Office 365
Dedicated and ITAR-support Plans

Exchange Online Dedicated Service Description

Applies to: *Exchange Online Dedicated – Legacy Platform Release*

Topic Last Modified: *2015-08-31*

Microsoft Exchange Online is an enterprise-class, remotely hosted, email messaging solution that uses the power of Microsoft Exchange Server to provide the mission-critical messaging services that businesses require today. Messaging content held in Exchange Online is accessible to users on a wide range of devices from inside your corporate network or over the Internet. The service gives users single sign-on access to email, calendar, and contacts from virtually anywhere and at any time.

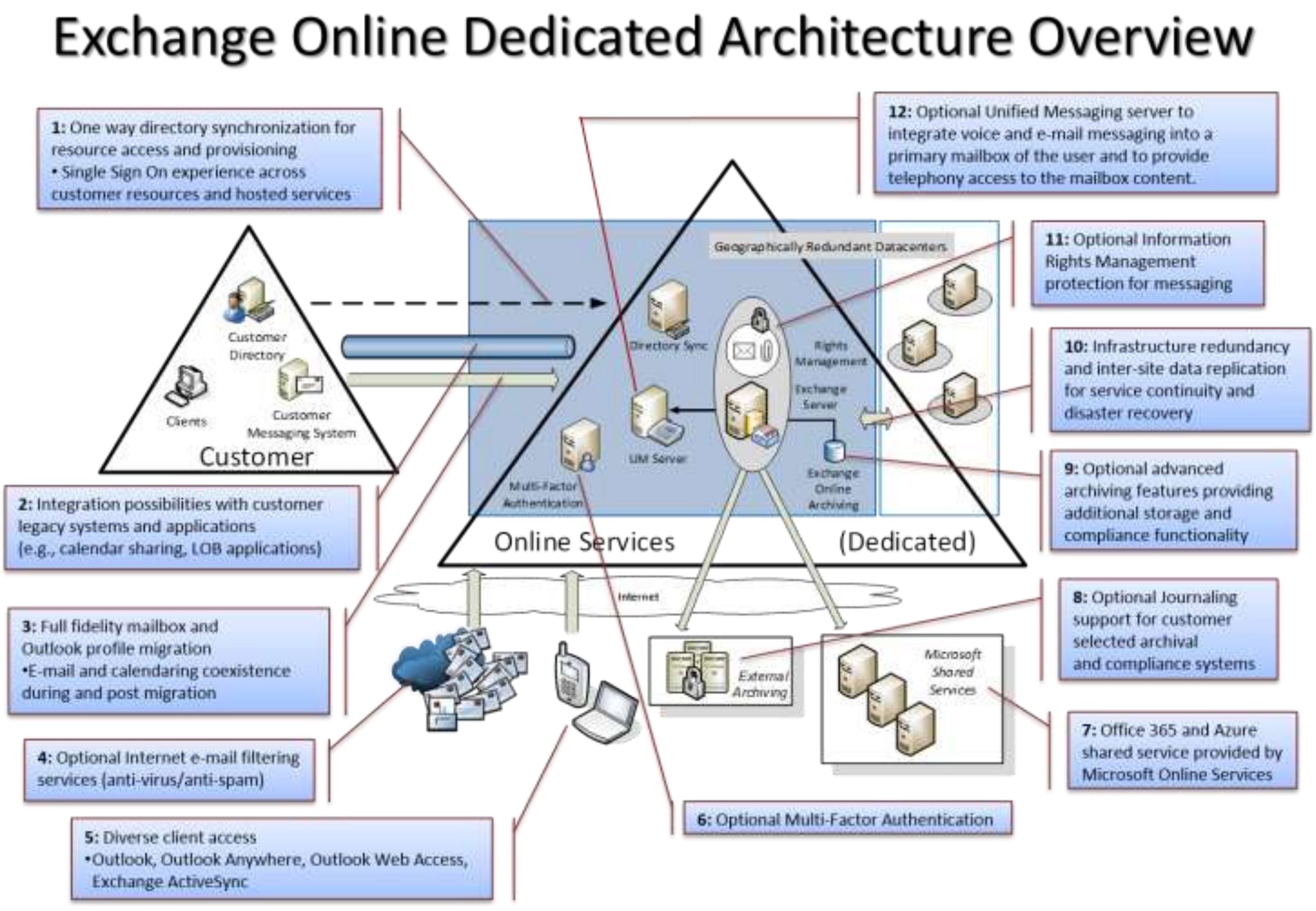
Microsoft offers several versions of Exchange Online for enterprise environments. In comparison to the commonly known "Exchange Online" service provided by a virtualized environment on multi-tenant hardware, the Exchange Online Dedicated offering is a premium service provided to a single tenant on dedicated hardware. When your organization subscribes to a dedicated plan of Exchange Online for enterprises, your messaging content is hosted on dedicated servers that are housed in reliable, security-enhanced, Microsoft data centers.

Messaging Infrastructure

Microsoft operates data centers around the world to support online services. For Exchange Online Dedicated, data centers equipped with highly reliable information systems and networking equipment are used to provide messaging solutions and to deliver 99.9 percent uptime. The service is backed by service level agreements (SLAs) that guarantee optimal performance.

Organizations that choose Exchange Online Dedicated have exclusive use of the servers that are needed to support their specific messaging requirements. Automated synchronization to allow your on-premises directory information to be synched continuously with your directory in the Microsoft data centers also is provided. The copy of your on-premises directory held within Office 365 Dedicated allows users to have seamless access to messaging applications from a wide range of devices while within the corporate network or on the Internet. Your organization also retains control over the messaging services offered to your users. The IT personnel of your organization can use the features of Active Directory to control service availability through existing group policies.

The Exchange Online service is built on the latest Exchange Server 2013 release and is integrated with other messaging components to provide a comprehensive, remotely hosted messaging service for the enterprise. The diagram below is a representation of the high-level infrastructure of the Exchange Online Dedicated environment.



Exchange Online Dedicated Architecture Overview

1: One way directory synchronization for resource access and provisioning
• Single Sign On experience across customer resources and hosted services

2: Integration possibilities with customer legacy systems and applications (e.g., calendar sharing, LOB applications)

3: Full fidelity mailbox and Outlook profile migration
•E-mail and calendaring coexistence during and post migration

4: Optional Internet e-mail filtering services (anti-virus/anti-spam)

5: Diverse client access
•Outlook, Outlook Anywhere, Outlook Web Access, Exchange ActiveSync

6: Optional Multi-Factor Authentication

7: Office 365 and Azure shared service provided by Microsoft Online Services

8: Optional Journaling support for customer selected archival and compliance systems

9: Optional advanced archiving features providing additional storage and compliance functionality

10: Infrastructure redundancy and inter-site data replication for service continuity and disaster recovery

11: Optional Information Rights Management protection for messaging

12: Optional Unified Messaging server to integrate voice and e-mail messaging into a primary mailbox of the user and to provide telephony access to the mailbox content.

Key Benefits Summary

The Exchange Online service offers the following benefits:

- **Flexible messaging services.** Email, shared calendar, Outlook connectivity, and Microsoft Outlook Web App provide the flexibility to meet diverse and evolving organizational needs.
- **Regulatory compliance features.** Meeting the increasingly complex regulatory requirements is eased with Sarbanes-Oxley and SAS 70 Type II self-assessment and audit support.
- **Multi-level data protection.** Safeguards are applied on multiple fronts, from message encryption support to the multilevel message filtering capabilities that include spam and virus protection, to the logical and physical security that protects your information in the data centers.
- **Mobility device support.** Mobility features provide the messaging agility that organizations require to stay competitive in the marketplace, allowing users to easily access their hosted services and stay connected anywhere in the world. At the same time, remote device wipe and policy provisioning help to ensure that sensitive data is protected.
- **Remote administration of key features.** Organization and user administration features are designed to help reduce Service Desk escalations, enhance service management, and empower users.

Notes:

- The content of this service description applies to the *legacy* platform release (ANSI high availability) of the Exchange Server 2013 operating environment available to existing Exchange Online Dedicated customers. New customers will utilize a newer release of Exchange Online which leverages the common service fabric designed to support either a multi-tenant or dedicated implementation of the service. All existing Exchange Online Dedicated customers gradually will be migrated to the new release. Contact your Microsoft account team for additional information.
- Unless otherwise indicated, the information in this service description also applies to the International Traffic in Arms Regulations (ITAR-support) version of Exchange Online.

Planning and Deployment

Planning is required to identify and deploy the Exchange Online Dedicated infrastructure, mailbox plans, optional features, and optional services to meet your specific messaging needs. The implementation chosen will support the migration of user accounts and user mailbox data from an on-premises environment to Exchange Online Dedicated. Infrastructure readiness must be addressed including verification that all client systems are compliant for use with Exchange Online Dedicated. Following the propagation of user objects from the on-premises Active Directory to Office 365 Dedicated, the execution of mailbox migrations can commence. Microsoft can assist with all aspects of planning and with providing specific process descriptions, tools, and design considerations to support establishing an Exchange Online Dedicated environment.

Implementation Options

Your organization has the following options for deploying Exchange Online Dedicated:

- **Cloud-only deployment.** In this type of deployment, your organization has all user mailboxes hosted in Exchange Online Dedicated. A cloud-only deployment is one where your Exchange Online Dedicated implementation isn't connected with an on-premises Exchange organization. All users and mailboxes are hosted and managed in Exchange Online Dedicated.
- **Hybrid deployment.** With this option, your organization has some number of user mailboxes hosted in an on-premises Exchange environment in addition to user mailboxes hosted in Exchange Online Dedicated. For organizations with Microsoft Exchange Server 2003 or later version on-premises, a hybrid deployment offers (a) a migration path to allow all user mailboxes to be hosted in Exchange Online Dedicated, (b) a long-term coexistence configuration allowing some mailboxes to be hosted on-premises and some mailboxes to be hosted in Exchange Online Dedicated, and (c) the ability to self-migrate mailboxes between the on-premises and Exchange Online Dedicated environments at any time on demand. Hybrid deployment features include secure mail transport, shared calendar free/busy information, and message tracking between the on-premises and Exchange Online organizations.

Important:

You must deploy a valid "hybrid" Exchange Server on-premises to facilitate the creation of a coexistence environment. Required is either an Exchange Server 2010 or Exchange Server 2013 configuration with specific server roles per the requirements described in the table below (a later version of Exchange Server is required to support federated sharing services and customer driven cross-forest migrations). Engaging Microsoft Premier Field Services or Microsoft Consulting Services to assist with defining specific configuration requirements is recommended.

On-premises Mail Server	Intended Coexistence Period	Recommended On-premises Hybrid Exchange Server Configuration	Notes
Exchange Server 2003	Migration Period Only	Single Exchange Server 2010 (with SP3 or later) server	Use Exchange Server 2010 as the hybrid server with at least the Client Access, Transport, and Mailbox server roles. Exchange Server 2003 must have SP2.
Exchange Server 2003	Long Term	Multiple Exchange Server 2010 (with SP3 or later) servers	Use an Exchange Server 2010 server as the hybrid server with at least the Client Access, Transport, and Mailbox server roles. Exchange Server must have SP2.

Exchange Server 2007	Migration Period Only	Single Exchange Server 2010 (with SP3 or later) or Exchange Server 2013 server	Use an Exchange Server 2010 or Exchange Server 2013 server as the hybrid server with at least the Client Access server role. Exchange Server 2013 also requires the Mailbox role to support the Mailbox Replication Service Proxy function. Exchange Server 2007 server must have SP3 RU10.
Exchange Server 2007	Long Term	Multiple Exchange Server 2010 (with SP3 or later) or Exchange Server 2013 servers	Use an Exchange Server 2010 or Exchange Server 2013 server as the hybrid server with at least the Client Access server role. Exchange Server 2013 also requires the Mailbox role to support the Mailbox Replication Service Proxy function. Exchange Server 2007 must have SP3 RU10.
Exchange Server 2010	Migration Period Only	Single Exchange Server 2010 (with SP3 or later) or Exchange Server 2013 server	

Exchange Server 2010	Long Term	Multiple Exchange Server 2010 (with SP3 or later) or Exchange Server 2013 servers
Exchange Server 2013	Migration Period Only	Single Exchange Server 2013 server
Exchange Server 2013	Long Term	Multiple Exchange Server 2013 servers

Infrastructure Readiness

During the initial planning stage to address your migration to Exchange Online Dedicated, Microsoft will engage your organization to assess all aspects of planning to migrate on-premises messaging services to Exchange Online Dedicated. Support for a coexistence configuration—the phase in which you begin using Exchange Online Dedicated while continuing to use your existing on-premises messaging system—will be a component of the planning process. Access and identity management also will be considered. Identity management considerations and a description of provisioning tools and directory synchronization processes are described in the Identity & Provisioning Service Description. The Network Service Description provides an overview of the private network implementation for Office 365 Dedicated and the use of customer provided network equipment.

Customer Responsibilities

- Provide network speed estimates between all your sites and the Microsoft data center.
- Ensure all client systems adhere to the Client System Requirements.
- Install a supported version of Microsoft Outlook with the appropriate profile on all client systems to achieve connectivity with the Microsoft data center and to ensure proper message routing and directory synchronization. Setting cached mode for your version of Outlook is recommended.

Microsoft Responsibilities

- Deploy and maintain Exchange Server and related components in Microsoft data centers.
- Provide processes and tools to (a) support the migration of mailboxes to the appropriate Microsoft data centers and (b) update Microsoft Active Directory objects in the on-premises environments.

Software and Feature Support Limitations

The following system software, applications, and features are either not supported or have limited support when used with Exchange Online Dedicated:

- Exchange Online Dedicated only supports BlackBerry® Enterprise Server (BES) 5.0 for the BlackBerry-managed mobile client. See Blackberry Enterprise Server for additional information.
- Administrative tools used to support Exchange Online Dedicated only include Exchange Admin Center (EAC) and Windows PowerShell.

