time to Live (TTL) of 5 minutes. Customers that have customized their client DNS settings and set a longer TTL may experience longer recovery times.
- After RPO and RTO objectives are met, there is a period of time before full data center redundancy is restored for the service. For example, Data Center 1 fails but services are restored by resources in Data Center 2. There may be a period of time until services in Data Center 2 have service continuity support either by restored resources in Data Center 1 or new resources in Data Center 3. Service Level agreements apply during this time.

You can obtain the most current information related to a service interrupting event by logging into the Service Health Dashboard at <https://portal.microsoftonline.com>.

Access to Exchange Online

Exchange Online allows users to connect to their mailboxes from a variety of devices and platforms. All network connectivity occurs over the Internet, and VPN connections are not required.

Note

Microsoft reserves the right to block or throttle connections from any client software that negatively impacts the health of the Exchange Online service.

Microsoft Outlook

Microsoft Outlook is a rich email program that includes support for calendaring, contacts, and tasks. Exchange Online supports Microsoft Outlook 2010 and Microsoft Office Outlook 2007, including key features such as:

- **Outlook Anywhere:** Outlook Anywhere lets Outlook users connect to Exchange Online over the Internet with no need for a VPN connection. Communication between Outlook and Exchange Online occurs via an SSL-secured tunnel, using the RPC-over-HTTP Windows networking component.
- **Exchange Autodiscover Service:** The Exchange Autodiscover service automatically configures Outlook to work with Exchange Online. Autodiscover enables Outlook users to receive their required profile settings directly from Exchange Online the first time they sign in with their email address and password.
- **Cached Exchange Mode:** Cached Exchange Mode allows users to access local copies of their Exchange mailboxes when they are not connected to the Internet. Cached Exchange Mode maintains a client-side copy of users' Exchange mailboxes in Outlook and automatically synchronizes this copy with the email server. In addition to providing offline access, it helps to provide a responsive user experience—even when network conditions between the client and the server are not ideal. *Online Exchange Mode* is also supported, but not recommended due to issues with latency inherent in Internet access.
- **Offline Address Book:** The offline address book is a snapshot of the Active Directory information available in the Global Address List. It is cached locally in Outlook to make it available when a user is working offline.

By default, Outlook access is enabled for all users. Administrators can disable access for specific users or groups through Remote PowerShell (`Set-CASmailbox <Identity> -mapienabled $false`).

Note

Organizations are responsible for procuring, deploying, managing, and supporting Outlook. Outlook is not provided as part of the Exchange Online subscription price, although Microsoft Office Pro Plus is included in some Office 365 plans, and can be purchased as a separate subscription.

Outlook 2010

Outlook 2010 supports the latest features of Exchange Online, including:

- Conversation view and conversation actions (for example, Ignore, Always Move)
- MailTips

- Personal archive (this feature is available only in certain versions of Outlook 2010. See the [Personal Archive](#) section of this document for details).
- User-assigned retention policies
- Alerts for users on legal hold
- Meeting room finder
- Outlook Protection Rules (this feature requires Active Directory Rights Management Services)
- Protected voicemail (this feature requires Active Directory Rights Management Services)
- Voicemail preview

Note

Some of these features are not available in previous versions of Outlook.

Outlook 2007

Outlook 2007 is supported for use with Exchange Online.

Outlook 2003

Outlook 2003 is not supported for use with Exchange Online.

Outlook Web App

Microsoft Office Outlook Web App is a web-based version of the Outlook email program that is used with Exchange Online. Wherever users are connected to the Internet—at home, at the office, or on the road—they can access their email through Outlook Web App.

Supported Browsers

Outlook Web App is supported with full functionality on the following browsers:

- Internet Explorer 7 and later versions
- Firefox 3 or higher
- Safari 3 or higher on Macintosh OS X 10.5
- Chrome 3 and later versions

See the help topic [Supported Browsers for Outlook Web App and Exchange Online](#) for details.

Outlook Web App Light

The light version of Outlook Web App supports older web browsers and is optimized to support users who are blind or have impaired vision. Users can read and send messages, organize contacts, and schedule appointments and meetings in the light version of Outlook Web App. The light version can be used with almost any browser.

See the help topic [Outlook Web App Light](#) for details.

Outlook Web App URLs

Users can access Outlook Web App from a link on the Microsoft Online Services Portal or at <http://mail.office365.com>. Administrators can provide users with customized URLs for accessing Outlook Web App (also known as “vanity URLs”) by using either of the following methods:

1. Set up a CNAME record in DNS (for example, <http://mail.contoso.com>) that points to mail.office365.com.
2. Redirect from a website (for example, <http://contoso.com/OWA>) to the standard Outlook Web App URL.

The exact procedure for redirecting users depends on where the domain name is registered or hosted.

Sign-in Page

Administrators can customize the Outlook Web App landing page if they have deployed Active Directory Federation Services 2.0 on-premises for single sign-on with Microsoft Office 365. In this case, the sign-in page is located on the on-premises servers, and the page can be customized. For example, usage guidelines or a disclaimer can be added for employees to view before logging on. The same logon page is used for Outlook Web App as well as other web-based Microsoft Office 365 applications.

If Active Directory Federation Services 2.0 is not deployed, a standard, non-customizable Outlook Web App sign-in page is displayed.

Public and Private Computer Sign-in Options

The Outlook Web App sign-in page does not offer Public Computer or Private Computer options.

Session Time-out

By default, the Outlook Web App session time-out is six hours. The session time-out can be customized by using Remote PowerShell (`set-OrganizationConfig -ActivityBasedAuthenticationTimeoutInterval`).

WebReady Document Viewing

Outlook Web App features WebReady document viewing, which converts documents (for example, Microsoft Word documents, Microsoft Excel[®] spreadsheets, Microsoft PowerPoint[®] presentations, and .pdf files) into HTML for read-only viewing in a web browser window. When WebReady document viewing is enabled, users see an Open as Web Page link next to supported document types in Outlook Web App. By default, this feature is enabled in Exchange Online. It can be disabled through Remote PowerShell (`set-OWAMailboxPolicy Default -WebReadyDocumentViewingOnPublicComputersEnabled $false`).

Preventing Attachment Downloads

Administrators can block users from downloading attachments in Outlook Web App. This helps prevent users from accidentally leaving content on an unsecure machine, such as an Internet kiosk. Attachment download settings in Outlook Web App are managed through Remote PowerShell (`Set-OwaMailboxPolicy Default -DirectFileAccessOnPublicComputersEnabled $false`).

Outlook Web App Customization

Administrators can use Outlook Web App mailbox policies to enable and disable specific features within Outlook Web App, such as calendaring, contacts, Global Address lists, and tasks. Administrators can customize these settings through Remote PowerShell (`set-OWAMailboxPolicy`) and apply the custom Outlook Web App settings to all users or a subset of users.

Outlook Web App includes a number of built-in themes that users can select to customize the look and feel of the Outlook Web App interface. However, there is no option to customize the Outlook Web App header with an organization's logo or color scheme.

Users and administrators cannot customize the Outlook Web App interface by adding links, buttons, or

custom forms because this type of extensibility would require adding and editing files on Client Access Servers in the Exchange Online infrastructure.

Disabling Outlook Web App Access

Administrators can disable access to Outlook Web App on a per-user basis through Remote PowerShell (set-CASMailbox <Identity> -OWAEnabled \$false).

Changing Passwords from Outlook Web App

If an organization is using Active Directory Federation Services 2.0 for single sign-on, users manage their credentials directly in their on-premises Active Directory. Users cannot change their passwords from Outlook Web App.

If an organization is not using Active Directory Federation Services 2.0 for single sign-on, the Outlook Web App Options page displays a link to a separate page where users can change their passwords for all Microsoft Online services.

Instant Messaging and Presence

Outlook Web App can interoperate with Lync Online and on-premises Lync Server 2010 to provide users with instant messaging (IM) and presence within the Outlook Web App interface. This capability is not available to users with Kiosk subscriptions, even if they have accounts in Lync Online or Lync Server.

IM and presence in OWA is enabled by default for users with active Lync Online accounts. To enable these features for users with on-premises accounts in Lync Server, administrators must configure an SRV record in DNS and install trusted certificates on local Lync servers. Administrators can disable IM and presence in OWA for individual users or for their entire organization by using Remote PowerShell (set-OWAMailboxPolicy Default -InstantMessagingEnabled \$false).

Microsoft Outlook for Mac 2011

Microsoft Outlook for Mac 2011 is a rich client for Macintosh users that provides email, calendaring, an address book, a task list, and a note list. Exchange Online supports Outlook for Mac 2011.

Note

Organizations are responsible for procuring, deploying, managing, and supporting Microsoft Outlook for Mac 2011.

Microsoft Office Entourage 2008 Web Services Edition

Exchange Online supports Microsoft Entourage 2008 Web Services Edition, which is available as free update to users of Entourage 2008.

Note

Organizations are responsible for procuring, deploying, managing, and supporting Entourage 2008 Web Services Edition.

IMAP

Exchange Online supports mailbox access through the IMAP4 protocol. IMAP is enabled by default for all users except those with Kiosk subscriptions. Users can view their IMAP connection settings on the Outlook Web App Options page. Administrators can disable IMAP access on a per-user basis using Remote PowerShell (`set-CASMailbox <Identity> -ImapEnabled $false`).

