# Table of Contents

1 **Introduction** ........................................................................................................... 8
   1.1 About Office 365 for Enterprises ........................................................................... 8
   1.2 How to Read This Guide .................................................................................... 8
   1.3 Assumed Knowledge ......................................................................................... 9
   1.4 Document Scope and Limits ............................................................................. 10
   1.5 Feedback .......................................................................................................... 11

2 **Deployment Overview** ......................................................................................... 12
   2.1 Deployment Phases ............................................................................................ 12
   2.2 Sample Deployment Schedule ........................................................................ 13
      2.2.1 Deployment Checkpoints ......................................................................... 13
   2.3 Customer Responsibilities ................................................................................ 13
   2.4 Microsoft Online Services Portal .................................................................... 15
   2.5 Administration Roles ....................................................................................... 16
      2.5.1 Partner Delegated Administrators ............................................................ 17
   2.6 Deployment Project Support ............................................................................ 17
   2.7 Key Pre-deployment Considerations ............................................................... 18
      2.7.1 License Validation .................................................................................... 18
      2.7.2 Roles-Based Security and Administration ................................................ 18
      2.7.3 Deployment Impacts to Customer Organization ........................................ 19
      2.7.4 Assessing Service Features and Organizational Requirements ............... 19
      2.7.5 Application Integration and Supported Interfaces .................................... 20
      2.7.6 Migration Groups ..................................................................................... 20

3 **Plan Phase** ............................................................................................................. 22
   3.1 Key Activities Summary .................................................................................... 22
   3.2 Kickoff Meeting ................................................................................................ 23
   3.3 Customer Environment Discovery .................................................................... 23
      3.3.1 Office 365 Deployment Readiness Tool .................................................. 24
3.3.2 Microsoft Assessment and Planning Toolkit................................................................. 25
3.4 Pilot Deployment .................................................................................................................. 25
3.5 Key Planning Considerations ............................................................................................ 26
  3.5.1 Long Lead Time Items ................................................................................................. 26
  3.5.2 Client Hardware and Software Requirements ............................................................. 26
  3.5.3 Migration Support for Existing Mail Environments .................................................... 27
3.6 Networking and Naming Services Planning ..................................................................... 27
  3.6.1 Adding a Domain ......................................................................................................... 28
  3.6.2 External DNS Records ............................................................................................... 28
  3.6.3 Third-Party SSL Certificates ..................................................................................... 30
  3.6.4 Ports and Protocols ..................................................................................................... 33
  3.6.5 Firewall Considerations ............................................................................................. 34
  3.6.6 WAN Accelerators ..................................................................................................... 34
  3.6.7 Hardware and Software Load Balancing Devices ....................................................... 34
  3.6.8 Internet Bandwidth Planning ....................................................................................... 34
3.7 User Identity and Account Provisioning Planning ............................................................. 38
  3.7.1 Adding and Provisioning User Accounts ................................................................. 38
  3.7.2 User License Activation ............................................................................................. 39
  3.7.3 Active Directory Synchronization .............................................................................. 39
  3.7.4 Single Sign-On ........................................................................................................... 41
  3.7.5 Directory Synchronization Tool ................................................................................ 49
3.8 Exchange Online Planning ............................................................................................... 52
  3.8.1 Email Coexistence ..................................................................................................... 53
  3.8.2 Email Migration .......................................................................................................... 61
  3.8.3 Certificates ................................................................................................................ 65
  3.8.4 Bandwidth ................................................................................................................. 65
  3.8.5 Public Folders ............................................................................................................ 66
  3.8.6 Email Client Software ............................................................................................... 66
  3.8.7 Mobile Devices .......................................................................................................... 67
3.8.8 Mail-Enabled Applications ................................................................. 68
3.8.9 Service Limits .................................................................................. 68
3.8.10 Exchange Online Administration .................................................... 69
3.8.11 Application Interoperability ............................................................. 77
3.8.12 Security .......................................................................................... 79
3.8.13 Unified Messaging Services .............................................................. 83
3.8.14 Contacts and Distribution Groups .................................................. 86
3.8.15 Calendar Sharing ............................................................................. 88
3.8.16 Conference Rooms and Resource Mailboxes ....................................... 89
3.9 SharePoint Online Planning ................................................................. 90
  3.9.1 About SharePoint Online ................................................................. 90
  3.9.2 Available Features .......................................................................... 92
  3.9.3 Service Limitations ......................................................................... 93
  3.9.4 Capacity Planning ........................................................................... 94
  3.9.5 SharePoint Online Planning Guide .................................................. 94
3.10 Lync Online Planning ......................................................................... 95
  3.10.1 Lync Domain Federation ............................................................... 96
  3.10.2 Federation Settings ....................................................................... 97
  3.10.3 Public IM Connectivity .................................................................. 97
  3.10.4 Lync Coexistence .......................................................................... 97
  3.10.5 Client Requirements and Limitations ............................................. 98
3.11 Client and End-User Experience ......................................................... 99
  3.11.1 Rich Experience Clients ............................................................... 99
  3.11.2 Web Experience Clients ............................................................... 103
  3.11.3 Web Conferencing ...................................................................... 105
  3.11.4 Browser Issues with Extended Protection for Authentication .......... 105
  3.11.5 Mobile Devices ............................................................................ 105
4 Prepare Phase .......................................................................................... 107
  4.1 Key Activities Summary ................................................................... 107
4.2 Network and Naming Services Tasks