Mailbox Data Migration

The Migration dashboard of the EAC is available to your organization to execute self-service migrations of Exchange mailboxes between the on-premises and online environments. A mailbox can be migrated in either direction. The move of a mailbox also includes its archive mailbox if it exists. If assistance is needed, Microsoft also can perform a mailbox migration as a consulting service.

Messaging content held on an on-premises Lotus Domino server also can be migrated to Exchange Online Dedicated. Microsoft must be engaged to perform the migration as a service. The migration of content from the on-premises environment to Exchange Online Dedicated is the only supported service offering.

An on-premises hybrid Exchange server is required to support an on-premises/online coexistence environment. Following verification of the hybrid server configuration, authorized staff within your organization are able to use EAC to execute a *remote move* migration. The Migration dashboard of EAC displays statistics about the overall migration in addition to statistics about a specific migration batch. You can create, start, stop, pause, and edit migration batches. If Microsoft is engaged to assist, the migration process is conducted with minimal end-user interaction and is completed on a schedule that is jointly determined by you and Microsoft.

Exchange mailboxes can be migrated from or to an on-premises Exchange Server version listed in Hybrid deployment. For additional information regarding the mailbox migration process, contact your Microsoft Service Delivery Manager.

Customer Responsibilities

- Maintain the existing on-premises message solution during the coexistence phase.
- Decommission the existing messaging solution, if necessary, after migration to Exchange Online Dedicated.

- If you're migrating from a Lotus Domino environment, contact your Microsoft Account Team regarding readiness activities, partner services, or additional consultation that may be required for data migration.

Microsoft Responsibilities

- For a consulting engagement, Microsoft will work with you to build a migration schedule that is optimized to process the maximum number of mailboxes for each set of mailbox migrations including consideration for mailbox size and network capacity.

Limitations

- Migrated data cannot exceed 85 percent of the capacity of the target mailbox. Migrated data volume has a direct relation to migration velocity. To achieve maximum migration velocity, mailbox size reduction may be required.
- Recurring meetings are migrated to the new mailbox but often cannot be edited after migration. Meeting organizers should expect to send out new recurring meetings and instruct attendees to manually delete the old series.

User Communications for Migration Support

The Microsoft deployment team can provide your organization with service-related training guides and user communication templates that can help you successfully complete the migration process and deliver important information to users moving to Exchange Online Dedicated.

Customer Responsibilities

- Customize the communication templates that are provided by Microsoft.

Microsoft Responsibilities

- Provide communication templates and user training guides.
- Work with your organization to create a communication strategy for the mailbox data migrations.

Mailbox Plans

This section describes available mailbox plans for Exchange Online Dedicated, including mailbox types, the management of mailboxes, and features available to mail clients.

Dedicated Plans Descriptions

Your organization can purchase Exchange Online Dedicated user subscriptions as a standalone plan or as part of an enterprise suite plan that includes other Office 365 Dedicated services. The following sections describe the key features of each plan type. A Microsoft sales representative can provide additional information regarding Office 365 subscription plans.

Standalone Dedicated Plans

As an Exchange Online Dedicated customer, you can provision a messaging plan for each subscriber in your organization. Each subscriber is assigned one (1) mailbox and each mailbox has a unique messaging plan. Folders and messages in these mailboxes reside within the Exchange Server infrastructure of Exchange Online Dedicated.

To simplify the provisioning process, messaging seat features are packaged according to the standalone Exchange Online Dedicated plan subscription assigned to the user as shown in the following table.

Features	Exchange Online Kiosk D Plan[1]	Exchange Online 1D Plan[1]	Exchange Online 2D Plan [1]
Mailbox size	2 gigabyte (GB) [2]	50 GB [2]	50 GB [2]
Access methods [1]	Outlook Web App (with some settings disabled) [3], Exchange ActiveSync (EAS), POP3 [4], Exchange Web Services (EWS) impersonation [5]	Outlook, Outlook Anywhere (RPC/HTTP) [6], Outlook Web App, Exchange ActiveSync (EAS), POP3 [4], IMAP4 [4], Exchange Web Services (EWS)	Outlook, Outlook Anywhere (RPC/HTTP) [6], Outlook Web App, Exchange ActiveSync (EAS), POP3 [4], IMAP4 [4], Exchange Web Services (EWS)
Mobile device connectivity support	Exchange ActiveSync	Exchange ActiveSync BlackBerry Enterprise Server (legacy deployment only)	Exchange ActiveSync BlackBerry Enterprise Server (legacy deployment only)
Office Online [7] (view only)	Included	Included	Included
In-Place Archiving	Optional [9, 10]	Included [8, 9, 10]	Included [10]
Data Loss Prevention	Not Available	Not Available	Included [11]
Outbound Fax	Not Available	Optional	Optional
Hosted Voicemail	Not Available	Not Available	Included

[1] Specific default protocols can be disabled, mailbox quotas can be altered, and/or custom Outlook Web App policies can be applied to mailbox plans; use of specific protocols or requests to access a specific application/service/resource can be blocked using client access rules. The Configuration Request process can be used to apply the restrictions. Contact your Service Delivery Manager (SDM) for assistance.

[2] Organizations are eligible for increased sizes representing up to the values shown only after (a) all Exchange Online mailboxes are hosted on the High Availability infrastructure of Exchange Online Dedicated.

[3] Inbox rules, instant messaging (IM) integration, short message service (SMS) integration, and access to other mailboxes are disabled for Kiosk D subscriptions.

[4] Default availability of protocol cited is for Intranet only. Internet use can be activated using the Client Access Rules feature of Exchange Online Dedicated.

[5] Direct access to Kiosk D user mailboxes via Exchange Web Services is not permitted; however, Line-of-Business (LOB) applications can use Exchange Web Services impersonation to access Kiosk user mailboxes.

[6] Use of RPC/TCP to directly access MAPI has been deprecated from Exchange Server 2013. LOB applications must use either Exchange Web Services (EWS) or Outlook Anywhere (RPC/HTTP) protocol. For more information, see Pre-upgrade priority actions for Exchange Online Dedicated.

[7] Use of the Office Online suite to render message attachments is a view-only shared services experience and requires the Exchange Server 2013 version of Exchange Online Dedicated.

[8] The size of the archive mailbox is a portion of the 50 GB allocation for the Plan 1D subscription. The archive becomes the balance of the mailbox quota set in the provisioning attribute for the subscriber. A 5 GB primary mailbox quota, for example, will result with the creation of a 45 GB archive.

[9] The Exchange Online Archiving (EOA) add-on feature set for the Kiosk D and Plan 1D offerings includes In-Place Archiving (100 GB archive mailbox), Retention Policies, In-Place Hold, Litigation Hold, In-Place eDiscovery, and Auditing features. To secure this optional feature set, contact your Service Delivery Manager for assistance.

[10] Each Exchange Online Archiving (EOA) subscriber receives a default archive mailbox quota of 100 GB. If a subscriber is in need of additional archive storage, a quota exception can be manually applied to the provisioning attribute for the subscriber to increase the quota to 200 GB. For provisioning options, see the *Office 365 Dedicated Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

[11] Licensing for the Data Loss Prevention (DLP) feature is only available for Plan 2D; DLP policies must be scoped to apply only to Plan 2D mailboxes.

Office 365 Dedicated Suite Plans

In addition to the standalone plans, an Exchange Online Dedicated subscription can be included as part of an Office 365 Dedicated suite plan as shown in the following table.

Office 365 Plan K1D/K2D	Office 365 Plan E1D	Office 365 Plan E3D	Office 365 Plan E4D
Exchange Online Plan Kiosk 1D	Exchange Online Plan 1D	Exchange Online Plan 2D	Exchange Online Plan 2D
SharePoint Online Plan Kiosk 2D	SharePoint Online Plan 1D	SharePoint Online Plan 2D	SharePoint Online Plan 2D
Office Online [1]	Lync Online Plan 2D	Lync Online Plan 2D	Lync Online Plan 3D
	Office Online [1]	Office Online [1]	Office Online [1]
		Office Professional Plus 2013 [2]	Office Professional Plus 2013 [2]

[1] When Office Online is used with Outlook Web App in Exchange Online Dedicated, supported attachments are presented as view-only. This capability is available only with the Exchange Server 2013 release of Exchange Online Dedicated.

[2] Volume licensing and streaming delivery options for Office Professional Plus 2013 are described within the *Microsoft Office Client Authentication Services* section of the Identity and Provisioning Service Description for Office 365 Dedicated.

Mailbox Provisioning and Administration

In Exchange Online Dedicated, each object held in Active Directory must utilize an Exchange *CustomAttribute* (also known as Active Directory extension attribute) to hold mailbox size, plan type, feature settings, and other optional provisioning parameters. For more information, see the *Office 365 Dedicated and ITAR-support Plans Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

In addition to its primary role to keep the Active Directory of your on-premises environment synchronized with Office 365, the MMSSPP tool is used to assist with the provisioning of additional mailboxes and to set specific service features for each mailbox held in Exchange Online Dedicated. For more information, see *Directory Synchronization and Service Provisioning* within the Identity & Provisioning Service Description.

Following the provisioning of a mailbox, two self-service mailbox administration options are available within Exchange Online Dedicated for self-service mailbox administration: (a) the menu driven Exchange Admin Center and (b) the command line oriented Windows PowerShell. For a summary of all administration tools, see Administration and Management.

Permissions

Exchange Online Dedicated uses Role-Based Access Control (RBAC) to allow organization admins to finely control what users and IT Pros can do in the service. For example, if a compliance officer is responsible for mailbox search requests, the admin can delegate this administrative feature to the officer through RBAC. Exchange Online Dedicated uses the same RBAC framework provided within Exchange Server 2013.

At its highest level, RBAC is made up of management *roles*, management *role groups*, and management *role assignment policies*. Only members of specific role groups are allowed to execute Windows PowerShell cmdlets assigned to a specific role. RBAC also includes the ability to apply role assignment policies to control settings exposed to end users and *role scopes* to define the specific scope of impact or influence of a management role. For detailed information describing the RBAC implementation for Exchange Online Dedicated, see the Self-Service Administration Feature Guide.

Message Policy, Recovery, and Compliance

Exchange Online Dedicated offers an extensive suite of message policy, recovery, and compliance functionality. The following table describes specific features and their availability status for each Exchange Online Dedicated subscription type.

Message Policy and Compliance Features

Features	Exchange Online Kiosk D	Exchange Online Plan 1D	Exchange Online Plan 2D
In-Place Archiving	Added charge[1]	Added charge[1]	Included
Litigation Hold & In-Place Hold	Added charge[1]	Added charge[1]	Included
Messaging Records Management	Included	Included	Included
Data Loss Prevention	Not available	Not available	Included
Message Journaling	Included	Included	Included
In-Place eDiscovery	Included	Included	Included
Auditing Reports	Included	Included	Included

[1] The Exchange Online Archiving add-on feature set subscription includes In-Place Archiving (100 GB archive mailbox), Retention Policies, In-Place Hold, Litigation Hold, In-Place eDiscovery, and Auditing features.

In-Place Archiving

The In-Place Archiving feature (previously known as Personal Archiving) provides an alternative location for a user to store historical messaging data. An In-Place Archive is an additional mailbox enabled for a mailbox user.

When using Office Outlook 2007 and later versions of Outlook or Outlook Web App, users have seamless access to their In-Place Archive mailbox. Use of these client applications enables them to view an In-Place Archive mailbox and move or copy messages between their primary mailbox and the In-Place Archive. Message Records Management (MRM) 2.0 policies also can be applied to a mailbox to automate the movement of messaging data from the primary mailbox to the In-Place Archive and reduce the risk of data loss caused by end user error. All primary and archive mailbox content present in Exchange is indexed, searchable, and discoverable. In-Place Archives present a consistent view of messaging data to a user and eliminate user overhead required to manage multiple .pst files.

An Exchange admin is able to enable and disable the In-Place Archiving feature on a per-mailbox basis. Feature subscribers receive an archive mailbox as described in Dedicated Plans Descriptions.

Customer Responsibilities

- Inform Microsoft of the intended number of mailboxes to receive In-Place Archiving through the Configuration Request process for Office 365 Dedicated.
- Contact your Microsoft Account Manager or Licensing Specialist to adjust subscription order quantities or to confirm pricing for the archiving feature.
- Follow instructions provided by Microsoft to enable provisioning for each mailbox that requires an In-Place Archive. For more information, see the *Office 365 Dedicated and ITAR-support Plans Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

Microsoft Responsibilities

- Provide additional storage capacity to accommodate all In-Place Archiving requests.

Limitations

- In-Place Archiving functionality is available for specific Exchange Online subscription plans per guidance provided in the Message Policy and Compliance feature table.

Messaging Records Management

Exchange Online Dedicated provides the Messaging Records Management (MRM) v2.0 feature set. MRM makes it easier to keep messages that are needed for compliance with company policies, government regulations, or other requirements. MRM also can be used to remove content that has no business value by using retention policies and retention tags.

Retention policies involve the use of retention tags to apply retention settings to email messages and folders. Retention tags define an age limit that indicates how long items are retained. Included in the tag is a retention action that specifies what happens to items that reach the retention age limit. Retention tags are linked to a retention policy; the retention policy is applied to a mailbox. All MRM tasks are managed directly by your organization by using remote Windows PowerShell.