POP

Exchange Online supports mailbox access through the POP3 protocol. POP is enabled by default for all users, who can view their POP connection settings on the Outlook Web App Options page. Administrators can disable POP access on a per-user basis using Remote PowerShell (`set-CASMailbox <Identity> -PopEnabled $false`).

SMTP

The SMTP protocol is used to send outbound mail for clients that connect to Exchange Online through IMAP or POP. Transport Layer Security (TLS) encryption and authentication is required when using SMTP to send email. SMTP is also used by applications that send email. Refer to [SMTP Relay](#) in the Application Interoperability section of this document for details.

Exchange ActiveSync (Mobile Devices)

Exchange Online supports the Microsoft Exchange ActiveSync protocol. Exchange ActiveSync provides synchronization of mailbox data between mobile devices and Exchange Online, so users can access their email, calendar, contacts, and tasks on the go.

Exchange ActiveSync is supported by a wide range of mobile devices, including Microsoft Windows Mobile® and Windows Phone, Nokia E and N series devices, Palm devices, Apple iPhone and iPad, and certain Android phones. Implementation of specific Exchange ActiveSync features varies by device and manufacturer. A community-maintained comparison of how Exchange ActiveSync features are implemented by various mobile clients is available at this [Comparison of Exchange ActiveSync Clients](#) page.

The Exchange ActiveSync Logo Program helps organizations identify enterprise-ready mobile devices that have implemented key Exchange ActiveSync user features and management policies. A list of Exchange ActiveSync Logo Program Qualified Devices is available in the TechNet article [Exchange ActiveSync Logo Program](#).

Exchange ActiveSync is not available to users with Kiosk subscriptions.

Note

Organizations are responsible for procuring, deploying, managing, and supporting mobile client software and compatible devices, as well as managing relationships with wireless carriers. Microsoft does not provide end-user device support.

Autodiscover

Exchange Online supports the Exchange Autodiscover service. Mobile devices that support Autodiscover provide users with a simplified setup experience when connecting to Exchange Online. Users do not need to know the address of their email server when connecting their mobile device to Exchange Online—they

simply enter an email address and password, and the device automatically obtains the additional server settings required to set up their mobile profile.

Remote Device Wipe

If users lose their mobile devices, they can remotely wipe the device of all data the next time the devices connect to Exchange Online. Users can trigger the remote wipe through the Outlook Web App Options page, or administrators can log on to the Outlook Web App Settings page to trigger the device wipe on behalf of the user. A confirmation message is sent to the users when the mobile devices acknowledge the remote wipe request.

Exchange ActiveSync Policies

Administrators can enforce security policies on mobile devices that connect to Exchange Online through Exchange ActiveSync. Administrators can customize these policies for specific users and groups within their company, using web-based graphical user interface (GUI) or Remote PowerShell. Exchange Online supports the same ActiveSync policies as Exchange Server 2010 Service Pack 1.

See the help topic [Change an ActiveSync Device Policy](#) for details.

Disable Exchange ActiveSync Access

Exchange ActiveSync access is enabled by default for all Exchange Online users, except those with Kiosk subscriptions. Administrators can disable Exchange ActiveSync access on a per-user basis through the web-based GUI in the Exchange Control Panel or through Remote PowerShell (`set-CASMailbox <Identity> -ActiveSyncEnabled $false`).

Allow, Block, and Quarantine Controls

Administrators can control which mobile device models and families can connect to the Exchange Online environment through Allow, Block, and Quarantine controls. Administrators can manage these controls through the web-based GUI in the Exchange Control Panel or through Remote PowerShell.

See the help topic [Allow, Block, or Quarantine New Device Connections](#) for details.

Certificate-based Authentication for Exchange ActiveSync

Exchange Online does not support certificate-based authentication for devices that connect via Exchange ActiveSync.

SMS Notifications

Exchange Online users can have text message alerts sent to their mobile phones when they receive email messages or meeting requests. Users who are enabled for hosted voicemail can also receive notifications of missed calls and voicemails. This feature does not require an Exchange ActiveSync device partnership. Users can set up these notifications on the Outlook Web App Options page.

This feature is currently available only to users in the United States, Canada, and Romania. It is not available to users with **Exchange Online Kiosk** subscriptions. Administrators can disable the feature on a per-user basis using Remote PowerShell (`Set-OwaMailboxPolicy Default -TextMessagingEnabled $false`).

Details on SMS notifications are available at the help topic [Learn About Text Messaging](#).

BlackBerry Devices

Users of Research in Motion (RIM) BlackBerry devices can connect their devices to Exchange Online using

the BlackBerry Internet Service (BIS). This service allows BlackBerry users to access their e-mail accounts without connecting through a BlackBerry Enterprise Server (BES). It does not provide the same capabilities as a BES server or a hosted BES service. **Exchange Online (Plan 1)** and **Exchange Online (Plan 2)** users can configure BIS to access their mailboxes via IMAP. **Exchange Online Kiosk** users can configure BIS to access their mailboxes via POP.

 **Note**

A hosted BES service is not currently available. Research in Motion (RIM) has announced a new hosted BES service for Office 365 customers that they plan to make available later this year. The service will be hosted, licensed, and supported by RIM, who have committed to offer their new BlackBerry cloud-based service for Exchange Online starting at \$0 per user per month. See the blog entry [Office 365 and BlackBerry](#) for details.

Email Features and Configurations

This section describes specific email features and configurations available with Exchange Online.

Delegate Access (Send on Behalf Permissions)

Exchange Online supports delegate access—that is, the ability for users to allow others to manage their email and calendars. Delegate access is commonly used between a manager and an assistant, where the assistant is responsible for processing the manager’s incoming email messages and coordinating the manager’s schedule. When delegates have Send on Behalf permissions, they can compose email messages and enter the manager’s name in the From field, where it will be displayed as “[delegate name] on behalf of [manager name]”. The ability to access other mailboxes via delegate access is not available to users with **Exchange Online Kiosk** subscriptions.

Users and administrators can set up and manage these delegate permissions using Outlook. For details on how Delegate Access works, see help topic [Allow someone else to manage your mail and calendar](#).

Send As Permissions

Exchange Online supports advanced delegation scenarios, including Send As permissions. Send As permissions allow users to send messages from another mailbox as if they are the mailbox owner. This scenario is common where there is a shared mailbox and several employees send email messages from that shared mailbox instead of their Exchange accounts. The ability to access other mailboxes via Send As permissions is not available to users with **Exchange Online Kiosk** subscriptions.

Shared Mailboxes

Shared mailboxes allow a group of users to view and send e-mail from a common mailbox (for example, info@contoso.com or sales@contoso.com). A shared mailbox does not have a username and password, so users cannot log on to it directly. They must sign in to their own mailboxes and then open the shared mailbox using Send As permissions.

In Exchange Online, shared mailboxes are created only via Remote PowerShell.

Shared mailboxes do not need to be assigned to a subscription plan, but each user that accesses a shared mailbox must be assigned to a subscription plan. Users with **Exchange Online Kiosk** subscriptions cannot access shared mailboxes. Each shared mailbox has a maximum size of 5 GB. If additional storage is required, the shared mailbox must be assigned an **Exchange Online (Plan 1)** or **Exchange Online (Plan 2)** subscription. If legal hold is required, the shared mailbox must be assigned an **Exchange Online (Plan 2)** subscription.

Shared mailboxes are subject to the same recipient limits and message rate limits as regular mailboxes. These limits are described in the [Recipient Limits](#) section of this document. A shared mailbox can’t be used to archive e-mails, except for those messages sent from the shared mailbox or received by the shared mailbox.

See the help topic [Set Up a Shared Mailbox](#) for details.

Catch-all Mailbox

A catch-all mailbox receives messages sent to email addresses in a domain that do not exist. Exchange Online anti-spam filters use recipient filtering to reject messages sent to mailboxes that don't exist, so catch-all mailboxes are not supported.

Inbox Rules

Exchange Online allows users to create inbox rules that automatically perform specific, criteria-based actions on messages as they arrive. For example, users can create a rule to automatically move all mail to a specific folder if the mail was sent to a certain distribution group. Inbox rules are managed from Outlook or Outlook Web App. Inbox rules are not available to users with **Exchange Online Kiosk** subscriptions.

See the help topic [Learn About Inbox Rules](#) for details.

In some situations, administrators may want to prevent users from setting up certain types of inbox rules. For example, they may want to disable server-side email forwarding so that users cannot automatically forward email to personal accounts. They may also want to disable server-side automatic replies—such as “Have Server Reply with Template Message”—so that these automatic replies cannot be used by outside parties to identify valid email addresses. Administrators can disable server-side forwarding and disable server-side automatic replies using Remote PowerShell (`set-remotedomain -AutoReplyEnabled $false` and `-AutoForwardEnabled $false`).

MailTips

MailTips provide automated alerts that help users avoid embarrassing email mistakes. They appear above the To: line of an email to prevent accidental delivery or policy violations. For example, MailTips generate an alert if senders try to send messages to large groups or to groups that contain external recipients. MailTips also provide alerts when a user composes a message to a distribution group that is moderated or restricted. MailTips are available in Exchange Online to users who access their mailboxes from Outlook Web App or Outlook 2010.

See the help topic [Configure MailTips](#) for details.