4.2.1 Add Domain and Verify Ownership

4.2.2 Change DNS Records at Domain Registrar

4.2.3 Create Autodiscover and Sender Policy Framework Records

4.2.4 Create Autodiscover Record

4.2.5 Create Internal Autodiscover Record

4.3 User Identity and Account Provisioning Tasks

4.3.1 Update Schema for Exchange Hybrid Deployment

4.3.2 Clean Up Active Directory

4.3.3 Deploy Federation Server Farm

4.3.4 Deploy Federation Proxy Server

4.3.5 Advanced Option: Deploy Federation Services with SQL Server

4.3.6 Deploy Directory Synchronization

4.4 Implement Password Policies for Non-Federated Identities

4.5 Activate User Licenses

4.6 Exchange Online Preparation

4.6.1 Deployment Pre-requisites

4.6.2 Establish Email Coexistence

4.6.3 Testing Exchange Online with Remote Connectivity Analyzer

4.7 SharePoint Online Preparation

4.7.1 Analysis of Existing SharePoint environment

4.7.2 Preparing for Customizations

4.7.3 Content Migration

4.8 Lync Online Preparation

4.8.1 Network Preparation for Conferencing

4.8.2 Enable and Disable Federation

4.8.3 Enable Federation with Windows Live Messenger

4.9 Client and End-User Experience

4.9.1 Rich Client Experience
4.10 Create Migration Groups

5 Migrate Phase

5.1 Key Activities Summary

5.2 Send Final End User Communications

5.3 Migrate Mailboxes

5.4 Change MX Record

5.5 Set Up Mobile Phones and Devices

5.5.1 ActiveSync Devices

5.6 Perform Post-migration Service Testing

6 Feature Enablement

7 Appendix A: Key Deployment Resources

8 Appendix B: Deployment Planning Template

9 Appendix C: Customer Deployment Checkpoints

9.1 Office 365 Deployment Entrance Requirements

9.2 Checkpoint 1: Planning Complete

9.3 Checkpoint 2: Preparation Complete

9.4 Checkpoint 3: Migration Complete

10 Appendix D: Key Deployment URLs, Ports, and IP Addresses

10.1 URLs

10.2 IP Address Ranges

10.3 Required Ports

11 Appendix E: Exchange Hybrid Deployment Domain and Host Names Worksheet

12 Appendix F: Directory Object Preparation

13 Appendix G: Sample Email Migration End User Communications

14 Appendix H: Post-deployment Services Test Plan

15 Appendix I: Glossary
1 Introduction

The *Microsoft Office 365 Deployment Guide for Enterprises* is intended to help you understand the requirements and workflows for onboarding your organization to Microsoft Office 365 for enterprises.