Customer Responsibilities

- To ensure an MRM 2.0 deployment is properly implemented, utilize a Microsoft Premier Field Engineer (strongly recommended) to review MRM 2.0 deployment plans, coordinate the implementation, and ensure deployment is successful.
- Create and manage retention polices.
- Create and manage retention tags and link retention tags to retention policies.
- Assign retention policies to mailboxes.
- Set up and control access to security groups to allow role-based access permissions for self-service features.
- Validate and test all policies to be implemented on a small set of mailboxes prior to deploying at full scale across a large number of mailboxes.
- Recovery of any data deleted by an incorrect policy.

Microsoft Responsibilities

- Grant role-based access to your security groups.

Limitations

- MRM is available for specific Exchange Online Dedicated subscription plans per guidance provided in the Message Policy and Compliance feature table.
- Conversion of MRM managed folders to retention policy tags is not supported.
- Microsoft Online Services Support will not provide restoration of items deleted as a result of retention policy actions.

- A mailbox cannot have both an MRM 1.0 policy and an MRM 2.0 policy assigned to it at the same time.
- Any mailbox that uses MRM 1.0 policies must be upgraded to use MRM 2.0 policies prior to the transition to the Exchange Server 2013 release of Exchange Online Dedicated. MRM 1.0 policies will not execute within Exchange Server 2013.

Encryption of data at rest

In Office 365 Dedicated, email data at rest is encrypted using BitLocker Drive Encryption. BitLocker encrypts the hard drives on a computer to provide enhanced protection against data theft or exposure on computers and removable drives that are lost or stolen, as well as more secure data deletion when BitLocker-protected computers are decommissioned or recycled. To learn more, see BitLocker Overview. For more information about security features in Office 365, see the Office 365 Trust Center.

Information Rights Management Integration

Information Rights Management (IRM) allows an organization to prevent information leakage by restricting the rights that email recipients have on messages and attachments. Restriction examples are blocking the forwarding of messages to other recipients, preventing the printing of a message or attachment, or preventing copy and paste actions for a message or attachment content.

Administrators can use the cloud-based Azure Rights Management or an on-premises Active Directory Rights Management Services (AD RMS) server in conjunction with Exchange Online Dedicated. Both options are identical to the offerings of the multi-tenant version of the Exchange Online.

If an on-premises AD RMS server is deployed, Outlook can communicate directly with the server to enable users to compose and read messages that are protected by AD RMS. There is no need for interoperability between the AD RMS server and Exchange Online Dedicated in order to use the AD RMS features of Outlook.

Microsoft Exchange Server 2010 introduced advanced IRM-related AD RMS features that organizations can use with Exchange Online. To enable these features, administrators import the Trusted Publishing Domain (TPD) key from their AD RMS server to Exchange Online Dedicated using remote Windows PowerShell.

After this one-time import, the following IRM-related features become available:

- **Support for IRM in Outlook Web App** Users can read and create IRM-protected messages natively in Outlook Web App. They can also view IRM-protected messages in Outlook Web App by using Internet Explorer, Firefox, Safari, and Chrome browsers (with no plug-in required). Viewing features 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 Exchange ActiveSync can open and work with IRM-protected messages without tethering the device or installing additional IRM software. Administrators can control this feature by using Role-Based Access Control (RBAC) or Exchange ActiveSync policies.
- **Search of IRM-protected messages** 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 rules to automatically apply AD RMS protection to email (including Microsoft Office and XPS attachments) in transit. This provides persistent protection anywhere a file is sent and prevents forwarding, copying, or printing depending on the rights policy template applied.
- **Journal report decryption** When journaling messages to an external archive, administrators can include both the IRM-protected message and a decrypted, clear-text copy of the message (including Microsoft Office and XPS attachments) in journal reports. This allows IRM-protected messages to be indexed and searched for legal and regulatory purposes.
- **Protected voice mail** Senders or administrators can apply Do Not Forward permissions to voice mail messages to prevent them from being forwarded to unauthorized persons regardless of the email client.

For additional feature information, see Information Rights Management in Exchange Online.

Note:

1. Exchange Online Dedicated customers on legacy infrastructure platforms (Exchange 2010 Aruna, Exchange 2010 ANSI-D, or Exchange 2013 ANSI-D) have a legacy AD RMS implementation which involves the placement of AD RMS servers on-premises and within Microsoft datacenters. See the information rights management reference material in the *Platform – Aruna & ANSI-D* section of the Office 365 Dedicated Platform Release Collateral page for additional information.
2. Exchange Online Dedicated customers currently without an AD RMS implementation that are utilizing the Exchange 2013 ANSI-D platform can leverage either the on-premises AD RMS configuration or Azure RMS as described above.
3. Exchange Online Dedicated customers currently utilizing the legacy AD RMS implementation and the Exchange 2013 ANSI-D platform can migrate to either the on-premises AD RMS configuration or Azure RMS as described above.

Limitations

- The Outlook Protection Rules feature is not available with the IRM implementation of Exchange Online Dedicated.
- Currently, Azure RMS Bring Your Own Key (BYOK) is not compatible with Exchange Online Dedicated. If Azure RMS is implemented, default key management mode (key management and generation is handled by Microsoft) can be used.
- Licensing requirements for the cloud-based Azure Rights Management service and the on-premises Active Directory Rights Management Services (AD RMS) are unique. See the **Features across Office 365 options** and the **Features across standalone options** descriptions in the Exchange Online Service Description (multi-tenant version) for additional information.

Office 365 Message Encryption

Office 365 Message Encryption (OME) is an online service that allows Exchange Online Dedicated users to send encrypted email messages to anyone. OME allows your organization to perform the following:

- **Define transport rules for encryption.** Admins can use the Exchange Admin Center (EAC) or remote Windows PowerShell to create rules to encrypt outgoing email messages and decrypt incoming encrypted replies to those messages.
- **Add branding to encrypted messages.** Admins can customize the encrypted email with a company or organization brand.

- **Send encrypted messages.** Messages that match admin-defined encryption rules are automatically encrypted and sent to the specified email address.
- **View and reply to encrypted messages.** Encrypted emails arrive in addressee inboxes with an HTML attachment, along with instructions for opening and viewing the attached encrypted email message.

To utilize OME, Office 365 Dedicated customers must be subscribers of Microsoft Exchange Online Protection (EOP) and Azure Rights Management. Contact your Service Delivery Manager (SDM) for implementation assistance.

S/MIME Certificate Support

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of email that is encapsulated in MIME. Admins can use Windows PowerShell to set up S/MIME after establishing and issuing public key infrastructure (PKI) certificates to users.

The identity and provisioning infrastructure of Office 365 Dedicated is capable of propagating your organization's S/MIME certificates for use within the Exchange Online Dedicated environment as part of Active Directory synchronization. S/MIME currently is only supported when using Windows Internet Explorer 9 or later versions. For more information, see Configuring S/MIME for additional information.

Customer Responsibilities

- Provide support and infrastructure for S/MIME to allow item-level security.
- Contact your SDM to submit a Configuration Request (CR) for S/MIME certificate synchronization.

Limitations

- For messages encrypted using S/MIME, Exchange Online doesn't provide antivirus or other content management services (such as including the message body text of an S/MIME message in multi-mailbox searches).
- S/MIME support is not provided for Outlook Web App when using the Firefox, Opera, or Chrome browsers.

In-Place Hold & Litigation Hold

When a reasonable expectation of litigation exists, organizations are required to preserve electronically stored information (ESI), including email that's relevant to the case. This expectation can occur before the specifics of the case are known and preservation is often broad. Organizations may preserve all email related to a specific topic or all email for certain individuals.

The Exchange Server 2013 release of Exchange Online Dedicated offers both the In-Place Hold and Litigation Hold features. In-Place Hold provides granular hold capability for select messages based upon query parameters, hold period, and the ability to place multiple holds; Litigation Hold only allows you to place all items on hold indefinitely or until the hold is removed. See Litigation Hold and In-Place Hold in Exchange 2013 and Exchange Online for a comparison of the functionality differences for each feature and see In-Place Hold and Litigation Hold for administration guidance for the feature set.

In-Place Hold also includes the following capabilities:

- A customized notification banner can be created using remote Windows PowerShell to alert users that they are on hold (requires Outlook 2010 or Outlook 2013 to see the alert).
- Self-service administration involving the EAC or remote Windows PowerShell can be used by an Exchange admin in your organization to add users to, or remove users from, a hold state.

Customer Responsibility

- Add and remove users from hold using self-service remote Windows PowerShell or EAC.
- Customize notification banner to alert users that they are on hold (optional).
- Create and provide to Exchange Online Dedicated a distribution group for use with reporting of users on hold.
- To maintain the data for each inactive mailbox on hold (for legal discovery purposes after users have left your organization), follow instructions provided by Microsoft to assign the inactive mailbox type status. For more information, see the *Office 365 Dedicated and ITAR-support Plans Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.
- Remove the inactive user from Distribution and Security Group membership after the mailbox has been placed into inactive status.
- After the inactive mailbox is no longer required to be on hold, you should remove the inactive mailbox from hold status and follow instructions provided by Microsoft to explicitly mark the inactive mailbox for deletion. This will trigger the mailbox and its data to be deleted according to your mailbox retention period.

Microsoft Responsibilities

- Configure self-service roles to support hold functionality management.

Limitations

- In-Place Hold is available for specific Exchange Online Dedicated subscription plans per guidance provided in the Message Policy and Compliance feature table.
- To receive the customized hold notification, users must be using Outlook 2010 or Outlook 2013.

In-Place eDiscovery

Compliance and security officials assigned appropriate role-based access permissions can search various mailbox item types including email, attachments, calendar appointments, tasks, and contacts. Rich search capabilities include searching for information in the sender, receiver, message type, sent/receive date, and Cc/Bcc fields. Search results include items in the Deleted Items folder if these items match the search query.

Results of In-Place eDiscovery searches can be stored in a special type of mailbox called a *discovery* mailbox. A discovery mailbox has a 50 GB quota which makes it capable of storing large numbers of search results. Admins can perform the following:

- Use EAC to create an exportable .pst file for the discovery mailbox.
- Connect Outlook to a discovery mailbox and export the search results to a .pst file.

By default, one discovery mailbox is created for each organization; admins can request additional discovery mailboxes through the Configuration Request process for Office 365 Dedicated. Each additional discovery mailbox is billed at the same rate as a Plan 2D mailbox. Discovery mailboxes cannot be used for any purpose other than storing mailbox search results.

See In-Place eDiscovery for more information regarding how to configure and utilize discovery searches.

Customer Responsibility

- Use the **In-Place eDiscovery & Hold Wizard** within EAC to perform eDiscovery searches and store results in discovery mailboxes, as required.

Microsoft Responsibilities

- Provide additional discovery mailboxes at your request.

Limitations

- In-Place eDiscovery works only with mailboxes in the Exchange Online Dedicated environment.
- In-Place eDiscovery does not search user .pst files.
- In-Place eDiscovery cannot search content of messages encrypted using S/MIME. Messages of this type will be returned as failed items if the user selects the option to include failed items in search results.
- Information Rights Management (IRM)-protected messages will be included in search results if the Trusted Publishing Domain (TPD) certificate of the on-premises environment is imported into Exchange Online Dedicated. See Information Rights Management Integration for additional information.
- The maximum number of mailboxes that can be searched in a single eDiscovery search is 10000.
- The maximum size of a discovery mailbox is 50 GB.

Transport Rules

Exchange Online Dedicated provides the ability to manage transport rules using the Exchange Admin Center (EAC) and remote Windows PowerShell.

Limitations

- Transport rules cannot be deleted due to restrictions in place related to Role-Based Access Control (RBAC) but can be disabled.
- Transport rules limits associated with Exchange Server 2013 (as described in Transport and Inbox rule limits across standalone options) apply to Exchange Online Dedicated.

Disclaimer Support

If disclaimers in email between recipients and senders inside and/or outside of your organization are required by law or other regulatory requirements, Exchange Online Dedicated is able to meet these compliance requirements. The following default settings apply:

- Global disclaimers can be applied to all messages sent to or from the Exchange Online Dedicated environment.

- Scenario-specific disclaimers that are defined in your requirements can be applied separately from global disclaimers.
- Scenario-specific disclaimers are scoped based on distribution group membership.
- Disclaimer text uses default font, size, and color settings of Exchange Server.
- Disclaimers are appended below the entire message thread for all outgoing messages.
- Disclaimers include a line separator between the message content and the disclaimer.
- If the disclaimer cannot be added in the original message (for example, within an encrypted message), a new message is created with the disclaimer and the original message is attached to the new message.

Customer Responsibilities

- Define requirements regarding disclaimers, including any scenario-specific requirements, if applicable.
- Define and manage distribution groups for scenario-specific disclaimers.
- Define and configure disclaimer content as a transport rule including text in all desired languages for all applicable distribution groups.
- Set up and control access to security groups to allow role-based access.

Microsoft Responsibilities

- Grant role-based access to your security groups.

Limitations

- Font type, color, and size apply only in HTML and rich-text messages. Plain-text messages have disclaimers that also appear in plain text.
- Exchange Online does not support the following in disclaimers:
  - Text greater than 1,000 characters.
  - Active Directory-related queries other than distribution group inclusion.
  - Images (including logos).
- Language translation services for disclaimers.
- Disclaimers are not programmatically localized.
- Users do not see disclaimers in the messages in the **Sent Items** folder because the disclaimers are appended by the server after messages are sent by the users. If a user is a member of multiple distribution groups that are used for specific disclaimer scenarios, the user’s outgoing messages display multiple disclaimers.

Data Loss Prevention

The Data Loss Prevention (DLP) feature helps you identify, monitor, and protect sensitive information in your organization through deep content analysis. DLP is a premium feature that is increasingly important for enterprise messaging systems due to its ability to protect sensitive data within business-critical email. DLP helps enable you to protect sensitive data without affecting worker productivity.