Connected Accounts

For users who have multiple email accounts and want to interact with all their messages in one place, Exchange Online provides a feature called Connected Accounts. This feature lets users connect external email accounts to their Exchange Online accounts, and use Outlook Web App to send and receive mail from these connected accounts. This feature is not available in the on-premises edition of Exchange Server. Administrators can enable and disable this feature for specific users or all users, by adjusting the MyMailSubscriptions role in the relevant Role Assignment Policy, via the Exchange Control Panel.

See the help topics [Learn About Connected Accounts](#) and [Change a Role Assignment Policy](#) for details.

Contacts and Distribution Groups

This section describes Exchange Online support for contacts and distribution groups.

Distribution Groups

A distribution group (or distribution list) is a collection of users, contacts, and other distribution groups that are available to all users in a company. A distribution group makes it easy to send messages to multiple people. Unlike personal distribution groups that individuals create in Outlook, these distribution groups are globally available. Distribution groups are created in the Exchange Control Panel or synchronized from on-premises Active Directory, and then appear in the Global Address List in Outlook.

Exchange Online supports advanced distribution group capabilities, including:

- Restricted distribution groups
- Dynamic distribution groups
- Moderated distribution groups
- Self-service distribution groups

See the help topic [Change Distribution Group Properties](#) for details.

Restricted Distribution Groups

By default, anyone can send emails to a distribution group. However, administrators can change the permissions of a distribution group to allow only specific individuals to send emails to that group. This restriction can discourage inappropriate use of large distribution lists. Administrators can also block external sources from sending email to distribution groups in order to prevent spam. Distribution group permissions can be managed via web-based GUI in the Exchange Control Panel and via Remote PowerShell. For distribution groups that are synchronized from on-premises Active Directory using the Directory Synchronization tool, the attributes for restriction are synchronized to the cloud automatically.

Dynamic Distribution Groups

The membership list for a dynamic distribution group (also known as a dynamic distribution list, or query-based distribution list) is calculated every time a message is sent to the group. This calculation is based on filters and conditions that the administrator defines. Dynamic distribution groups are supported in Exchange Online. They are managed through Remote PowerShell, and they do not appear in the web management GUI.

The Office 365 Directory Synchronization tool ignores dynamic distribution groups in on-premises Active Directory, and does not synchronize these to Exchange Online. Organizations that use the Directory Synchronization tool should use a naming convention that avoids conflicts between the regular distribution groups managed on-premises and the dynamic distribution groups that are managed in Exchange Online.

See the help topic [Dynamic Distribution Groups](#) for details.

Moderated Distribution Groups

Administrators can select a moderator to regulate the flow of messages sent to a distribution group. With moderated distribution groups, anyone can email the distribution group alias, but before the message is delivered to the members of the group, a moderator must review and approve it. This can help to prevent users from sending inappropriate emails to large audiences. Distribution group moderation can be managed in the Exchange Control Panel.

Self-Service Distribution Groups

Administrators can give users the ability to manage their own distribution group membership from an easy-to use, web-based interface. These self-service capabilities can help users be more productive and lighten the burden on an organization's help desk. Users can be given permissions to:

- Create distribution groups
- Delete distribution groups
- Join or leave distribution groups

These capabilities are enabled by default for all Exchange Online users. Administrators can disable these self-service features and let the IT department manage distribution groups, if desired, by adjusting role assignment policies as described in the help topic [Prevent Users from Creating Distribution Groups](#).

Self-service capabilities are not available for distribution groups that synchronized from on-premises Active Directory to Exchange Online. Organizations that use Directory Synchronization should use a naming convention that avoids conflicts between distribution groups managed on-premises and distribution groups managed in the cloud.

Global Address List

Exchange Online supports the Global Address List, an organization-wide directory of all mail-enabled users, distribution groups, and external contacts.

Administrators can hide users, distribution groups, and contacts from the Global Address List by setting the *HideInAddressList* attribute for the object in on-premises Active Directory (if using the Directory Synchronization tool) or through Remote PowerShell. See the help topic [Hide a User from the Shared Address Book in Office 365](#) for details.

Custom Address Lists

Hierarchical address lists, Global Address List segmentation, custom Global Address List views, and multiple address lists per organization are not available in Exchange Online. For example, users cannot create address lists that put contacts from North America in one view and those from Europe in another view. Similarly, it is not possible to prevent users in one of an organization's subsidiaries from viewing users in another subsidiary.

External Contacts

An external contact is a record with information about a person who works outside of a specified organization. External contacts are available to all users in an organization, which makes external contacts different from the personal contacts that individuals create in Outlook. External contacts are created in the Exchange Control Panel, created via Remote PowerShell, or synchronized from on-premises Active Directory. They appear in the Global Address List in Outlook.

See the help topic [External Contacts in the Address Book](#) for details.

Calendar Features

Exchange Online calendar features are described in this section.

Out-of-Office Replies

Out-of-office messages are automatic replies to incoming messages, sent by Exchange Online behalf of a user. Users can schedule out-of-office messages in advance, with specific start and end times and can format them as rich HTML messages with hyperlinks rather than plain text. Users can configure separate out-of-office messages for internal and external users. Junk email and mailing list awareness in Exchange Online prevents users from sending external out-of-office messages to extended mailing lists and people who send spam. Exchange Online also lets users set out-of-office messages from mobile devices that support this Exchange ActiveSync feature.

Administrators can prevent users from sending out-of-office messages to external users through Remote PowerShell (`set-remotedomain -AllowedOOFTYPE Internal`).

Federated Calendar Sharing

Exchange Online customers can share free/busy calendar data with other organizations hosted by Exchange Online as well as with organizations running Exchange Server 2010 on-premises. Administrators do not need to set up a trust with the Microsoft Federation Gateway because this trust is pre-configured for all customers on the Exchange Online platform.

A Default Sharing Policy allows users to share basic free/busy data with users in other federated organizations, by sending calendar sharing invitations in OWA or Outlook 2010. Administrators can use Remote PowerShell to disable the Default Sharing Policy, as well as configure additional calendar sharing policies which specifies what level of free/busy calendar data users can share.

Administrators can also create an organization-to-organization relationship with another federated org, which allows the desired level of free/busy information for every user to be visible cross-org without the need for individual users to make a sharing invitation of any kind. Within the scope of administrator-defined Sharing Policies and/or org-org relationships, users can individually limit the detail of their sharing further.

See the help topic [Configure Federated Delegation in the Cloud](#) for details.

Calendar Sharing through iCal

Exchange Online allows users to publish their calendars using the iCal format for anonymous access by anybody, inside or outside the organization. Recipients can be using Exchange, another platform, or simply a web browser. Exchange Online users can also subscribe to calendars that others have published to Internet locations through iCal. This personal calendar sharing is different than federated calendar sharing, which is configured by an administrator and provides organization-to-organization free/busy sharing. No user can publish calendar data in iCal format until the administrator has set and applied a Sharing Policy that allows it. Administrators can disable iCal publishing and iCal subscriptions for users in an organization by changing their Sharing Policy through Remote PowerShell.

Conference Rooms and Resource Mailboxes

Conference room mailboxes represent a company's meeting rooms or other facilities. Users can reserve rooms by adding the conference room email alias to meeting requests in Outlook or Outlook Web App. Conference rooms appear in the Global Address List in Outlook and Outlook Web App, and administrators

can create conference rooms in the Exchange Control Panel or through Remote PowerShell. Administrators can also use the Directory Synchronization tool to synchronize conference rooms from on-premises Active Directory. The mailbox quota for conference rooms is 250 MB. Conference rooms do not require a user subscription license.

See the help topic [Create a New Room Mailbox](#) for details.

Resource Booking Attendant

Exchange Online includes the Resource Booking Attendant (RBA), which helps to automate the scheduling of conference rooms. A conference room mailbox uses the Resource Booking Attendant to automatically accept, decline, or acknowledge meeting requests based on its calendar availability. Through the Outlook Web App Options page, administrators can customize automated conference room responses and configure booking policies. These policies include who can schedule a conference room, when it can be scheduled, what meeting information is visible on the resource's calendar, and what percentage of scheduling conflicts is allowed. Administrators can disable the Resource Booking Attendant and assign specific users to manually manage meeting requests for conference rooms.

See the help topic [Resource Scheduling Options](#) for details.

Outlook 2010 Room Finder

Exchange Online supports the Room Finder feature of Outlook 2010, which arranges rooms into lists (for example, a list called "Building 5 rooms") to make it easier to find a nearby room when scheduling a meeting. To appear in the room list, a distribution group must be specially marked using one of two methods:

- A new room list can be created using Remote PowerShell (see the TechNet article [Create a Room List Distribution Group](#)).
- Any distribution group that contains only rooms can be converted to a room list through Remote PowerShell.

Voicemail and Fax Features

Exchange Online voice and fax features are presented in the sections that follow.

Hosted Voicemail (Unified Messaging)

Exchange Online offers hosted unified messaging services, which provide:

- Call answering (voicemail)
- Dial-in user interface to Exchange (Outlook Voice Access)
- Dial-in interface for callers (Automated Attendant)

Hosted unified messaging allows a company to connect its on-premises phone system to voicemail services provided by Exchange Online. Voicemails are recorded and stored in the Exchange Online infrastructure, allowing users to access their voice messages from Outlook, Outlook Web Access, or mobile phones.