1.1 About Office 365 for Enterprises

Microsoft Office 365 brings together cloud versions of our most trusted communications and collaboration products with the latest version of our Microsoft Office Professional Plus desktop suite. The Office 365 for enterprises solution includes the following cloud-based services:

- Microsoft Exchange Online
- Microsoft SharePoint® Online
- Microsoft Lync™Online
- Microsoft Office Professional Plus

Detailed information about these Office 365 service offerings is available in separate service description documents, which are available at the Microsoft Download Center. Information about Office 365 for enterprises subscription plans is available at the Office 365 plans page.

*Note:* Office 365 is replacing the Microsoft Business Productivity Online Standard Suite (BPOS), the first set of cloud-based business productivity offerings from Microsoft Online Services. Existing BPOS customers can visit the Microsoft Office 365 transition center for information about moving to Office 365 service offerings.

1.2 How to Read This Guide

This document presents the deployment process for Office 365 in a way that explains both important deployment concepts and detailed deployment procedures. It is also intentionally organized into the sections that provide specific types of information for specific types of deployment personnel in your organization. Here is a quick overview of what you will find:

- **Deployment Overview section.** This material provides the high-level look at the deployment and organizational requirements to deploy Office 365. It has valuable information for your IT decision-makers, program managers, and technical implementation leads.

- **Plan and Prepare sections.** These sections describe the particular tasks and activities required to get ready and fully implement your Office 365 deployment. The tasks are generally presented in the order in which you address them during your deployment.
Topics discussed in the Plan section generally reappear in the Prepare section with instructions for carrying out a task. The Plan and Prepare sections contain content that will interest specific types of technology experts in your organization.

- **Migrate section.** This section describes the tasks for moving your users’ mailboxes to the Office 365 environment so you can begin using the Office 365 as part of your production environment.

### 1.3 Assumed Knowledge

Deployment of Office 365 for enterprises is a multi-phased project that requires close communication and coordination of activities between your internal teams and any partners you engage. Although project personnel will have varied technical backgrounds, all should have project management, technical consulting, or technical support backgrounds.

For the technical areas of an Office 365 deployment, this guide assumes that your organization has personnel with Microsoft Certified Systems Engineer (MCSE) and Microsoft Certified IT Professional (MCITP) certifications or equivalent skills. Your personnel should also have experience in deploying Microsoft Exchange Server, Microsoft SharePoint Portal Server, Microsoft Lync Server, the Windows Server® operating system, and Active Directory® Domain Services. A detailed list of assumed technical knowledge is provided below.

- **Knowledge and proficiency in the following Microsoft server technologies:**
  - Active Directory Domain Services
  - Active Directory Federation Services (AD FS) 2.0
  - Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007
  - Microsoft SharePoint Server 2010 or Office SharePoint Server 2007
  - DNS and related technologies
  - Windows PowerShell™ 2.0

- **Knowledge and proficiency in the following Microsoft client technologies:**
  - Microsoft Office 2010 and Office 2007
  - Windows Internet Explorer® and other Internet browser technologies
  - Windows Update and Microsoft Update
  - Windows Phone® and mobility

- **Knowledge of the customer network topology:**
- Active Directory sites, trusts, and topology
- Wide area connectivity: on-premises networks and equipment
- Wide area connectivity: Internet bandwidth and latency
- Firewall technologies
- SSL certificates

- Knowledge of the legacy messaging systems including, but not limited to:
  - Microsoft Exchange Server-based systems
  - POP3/IMAP4/SMTP-based mail systems
  - Lotus Notes Domino
  - Novell GroupWise
  - Archival systems
  - Email encryption

### 1.4 Document Scope and Limits

This guide is focused on Office 365 deployments that implement email coexistence in a hybrid deployment configuration with enterprise single sign-on services. It is strongly recommended that you use the Exchange Server Deployment Assistant for configuring Exchange hybrid deployments. The [Exchange Server Deployment Assistant](#) section presented later in his guide provides more information about this Microsoft online tool.

The document has *does not* address these topics:

- Office 365 sales activities and pre-deployment entrance criteria. Entrance criteria including the following activities:
  - **Review of Office 365 service descriptions to ensure solution alignment.** Your organization should not move forward with its deployment until all aspects of the service have been evaluated for alignment with your existing business and IT requirements.
  - **Review of your Active Directory environment.** Your organization should ensure that your Active Directory complies with the requirements for Office 365. During your review, you should keep in mind that hybrid deployments only support email coexistence with a single Active Directory forest and that the directory synchronization service requires a support exception for synchronization of more than 20,000 users.
  - **Purchase of Office 365 for enterprises user licenses.** To provision users for Office 365 services, your organization will need to have valid user licenses available to assign to users.