You can configure DLP policies and review reports in the EAC management interface. The recommended implementation approach for DLP includes the following:

- Start with a pre-configured policy template that can help you detect specific types of sensitive information such as Payment Card Industry Data Security Standard (PCI-DSS) data, Gramm-Leach-Bliley act data, or even locale-specific personally identifiable information (PII).
- Use the full power of existing transport rule predicates and actions and add new transport rules.
- Test the effectiveness of your DLP policies before fully enforcing them.
- Incorporate your own custom DLP policy templates and sensitive information types.
- Detect sensitive information in message attachments, body text, or subject lines and adjust the confidence level at which Exchange Online Dedicated takes action.
- Add Policy Tips which can help reduce data loss by displaying a notice to your Outlook users and can also improve the effectiveness of your policies by allowing false-positive reporting. See Manage policy tips for additional information.
- Review incident data in DLP reports or add your own specific reports by using a generate incident report action. See View DLP policy detection reports for additional information.

Customer Responsibilities

- Provide a list of policy items including sensitive words for subject line or message body filtering during initial Exchange Online Dedicated configuration.

Limitations

- DLP is available for specific Exchange Online Dedicated subscription plans per guidance provided in the previously shown Message Policy and Compliance Feature table.
- The use of DLP as described in this section applies only to messages originated within the Exchange Online Dedicated messaging environment. See the Exchange Online Protection Service Description for a description of DLP protection for Internet inbound and outbound messages.

Message Journaling

In addition to advanced archiving features available with the Exchange Online Archiving add-on feature set subscription, Exchange Online Dedicated also provides message journaling functionality to capture all email and optional hosted voice mail communications in an organization for inclusion in the organization's message retention or archival strategy. To meet an increasing number of regulatory and compliance requirements, many organizations must maintain records of communications that occur when employees perform daily business tasks. Exchange Online Dedicated provides the ability to journal messages and make them available for the following archival scenarios:

- An archival mailbox hosted by a third-party archival solution provider.
- An archival mailbox within your on-premises environment.

A backup mailbox (a billable Plan 1D or Plan 2D mailbox) must be provisioned within Exchange Online Dedicated by your organization to accept non-delivery report (NDR) messages to address certain conditions (for example, the external journaling site being non-accessible or incapable of accepting messages). For more information, see Journaling and Configure or Remove an Alternate Journaling Mailbox. To complete the process to forward NDR messages to the backup mailbox, contact your Service Delivery Manager (SDM) to request assistance with submitting a CR.

Customer Responsibility

- Create a contact object in your directory for the SMTP target email address to be used for journaling.
- For messaging content forwarded to an on-premises or third party archive mailbox, maintain proper management, redundancy, availability, performance, and functionality levels of the SMTP target journaling system and configure a backup mailbox in Exchange Online Dedicated.

Microsoft Responsibilities

- Send journal messages to the target archival location established by your organization.

Limitations

- The journaling solution must be able to utilize existing network connectivity between Office 365 Dedicated and your journaling system.
- The external SMTP target system used to hold archival messages must not have a dependency on specific software versions of Exchange Online Dedicated.
- For journaling to execute successfully, the mailbox accounts must be a member of a distribution group that you manage and that is recognized to allow the journaling of messages to the SMTP target of the your choice. No other integration methods will be provided.
- Journaling of instant messaging conversation history is not provided.

Anti-Spam and Anti-Malware Protection

For Exchange Online Dedicated customers, anti-malware protection is applied within the Exchange servers of the messaging service. All messages that are transported through Exchange Online Dedicated are scanned for malware. If malware is detected, the message is deleted. Notifications can be sent to senders or admins that exist within the Exchange Online Dedicated environment when an infected message is deleted and not delivered. You can also use the Exchange Admin Center (EAC) to provide a replacement message for infected attachments with either default or custom text that notifies the recipients of the malware detection.

Optionally, your organization can use Exchange Online Protection (EOP) service. The premium level version of EOP, referred to as the Exchange Enterprise Client Access License (CAL) with Services, is provided with Exchange Online Dedicated subscriptions at no additional charge. See the Exchange Online Protection Service Description for more information.

Note:

- Anti-malware protection features offered in Exchange Online Dedicated provide protection for messages routed within your online environment (effectively your “intranet”). If appropriate subscription licenses have been purchased, Exchange Online Dedicated also will provide Data Loss Prevention (DLP) protection for intranet traffic. The EOP service is used to apply filtering and protection for all messages delivered via the Internet, including anti-spam protection. DLP is provided by EOP regardless of the Exchange Online Dedicated subscription type of the message originator.
- Certain kinds of email attachments from non-trusted sources are blocked from entry into the Exchange Online Dedicated environment by a transport rule. Exchange Online Dedicated applies a default transport rule that an Exchange admin in your organization can view and edit to allow anti-malware filtering to be tailored to meet the requirements of your organization.

Customer Responsibilities

- During initial configuration of the Exchange Online Dedicated service, provide a list of IP email addresses to be blocked, allowed, or blocked and allowed via policy..
- Default setting for user notification of messages in quarantine is 15 days; self-service administration within EOP can be used to alter setting.
- Control timing and deployment of Mail Exchange (MX) record changes.

- Manage changes to policy settings after deployment through the EAC   extension used to manage EOP.

Microsoft Responsibilities

- If your organization will use EOP for Internet inbound and outbound email filtering, configure EOP to support the filtering of this traffic.

Limitations

- Anti-malware detection notifications are sent only to Exchange Online Dedicated senders who are sending mail within the Exchange Online Dedicated environment.

Mail Flow

Exchange Online Dedicated provides Exchange admins with the ability to customize the delivery and acceptance methods for messages that flow through the service. The application of transport rules, supplemental messages, and mail routing customization can be managed by your organization. Specific message and recipient limits also apply in Exchange Online Dedicated.

Outbound Mail Flow Path

For outbound mail flow, either of the following mail routing options for outbound messages is available with Exchange Online Dedicated:

- **Deliver Internet-bound messages to Exchange Online Protection (EOP).** Select this option if Exchange Online Dedicated will not use on-premises transport servers when routing outbound messages to external recipients.
- **Route all Internet-bound messages through on-premises Exchange servers.** Select this option to send all Exchange Online Dedicated outbound messages destined for external recipients via on-premises transport servers maintained by your organization. The on-premises hybrid transport servers will be responsible for delivering the messages to external recipients.

Inbound SMTP Traffic Management

Simple Mail Transfer Protocol (SMTP) is used by on-premises servers, clients, or Line-of-Business (LOB) applications that you configure to send email to Exchange Online Dedicated mailboxes. If management of the inbound SMTP traffic sent via the private Gateway Network/Customer (GN/C), the following options are available:

- **SMTP relay.** An SMTP relay is used to send mail from your organization by authenticating the X.509 security certificate of the sender. The certificate must be issued by a publicly trusted certificate authority (CA) and the same certificate must be loaded on all on-premises SMTP clients.
- **Client SMTP submission.** Client SMTP submission allows your device or LOB application to send email using an email address associated with an Exchange Online Dedicated mailbox by authenticating itself using that account. Each device can have its own sender address or all devices can use one address, like printer@yourdomain.com.

- **Direct Send.** Direct Send can be used if the device or LOB application has the ability to send mail using its own SMTP method. The mail is received by the Office 365 Dedicated infrastructure for delivery to an Exchange Online Dedicated account.

Customer Responsibilities

- To activate the SMTP Relay option, contact your Service Delivery Manager to place a Configuration Request (CR). The request will require the “Subject” string of the X.509 security certificate.

Limitations

- Originating IP addresses for on-premises servers, clients, or applications that originate SMTP traffic are not filtered by Exchange Online Dedicated. Your organization can block SMTP traffic from specific on-premises IP addresses by applying access control policies on firewall and routing equipment or by using Group Policy Object (GPO) settings.

Message Encryption

All channels used by Exchange Online Dedicated to transmit messages are encrypted by default. Transport Layer Security (TLS) encryption is used for server-to-server traffic and client access traffic (Outlook Web App, Outlook Anywhere, and Exchange ActiveSync). For more information on the use of POP3 and IMAP4 by client systems and the use of SMTP relay services to deliver messages between Exchange Online and external systems, see POP3 and IMAP4.

Message and Recipient Limits

The message and recipient limits described as follows apply to users of Exchange Online Dedicated.

Message Limits

Message size and delivery rate limits are necessary to ensure message delivery from other mailboxes is not blocked, system performance is not degraded, and the Exchange Online Dedicated environment is not used for inappropriate purposes. Message limits are described in the following table.

Description	Limit
Message Size Limit. The maximum total size of an email message. The total size includes the message header, the message body, and any file attachments. The limit applies organization-wide to all messages (inbound, outbound, and internal). Messages larger than the limit will not be delivered and the sender will receive a non-delivery report (NDR). Although a message size limit cannot be increased, decreased, or changed on a per-user basis, admins can create transport rules to limit the maximum size of any individual attachment. To increase the Message Size Limit beyond the default value, contact your Service Delivery Manager for assistance with the placement of a Configuration Request.	Up to 100MB (default is 50 MB including attachments)
Message Rate Limit. The maximum number of email messages that can be sent from a single email client per minute. The client is identified by the user account. If a user submits messages at a faster rate beyond the limit, Exchange Online Dedicated delivers the messages but queues them at the server and throttles the rate of delivery.	Unlimited

Recipient Limits

To discourage the delivery of unsolicited bulk messages, Exchange Online Dedicated has recipient limits that prevent users and applications from sending large volumes of email. The limits apply to all messages (inbound, outbound, and internal). 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. Recipient limits are described in the following table.

Description	Limit
Recipient Rate Limit. The maximum number of recipients that can receive email messages sent from a single Exchange Online Dedicated mailbox in a 24 hour period.	Unlimited
Recipient Limit. The maximum number of message recipients allowed in the To:, Cc:, and Bcc: fields.	5,000 recipients/message

If your organization needs to send legitimate bulk commercial email (for example, newsletters) you should use third-party providers that specialize in these services.

Recipients

User Mailbox

A standard user mailbox is available for the Kiosk, Plan 1D, and Plan 2D subscriptions. The assigned mailbox size is represented in an extension attribute associated with the Active Directory object for the user. Your organization is responsible for populating the extension attribute with an allowed mailbox size value as described in the Mailbox Provisioning and Administration section.

When the amount of consumed space within a user mailbox reaches specific threshold levels, Exchange Online Dedicated provides the following notifications to users:

- **Warning.** The user receives an email warning when the mailbox is approaching the maximum size limit.
- **Prohibit send.** The user receives an email prohibit-send notification when the mailbox size limit is reached. The user cannot send new messages until enough email is deleted that the mailbox is below the size limit again
- **Prohibit send/receive.** Exchange Online Dedicated rejects any incoming mail when the mailbox size limit is reached, and sends a non-delivery report (NDR) to the sender. The sender has the option to try resending the mail later. To receive messages again, the user must delete email until the mailbox is below the size limit.

The following table summarizes mailbox sizes for Exchange Online Dedicated plans and the thresholds at which notifications and restrictions take effect.

Messaging Plan	Mailbox Size	Warning[1]	Prohibit Send[1]	Prohibit Send/Receive[1]
Kiosk D Plan	Up to 2 GB	98% of set mailbox size	99% of set mailbox size	100% of set mailbox size
Plan 1D	Up to 50 GB[2]	98% of set mailbox size	99% of set mailbox size	100% of set mailbox size
Plan 2D	Up to 50 GB[2]	98% of set mailbox size	99% of set mailbox size	100% of set mailbox size

[1] Any mailbox type configured to a size of 1GB or less will utilize a Warning value of 90%, Prohibit Send value of 95%, and a Prohibit Send/Receive value of 100%.

[2] The maximum mailbox size supported by Office Outlook 2003 and Outlook 2007 is 20GB. A maximum mailbox size of 50GB is allowed with Outlook 2010 or Outlook 2013. However, a mailbox size in excess of 20GB has the potential to degrade the performance of the Outlook client and the replication of mailbox data between datacenters.

Customer Responsibility

- Identify and populate the defined extension attribute in your on-premises Active Directory to set mailbox size, plan type, features, and options (including resource and shared mailbox designation). For more information, see the *Office 365 Dedicated and ITAR-support Plans Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

Inactive Mailbox on Compliance Hold

Exchange Online Dedicated offers provides special purpose mailbox types for the retention of messages associated with a deleted user account that was placed in a hold state for compliance purposes. Inactive mailboxes are provided at no charge if you apply specific provisioning parameters. For more information, see the *Office 365 Dedicated and ITAR-support Plans Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

Before you delete an Exchange Online Dedicated user account that has been placed under In-Place Hold or Litigation Hold, you can convert the user's mailbox to an inactive mailbox. This allows the contents of the mailbox to be preserved for compliance purposes for the duration of time that the user is on hold. Admins, compliance officers, or record managers can use the eDiscovery feature in Exchange Online to access the contents of an inactive mailbox.

You are able to convert an active mailbox that was previously on a compliance hold to an inactive mailbox only if the user's mailbox was previously assigned to either of the following Exchange Online plans: (a) Exchange Online Plan 2D or (b) Kiosk D or Plan 1D with the optional Exchange Online Archiving add-on feature. After an active mailbox on hold is converted to an inactive mailbox, you have the option to reassign that user's original plan type subscription to a new user account.

The following characteristics apply to an inactive mailbox:

Special Purpose Mailbox Type	Mailbox Size	Warning	Prohibit Send	Prohibit Send/Receive[1]
Inactive	No Size Limit [1]	No Limit	No Limit	No Limit

[1] See the qualification requirements in the following Limitations section.