All telephony connections to Exchange Online require voice-over-IP (VoIP) protocols. Administrators can connect on-premises PBX phone systems to Exchange Online using VoIP media gateways and session border controllers (SBCs). A VoIP media gateway is not required if the PBX supports VoIP directly and is interoperable with Exchange unified messaging. SBCs are deployed in the perimeter of the customer network and help secure the communications (and the customer network) against eavesdropping and intrusion. Interoperability with the voice capabilities of Lync Server 2010 is also supported.

Note

Currently, customers hosted from data centers in the Europe and Asia-Pacific regions cannot integrate Lync Server 2010 with hosted voicemail services, because the hardware for Lync Server integration has not yet been deployed in those datacenters.

The unified messaging features available in Exchange Online are similar to those offered in Exchange Server 2010 Service Pack 1, except speech access to the directory is not supported in Exchange Online. Instead of speaking names, users must spell names using the touchpad when searching for someone in the directory by name in Outlook Voice Access or the company auto attendant. Speech access to Personal Contacts and Personal Distribution Lists is supported.

The following unified messaging features work similarly online and on-premises:

- Play on phone from Outlook and Outlook Web App
- Missed call notifications
- Caller ID (using information in the Global Address List and users' Outlook contacts)
- Voicemail PIN reset from Outlook Web App and Outlook
- Message waiting indicator
- Call answering rules
- Protected voicemail (see the [Information Rights Management](#) subsection of this document for details)
- Voicemail preview (see the [Client Languages](#) subsection of this document for language support)

The Exchange Control Panel includes screens to configure and manage unified messaging interoperability. See the help topic [Use Unified Messaging to Connect Exchange to Your Telephone System](#) for complete details about hosted voicemail and unified messaging.

Interoperability with On-Premises Voicemail Systems

On-premises voicemail solutions from third-party providers can interoperate with Exchange Online if they can forward voicemails through SMTP or if they support Microsoft Exchange Web Services. If the voicemail system does not natively support forwarding voicemails through SMTP, an email server can be kept on-premises to receive messages from the voicemail system and then forward them to the cloud using SMTP. Because many third-party voicemail systems use MAPI/CDO to interoperate with Exchange Server for advanced unified messaging features, the full capabilities of these systems may not be available when SMTP is used for interoperability with Exchange Online.

Fax Interoperability

Outbound Fax Services

Exchange Online does not provide outbound fax services. Solutions for outbound fax, including Internet-based fax services, are available from third-party providers. Generally, these outbound fax solutions are independent from an organization's email infrastructure and require no special interoperability with Exchange Online.

Inbound Fax Services

Exchange Online does not provide inbound fax services. If an organization uses a third-party fax solution that is capable of receiving faxes and forwarding them to recipients via email, the administrator can specify Exchange Online mailboxes as a destination. If the organization has deployed Unified Messaging in Exchange Online, advanced interoperability with inbound fax solutions is available. This interoperability enables features such as one-number fax receiving (a single phone number for voice calls and fax), rich caller-ID information through Active Directory and Exchange personal contacts, and identification of fax messages as a special message class in Exchange and Outlook.

Security Features

Exchange Online security features are presented in the sections that follow.

Anti-Spam and Antivirus Filtering

Exchange Online uses Microsoft Forefront® Online Protection for Exchange and Microsoft Forefront® Protection for Exchange Server to help protect incoming, outgoing, and internal messages from malicious software transferred through email.

This service uses proprietary anti-spam technology to help achieve high accuracy rates, and multiple, complementary antivirus engines to help detect viruses and other malicious code spread through email. Administrators do not need to set up, configure, or maintain the filtering technology because antivirus and anti-spam protections are preconfigured.

Administrators can manage advanced controls over anti-spam and email control settings directly through the Forefront Online Protection for Exchange (FOPE) Administration Center. See the [Administration](#) section of this document for more details.

Safe and Blocked Senders

Users can manage their safe and blocked senders from within their inboxes in Outlook or Outlook Web App. They can right-click any message and specify several actions, including:

- Block the sender.
- Never block the sender.
- Never block the sender's domain (@example.com).
- Never block this group or mailing list.

They can also manage their advanced Junk Mail options and view complete lists of safe and blocked senders.

Administrators can manage organization-wide safe and blocked sender lists via the Forefront Online Protection for Exchange (FOPE) Administration Center, specifying the IP addresses, domains, or email addresses to allow or restrict.

Junk Mail and Spam Quarantine

When Exchange Online receives messages, they are evaluated and assigned a spam confidence level (SCL) value. Messages with high SCL values are deleted at the gateway, and messages with low SCL values are delivered to users' inboxes. Messages with borderline SCL values are placed in users' Junk Mail folders in Outlook and Outlook Web App, where they are automatically removed after 30 days.

By default, no emails are kept in the Forefront Online Protection for Exchange (FOPE) spam quarantine and no FOPE spam digest emails are sent. This eliminates the need for administrators and users to log on to a separate quarantine. However, organizations can choose to use FOPE's spam quarantine rather than the integrated Junk Mail experience in Outlook and OWA. Administrators can change the spam action settings for their organization by accessing the FOPE Admin Center and following the instructions at the TechNet article [Spam Quarantine](#).

Use of Other Filtering Services for Inbound Email

An on-premises appliance or another hosted service can be used to filter email before it reaches Exchange Online. In this scenario, the email domain's MX record is pointed to the appliance or service, which then

relays the email to Exchange Online. This same configuration can also be used in email coexistence, when some users have mailboxes in an on-premises email server while others are hosted in Exchange Online. See the TechNet article [Inbound Safe Listing Scenario](#) for details.

Custom Routing of Outbound Email

Exchange Online provides the ability to route outbound mail through an on-premises server or a hosted service (sometimes called "smart hosting"). This capability allows organizations to utilize data loss prevention (DLP) appliances, perform custom post-processing of outbound e-mail, and deliver e-mail to business partners via private networks. Administrators configure custom e-mail routing within the Forefront Online Protection for Exchange (FOPE) Administration Center.

See the TechNet article [Outbound Smart Host](#) for details.

Address Rewrite

Some organizations modify outbound email to hide sub-domains, to make email from a multi-domain organization appear as a single domain, and to make partner-relayed email appear as if it were sent from inside the organization. Customers can route outbound email through an on-premises gateway to rewrite addresses in this way.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is method of encrypting the connection between email servers to help prevent spoofing and provide confidentiality for messages in transit. TLS is also used for securing on-premises mail server traffic to Exchange Online during migration and coexistence.

Opportunistic TLS

Exchange Online supports opportunistic TLS for inbound and outbound email, and this feature is enabled by default. If the other party's mail server has a public certificate that is trusted by Forefront Online Protection for Exchange and supports the *starttls* command, a TLS connection is automatically established between the servers. If TLS cannot be established, the server will still transmit the email, but the connection will not be encrypted.

Forced TLS

Exchange Online supports forced TLS for outbound and inbound connections. Administrators can configure forced TLS on a per-IP address or per-domain basis within the Forefront Online Protection for Exchange (FOPE) Administration Center.

See the TechNet article [Regulated Partner with Forced TLS Scenario](#) for details.

Encryption Between Clients and Exchange Online

Client connections to Exchange Online use the following encryption methods to enhance security:

- SSL is used for securing Outlook, Outlook Web App, Exchange ActiveSync, and Exchange Web Services traffic, using TCP port 443.
- SSL is also used for POP3 and IMAP, using TCP port 995.

S/MIME

Exchange Online will transport and store Secure/Multipurpose Internet Mail Extensions (S/MIME)

messages. However, Exchange Online does not host S/MIME functions, nor does it provide key repository, key management, or key directory services.

To use S/MIME, users must store in their Outlook contacts the public key for every recipient to whom they send encrypted messages. Outlook cannot use the S/MIME certificates stored for users in on-premises Active Directory because the Directory Synchronization tool does not synchronize the Active Directory *userSMIMECert* attribute to Exchange Online.

S/MIME is supported in Outlook but not in Outlook Web App. Customers are responsible for all PKI infrastructure and user S/MIME certificate enrollment.

PGP

Exchange Online will transport and store messages that are encrypted using client-side, third-party encryption solutions such as PGP. Exchange Online does not host the public keys, nor does it provide key repository, key management, or key directory services.

Information Rights Management

Exchange Online does not provide hosted Information Rights Management (IRM) services, but administrators can use on-premises Active Directory Rights Management Services in conjunction with Exchange Online. If an Active Directory Rights Management Services server is deployed, Outlook can directly communicate with the Active Directory Rights Management Services server, enabling users to compose and read messages protected by Active Directory Rights Management Services. There is no need for interoperability between the Active Directory Rights Management Services server and Exchange Online in order to use the Active Directory Rights Management Services features of Outlook.

To enable advanced Active Directory Rights Management Services features introduced in Exchange 2010, administrators can import the Trusted Publishing Domain from their Active Directory Rights Management Services server to Exchange Online using Remote PowerShell. After this one-time import, the following features become available:

- Support for IRM in Outlook Web App
- Support for IRM in Exchange ActiveSync
- IRM search
- Transport protection rules
- Protected voicemail
- Journal report decryption
- Outlook Protection Rules

See the help article [Set Up and Manage Information Rights Management in Exchange Online](#) for details.