- Office 365 operations activities that occur after deployment.
• Moving an existing BPOS implementation to an Office 365. Information about transitioning from BPOS to Office 365 is available at the Microsoft Office 365 transition center.

Finally, note that the Office 365 deployment guidance described in this guide is subject to change. Please periodically check for updated versions of the guide at the Microsoft Download Center.

1.5 Feedback

Readers are encouraged to submit feedback about this deployment guide to modgfdbk@microsoft.com. Your feedback is important to the continued improvement of this document.
2 Deployment Overview

This section provides a high-level orientation to Office 365 for enterprises deployment.

2.1 Deployment Phases

Microsoft recommends that you expedite your Office 365 deployment by proceeding in three distinct phases: Plan, Prepare, and Migrate. Organizing your deployment according to these phases provides your project team with high-level timeframes that control the pace of the deployment while keeping individual tasks serialized. It is common for tasks outlined in the Plan phase and Prepare phase to occur simultaneously and for tasks in the Prepare phase and Migrate phase to overlap.

Figure 1 depicts the phases and key activities for organizations deploying Office 365.

To help your organization plan your deployment project according to the Plan, Prepare, and Migrate phases, see Appendix B: Deployment Planning Template.
2.2 Sample Deployment Schedule

Figure 2 illustrates a high-level sample schedule for an Office 365 deployment project that involves migrating 8,000 users.

The number of weeks required to complete all migrations will vary based on a number of factors including number of users you are migrating and the complexity of your organization’s environment.

2.2.1 Deployment Checkpoints

As shown in Figure 2, there are several checkpoints identified in the Office 365 deployment schedule. At these points in the deployment, you should ensure you have completed the tasks that come before the checkpoint. If your deployment team has not completed these tasks, you should not move forward on the project until all those tasks are completed.

See Appendix C. Customer Deployment Checkpoints for details on the exit criteria associated with the key deployment checkpoints.

2.3 Customer Responsibilities

Office 365 for enterprises customers are required to assume specific responsibilities in the deployment process. Understanding these responsibilities at the start of the deployment is
critical to achieving a successful deployment and migration.

Key tasks for organizations that are deploying Office 365 and Exchange Online in a hybrid deployment configuration include:

- **Assign a qualified project manager**
  Your organization must assign a person to manage your Office 365 deployment project and lead your deployment team.

- **Develop a project plan**
  Your deployment project plan is used to schedule and track Office 365 deployment workstream progress. The plan should include a migration schedule that shows when each user’s mailbox will be migrated to Office 365. A high-level planning template is available in Appendix B: Deployment Planning Template for organizations to use for deployment project planning.

- **Obtain hardware**
  You organization must procure the necessary hardware for on-premises components of Office 365 — such as the hardware for a hybrid deployment and identity federation servers.

- **Evaluate network**
  Ensure your on-premises network meets bandwidth requirement and implement changes or upgrades as needed.

- **Acquire SSL certificates**
  Third-party SSL certificates must be obtained and installed in your infrastructure to provide enterprise-security for Office 365 service offerings.

- **Install and configure Active Directory Federation Services 2.0**
  To enable single sign-on, your organization must setup Active Directory Federation Services (AD FS) 2.0 federation and proxy servers prior to the migration of the first production mailbox.

- **Install and configure Exchange hybrid servers**
  For the Exchange hybrid deployment scenario in which some of your Exchange users have mailboxes on-premises and other mailboxes on Exchange Online, you must set up an Exchange 2010 hybrid server prior to the migration of the first production mailbox.

- **Install and configure the Directory Synchronization Tool**
  In an Exchange hybrid deployment scenario, the Microsoft Online Services Directory Synchronization Tool (DirSync) is required to keep your local Active Directory environment synchronized with your Microsoft Office 365 directory. The synchronization tool must be installed prior to migration of first production mailbox.