◆ **Important:**

- If a compliance hold is not placed on a mailbox before the mailbox is deleted, the contents of the mailbox will not be preserved and therefore will not be discoverable. The mailbox can be recovered within 30 days of deletion as described in Deleted Mailbox Retention.
- If a mailbox on a compliance hold needs to be retained as an inactive mailbox, specific provisioning instructions must be followed. For more information, see the *Office 365 Dedicated and ITAR-support Plans Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

Customer Responsibility

- Set compliance hold parameters on any mailbox that must be retained for compliance purposes. This is done to ensure the mailbox isn't removed if an account deletion is performed.

Limitations

- An inactive mailbox can be created only for a Plan 2D mailbox or the Kiosk D or Plan 1D mailbox types that also have an Exchange Online Archiving add-on feature set subscription; no additional charge is incurred for the created inactive mailbox.
- Users will not be able to access inactive mailboxes.
- Inactive mailboxes will be hidden from the Global Address List (GAL).
- Messages sent to inactive mailboxes will not be delivered and will result in non-delivery reports (NDRs) being returned to the sender.
- The size of the inactive mailbox cannot exceed the size of the original active mailbox type.

Mailbox Client Features

Mailbox features provided to users in an on-premises Exchange Server environment are also available to Exchange Online Dedicated clients. Many of the features are managed by your staff using the self-service capabilities provided in Exchange Online. Several features involve engaging Microsoft to provide customization support as described in the following sections.

Custom Address Lists

Custom address lists help users easily find contacts and resources contained within the GAL of Exchange. In Exchange Online Dedicated, customized views of the GAL can be created and each address list created can be available to users as an Outlook Address Book selection.

Customer Responsibility

- Utilize self-service administration to manage custom address lists.

Limitations

- Customization of the Outlook Details Template is not permitted.
- Address Book fields are limited to the Exchange custom attributes.
- Address Lists are not added to the Offline Address Book (OAB).

Sender Thumbnail Photo

User thumbnail photos can either (a) be placed in the on-premises Active Directory of your environment and propagated to the online Active Directory environment by the MMSSPP provisioning tool or (b) updated by each member of your user community via Outlook Web App. When an Outlook 2010 or Outlook 2013 client is used to interact with Exchange Online Dedicated, the photo of the sender will be displayed in the message window.

Customer Responsibility

- Provide solution for service desk staff or end users to upload and modify thumbnail photos.
- If the on-premises Active Directory will be used as the photo source, submit a Configuration Request to enable the flow of the thumbnailPhoto attribute to the Active Directory of Office 365 Dedicated. If end users will be allowed to update their photo on their own, use self-service administration to set an OWA mailbox policy to allow the action to occur and assign the policy to end user mailboxes. For more information, see the *Office 365 Dedicated and ITAR-support Plans Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

Microsoft Responsibility

- If your on-premises Active Directory will be the photo source, enable thumbnail photo synchronization flow from your organization's on-premises Active Directory to Office 365 Active Directory.

Limitations

- Photos will be displayed only in Outlook 2010 or Outlook 2013; support for Outlook Web App requires the High Availability infrastructure of Exchange Online Dedicated.

Resource Mailbox

A resource mailbox is used for managing resources such as conference rooms and equipment. This type of mailbox optionally can be configured to enable the Resource Booking Attendant (RBA), which automates scheduling of conference rooms and equipment based on resource availability. A resource mailbox that is RBA-enabled accepts, declines, or acknowledges messages from a meeting organizer. Exchange Online Dedicated helps enable your organization to customize these responses through Outlook Web App.

You can also set booking policies or rules for the resource mailboxes of your organization. Examples include who can schedule a resource, when it can be scheduled, what meeting information is visible on the calendar of the resource, and the percentage of schedule conflicts allowed.

A *standard* resource mailbox set to a size of 5GB, 10GB, or 50GB is available at no additional charge in Exchange Online Dedicated. If a resource mailbox requires features such as In-Place Archiving, In-Place Hold, Data Loss Prevention, or Hosted Voicemail features, a *custom* resource mailbox can be created by utilizing a billable Exchange Online Plan 1D or 2D subscription.

For more information on how to provision a standard or custom resource mailbox, see the *Office 365 Dedicated and ITAR-support Plans Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

The following characteristics apply to a resource mailbox:

Mailbox Type	**Mailbox Size**	**Warning**	**Prohibit Send**	**Prohibit Send/Receive**
Resource	5GB, 10GB, or 50GB	98% of mailbox size	99% of mailbox size	100% of mailbox size

Customer Responsibility

- Define all required resource mailbox objects in the on-premises Active Directory.
- Define and manage RBA settings through remote Windows PowerShell to support the resource mailboxes feature.

Limitations

- Resource mailboxes of 5GB, 10GB, or 50GB in size are available to your organization at no extra charge only if specific instructions are followed as described in provisioning guidance provided by Microsoft.
- Resource mailboxes are subject to the same recipient limits and message rate limits as regular mailboxes. The limits are described in the Mail Flow section.
- A resource mailbox cannot be used to archive email for individual users. If an In-Place Archive is required for the resource mailbox, the resource mailbox must be either (a) an Exchange Online Plan 1D subscription with the Exchange Online Archiving add-on feature set subscription or (b) an Exchange Online Plan 2D subscription.
- If In-Place Hold or Litigation Hold is required for a resource mailbox, the resource mailbox must be either (a) an Exchange Online Plan 1D subscription with the Exchange Online Archiving add-on feature set subscription or (b) an Exchange Online Plan 2D subscription.

Reporting Features and Troubleshooting Tools

Auditing Reports

You can use audit logging to troubleshoot configuration issues by tracking specific changes made by admins and to meet regulatory, compliance, and litigation requirements. Exchange Online Dedicated provides two types of audit logging:

- **Admin audit logging** records any action performed by an admin. This can help you troubleshoot configuration issues or identify the cause of security- or compliance-related problems.
- **Mailbox audit logging** records when a mailbox is accessed by someone other than the person who owns the mailbox (also known as non-owner mailbox audit logging). This can help you determine who has accessed a mailbox and what was performed on the box.

Customer Responsibility

- Set up and control access to security groups used to manage Role-Based Access Control (RBAC) permissions for the generation of auditing reports.

Limitations

- Admin audit logging records are retained for 180 days.
- Mailbox audit logging is enabled by default and the logs are retained for 90 days.

Sharing and Collaboration

Calendar Free/Busy Sharing

Exchange Online Dedicated offers the capability to transfer user schedule availability data on-demand between Exchange Online Dedicated and mail servers within (a) on-premises forests in your environment, (b) ancillary forests associated with your organization, and/or (c) forests within the multi-tenant version of Exchange Online. To facilitate the transfer of Exchange Server calendar free/busy data, the Microsoft Federation Gateway (MFG) is used to establish a federation trust between the environments. The trust is a claims-based authentication method which uses the Security Assertion Markup Language (SAML) protocol. When you use this method for the transfer of data, the Active Directory object that provides the data is not required to exist in the Exchange Online Dedicated environment. For an on-premises IBM Lotus Domino environment, a service account access method is used in place of the federated trust to provide direct interaction between Exchange Online and a Lotus Domino server.

Customer Responsibilities

- Contact your Service Delivery Manager (SDM) to initiate the discovery process for the federation trust solution and to obtain detailed implementation procedures. These procedures include establishing a trust, installing signed certificates on Client Access servers, exchanging certificates with the federation gateway, and applying domain record updates.

Microsoft Responsibilities

- Assist your organization with implementation of the required calendar free/busy sharing method for your environment as needed.

Limitations

- An Exchange Server 2010 or Exchange Server 2013 system with Internet access must be present in your on-premises environment to support data transfers with Exchange Online Dedicated. If an Exchange Server 2003 or Exchange Server 2007 system in your organization's environment is providing the calendar free/busy data, an Exchange Server 2010 or Exchange Server 2013 configuration must be used as a proxy server to communicate with Exchange Online (see specific requirements in the Hybrid deployment section).

- Office Outlook 2007 clients cannot access free/busy data using an SMTP address. The user object being queried by an Office Outlook 2007 client must be represented in the Office 365 Active Directory.
- If federated calendar free/busy sharing is in effect between the on-premises environment and an ancillary forest (for example, a partner organization), the ability to add the sharing of on-premises information with Exchange Online Dedicated is not possible if the SMTP namespace is shared. Alternative scenarios are available to support a federated arrangement with Exchange Online Dedicated.

Public Folders

Public folders in Exchange Online Dedicated have been modernized to take advantage of the high availability features and existing storage technologies of the mailbox database. The public folder architecture uses specially designed mailboxes to store both the hierarchy and the public folder content within the mailbox database. This means a separate public folder database is no longer required.

Public folder replication now involves the use of the continuous replication model. A database availability group (DAG) in the Office 365 Dedicated data center supports the high availability characteristics of the hierarchy and content mailboxes.

In Exchange Online Dedicated, the maximum size of the public folder allocation (cumulative size of all public folders combined) is 5 TB. The Exchange Admin Center (EAC) is used to manage public folders that exist within the public folder mailbox. A public folder is accessible using any subscription plan type in Exchange Online Dedicated.

Customer Responsibility

- Prior to using the EAC to create public folders, contact your Service Delivery Manager (SDM) to request assistance with the Configuration Request process to create the initial public folder mailbox.

Shared Mailbox

A shared mailbox allows a group of users to view mail in, and send email from, a common mailbox (for example, info@contoso.com or sales@contoso.com). A shared mailbox is created by your organization by assigning a specific value in the mailbox provisioning attribute for the mailbox object held in the on-premises Active Directory. A *standard* shared mailbox set to a size of 5GB, 10GB, or 50GB is available at no additional charge in Exchange Online Dedicated. To access a standard shared mailbox, a user must be granted Send As or Full Access permissions to the mailbox. The user then signs into their own mailbox to gain access to the shared mailbox.

If there is a need for features such as In-Place Archiving, In-Place Hold, Data Loss Prevention, Hosted Voicemail, or POP/IMAP connectivity for a shared mailbox, a *custom* shared mailbox can be created by utilizing a billable Exchange Online Plan 1D or 2D subscription. Following the creation of a custom shared mailbox, the shared mailbox owner can grant Send As or Full Access permissions to users, and these users then will have direct access to the mailbox.

For more information on how to provision a standard or custom shared mailbox, see the *Office 365 Dedicated and ITAR-support Plans Provisioning Tools Handbook* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

Shared mailboxes have the following characteristics:

Mailbox Type	Mailbox Size	Warning	Prohibit Send	Prohibit Send/Receive
Shared	5 GB, 10 GB, or 50 GB	98% of mailbox size	99% of mailbox size	100% of mailbox size

Limitations

- Shared mailboxes of 5GB, 10GB, or 50GB in size are available to your organization at no extra charge only if specific instructions are followed as described in provisioning guidance provided by Microsoft.
- If In-Place Hold or Litigation Hold is required for a shared mailbox, the shared mailbox requires a license and must be either (a) an Exchange Online Plan 1D subscription with the Exchange Online Archiving add-on feature set subscription or (b) an Exchange Online Plan 2D subscription.
- A shared mailbox cannot be used to archive email for individual users. If an In-Place Archive is required for the shared mailbox, the shared mailbox must be either (a) an Exchange Online Plan 1D subscription with the Exchange Online Archiving add-on feature set subscription or (b) an Exchange Online Plan 2D subscription.
- Each user that accesses a shared mailbox must be assigned a subscription plan license. Users with Exchange Online Kiosk D subscriptions are only able to access a *custom* shared mailbox.
- Shared mailboxes are subject to the same recipient limits and message rate limits as regular mailboxes. These limits are described in the Mail Flow section.

Clients and Mobile Devices

Microsoft client applications, custom applications, and specific mobile devices can be used to access Exchange Online Dedicated. Support for several access methods are described in the following sections.

Accessing Exchange Online Services

The following user access options are enabled by default and supported by Exchange Online Dedicated:

- Office Outlook 2007 with the latest service pack installed, Outlook 2010, and Outlook 2013.
- Microsoft Outlook Web App.
- Exchange ActiveSync (EAS) devices (as described in the Comparison of Exchange ActiveSync clients).
- Legacy BlackBerry 7.1 and earlier devices (non-EAS) for use with the optional BlackBerry Enterprise Server (BES) service (see BlackBerry Enterprise Server).
- Microsoft Outlook for Mac applications (see Macintosh Clients).
- Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) protocol support. (Limitations for the use of Office Outlook 2003 and other client applications are described in the sections below.)
- Simple Mail Transfer Protocol (SMTP) submission and relay.
- Applications developed to use Exchange Web Services.

Customer Responsibility

- Use remote Windows PowerShell to configure the user or set of users that have access to common service access protocols such as Outlook Web App, Exchange ActiveSync, and Outlook Anywhere.

The following topics describe the client requirements and the advantages and limitations of each access method.

Client System Requirements

The Office Applications Service Description provides an overview of Office client application compatibility across Office 365 plans, enterprise-specific features for clients, and links to client requirements for operating systems, Office applications, and Web browsers.

To allow iOS and Android mobile devices to use Office Mobile applications with Office 365 Dedicated, the Office Mobile subscription service for your online environment must be activated. For more information, see the *Microsoft Office Client Authentication Services* section of the Identity and Provisioning Service Description for Office 365 Dedicated.

Limitations

- The following system software, applications, and features are not supported or have limited support when used with Exchange Online Dedicated:
  - **Office Outlook 2003.** Only standard email send/receive functions are supported between Exchange Online Dedicated and Office Outlook 2003 clients. The use of the POP3 or IMAP4 protocols is required when using an Office Outlook 2003 client. For a summary of specific Office Outlook 2003 limitations, see Outlook Clients. Support for Office Outlook 2003 was discontinued effective April 8, 2014. For more information, see Support has ended for Office 2003.
  - **Windows XP.** Support for Windows XP was discontinued effective April 8, 2014. For more information, see Support for Windows XP has ended.
  - **Internet Explorer.** Several versions of Internet Explorer are compatible with Office 365 services; the user experience varies depending on the version of Internet Explorer being used.
- When you use a mobile device that is not licensed to use a version of Office Mobile, any supported file types attached to an email message in Exchange Online Dedicated are presented either by an attachment handler within your mobile application or as a rendering generated by Office Online that is presented in the Web browser of the device. In both cases, the attachment is a view-only rendering of the file.