Support for IRM in Outlook Web App

Users can read and create IRM-protected messages natively in Outlook Web App, just like in Outlook. IRM-protected messages in Outlook Web App can be accessed through Internet Explorer, Firefox, Safari, and Chrome (with no plug-in required) and include full-text search, conversation view, and the preview pane.

Support for IRM in Exchange ActiveSync

Users with mobile devices that support the IRM features of the Exchange ActiveSync protocol can open and work with IRM-protected messages with the appropriate rights—without tethering the phone or

installing additional IRM software. Administrators can control the use of this feature using Role-Based Access Control (RBAC) and Exchange ActiveSync policies.

IRM Search

IRM-protected messages are indexed and searchable, including headers, subject, body, and attachments. Users can search protected items in Outlook and Outlook Web App and administrators can search protected items by searching multiple mailboxes.

Transport Protection Rules

Administrators can set up transport protection rules that automatically apply Active Directory Rights Management Services protection to email in transit (including Microsoft Office and XPS attachments). This provides persistent protection for the file regardless of where it is sent and prevents forwarding, copying, or printing, depending on the rights policy template applied.

Protected Voicemail

Either senders or administrators can apply Do Not Forward permissions to voicemail messages in order to prevent them from being forwarded to unauthorized persons, regardless of the email client. These permissions can be applied to all voicemail messages in the organization, or just to voicemail messages that have been marked as private by the sender.

Journal Report Decryption

When journaling messages to an external archive, administrators can include a decrypted, clear-text copy of IRM-protected messages in journal reports, including Microsoft Office and XPS attachments. This allows IRM-protected messages to be indexed and searched for legal discovery and regulatory purposes. The original IRM-protected message is also included in the report.

Outlook Protection Rules

Outlook Protection Rules are a new feature in Outlook 2010. They automatically trigger Outlook to apply an Active Directory Rights Management Services template, based on sender or recipient identities, before users can send an email message. Unlike Transport Protection Rules, Outlook Protection Rules can be configured so that users can turn off protection for less sensitive content.

Archiving and Compliance Features

Exchange Online archiving and compliance features are presented in the sections that follow.

Disclaimers

Laws or other regulatory requirements may require organizations to add disclaimers to users' email messages. Exchange Online lets administrators add disclaimers to messages in transit using transport rules. Administrators can create custom disclaimers for different groups in an organization and can control whether the disclaimers are applied to internal messages, outbound messages, or both.

See the help topic [Add Disclaimers to Messages](#) for details.

Transport Rules

Transport rules are used to inspect emails in transit (including inbound, outbound, and internal messages) and take actions, such as applying a disclaimer, blocking messages, or sending a blind carbon copy to a mailbox for supervisory review. Transport rules use a set of conditions, actions, and exceptions similar to inbox rules. Exchange Online supports the transport rule functionality of Exchange Server 2010 Service Pack 1, including:

- **Granular Transport Rule Conditions:** Administrators can create transport rules to inspect messages for a variety of email attributes, such as specific senders, recipients, distribution lists, keywords, and regular expressions (for common patterns like those associated with credit card numbers or social security numbers). Administrators can also include users' Active Directory attributes (for example, department, country, or manager) and distinguish by message types (such as automatic replies, meeting requests, and voicemail messages).
- **Ability to Moderate:** Administrators can use transport rules to route email messages to a manager or trusted moderator for review. Reviewers can then approve or block the message and, if blocked, provide an explanation to the sender.
- **Message Classifications:** Administrators can use transport rules to apply metadata to messages, describing the intended use or audience (for example, attorney–client privileges). Users can also apply classifications manually and have transport rules check messages when they enter the transport pipeline. If messages do not meet the conditions of the classification, an action can be applied to modify, protect, or block the messages.
- **Attachment Inspection:** Administrators can create transport rules based on content in a Microsoft Office attachment. However, file types, such as Adobe .pdf, that require installation of third-party IFilters on the email server cannot be inspected in Exchange Online.

Administrators can manage transport rules using the Exchange Control Panel or Remote PowerShell. Transport rules can act on all email traffic in an organization, including messages sent and received by users with Kiosk subscriptions. Using transport rules to copy messages to an Exchange Online mailbox for the purposes of archiving is not permitted.

See the help topic [Organization-Wide Rules](#) for details.

Personal Archive

Note

This section describes archiving capabilities available for cloud-based mailboxes in Exchange Online. For details about Microsoft Exchange Online Archiving, a hosted archiving solution for *on-premises* Exchange 2010 mailboxes, refer to the [Exchange Online Archiving Service Description](#).

Exchange Online provides built-in archiving capabilities, including a personal archive that gives users a convenient place to store older emails. A personal archive is a specialized mailbox that appears alongside users' primary mailbox folders in Outlook or Outlook Web App. Users can access the archive in the same way they access their primary mailboxes. In addition, users can search both their personal archives and primary mailboxes.

Administrators can use the Exchange Control Panel or Remote PowerShell to enable the personal archive feature for specific users. The personal archive is not available to users with **Exchange Online Kiosk** subscriptions. See the help topic [Enable an Archive Mailbox](#) for details.

Note

Using journaling, transport rules, or auto-forwarding rules to copy messages to an Exchange Online mailbox for the purposes of archiving is not permitted.

Client Support for the Personal Archive

Outlook 2010 and Outlook Web App provide users with the full features of the personal archive, as well as related features like retention and archive policies.

Outlook 2007 provides basic support for the personal archive, but not all archiving and compliance features are available in Outlook 2007. For example, with Outlook 2007, users cannot apply retention or archive policies to items in their mailboxes. They must rely on administrator-provisioned policies instead. Outlook 2007 users require the Office 2007 Cumulative Update for February 2011 to access the personal archive.

Note

The personal archive has specific licensing requirements for Outlook users, which are described at the help topic [License requirements for Personal Archive and retention policies](#).

Size of the Personal Archive

Each personal archive can be used only for storage of one user's messaging data. An **Exchange Online (Plan 1)** user receives 25 gigabytes (GB) of total storage, which the user can apportion across the user's primary mailbox and personal archive. Therefore, the personal archive for an **Exchange Online (Plan 1)** user cannot exceed 25 GB in size.

An **Exchange Online (Plan 2)** user receives 25 GB of storage in the primary mailbox, plus unlimited storage in the personal archive. For **Exchange Online (Plan 2)** users, a default quota of 100 GB is set on the personal archive, which will generally accommodate reasonable use, including the import of one user's historical email. In the unlikely event that a user reaches this quota, a call to Office 365 support is required. Administrators cannot adjust this quota upward or downward.

Importing Data to the Personal Archive

Users can import data to personal archives in the following four ways:

- Import data from a .pst file using Outlook's Import and Export wizard.
- Drag email messages from .pst files into the archive.
- Drag email messages from the primary mailbox into the archive.
- Let archive policies automatically move email messages from the primary mailbox, based on the age of the messages.

Administrator-driven import of .pst files, using the *new-mailboximportrequest* PowerShell commandlet introduced in Exchange Server 2010 Service Pack 1, is not available in Exchange Online.

Journaling

Administrators can configure Exchange Online to journal copies of emails to any external archive that can receive messages via SMTP. For example, administrators can journal emails to an on-premises archiving solution. The journaling destination cannot be an Exchange Online mailbox. Administrators can manage journal rules in the Exchange Control Panel or Remote PowerShell and can configure journaling on a per-user and per-distribution list basis, scoping the journaling to internal recipients, external recipients, or both. Journalled messages include not only the original message but also information about the sender, recipients, copies, and blind copies.

See the help topic [Journal Rules](#) for details.

Retention Policies

Exchange Online offers retention policies to help organizations reduce the liabilities associated with email and other communications. With these policies, administrators can apply retention settings to specific folders in users' inboxes. Administrators can also give users a menu of retention policies and let them apply the policies to specific items, conversations, or folders using Outlook 2010 or Outlook Web App. In Exchange Online, administrators manage retention policies using Remote PowerShell.

Exchange Online offers two types of policies: archive policies and delete policies. Both types can be combined on the same item or folder. For example, a user can tag an email message so that it is automatically moved to the personal archive in a specified number of days and deleted after another span of days.

With Outlook 2010 and Outlook Web App, users have the flexibility to apply retention policies to folders, conversations, or individual messages and can also view the applied retention policies and expected deletion dates on messages. Users of other email clients can have emails deleted or archived based on server-side retention policies provisioned by the administrator, but they do not have the same level of visibility and control.

The retention policy capabilities offered in Exchange Online are the same as those offered in Exchange Server 2010 Service Pack 1. Administrators can use Remote PowerShell to migrate retention policies from on-premises Exchange Server 2010 environments to Exchange Online. Managed Folders, an older approach to messaging records management that was introduced in Exchange 2007, are not available in Exchange Online.

See the help topic [Set Up and Manage Retention Policies in Exchange Online](#) for details.

Legal Hold

Exchange Online provides legal hold capabilities to preserve users' deleted and edited mailbox items

(including email messages, appointments, and tasks) from both their primary mailboxes and personal archives. Administrators can use the Exchange Control Panel or Remote PowerShell to set legal holds on individual mailboxes or across an organization. This feature also includes an option that sends an email notification to users or automatically alerts them through Outlook 2010 that a hold has been placed on their mailboxes.