- **Ensure that each end user workstation meets Office 365 client prerequisites**
  Each end user PC must meet the Office 365 client requirements.

- **Configure Outlook Anywhere**
  You must configure Outlook clients to connect to Exchange Online over the Internet using the Outlook Anywhere connectivity (remote procedure call over HTTP) feature.
• **Plan and coordinate all end user support**
  Before migration of first production mailboxes, you must plan for support of Office 365 users. This includes planning for escalation of support issues to Microsoft via a maximum of two points of contact (for example, the customer’s project manager and technical lead or Exchange Administrator).

• **Plan, develop and execute training plans**
  You will need to implement training for your Office 365 end users.

• **Plan, develop and execute communication plans**
  You will need to inform all end users about the transition to Office 365 service offerings and what is required of them.

• **Perform migration of client-side data**
  Moving mailbox data and other client content to the Office 365 environment is the responsibility of the customer organization.

• **Assign resources to initiate, monitor, and complete migrations**
  During migration windows, personnel in your organization must be available to manage migration activities, which often occur on evenings and weekends.

### 2.4 Microsoft Online Services Portal

The Admin area within the [Microsoft Online Services Portal](#) is where you will carry out a number of key Office 365 deployment tasks. Using the features and tools available in the Admin area, you can configure and manage settings for the following:

- Domains
- Security groups
- Users and user licenses
- Email settings and protection via connections to the Exchange Control Panel and ForeFront Online Protection for Exchange Administration Center
- SharePoint site collections, user profiles, and InfoPath forms
- Lync Online domain federation and public IM

The Admin area within the Microsoft Online Services Portal page is shown in Figure 3.
Figure 3

You can also assign specific administration roles to personnel through the portal—generally after directory synchronization with the Office 365 environment is completed. Your organization should begin planning for these role assignments early in the deployment process. See the Role-Based Security and Administration section for more planning guidance.

2.5 Administration Roles

Table 1 lists the built-in roles that are available to your organization’s Office 365 team in the Microsoft Online Services Portal.

Table 1. Customer Security and Administration Roles in Microsoft Online Services Portal

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Administrator</td>
<td>Global Administrator role has full access to perform any operation in the scope of your organization.</td>
<td>Has full permissions to your organization. The initial user created when signing up for Office 365 will be assigned this role. You may assign administrator permissions to other users in your organization.</td>
</tr>
<tr>
<td>Billing Administrator</td>
<td>Billing Administrator has access to perform common billing related tasks.</td>
<td>Has full permissions for billing tasks, and read-only permissions for company objects (domains and users). Any user with this role will also receive notifications for billing events.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
<td>Details</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Management Administrator</td>
<td>User Management Administrator has access to perform common user management related tasks.</td>
<td>Has read-only permissions to all company objects and has administration permissions. Cannot make changes to Billing or Global Administrators.</td>
</tr>
<tr>
<td>Service Administrator</td>
<td>Service Administrator has access to perform common support tasks.</td>
<td>Has read-only permissions to all company objects. Also has the ability to manage service requests and monitor service health.</td>
</tr>
<tr>
<td>Password Administrator</td>
<td>Password Administrator has access to perform common support tasks and reset user passwords.</td>
<td>Has read-only permissions to all company objects. Also resets passwords, manages service requests, and monitors service health. Password administrators can reset passwords only for users and other password administrators.</td>
</tr>
<tr>
<td>User</td>
<td>A person consuming Office 365 service offerings.</td>
<td>This is the default role and does not include any administrator permissions.</td>
</tr>
</tbody>
</table>

2.5.1 Partner Delegated Administrators

If your organization uses a third party, partner, or syndication partner to manage your Office 365 for enterprises environment, you can manage your subscription partner in the Microsoft Online Services Portal. See the Help topic [Add, change, or remove a subscription advisor partner](#) to learn more.

You may also authorize your partner as a delegated administrator. This process must be initiated by your partner. See the Help topic [Add or remove a delegated administrator](#) to learn more.

Partners that will administer a company account on behalf of a customers should review the Help topic [Offer delegated administration](#) to learn about the types of tasks they can perform.