Outlook Clients

Microsoft Outlook is an email program that includes calendaring, contacts, and tasks features. Supported Outlook client versions receive the following Exchange Online Dedicated features:

Outlook Anywhere

With the Outlook Anywhere feature of Outlook, users can connect to an Exchange Online mailbox using remote procedure call (RPC) over HTTP. The feature gives a user a reliable and efficient way to remotely connect to their mailbox. The feature is typically used to access Exchange Online from outside of the firewall of an organization.

Customer Responsibilities

- Provide configuration instructions to users.
- Enable the Outlook Anywhere setting within Outlook, if necessary.

Limitations

- Outlook Anywhere requires Windows XP Service Pack 2, or a later version of the Windows operating system.

Autodiscover Service

With the Exchange Autodiscover service, Outlook clients can receive user profile settings directly from Exchange Online when client domain credentials are submitted. These settings automatically update the client with the information necessary to create and maintain the user's profile.

An X.509 certificate to support Transport Layer Security (TLS) is required in conjunction with the Autodiscover service. Autodiscover FQDNs in the certificate are limited to a single entry that matches the primary vanity domain.

Customer Responsibilities

- Provide written proof of ownership of the requested primary domain through the Office 365 deployment discovery process and associated documentation.
- Provide a single primary domain for inclusion in certificate requests for the Autodiscover service and generate SRV (service) records for all other primary domains.
- Create a DNS record for mobility-related URLs.

Microsoft Responsibilities

- Request an X.509 certificate that includes your primary domain.
- Install X.509 certificates.

Limitations

- Requires Office Outlook 2007 (with latest service pack installed), Outlook 2010, or Outlook 2013.
- You must provide written proof of domain ownership before Microsoft can request the certificate for the primary domain.

Cached Exchange Mode

The Cached Exchange Mode feature allows Outlook users to access local copies of their Exchange Online mailboxes when they aren't connected to the Internet. Cached Exchange Mode retains a client-side copy of users' Exchange mailboxes in Outlook and automatically synchronizes this copy with the email server.

We recommend using Outlook in Cached Exchange Mode because it provides offline access and helps provide a responsive user experience, even when network conditions between the client and the server are not ideal.

Important:

- For Office Outlook 2003, standard email interaction with Exchange Online Dedicated is supported only when the POP3 or IMAP4 protocols are used. The following limitations apply to Office Outlook 2003 clients:
- Calendar scheduling information, calendar free/busy information of other Exchange Online users, and the Global Address List (GAL) held within Exchange Online are not accessible to an Office Outlook 2003 client.
- Exchange Online will not automatically push email to the Office Outlook 2003 client.
- All messages downloaded to the Office Outlook 2003 client using POP3 will not be synchronized between multiple computers or devices (for example, between a laptop and a mobile phone).
- The maximum mailbox size supported by Office Outlook 2003 and Office Outlook 2007 is 20GB.

Outlook Web App

Outlook Web App (OWA) provides users with the ability to access email, calendar data, and contacts using a thick client or mobile device Web browser or by using a version of OWA designed as a native application for a specific mobile device. The client application provides Exchange Online Dedicated users with feature-rich Outlook messaging functionality including a light instant messaging client for, and presence status provided by, Lync Online Dedicated.

The thick client experience involves the use of the premium version of OWA in a Web browser, such as Windows Internet Explorer. The mobile experience is provided using the Light version of OWA or a native version of the application provided by Microsoft that has been designed for a specific mobile device. For more information about the different features available in the Premium and Light versions of OWA and the supported mobile versions, see What's new for Outlook Web App in Exchange 2013.

In offline access mode, OWA can be used to process mail, calendar, and people data even if you are not connected to a network. The data stored in offline mode is not encrypted. Customer admins can enable or disable this functionality. Typical offline OWA access scenarios include the following:

- Read and triage email to mark as read, flag/delete/move.
- Write email, save and modify drafts, or queue to outbox.
- View and be reminded of upcoming events.
- Add calendar appointments and meetings.
- Find and view contacts with contact details.
- Add, update, and delete contacts.

The OWA implementation in Exchange Online Dedicated has the following default automatic timeout values.

Outlook Web App Version	Public Computer Timeout	Private Computer Timeout
Outlook Web App Premium client	Fifteen (15) minutes	Eight (8) hours
Outlook Web App Light client	Fifteen (15) minutes	Thirty (30) minutes

OWA also allows a user to configure delegate access to their Exchange Online mailbox folders and calendar. For more information, see Configuring delegate access in Outlook Web App, and the **Limitations** section below.

Options

- A global update for the OWA sign-in page is available to enable your organization to include usage guidelines or a disclaimer.
- Multi-factor authentication options are available to Exchange Online Dedicated customers using the premium version of OWA. For more information, see Multi-Factor Authentication for Outlook Web App.

Customer Responsibility

- Provide localized text if a language-specific email message disclaimer is required.

Microsoft Responsibility

- Provide URL for all client versions of OWA.

Limitations

- The OWA interface automatically localizes standard content to the language pack preference that is selected in the OWA configuration options. Any disclaimer additions to the OWA logon page appear only in the language in which the disclaimer was provided.
- Internet Explorer versions prior to and including version 7.0 can use only the Light versions of OWA. An upcoming change in the Exchange Online Dedicated will restrict Outlook Web Access to Light mode for all Internet Explorer 8 users. For more information, see Client System Requirements.
- Lync Online Dedicated is required for instant messaging (IM) and presence integration in OWA.
- Access to OWA requires an encrypted SSL connection.

- Use of any of the mobile device applications described below require the latest version of Exchange Online Dedicated (Exchange Server 2013 release).
  - OWA for iPhone
  - OWA for iPad
  - OWA for Android
  - Outlook for iOS (iPhone or iPad applicability)
  - Outlook for Android
- Offline access in OWA requires Exchange 2013. The following offline limitations also apply:
  - Users can't search or sort messages while offline.
  - Attachments are not available when offline.
  - Multiple calendars are not available when offline.
- The OWA delegation feature cannot be used to delegate access to a user account in another Active Directory forest – the Outlook application must be used.

Exchange ActiveSync Mobile Devices

Exchange Online offers the Microsoft Exchange ActiveSync (EAS) protocol for mobile device connectivity and management. EAS provides synchronization of mailbox data between mobile devices and Exchange Online to allow users to access their email, calendar, contacts, and tasks on the go. In addition to the native device management functionality of EAS, an optional on-premises or third party hosted Mobile Device Management (MDM) solution to secure, monitor, manage, and support mobile devices that are deployed across a variety of telecommunications service providers also can be accommodated if specific implementation guidance provided by Microsoft is followed.

EAS is supported by a wide range of mobile devices as described in the Comparison of Exchange ActiveSync clients. Several important EAS features include the following:

- **Direct push technology.** This technology allows timely message delivery to mobile devices without delay.
- **Remote wipe.** With this feature, users can manage the process of remotely erasing lost, stolen, or otherwise compromised mobile devices using the Exchange Control Panel in Outlook Web App or through remote Windows PowerShell.
- **Mobile device security policy.** Admins can enforce security policies on mobile devices that connect to Exchange Online through Exchange ActiveSync. Your admins can customize these

policies for specific users and groups within your company using web-based graphical user interface (GUI) or remote Windows PowerShell. Exchange Online supports the same Exchange ActiveSync policies as Exchange Server 2013.

- **Free/busy lookup.** Users can view the calendar of a contact directly from their mobile devices. A free/busy information timeline shows when contacts are available for a call or meeting. Users also can look at the contact card of a contact and to see when that person is available.
- **SMS sync.** Exchange ActiveSync provides the ability to send and receive SMS text messages from Outlook and Outlook Web App. Incoming messages sent via Exchange ActiveSync to the user's mobile device can be seen both in the usual SMS message location and in the email inbox.
- **Device allow, block, and quarantine control.** This feature provides control over which devices are allowed to connect to Exchange Online via Exchange ActiveSync. With the Allow, Block, and Quarantine feature, admins can create approved device lists and block specific devices when necessary. Admins can also set exceptions at the individual level and can quarantine any device not on the block or allow lists for additional evaluation.

For a comparison of Exchange ActiveSync features implemented by various mobile clients, see Exchange ActiveSync Client Comparison Table.

For additional information describing the native device management capabilities of Exchange Server and EAS, see the collection of TechNet articles Understanding Exchange ActiveSync. If additional MDM capabilities are required, the use of a third-party MDM solution must meet specific requirements as described in the **Limitations** section below. Due to the unique set of features required by each individual customer, Microsoft does not host an MDM solution.

Customer Responsibilities

- Procure, deploy, manage, and support client software and compatible devices, including all relationships with wireless carriers.
- Define the Exchange ActiveSync policy settings and configure in the Exchange Online environment using remote Windows PowerShell. Each policy may contain multiple settings.
- Define and configure which users are assigned to each Exchange ActiveSync policy through remote Windows PowerShell.
- Set up and control distribution groups to allow for role-based access permissions for custom Exchange ActiveSync policy configuration.
- Supply educational material to users to make them aware of the Exchange ActiveSync policies.
- Choose whether to configure Exchange ActiveSync policy to allow downloading of device .cab files via an email notification sent to the end-user.

- Educate and train end users and support teams about the email message that is sent to the Inbox of the end-user which describes instructions for downloading the device .cab file.
- If MDM will be implemented, contact your Microsoft Service Delivery Manager to request guidance regarding supported MDM solutions.

Limitations

- The High Availability infrastructure of Exchange Online Dedicated offers a maximum of 100 EAS device connections per user.
- Microsoft does not provide support for user devices. 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.
- For Exchange ActiveSync, certain features (such as Direct Push technology, remote wipe, or device security settings) require Windows Mobile 6.1, Windows Mobile 6.0, or Windows Mobile 5.0 with the Messaging and Security Feature Pack (MSFP) and an active Exchange ActiveSync policy.
- The customer-selected MDM solution must not interfere with the basic functionality of an EAS client, the functionality of the EAS protocol, or the ability of the EAS client to automatically process an EAS URL redirect request from Exchange Online following an automated failover to another Microsoft data center. The use of any MDM equipment which performs a proxy service for EAS traffic is not recommended.
- The customer is required to deploy and validate their selected on-premises or third party hosted MDM solution and address any connectivity support issues that arise.
- All MDM applications that interface with Exchange Online must utilize supported application programming interfaces (APIs) and protocols such as Exchange Web Services, remote Windows PowerShell, and Exchange ActiveSync. Software or hardware to support the MDM application cannot be installed in the Exchange Online data center and the third-party application must not adversely affect the performance of Exchange Online.

POP3 and IMAP4

Exchange Online supports access to POP3 and IMAP4 protocols from your internal network and the Internet as described in the Dedicated Plans Descriptions topic. Qualified users can view their POP3 and IMAP4 connection settings on the **Options** page of Outlook Web App. Admins can disable POP3 or IMAP4 access on a per user basis using remote Windows PowerShell.

Customer Responsibility

- If Internet access to POP3 and IMAP4 has been enabled by Microsoft, it must be enabled for all mailboxes by default. You can restrict POP3 and IMAP4 access on a per-user basis using remote Windows PowerShell.

Microsoft Responsibility

- Enable access from your internal network to POP3 and IMAP4 as a default setting for qualified Exchange Online plans.
- Enable Internet access to POP3 and IMAP4 for qualified Exchange Online plans upon your request.

Limitations

- POP3 and IMAP4 access from your internal network requires encryption using SSL.
- When Internet access to IMAP4 is enabled for qualified Exchange Online plans, IMAP4 becomes available to all users by default.
- Delegated logon is not supported.
- For outbound email, the SMTP client must authenticate over an encrypted channel via Transport Layer Security (TLS) using port 587.
- When Internet access to POP3 and IMAP4 are enabled for qualified Exchange Online plans, POP3 and IMAP4 become enabled for all qualified users by default. The customer may restrict POP3 and IMAP4 access for specific users via remote Windows PowerShell.

Macintosh Clients

Exchange Online supports two email clients developed by Microsoft for the Apple Macintosh operating system:

- Microsoft Outlook for Mac 2011
- Microsoft Outlook for Mac for Office 365

Both clients use Exchange Web Services to communicate with Exchange Online Dedicated. See Office Applications Service Description for additional information.

Customer Responsibility

- Procure, deploy, and configure the Outlook for Mac applications.

BlackBerry Devices

BlackBerry 10 smartphones can connect to Exchange Online directly using Microsoft Exchange ActiveSync. See Blackberry Enterprise Server for information regarding limited support for legacy BlackBerry 7 and earlier BlackBerry devices that do not use the Exchange ActiveSync (EAS) protocol.

Custom Application Connectivity

Custom applications that use messaging protocols such as Messaging Application Programming Interface (MAPI), SMTP, POP3, and IMAP4 are allowed to connect to Exchange Online Dedicated. Applications developed by Exchange Web Services (EWS) or the EWS Managed API client can also connect to the service.

Note:

The use of the RPC/TCP protocol to directly access MAPI message stores has been deprecated from Exchange Server 2013. The alternative protocols for customer Line-of-Business (LOB) applications are EWS or Outlook Anywhere (RPC/HTTP). On the Exchange Server 2013 release of Exchange Online Dedicated, the latest version of the Collaboration Data Objects (CDO) API will be available to allow MAPI clients to use the Outlook Anywhere protocol.