See the help topic [Put a Mailbox on Litigation Hold](#) for details.

Rolling Legal Hold (Single Item Recovery)

Some organizations want to preserve users' mailbox contents for archiving and eDiscovery purposes, but only for a specific amount of time, such as one year. The Single Item Recovery feature in Exchange Online can be used to meet this need, by providing rolling legal hold capabilities.

Single Item Recovery is enabled by default on all mailboxes in Exchange Online, with a 14-day retention period, in order to facilitate recovery of deleted items. By extending the Single Item Recovery retention period, organizations can ensure that mailbox items are preserved for a specified amount of time. Single Item Recovery uses the same mechanisms as legal hold to preserve original copies of items that have been modified or deleted.

Note

To change the Single Item Recovery period for a mailbox, an administrator must contact the Office 365 help desk. The Single Item Recovery period can be set to any length of time. If the desired period is longer than 30 days, the mailbox must have an **Exchange Online (Plan 2)** subscription.

Single Item Recovery can be disabled using Remote PowerShell. See the help topic [Disable single item recovery](#) for details.

Multi-Mailbox Search

Exchange Online provides a web-based interface for searching the contents of mailboxes in an organization. Through the Exchange Control Panel, administrators can search a variety of mailbox items—including email messages, attachments, calendar appointments, tasks, and contacts. Multi-mailbox search can search simultaneously across primary mailboxes and personal archives. Rich filtering capabilities include sender, receiver, message type, sent/receive date, and carbon copy/blind carbon copy, along with Advanced Query Syntax.

See the help topic [Create a New Multi-Mailbox Search](#) for details on how to run multi-mailbox searches.

Results of multi-mailbox searches are stored in a special type of mailbox, called a discovery mailbox. A discovery mailbox has a 50 GB quota so it can store large numbers of search results. Administrators can connect Outlook to a discovery mailbox, and export the search results to a .pst file. In Exchange Online, administrators cannot directly export mailbox search results to a .pst file.

By default, one discovery mailbox is created for each organization, but administrators can create additional ones via remote PowerShell. Discovery mailboxes cannot be used for any purpose other than storing mailbox search results. See the help topic [Create a Discovery Mailbox to Store Search Results](#) for details about discovery mailboxes.

Administrators can also search for and delete inappropriate email messages sent to multiple mailboxes across their organizations. For example, if confidential salary information was accidentally emailed to all employees, an administrator could delete the email from users' mailboxes. This type of search is not available in the Exchange Control Panel. It must be performed using Remote PowerShell.

See the help topic [Search For and Delete Messages from Users' Mailboxes](#) for details on how to delete messages from users' mailboxes.

Administration Features

Exchange Online administration features are presented in the sections that follow.

Microsoft Online Services Portal

The Microsoft Online Services Portal allows administrators to add users and user domains, manage licenses, create groups, and perform other administration tasks common across the services in Office 365. From within the console, administrators can follow links to the Exchange Control Panel, where they can manage settings specific to Exchange Online.

Exchange Control Panel

The Exchange Control Panel allows administrators to configure and manage the Exchange Online environment from a web browser. Administrators can access the Exchange Control Panel by choosing one of the following options:

- Clicking a link in the Microsoft Online Services Portal.
- Opening the Outlook Web App Options page and selecting "My Organization."

The Exchange Control Panel provides several management capabilities, which are organized into four high-level categories:

- **Users and Groups:** Mailboxes, distribution groups, external contacts, and email migration
- **Roles:** Administrator roles, user roles, and auditing
- **Mail Control:** Rules, journaling, e-discovery, and delivery reports
- **Phone and Voice:** Unified messaging dialing plans, unified messaging gateways, Exchange ActiveSync access, and Exchange ActiveSync device policy

Administrators can give users access to selected features in the Exchange Control Panel, using the [Role-Based Access Control framework](#) described later in this document.

Forefront Online Protection for Exchange Administration Center

The Microsoft Forefront® Online Protection for Exchange (FOPE) Administration Center allows Exchange Online customers to manage advanced settings relating to email flow and email hygiene. Within the FOPE Administration center, administrators can:

- Access reports and statistics on e-mail hygiene for their domains
- Set advanced policy filters that are not available via Exchange Online transport rules, such as rules that are triggered by the IP address of inbound or outbound servers
- Configure forced TLS connections for their domains
- Perform advanced message tracing
- Configure organization-level safe and blocked senders

Note: Some settings are read-only in the FOPE Administration Center to help prevent administrators from inadvertently causing problems with their organizations' mail flow.

Remote PowerShell

Using Remote PowerShell, administrators can connect to Exchange Online to perform management tasks that are not available or practical in the web management interface. For example, they can use Remote PowerShell to automate repetitive tasks, extract data for custom reports, customize policies, and connect

Exchange Online to existing infrastructure and processes.

To use Remote PowerShell, administrators' computers must be running the Windows Management Framework, which contains Windows PowerShell v2 and WinRM 2.0. These components are already installed in computers running Windows 7 or Windows Server 2008 R2. Administrators can manually download these components for computers running other operating systems. Administrators do not need to install any Exchange Server management or migration tools in order to use Remote PowerShell. See the help topic [Use Windows PowerShell in Exchange Online](#) for instructions on how to use Remote PowerShell.

Exchange Online uses the same PowerShell commandlets as Exchange Server 2010 Service Pack 1, with certain commands and parameters disabled because these features do not apply in the hosted environment. For a list of the commandlets available to Exchange Online administrators, see [Reference to Available PowerShell Cmdlets](#).

Role-Based Access Control

Exchange Online uses a Role-Based Access Control (RBAC) model that allows organizations to finely control what users and administrators can do in the service. Using RBAC, administrators can delegate tasks to employees in the IT department as well as to non-IT employees. For example, if a compliance officer is responsible for mailbox search requests, the administrator can delegate this administrative feature to the officer.

Exchange Online uses the same RBAC framework as Exchange Server 2010 Service Pack 1. Administrators can use the Exchange Control Panel to assign users to built-in roles and role groups. Alternatively, they can use Remote PowerShell to create custom RBAC roles. For example, an administrator can create a custom role to let the help desk team manage mailboxes only for users in a certain subsidiary or geographic region.

The following role groups are available by default in Exchange Online:

- Organization Management
- View-Only Organization Management
- Recipient Management
- Unified Messaging Management
- Help Desk
- Records Management
- Discovery Management

The Microsoft Online platform has an implementation of role-based permissions that is separate from Exchange Online RBAC. Users who are Global Administrators or Service Administrators in Microsoft Online are automatically assigned to the Organization Management role group in Exchange Online. Users who are Help Desk Administrators in Microsoft Online are automatically assigned to the Help Desk role group in Exchange Online. Otherwise, the two security models are managed separately.

By default, users in the Organization Management role group cannot log in to other user's mailboxes, and cannot search the content of other user's mailboxes using multi-mailbox search. However, they can assign themselves these permissions via RBAC. Organizations who want to prevent their administrators from reading other users' mail can assign these administrators other Role Groups that do not have the ability to modify RBAC permissions. Organizations can also use auditing reports to monitor changes that administrators make to Role Groups and RBAC permissions.

To learn more about configuring RBAC in Exchange Online, see the help topic [Role Based Access Control in Exchange Online](#).

Message Tracking

Administrators can use delivery reports to view detailed reporting on email messages within the Exchange Online environment. Using the Exchange Control Panel, they can search for messages and view information such as time and date of delivery, reasons for non-delivery, and policies applied. Users can also view delivery report information for the emails they have sent by accessing the Outlook Web App Options page.

See the help topic [Track Messages with Delivery Reports](#) for details.

To access delivery information for messages sent to external destinations, administrators can use the message tracking capabilities within the Forefront Online Protection for Exchange (FOPE) Administration Center.

Usage Reporting

Administrators can use Remote PowerShell to retrieve information about how people in their organizations use the Exchange Online service. Available information includes:

- Showing the mailbox size for each user in the organization.
- Displaying custom permissions that are set on mailboxes, such as delegate access.
- Extracting data about mobile device access, such as which users are connecting through Exchange ActiveSync, what devices they are using, and when they last connected.

Remote PowerShell commandlets that start with "get-" have the ability to fetch data from the Exchange Online system. Administrators can export this information from PowerShell in .csv format for advanced analysis or reporting.

Auditing

Exchange Online provides two types of built-in auditing capabilities:

- **Administrator Audit Logging:** Allows customers to track changes made by their administrators in the Exchange Online environment, including changes to RBAC roles or Exchange policies and settings.
- **Mailbox Audit Logging:** Allows customers to track access to mailboxes by users other than the mailbox owner, including access by delegates and access to shared mailboxes.

Several predefined audit reports are available in the Exchange Control Panel, including Administrator Role Changes, Litigation Hold, and Non-Owner Mailbox Access. Administrators can filter reports by date and role, and can export all audit events for specified mailboxes in XML format for long-term retention or custom reporting.

Administrator audit logging is on by default, and log entries are retained for 90 days.

Mailbox audit logging is off by default. Administrators can use Remote PowerShell to enable mailbox audit logging for some or all mailboxes in their organization. When mailbox audit logging is enabled, log entries are retained for 90 days by default. This value can be raised or lowered using Remote PowerShell (Set-Mailbox <Identity> -AuditLogAgeLimit).