2.6 Deployment Project Support

Before starting your Office 365 deployment project, you should become familiar with the support options that are available to help you resolve issues that may arise during the deployment process. Begin by reviewing the Microsoft Office 365 for Enterprises Support Service Description, which is available from the [Microsoft Download Center](#). This document provides a single source of information for customer organizations about the technical and nontechnical support that is available with every Office 365 for enterprises plan subscription.
**Note:** Microsoft Office 365 support will only be provided to Office 365 Global Administrators. Any organization end-users who require assistance will need to contact their Global Administrator or Service Administrator, who may escalate the issue to Microsoft Office 365 support as needed.

### 2.7 Key Pre-deployment Considerations

This section identifies several key considerations as you begin planning and preparing for your deployment of Office 365.

#### 2.7.1 License Validation

Be aware that your organization will need to validate that it has Office 365 user licenses available to provision users for Office 365. You should understand in advance of your deployment the details of the licensing plans you have purchased including the total number of licenses you have available to allocate and what services are included with each type of license. As shown in Figure 4, user licenses are assigned through the Admin area within the Microsoft Online Services Portal.

![Figure 4](image)

#### 2.7.2 Roles-Based Security and Administration

Office 365 for enterprises allows for roles-based security for your organization. It is important to understand the Office 365 roles available to your organization and how to integrate them with your organization’s processes.

The following are examples of questions you should answer during your roles-based security assessment:

- Who will manage user administration on-premises and in the Office 365 environment?
- Who will manage access control and what processes are needed for these scenarios:
  - Hiring users
• User that leaves the company
• User that transfers to a different role or group

- What will your organization’s support policy, processes, and escalation plans encompass and what are the critical components that must be included?
- Who will track and respond to issues for on-premises and for Office 365 components?
- What will your training plan be for each of the administrative roles?
- What do you do if the primary administrator is ill or unavailable when a critical administrative request occurs? In particular, note that Office 365 Global Administrators will have full administrator functionality and access to all Office 365 administrative features such as the Microsoft Online Services Portal, user mailboxes, and Lync Online administration.

**Note:** None of Office 365 administrator roles are granted SharePoint Online site collection or administration access by default. They must explicitly be added.

After your organization has completed an assessment and devised a plan for role-based security and administration, you should be able to identify who will be your organization’s service administrators and how will you manage access to Office 365 administration components.

### 2.7.3 Deployment Impacts to Customer Organization

If your organization has established specific messaging or collaboration workflows, you should assess what impacts, if any, your migration to Office 365 may have on those workflows. You may need to modify or recreate specific document and messaging workflows with the introduction of the Office 365 service offerings.

It is important to involve each workflow’s stakeholders in assessing Office 365 impacts so that they can plan and prepare for any changes during the deployment process.

### 2.7.4 Assessing Service Features and Organizational Requirements

Your organization should assess your business and regulatory requirements to determine which Office 365 features and components will best suit your deployment. You can find detailed information about these features in the Office 365 service descriptions.

The Office 365 service descriptions are available at the [Microsoft Download Center](https://www.microsoft.com).

#### 2.7.4.1 Integration with Line-of-Business Applications

When assessing how Office 365 will meet your business requirements, your organization should take an inventory of your line-of-business applications and determine which messaging or collaboration components, if any, will need to integrate with Office 365 service offerings. In
some cases, your organization may need to make changes to the application or custom code to ensure that it functions properly with Office 365 service offerings.

For example, Exchange Web Services (EWS) is the only Exchange API that your organization can use with Exchange Online services. If you have an existing application that relies on pre-Exchange Server 2010 APIs, you will need to devise a plan to modify the application to utilize EWS. See the Exchange Online Application Interoperability section of this document for additional information.

2.7.5 Application Integration and Supported Interfaces

The following interfaces are available to your organization to provide application integration with Office 365:

- **Windows PowerShell for user identity and account provisioning.** Provides your organization the ability to programatically complete virtually all the user management tasks in the Microsoft Online Services Portal.
- **Windows PowerShell for Exchange Online.** Provides the ability to complete tasks in the Exchange Management Console (EMC) via PowerShell.
- **Exchange Web Services (EWS) for Exchange Online.** Provides the capability to complete virtually any task that the Outlook client is able to do programatically.
- **SharePoint Web Services.** Provides methods and services accessible through client applications such as Silverlight and ECMAScript. See the MSDN page SharePoint Online: An Overview for Developers for more about SharePoint web services and the SharePoint Client Object Model.