The following conditions apply to the use of all custom applications and equipment.

Customer Responsibilities

- Test applications and equipment to understand the impact, if any, on the Exchange Online Dedicated service.
- Provide support for individual applications, add-ins, related application, and equipment compatibility testing.

Microsoft Responsibility

- Assist your organization to resolve problems with applications that have a negative impact on the Exchange Online Dedicated service.

Limitations

- Customer-managed applications cannot be hosted in Microsoft managed data centers.
- Exchange Online does not provide support for Outlook add-ins.
- Connectivity using web-based Distributed Authoring and Versioning (WebDAV) is not allowed with Exchange Online.
- Third-party or custom developed applications cannot be added to Client Access servers.
- Exchange Online does not provide guidance for custom application development.

Client Access Rules

The Client Access Rules feature of the Exchange 2013 release of Exchange Online Dedicated blocks the ability of a client to use a particular protocol, application, service, or resource based upon username, source IP address/range, authentication type, or recipient. Examples include blocking Exchange ActiveSync (EAS) clients, preventing client access using federated authentication, blocking access for users of a particular country or region, and preventing client access to Windows PowerShell, Exchange Admin Center (EAC), Outlook Web Access (OWA), or the Offline Address Book (OAB).

Client Access Rules are a self-service administration feature of Exchange Online Dedicated. See Managing Client Access Rules for additional information.

Voice Messaging Services

Exchange Online Dedicated supports Hosted Voicemail provided by the optional Unified Messaging (UM) capability of Exchange Server 2013. Support is provided for Lync Online, on-premises Lync Server, or on-premises Private Branch Exchange (PBX) systems.

The Hosted Voicemail feature set gives a user a single inbox for both email and voicemail messages that can be accessed from Outlook, Outlook Web App, a Lync client, mobile devices, or a standard telephone through Outlook Voice Access. Organizational or personal auto attendant functionality is available to route callers to specific Lync or telephony endpoints. Spoken email, audible interaction with calendar elements, directory search, and outbound calling also are part of the voice-integrated UM experience.

The following is a complete list of hosted voicemail features provided by Exchange Online Dedicated:

- Delivery of voicemail to an Exchange Online mailbox.
- Voicemail preview (speech-to-text transcript).
- Voicemail form to play voice messages.
- Play on Phone (ability to dynamically establish a connection to a phone to play a message).
- Outlook Voice Access allowing the use of voice commands to interact with the Inbox and Calendar or to perform a directory search to initiate an outbound call, group addressing, and sending a voice message.
- Organizational auto attendants (automated responses and call-tree functionality presented to callers).
- Personal auto attendant (use of call answering rules to forward a call to another telephony end point based upon user defined criteria).
- Information Rights Management (IRM) protected voicemail. For more information, see Information Rights Management Integration.
- User self-service administration of select features (Call Answering Rules, PIN Reset, Greetings, Outlook Voice Access, Voice Mail Preview, Notifications).
- Support for 26 languages.

Lync Online Integration

Hosted voicemail support is available for organizations that use Lync Online Dedicated with Exchange Online Dedicated. See the Lync Online Dedicated Service Description for more information. Your Service Delivery Manager can assist with providing the specific requirements to implement the Hosted Voicemail feature for Lync Online.

Microsoft Responsibilities

- Configure Exchange Online Dedicated to accept voicemail messages forwarded by Lync Online Dedicated.
- Associate UM dial plans for Lync Online with Exchange Online Dedicated UM servers.

Limitations

- Missed call and voice mail notifications using SMS are not supported.
- The processing of incoming fax transmissions is not supported.

On-Premises Lync Server Integration

Hosted Voicemail support for on-premises Microsoft Lync Server is available if your organization is using Lync Server 2010 on-premises with at least Cumulative Update 4 (CU4) or Lync Server 2013. All users of the UM feature must have a Microsoft Lync client and the Lync voice services feature must be enabled for all of these users.

Customer Responsibilities

- Obtain Exchange Online Plan 2D subscription for every mailbox enabled to use hosted voicemail services.
- Deploy the minimally required release of Microsoft Lync Server on-premises, provide the Microsoft Lync client to all users of the feature, and enable voice services.
- Obtain the Configuration Request template for on-premises Lync integration from Microsoft, address all pre-requisites described in template, submit completed template to Microsoft, and complete UM integration per guidance provided by Microsoft.
- Use a Secure Sockets Layer (SSL) certificate generated by a public certificate authority and trusted by all Lync servers, clients, and Session Initiation Protocol (SIP) devices.

- Create all required universal security groups, confirm specific firewall ports are opened and using specific protocols, confirm the on-premises Lync Server is able to communicate with the Exchange Online Dedicated UM servers.
- Provide technical staff familiar with telephony terminology and capable of performing configuration changes and advanced troubleshooting for the Lync Server, associated telephony equipment of the on-premises environment, and your IP network.

Microsoft Responsibilities

- Configure Exchange Online Dedicated to accept voicemail messages forwarded by the on-premises Lync Server.
- Associate UM dial plans for an on-premises Lync Server with Exchange Online Dedicated UM servers.

Limitations

- Missed call and voice mail notifications using SMS are not supported.
- The processing of incoming fax transmissions is not supported.
- The Voice Mail Form feature requires Outlook 2007 (with latest service pack installed), Outlook 2010, Outlook 2013, or Outlook Web App, and the use of Windows Media Player 7.0 or later.
- Round-trip time maximum transmission delay of 300 milliseconds must be maintained between the on-premises equipment and the Exchange Online Dedicated UM server.

On-Premises Third-party Vendor PBX Systems Integration

Hosted Voicemail support is available for an on-premises PBX telephony system which meets specific equipment and configuration criteria. If the on-premises system is a legacy PBX rather than an IP-PBX or SIP-enabled PBX, a VoIP Gateway will be required. The following criteria must be met for the on-premises telephony system to integrate with Exchange Online Dedicated:

- The equipment must be listed on the Telephony advisor for Exchange 2013.
- The equipment must support secure SIP communication (SIP TLS over 5061/TCP) with a remote host that utilizes wild card certificates in the Subject Alternative Name (SAN).

- The SSL certificate must be from a Certificate Authority (CA) that is listed as Trusted CA.
- The equipment must support Domain Name System (DNS) resolution.
- The equipment must support DNS load balancing.

Customer Responsibilities

- Obtain Exchange Online Plan 2D subscription for every mailbox enabled to use hosted voicemail services.
- Confirm the on-premises telephony system meets all integration requirements.
- Obtain the Configuration Request template for on-premises third party PBX integration from Microsoft, address all pre-requisites described in template, submit completed template to Microsoft, and complete UM integration per guidance provided by Microsoft.
- Use a SSL certificate generated by a public certificate authority and trusted by all Lync servers, clients, and SIP devices.
- Provide technical staff familiar with telephony terminology and capable of performing configuration changes and advanced troubleshooting for the telephony equipment of the on-premises environment and your IP network.

Microsoft Responsibilities

- Configure Exchange Online Dedicated to accept voicemail messages forwarded by the on-premises PBX.

Limitations

- Missed call and voice mail notifications using SMS are not supported.
- The processing of incoming fax transmissions is not supported.
- Voice Mail Form feature requires Outlook 2007 (with the latest service pack installed), Outlook 2010, Outlook 2013, or Outlook Web App, and the use of Windows Media Player 7.0 or later.
- On-premises PBX integration requires all network traffic between the on-premises equipment and Exchange Online Dedicated to be via the Gateway Network/Customer (GN/C) path.
- Round-trip time maximum transmission delay of 300 milliseconds must be maintained between the on-premises equipment and the Exchange Online Dedicated UM server.

High Availability and Business Continuity

Exchange Online Dedicated offers extensive email infrastructure retention and recovery support, including mailbox replication at the data centers level and the ability to restore deleted mailboxes and deleted items.

Service Continuity Management

Service Continuity Management addresses the commitment made by Microsoft to meet specific managed service standards for Exchange Online Dedicated. A Service Level Agreement (SLA) exists for the services provided by Microsoft, usage and performance metrics are provided to support the SLA, and specific service continuity measures are applied to maintain service availability.

Exchange Online Dedicated is hosted in enterprise-level Microsoft data centers designed to deliver highly available and highly resilient online services. A key aspect of the infrastructure design is a 99.9 percent availability metric for Exchange Online.

Circumstances including hardware failures, natural disasters, and human error can impact service availability. Exchange Online Dedicated offers service continuity management, which is a process for managing risks to ensure that the Office 365 Dedicated infrastructure is capable of providing continuing services if normal availability solutions fail.

Two metrics commonly used in service continuity management to evaluate disaster recovery solutions are the following:

- **Recovery point objective (RPO).** The acceptable amount of data loss at the conclusion of the data recovery process.
- **Recovery time objective (RTO).** The acceptable amount of time the service can be down before being brought back online.

Exchange Online Dedicated has set the following RPO and RTO in the event of a disaster:

- **Nearly instantaneous RPO.** Microsoft maintains a copy of your Exchange Online data at multiple data centers and will make available a nearly instantaneous copy of the data.
- **One-hour RTO.** Organizations will be able to resume service within 60 minutes after service disruption occurs.

Standard services restored with service continuity management are core mail (Exchange Online mailboxes), client access (Outlook Web App and mobile devices), transport, Unified Messaging (UM), and delegated administrative controls through Exchange Admin Center (EAC) and remote Windows PowerShell. For an overview of service continuity measures applied across all Office 365 Dedicated plans, see the Service Continuity Management Service Description.

Customer Responsibilities

- Provide technical staff to work with the Exchange Online Dedicated team in the event of a declared disaster.

Microsoft Responsibilities

- Enable the Service Continuity Management process to restore access to core services and data within the stated RPO and RTO.
- Provide, per customer request, a summary report of each forced data center failover executed within the previous 180 day period. The summary report will be available within 10 business days following the completion of the latest failover exercise.

Limitations

- Client access after recovery from a service disruption does not require reconfiguration on the part of the Exchange Online Dedicated subscriber. Microsoft is not responsible for the reconfiguration of any systems or processes outside of its control.
- Due to external dependences, the RPO/RTO objectives of Exchange Online Dedicated are not guaranteed for system processes and optional services including, but not limited to, (a) mailbox migration, (b) calendar free/busy sharing involving the service account access method, and (c) BlackBerry Enterprise Server, multi-factor authentication, and message journaling to external systems.
- To achieve the stated RPO/RTO, the following requirements must be met:
  - Your organization must have all mailboxes hosted in the High Availability infrastructure of Exchange Online Dedicated.
  - Your networking infrastructure must honor the Domain Name System (DNS) record Time to Live (TTL) of 5 minutes.

Mailbox Data Protection and Recovery

Continuous replication of mailbox data to multiple servers provides data recovery capability in the event of a local messaging infrastructure failure. For large-scale failures, established Service Continuity Management processes are initiated.

Limitations

- Data restoration limits are defined in the Deleted Mailbox Retention and Deleted Item Retention and Recovery sections of this topic.

Deleted Mailbox Retention

Exchange Online Dedicated retains a deleted mailbox for a 30-day period. Deleted mailboxes can be recovered by placing a Service Request with Microsoft Online Services Support or, under certain circumstances, automatically through the directory synchronization process. Changes to the default mailbox retention period can be requested through the Configuration Request process for Office 365 Dedicated. Contact your Service Delivery Manager for assistance.

Limitation

- When the deleted mailbox retention period has passed for a deleted mailbox, the mailbox cannot be recovered.

Deleted Item Retention and Recovery

Exchange Online Dedicated provides a deleted item retention policy and the capability to provide single item recovery for messages deleted due to user initiated actions. When a user performs a soft delete of messages within their **Deleted Items** folder, the items are moved to the **Deletions** subfolder of the **Recoverable Items** folder associated with the user mailbox. The user can manually recover items from the **Deletions** subfolder within 30 days using Outlook or Outlook Web App. If the user accessed the **Deletions** subfolder and performed a hard delete of any of the items, the deleted items will be placed in the **Purges** subfolder for the balance of the 30-day period. Only an Exchange admin can view and restore messages placed in the **Purges** subfolder.

Limitations

- If In-Place Hold is enabled for a mailbox, none of the items in the **Deletions** subfolder are permanently deleted from Exchange Online Dedicated while the hold is in effect; the items are held in the system in a manner that is not visible to the mailbox owner.

Note:

If the **Recoverable Items** folder for a mailbox placed on In-Place Hold reaches the 30 GB quota, contact Microsoft Online Services Support to increase the quota for the folder.

Interoperability, Connectivity, and Compatibility

This topic describes the interoperability, connectivity, and compatibility features that are available with Exchange Online Dedicated.

SMTP

Simple Mail Transfer Protocol (SMTP) is used to send outbound mail for clients that connect to Exchange Online Dedicated through Internet Message Access Protocol (IMAP) or Post Office Protocol (POP). It is the primary protocol for routing and delivery through Exchange Server. Exchange Online supports two types of SMTP relay services for authorized internal customer applications that require SMTP mail submission:

- SMTP message submission to users inside the managed environment.
- Authenticated SMTP message relay to deliver messages outside of the managed environment.

Customer Responsibilities

- Manage and implement necessary changes in your environment to allow mail flow from your on-premises environment to the Exchange Online Dedicated environment.

Exchange Web Services

Applications developed to use Exchange Web Services (EWS) or the EWS Managed API client have the ability to add or access data in Exchange Online Dedicated. The applications can be invoked on-premises, in Azure, or in other hosted services. Applications that use EWS must be granted permissions to the mailbox accounts to be accessed in Exchange Online Dedicated. For example, The use of Exchange Impersonation is one method used to grant permissions. For more information on application development using EWS, see EWS Managed API, EWS, and web services in Exchange.