See the help topic [Use Auditing Reports in Exchange Online](#) for details.

Application Interoperability Features

Administrators can connect many kinds of on-premises and hosted applications to Exchange Online, including custom line-of-business applications and software from third-party vendors.

- The application vendor must provide support for the application and perform all related application compatibility testing.
- Custom applications cannot be hosted in a Microsoft data center, unless they are hosted on the Windows Azure™ platform.
- Exchange Online does not host custom code or third-party applications, including .dlls, custom code packaged in transport agents, or allow modifications to files on servers in the data center.
- Applications that send email messages are subject to the same recipient limits and message rate limits as regular mailboxes. These limits are described in the [Recipient Limits](#) section of this document.

The following sections describe the methods available for connecting applications to Exchange Online and identify some Exchange Server application programming interfaces (APIs) that are unavailable in Exchange Online.

Exchange Web Services

Exchange Web Services (EWS) is the preferred development API for Exchange Server and Exchange Online. Using EWS or the EWS Managed API, administrators can access data stored with Exchange Online from applications that are running on-premises, in Windows Azure, or in other hosted services. EWS can perform specialized actions, such as querying the contents of a mailbox, posting a calendar event, creating a task, or triggering a specific action based on the content of an email message.

For details on how to use Exchange Web Services with Exchange Online, refer to the technical articles at the [Exchange Online Developer Center](#).

SMTP Relay

Exchange Online can be used as an SMTP delivery service to relay email messages sent from fax gateways, network appliances, and custom applications. For example, if a line-of-business application sends email alerts to users, it can be configured to use Exchange Online as the mail delivery system. The application or service must authenticate with the username and password of a valid, licensed Exchange Online mailbox, and connect using TLS. The SMTP server name to use can be found by logging into Outlook Web App, viewing the Options page, and clicking "Settings for POP, IMAP, and SMTP access." Applications that use SMTP relay are subject to the same recipient limits and message rate limits as regular users. These limits are described in the [Recipient Limits](#) section of this document.

Outlook Web App Web Parts

Exchange Online supports Outlook Web App Web Parts via the PageViewer control in Microsoft SharePoint Online and Microsoft SharePoint Server, or via manually configured URLs. Built-in SharePoint OWA Web Part controls will not work against Exchange Online.

Outlook Add-Ins and Outlook MAPI

Most Outlook add-ins will work with Exchange Online. Microsoft does not provide support or troubleshooting help for Outlook add-ins. Customers must contact the vendor that created the add-in for

assistance.

Custom applications that use the Outlook MAPI library typically can connect to Exchange Online, but those that use the Exchange Server MAPI library will not connect (see the next section for details). If a custom application requires Outlook to be installed in order to function, it probably uses the Outlook MAPI library.

Exchange Server MAPI/CDO

Some third-party applications use Exchange Server MAPI Client and Collaboration Data Objects (MAPI/CDO) for server-to-server communication with Exchange. These applications need to be installed within the same local network as Exchange and will not connect over the Internet to Exchange Online.

WebDAV

The Exchange WebDAV API was removed from Exchange Server 2010 and is not available in Exchange Online.

Lync Server 2010 or Office Communications Server 2007 R2

For customers who have deployed Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007 R2 on premises, Microsoft Office Communicator can connect to Exchange Online using Exchange Web Services to access out-of-office messages and calendar data.

On-premises Lync Server 2010 can interoperate with Exchange Online in two additional ways:

- IM and presence interoperability in Outlook Web App (see the [Office Web App](#) section of this document for details)
- Voicemail interoperability (see the TechNet article [Providing Lync Server 2010 Users Voice Mail on Hosted Exchange UM](#) for details)

Other Information

Public Folders

Public folders are not available in Exchange Online. To learn about strategies for transitioning away from public folders as part of a migration to Exchange Online, see the [Migrate from Exchange Public Folders to BPOS](#) whitepaper:

Directory Synchronization

To simplify management of the Microsoft Office 365 environment, Microsoft provides the Microsoft Online Services Directory Synchronization tool to help synchronize a company's local Active Directory data with Exchange Online, SharePoint Online, and Lync Online. The tool is available free of charge.

Administrators can download the Directory Synchronization tool from the Administration Center and install it on a computer in the on-premises network where Active Directory resides. The Directory Synchronization tool creates an account in Exchange Online for all mail-enabled users in the Active Directory forest as well as for distribution groups, and global contacts. Subsequent updates to user accounts—such as adding, deleting, or modifying user accounts—are pushed by the Directory Synchronization tool to Exchange Online.

The Directory Synchronization tool plays an important role in hybrid email scenarios, enabling smooth migration from on-premises Exchange Server to Exchange Online. After the migration is complete, the Directory Synchronization tool helps simplify management of the Exchange Online environment by eliminating the need to manage Active Directory users and groups in two places.

Note

The Directory Synchronization tool supports synchronization from only one customer Active Directory forest to Microsoft Office 365.

The Directory Synchronization tool performs a one-way synchronization from on-premises Active Directory to Exchange Online. Changes made in Exchange Online are not synchronized to the on-premises Active Directory, and no on-premises Active Directory objects are updated by Directory Synchronization tool, unless the administrator enables an optional feature called Directory Sync Writeback.

Directory Sync Writeback makes it easier for organizations that configure a hybrid deployment between Exchange Server 2010 and Exchange Online to move cloud mailboxes back on-premises (see the [Migration and Hybrid Deployments](#) section). When users are moved back on-premises, Directory Sync Writeback automatically updates selected Active Directory properties to preserve their ability to reply to historical messages in their mailboxes. It also brings users' safe and blocked sender lists back to the on-premises environment.

Directory Sync Writeback is required for organizations that deploy Exchange Online Archiving, a cloud-based email archive for users with on-premises Exchange Server 2010 mailboxes. See the [Exchange Online Archiving Service Description](#) for details.

Migration and Hybrid Deployments

Microsoft provides tools to help migrate an existing email environment to Exchange Online. Using these tools, administrators can migrate to Exchange Online from:

- IMAP-based email systems
- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010

Tools for migrating from other email systems, such as IBM Lotus Notes/Domino and Novell GroupWise, will be provided by third-party vendors.

Organizations should choose migration options based on their source email systems, desired end state (fully hosted or partially hosted), the number of users to migrate, and how quickly the end state needs to be reached. At a high level, organizations have the following options:

- **IMAP migration:** Migrate data from IMAP-based email systems to Exchange Online with a single cutover migration.
- **Cutover Exchange migration:** Migrate data from Exchange 2003, Exchange 2007, Exchange 2010, and Hosted Exchange systems to Exchange Online in a single cutover migration.
- **Staged Exchange migration:** Perform a staged migration from Exchange 2003, Exchange 2007, and Exchange 2010 with web-based migration tools and minimal changes to on-premises infrastructure.
- **Exchange hybrid deployment:** Add an Exchange 2010 Service Pack 1 server to the on-premises Exchange 2003 or Exchange 2007 environment and use the Exchange Management Console to move mailboxes to Exchange Online.

For more details on migration and hybrid deployment options, see the help topic [Choose a migration or coexistence option](#).

IMAP Migration

Exchange Online offers a web-based tool for migrating 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 PowerShell).
2. Enter the remote server connection settings.
3. Specify a list of mailboxes to be moved.
4. After this information is entered, Exchange Online begins to migrate email content via IMAP (calendar items, contacts, tasks, and other non-mail items are not migrated).

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

See the help topic [Migrate E-Mail from an IMAP Server to Cloud-based Mailboxes](#) for details about IMAP Migration.

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. Enter the address of the remote Exchange Server and credentials for an on-premises administrator account.
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 finalizes the migration.

To switch users to their cloud mailboxes, administrators 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 this migration method, Exchange Online needs to connect to an on-premises Exchange Server, so the on-premises server must have a certificate issued by a trusted certificate authority and public IP address. Administrators cannot use this migration method to migrate more than 1,000 users.

See the help topic [Migrate All Mailboxes to the Cloud with a Simple Exchange Migration](#) for details about Exchange cutover migration.

Staged Exchange Migration

With a staged migration, users can be migrated to the cloud using the web-based Exchange migration tool described earlier in this document. The same conditions and limitations of regular Exchange migration apply. However, instead of migrating all users at once, administrators migrate users in stages. This is accomplished by uploading a .csv file to specify a partial list of users to migrate.

Staged Exchange migration requires administrators to use the Directory Synchronization tool. This provides users with a unified Global Address List where the online environment is continuously synchronized with the on-premises environment. In a staged migration, all of the users in an organization can share the same email domain name, but on-premises users cannot see calendar or free/busy information for Exchange Online users, and vice versa.

See the help topic [Migrate a Subset of Mailboxes to the Cloud with a Staged Exchange Migration](#) for details.

Exchange Hybrid Deployment

Organizations running Exchange Server 2003, Exchange Server 2007, or Exchange Server 2010 can establish a hybrid deployment between Exchange Server and Exchange Online. Hybrid deployments enable a smooth migration experience and allow organizations to keep a mix of on-premises users and online users for an extended period of time. Hybrid deployments provide these advantages:

- Cloud and on-premises users can share free/busy calendar data. This includes full free/busy details, including meeting subject and location, for users on Exchange Server 2007 or Exchange Server 2010, and basic free/busy information for users on Exchange Server 2003.
- Administrators can use the Exchange Management Console to manage cloud and on-premises environments.
- Administrators can use powerful and familiar Exchange management tools to move users to the cloud.
- Administrators do not need to manually reconfigure Outlook profiles or resynchronize .ost files after moving users' mailboxes.
- MailTips, out-of-office messages, and similar features understand that cloud and on-premises users are part of the same organization.
- Delivery reports and multi-mailbox search work with users who are on-premises and those working in the cloud.

- Authentication headers are preserved during cross-premises mail flow, so all mail looks and feels like it is internal to the company (for example, recipient names resolve in the Global Address List). This feature requires a direct SMTP connection between Exchange Online and on-premises Exchange Server 2010 SP1 Edge servers or Hub Transport servers (email must not be routed through any other SMTP gateway).
- If necessary, administrators can easily move mailboxes back to the on-premises Exchange environment.

To implement a hybrid deployment, administrators deploy an Exchange Server 2010 Service Pack 1 server in their Exchange Server 2003 or Exchange Server 2007 environments and configure Exchange federation with Exchange Online. The Exchange 2010 server acts as a bridge between Exchange 2003 or Exchange 2007 environments and Exchange Online. Organizations do not need to upgrade mailboxes to Exchange 2010 prior to moving them to the cloud.

Note

Organizations that install an Exchange 2010 server solely to act as a bridge between their Exchange Server 2003 or Exchange Server 2007 on-premises environments and Exchange Online can request a Hybrid Edition server key to license the server. See the [Exchange Online Licensing page](#) for details.

Hybrid deployments require the Directory Synchronization tool to be running in the local environment. Directory Sync Writeback is recommended to enable smooth offboarding of users (see the Directory Synchronization section of this document for details). Deployment of Active Directory Federation Services 2.0 is also recommended to enable single sign-on.

See the help topic [Exchange Online Hybrid Deployment and Migration with Office 365](#) for details about Exchange hybrid deployments.

Exporting Data from Exchange Online

To export data from Exchange Online, an administrator can connect Outlook to Exchange Online mailboxes, and then export the data to PST files. See the help topic [Cancel Your Exchange Online E-Mail Service](#) for details.

Organizations that have configured an Exchange hybrid deployment also have the option of off-boarding mailboxes to on-premises Exchange Server 2003, 2007, or 2010. See the [Exchange Hybrid Deployment](#) section of this document for details.

Appendix A: Exchange Online and Exchange Server Feature Comparison

	Exchange Server 2010 Service Pack 1	Exchange Online
SERVICE FEATURES		
Mailbox size	Configurable	500 MB for Exchange Online Kiosk user, 25 GB for Exchange Online Plan 1 user, unlimited for Exchange Online Plan 2 user
Message size limits (max attachment size)	Configurable	25 MB
Recipient limits	Configurable	1,500 recipients/day
Message rate limits	Configurable	30 messages/minute
Deleted item recovery	Configurable	14 Days
Deleted mailbox recovery	Configurable	30 Days
CLIENT ACCESS		
Outlook 2010	Yes	Yes
Outlook 2007	Yes	Yes
Outlook 2003	Yes	No
Outlook Anywhere (RPC over HTTPS)	Yes	Yes
Outlook Cached Mode	Yes	Yes
Outlook Online Mode	Yes	Yes (not recommended)
Autodiscover	Yes (for Outlook and mobile)	Yes (for Outlook and mobile)
Outlook Web App	Internet Explorer 7+, Safari 3+, Firefox, Chrome	Internet Explorer 7+, Safari 3+, Firefox, Chrome
Outlook Web App light experience	Almost any browser	Almost any browser
Outlook Web App: Vanity URL (http://mail.contoso.com)	Yes	Customer can set up a redirect
Public/private computer logon option	Yes	No
Outlook Web App: session time-out	Configurable	Default: 6 hours Configurable up to 24 hours.
WebReady document viewing	Yes	Yes
Disable web access	Yes	Yes
Instant messaging and presence connected to web email client	Yes	Yes
Macintosh support (rich client)	Outlook for Mac 2011, Entourage 2008 Web Services Edition	Outlook for Mac 2011, Entourage 2008 Web Services Edition
IMAP	Yes	Yes
POP	Yes	Yes
MOBILITY		
Windows Phone 7 devices	Yes	Yes
Windows Mobile devices	Windows Mobile 5.0+	Windows Mobile 6.0+
Other Exchange ActiveSync devices (such as iPhone)	Yes	Yes

	Exchange Server 2010 Service Pack 1	Exchange Online
Remote device wipe (implementation varies by mobile device manufacturer)	Yes	Yes
Customize Exchange ActiveSync security policies and settings, including PIN/password lock	Yes	Yes
Disable Exchange ActiveSync access	Yes	Yes
Mobile device allow/block/quarantine	Yes	Yes
Certificate-based authentication for Exchange ActiveSync	Yes	No
Over-the-air-update for Outlook Mobile	Yes	Yes
Mobile SMS sync (through Exchange ActiveSync)	Yes	Yes
SMS (text messaging) notifications	Yes	Yes
BlackBerry (via Blackberry Enterprise Server)	Yes	Coming later this year
BlackBerry (via Blackberry Internet Service)	Yes	Yes
EMAIL/INBOX		
"Send on behalf of" and "send as"	Yes	Yes
Shared mailboxes	Yes	Yes
Catch-all mailbox	Yes	No
Server-side email forwarding	Yes	Yes
Inbox rules	Yes	Yes
Tasks	Yes	Yes
Conversation view and actions (such as ignore conversation)	Yes	Yes
MailTips and MailTips customization	Yes	Yes
Connected accounts (aggregate mail from multiple external email accounts)	No	Yes
CONTACTS/DIRECTORY		
Personal contacts	Yes	Yes
Personal distribution groups	Yes	Yes
Shared distribution groups (in Global Address List)	Yes	Yes—managed via web or synchronized from Active Directory
Restricted distribution groups	Yes	Yes
Dynamic distribution groups	Yes	Yes
Moderated distribution groups	Yes	Yes
Self-service distribution groups	Yes	Yes (for groups not synchronized from on-premises Active Directory)
Global Address List	Yes	Yes
Hide users from Global Address List	Yes	Yes
Custom address lists	Yes	No
Hierarchical address lists	Yes	No
Global Address List segmentation	Yes	No
Offline Address Book	Yes	Yes
External contacts (in Global Address List)	Yes	Yes
CALENDAR		
Out-of-office auto-replies	Yes	Yes
Cross-premises calendar free/busy (mix of on-premises/cloud users)	Not applicable	Yes
Federated calendar sharing	Yes	Yes

	Exchange Server 2010 Service Pack 1	Exchange Online
Publish or subscribe to calendar through iCal	Yes	Yes
Side-by-side calendar view in web client	Yes	Yes
Resource mailboxes (for example, for conference rooms or equipment)	Yes	Yes
Outlook 2010 Room Finder	Yes	Yes
UNIFIED MESSAGING, FAX		
Interoperability with on-premises voicemail systems	Yes	Via SMTP or Exchange Web Services
Exchange Unified Messaging (hosted voicemail)	Yes	Yes
SECURITY		
Anti-spam (AS)	Customer chooses AV/AS solution	Forefront Online Protection for Exchange
Antivirus (AV)	Customer chooses AV/AS solution	Forefront Protection for Exchange
Safe and blocked senders (configurable at the organization level)	Yes	Yes
Opportunistic TLS for inbound/outbound email	Yes	Yes
Forced TLS for inbound/outbound email	Yes	Yes
S/MIME	Yes	Yes, with limitations No Outlook Web App support
PGP	Yes	Yes
COMPLIANCE/ARCHIVING		
Disclaimers	Yes	Yes
Transport rules	Yes	Yes
Personal archive	Yes	Yes
Retention policies	Yes	Yes: Exchange 2010 retention policies No: Exchange 2007-style managed folders
Journal messages to external or on-premises archive	Yes	Yes
Multi-mailbox search (e-discovery)	Yes	Yes
Legal hold	Yes	Yes
Rolling legal hold (single item recovery)	Yes	Yes
ADMINISTRATION		
Administration through a Web-based interface (Exchange Control Panel)	Yes	Yes
Forefront Online Protection for Exchange Administration Center access	Optional	Yes
Administration through command line shell (PowerShell)	Yes	Yes
Role-Based Access Controls (RBAC)	Yes	Yes
Message tracking	Yes	Yes

	Exchange Server 2010 Service Pack 1	Exchange Online
Usage reporting	Some data can be extracted using PowerShell	Some data can be extracted using PowerShell
Auditing	Yes	Yes
APPLICATION ACCESS/CUSTOMIZATION		
Application connectivity through web services	Yes	Yes
SMTP relay	Yes	Yes
Outlook Web App Web Parts	Yes	Yes
Outlook add-ins and Outlook MAPI	Yes	Yes
Application connectivity through Exchange Server MAPI/CDO API	Yes	No
Application connectivity through DAV	No	No
OTHER		
Public folders	Yes	No
Global Address List synchronization from on-premises directory (Active Directory)	Not applicable	Yes—one-way through the Directory Synchronization tool
Global Address List synchronization from multiple on-premises Active Directory forests	Yes	No