Customer Responsibilities

- Identify the account that is to be granted impersonation rights and provide the rights using self-service administration.

Limitations

- The EWS maximum subscriptions throttling limit (for example, the number of subscription connections allowed by a service account) for Exchange Online Dedicated is 5000. Use remote Windows PowerShell to view all EWS settings with the following code string: `Get-ThrottlingPolicy | Format-List ews*`

Optional Services and Features

This topic describes the following optional services and features that are available with Exchange Online Dedicated:

- Blackberry Enterprise Server
- Multi-Factor Authentication for Outlook Web App
- Outbound Desktop Fax Support
- Inbound and Outbound Fax Integration
- Multiple Language Support

Blackberry Enterprise Server

The hosted BlackBerry® Enterprise Server (BES) 5.0.4 offering for Exchange Online Dedicated was offered as an optional service used to support legacy BlackBerry 7 and earlier BlackBerry devices that do not use the Exchange ActiveSync (EAS) protocol. The BES offering has been deprecated. Support for the offering is only provided to current Exchange Online Dedicated customers that have an existing BES support agreement.

The legacy BES service description and related reference material are available in the *BlackBerry* section of the Exchange Online Dedicated Release Collateral page.

Multi-Factor Authentication for Outlook Web App

Typical authentication practices that require only a password to access resources might not provide the appropriate level of protection for information that is sensitive or vulnerable. Multi-factor authentication (MFA) is an authentication method that applies a stronger means to identify a user. It requires a user to submit two of the following three types of identify proofs:

- Something known (like a password).
- Something possessed (like a smart card).
- Something unique about the user's appearance or person (like a fingerprint or other biometric indicator).

The Exchange 2013 release of Exchange Online Dedicated offers an enhanced MFA model that utilizes federated authentication. The model is implemented by using the Office 365 Dedicated Federation Hub (an Active Directory Federation Services system) in conjunction with a customer-hosted Secure Token Server (STS) and a customer-selected third party MFA solution(s).

Access to additional MFA services can be achieved through integration with the Microsoft Azure Multi-Factor Authentication service. Interaction with Azure MFA apps used on mobile devices, automated client verification via any telephony device, or the delivery of a text message verification code to a mobile device are functions provided by the Azure MFA service

When MFA is implemented within your environment, the Web browser client used to access Outlook Web App (OWA) and Exchange Admin Center (EAC) is evaluated by the Office 365 Dedicated Federation Hub to determine if MFA must be applied. The Web browser of an OWA or EAC user can be configured for Integrated Windows Authentication to support a single sign-on experience for the user from within your corporate network. If MFA is enabled within your environment, your STS must be capable of identifying an intranet client access request in order for the single sign-on method to work correctly.

For additional information on all MFA implementation options, see Multi-Factor Authentication for OWA for additional information.

Customer Responsibilities

- Provide access to an STS system that conforms to the WS-Federation identity federation specification and the WS-Trust security token management specification including the issuance of security tokens conforming to Secure Access Markup Language (SAML) 1.1 or later version.
- Select and implement one or several MFA solutions compatible your chosen STS implementation.
- Provide a version 1.0 or later version of a Transport Level Security (TLS) certificate for the URL used for MFA. All federation identity provider STS certificates (encryption, signing, and TLS) must be issued by, and chained to, a publicly trusted root authority.

Microsoft Responsibilities

- Provide a dedicated HTTPS URL namespace to access Exchange Online Dedicated.
- Provide access to the Office 365 Dedicated Federation Hub via the Internet.

Limitations

- When MFA is implemented, the OWA options to select a public or private computer setting are not available to users. The default security mode is **This is a private computer**. OWA mailbox policies can be configured and applied to implement more restrictive access security settings.
- Outlook Web App and Outlook applications for iOS or Android mobile devices cannot be used with MFA.
- The Office 365 Dedicated Federation Hub is only accessible via the Internet.
- Issues arising from the use of third-party MFA products on your premises or your chose STS implementation do not impact the Service-Level Agreement (SLA) for Exchange Online Dedicated.

Outbound Desktop Fax Support

Exchange Online Dedicated offers the ability for users to send content as a facsimile transmission via Outlook. Fax content is sent via a secure Internet connection to a third-party carrier for transmission.

Customer Responsibilities

- Provide and deploy specific templates for outbound fax content.

Microsoft Responsibilities

- Configure Exchange Online Dedicated to recognize each primary domain of your environment.

Limitations

- Exchange Online Dedicated outbound fax transmissions are available only with Microsoft Office applications.
- The Exchange Online Dedicated outbound fax feature doesn't integrate with Outlook Web App.
- Outbound fax transmissions are available only with 32-bit client computers due to current application constraints.

Inbound and Outbound Fax Integration

Exchange Online Dedicated can integrate with an existing customer-provided fax solution that allows fax content to be routed via Simple Mail Transfer Protocol (SMTP).

Customer Responsibilities

- Configure the existing fax solution for integration with Exchange Online Dedicated.
- Configure Outlook clients to send fax content per instructions of the fax solution provider.

Microsoft Responsibilities

- Provide SMTP transport to deliver fax content prepared by your fax solution.

Multiple Language Support

Exchange Server provides multiple language packs that provide a localized experience in Outlook Web App and Outlook for Exchange Online Dedicated users. The availability of languages may differ between Outlook Web App and Outlook. For the current list of languages, see Client Language Support for Outlook and Client Languages for Outlook Web App.

Customer Responsibilities

- Deploy language packs to users.

Microsoft Responsibilities

- Install available server-side language packs.

Limitation

- Microsoft support is available only in the English language.

Administration and Management

Exchange Online Dedicated offers several tools to provide robust administration and management functions for the service. By using the Role-Based Access Control (RBAC) model of Exchange Server 2013, Exchange Online Dedicated helps enable admins to use remote Windows PowerShell and the Exchange Admin Center (EAC) to perform self-service administration. The Office 365 Dedicated Customer Portal is available to provide usage and performance metrics for your environment.

Windows PowerShell

Windows PowerShell can be run on a local computer by IT Pros and service desk personnel to remotely connect to an Exchange Online Dedicated environment and perform management tasks. When a connection is established to Exchange Online Dedicated, cmdlets and exposed parameters for each cmdlet can be executed. Remote Windows PowerShell also can be used to create scripts to automate routine tasks or to perform batch processing.

Exchange Admin Center

The Exchange Admin Center (EAC), the successor to the Exchange Control Panel, provides self-service administration capabilities through a Web-based management interface that is accessible from Outlook Web App. Exchange admins use EAC for specific administrative functions and user-level management of mailbox settings. Admins also can delegate specific EAC functions to other users.

Note:

> Access to EAC requires the Exchange Server 2013 release of Exchange Online Dedicated. Office 365 organizations that have not been upgraded to Exchange Server 2013 will continue to use similar administrative and user-level management functions offered by the Exchange Control Panel.

The following is a summary of the current collection of EAC administration features:

- **Delivery Reports.** EAC users are able to perform a custom search to obtain a report of messages delivered to, or received from, specific mail addresses. IT Pros who are assigned appropriate RBAC permissions can view message tracking information for multiple users. The ability to view this information using self-service administration helps to reduce one of the most common types of service desk calls. The amount of delivery report data available in Exchange Online Dedicated varies based upon storage constraints. Typically, one week of information is available.

- **In-Place eDiscovery.** Compliance and security officials who are assigned appropriate RBAC permissions can search a variety of mailbox items including email, attachments, calendar appointments, tasks, and contacts through EAC. For more information, see In-Place eDiscovery.
- **In-Place Hold.** EAC can be used to place a specific user mailbox in litigation hold or to disable the setting. For more information, see In-Place Hold & Litigation Hold.
- **Remote Device Wipe.** With this EAC feature, users can manage the process of remotely erasing lost, stolen, or otherwise compromised mobile devices.
- **ActiveSync Device and Policy Management.** Using EAC, admins can carry out a variety of tasks related to Exchange ActiveSync mobile phones and devices. These tasks include the following:
  - Manage the default access level for all or specific mobile phones and devices.
  - Set up email alerts when a mobile phone or device is quarantined.
  - Personalize the message that users receive when their mobile phone or device is either recognized or quarantined.
  - Provide a list of quarantined mobile phones or devices.
  - Create and manage Exchange ActiveSync device access rules.
- **MailTips.** With this feature, informative messages are displayed to users while they are composing a message. These messages, which provide information about the recipient to help avoid non-delivery reports (NDRs), can be configured using EAC.
- **Resource Booking Agent.** In EAC, reservation or delegation settings can be set for a resource mailbox that represents a meeting room mailbox or an equipment mailbox. For example, a resource mailbox can be configured to designate users who can reserve the resource without approval, or to prevent users from scheduling repeating reservations. You can set attributes that represent room capacity, and configure the ability for Exchange Online Dedicated to automatically accept or decline booking requests.
- **Transport Rule Management.** Transport rules provide the ability to apply messaging policies and message hygiene restrictions consistently to email messages as they pass through the transport pipeline during message delivery. Using EAC, transport rules can be created using drop-down menu selections.
- **Mailbox Administration.** EAC provides the following mailbox administration features:
  - **Mailbox Delivery Options:** Deliver and forward, forward to a contact, and forward to a group.

- **Mailbox Permissions:** Ability to apply Full Mailbox access rights, Send-As rights, and Send-on-Behalf rights.
- **Mailbox Export to a PST File:** Ability to place a copy of mailbox content within a PST file. The In-Place eDiscovery feature is used to prepare and generate the export. The mailbox is *not* required to be in a hold state to perform the export. For more information, see In-Place eDiscovery.

Office 365 Dedicated Customer Portal

To help you monitor usage and performance of the Exchange Online Dedicated service, Microsoft reports on a set of service usage metrics and Key Performance Indicators (KPIs) visibility using the Office 365 Dedicated Customer Portal. Usage metrics provide you with information about service usage patterns and activities. KPIs provide information that Microsoft uses as part of its continuous service improvement. The information also may be of use to you in evaluating aspects of the service which address their scope of responsibility. The KPI information also may be of use to you in evaluating aspects of the service. Microsoft measures and reports the same KPI values for all customers.

Note:

Microsoft is only responsible for specific elements of the service offering and cannot control all of the elements that collectively support the Office 365 Dedicated user experience. For example, Microsoft provides services from a global network of Microsoft data centers; however, it is not responsible for the network connections to the data centers provided by telecommunications carriers, the balance of your wide area network (WAN), and your local area networks (LANs). In addition, Microsoft doesn't manage your on-premises Active Directory environment or any devices used to access Microsoft services. All of these factors have significant effects on the user experience.

Usage Metrics

When you subscribe to Exchange Online Dedicated, the following usage metrics are reported monthly to your organization:

- Number of mailboxes by type.
- User detail report that lists every mailbox along with its display name, email address, optional services enabled for the user, mailbox size, current mailbox capacity, and last logon information.
- Average mailbox size for the user community.
- Email summary report that includes email traffic count and email traffic volume (applicable only to organizations using message filtering).

Key Performance Indicators

As a subscriber to Exchange Online Dedicated, Key Performance Indicator (KPI) metrics for your specific environment are available to your organization through your customized Customer Portal environment. In the portal, note that Exchange KPI metrics may or may not include KPI target values by design. KPI entries that already show target values in your Office 365 Dedicated Customer Portal should indicate that there is a known and expected value for service performance, and that the service is performing well against this expectation if the actual value exceeds the target value. KPI entries without targets are meant to show a focused view of relative service performance over time, or are informational only to provide greater service insight. KPI entries are not intended to set a specific level of performance expectation for customers. As the Exchange Online Dedicated service continues to evolve, Microsoft will evaluate which metrics and targets can provide optimal service insight to customers and these enhancements will be applied to the portal user interface.

Service Growth and Transitions

Microsoft provides various resources and levels of support to address the service growth and customer organizational restructuring that may impact the Exchange Online Dedicated service and trigger a service transition.

Service Growth

Exchange Online Dedicated is designed and deployed based upon the number of contracted Exchange Server mailboxes identified during your organization's detailed discovery activities with Microsoft. Additional capacity is built into the initial planning and deployment of services based upon common growth scenarios and stated customer growth.

When predicted user growth exceeds five percent, you should notify Exchange Online Dedicated through the Configuration Request (CR) process for Office 365 Dedicated plans. The CR process enables you to evaluate and plan service expansion in coordination with Microsoft. The notification process applies to the following scenarios:

- Increase in the number of total mailboxes.
- Scope expansion related to customer usage scenarios (such as deployment of mobile devices).
- Introduction of new applications that run within the Exchange Online Dedicated environment.

Service Transitions

Service transitions typically occur in relation to customer organizational restructuring (for example, divestiture, merger, acquisition, or required movement of mailboxes and Active Directory objects to other platforms). Microsoft offers various levels of transition services ranging from direct assistance, fee-based consultation, and self-service guidance. Service transitions are treated as separate projects involving detailed discovery, resource assessments, infrastructure design assistance, and execution planning, including the selection of appropriate migration options.

Customer Responsibilities

- Provide mailbox and messaging service usage and growth estimates.
- Provide advance notification of any significant user growth or messaging service usage beyond initial estimates.
- Utilize the CR process for Office 365 Dedicated plans to request assistance with anticipated service transitions due to organizational restructuring.

Microsoft Responsibilities

- Plan capacity based on the customer's sustained growth rate, and add infrastructure as required.
- Adjust growth capacity to enable evaluation and planning for necessary service expansion.
- Determine type of resources required to accommodate the planning, design, and execution of service transitions due to organizational restructuring.

Limitations

- Service transitions due to organizational restructuring (divestiture, merger, acquisition, or required movement of mailboxes and user account objects to other platforms) are handled as separate projects outside of the standard capacity planning process.