The following APIs are not supported by Office 365:

- Collaborative Data Objects Messaging (CDO)
- WebDAV protocol
- Custom code requiring changes to Exchange Online

2.7.6 Migration Groups

For organizations that will have a large number of Office 365 users, migration of user mailboxes to Office 365 must occur over an extended period with selected groups of users migrated at the different times. You need to create these migration groups. The guiding rule is to create migration groups in a way that has the least impact on users.

When creating your groups, you should know that Office 365 supports migration of delegates. It is recommended that mailbox migration of delegates and managers occurs at the same time. For example, the mailboxes for an executive and the administrative assistant to that executive should be migrated together. Mailboxes and any delegates must be located on the same
Exchange infrastructure (both with Office 365 or both on-premises) for the highest fidelity and end user experience.

See the [Create Migration Groups](#) topic in this document for additional guidance.
3 Plan Phase

During the Plan phase, your organization’s deployment team begins gathering information and developing strategies for deploying Office 365 service offerings.

3.1 Key Activities Summary

The following tasks represent the significant work items that your organization will carry out in the Plan phase:

- **Hold project kickoff meeting**
  
  Your kickoff meeting launches the Office 365 deployment project and includes review of how the Office 365 solution aligns with your organization’s business requirements.

- **Build risk and issue tracking system**
  
  You will need a process for tracking deployment project risks and issues and generating project status reports.

- **Develop migration strategy**
  
  Your mailbox migration strategy should include evaluating and, if necessary, purchasing third-party email migration toolsets and identifying hardware requirements.

- **Identify mailbox size and item counts**
  
  You need to know the size of mailboxes and number of items in mailboxes that will be migrated to Office 365. Along with available bandwidth to the Internet, mailbox size and item number will affect migration velocity.

- **Plan for mail-enabled applications**
  
  If you have mail-enabled applications, your organization should determine whether they could be modified to work with Exchange Online using Exchange Web Services (EWS).

- **Identify options for user identity and account provisioning**
  
  The services provided by Office 365 for enterprises solution require that user accounts or “identities” be created in the Office 365 environment for each Office 365 user.

- **Identify your email coexistence strategy**
  
  You need to develop your strategy for configuring an Exchange hybrid deployment between your on-premises environment and the Office 365 environment.

- **Identify available Internet bandwidth testing tools**
  
  You should have bandwidth-testing tools available to calculate migration velocity for mailbox data.

- **Identify on-premises infrastructure server requirements**
  
  Single sign-on (identify federation) and Exchange hybrid deployment will require deployment of on-premises hardware.

- **Identify the operating systems and client applications**
  
  You must inventory the applications that are currently used in your environment to see if they meet the requirements for Office 365.
• **Identify the mobile platform that your organization will use**  
  You must plan for any changes required to your organization’s mobile platform with the move to Office 365. Microsoft Exchange ActiveSync enables users to synchronize their mobile phones with their Exchange Online mailboxes.

• **Develop an end user and administrator training schedule and delivery mechanism**  
  Training administrators and users how to work with Office 365 service offerings must be included in your deployment planning.

• **Develop end-user communications strategy**  
  You will need to create and schedule a series of communications to end users that notifies them about their transition to Office 365 service offerings and provides instructions regarding what is required of them.

### 3.2 Kickoff Meeting

Your organization should schedule a kickoff meeting to launch its Office 365 deployment project. The kickoff meeting can serve a number of purposes. You can use it to familiarize your project team members with the overall business perspective of the project. You can also review the solution alignment evaluation conducted prior to moving forward with your deployment.

Another objective of the kickoff meeting is to help your team identify and prepare for deployment tasks or milestones that typically require a significant lead time to complete. See the [Long Lead Time Items](#) topic in this document for more details.

### 3.3 Customer Environment Discovery

It is important at the outset of your deployment project to gather and capture information about your existing IT environment. This process is commonly called “discovery.” Discovery activities provide a comprehensive and up-to-date record of the technology solutions implemented by our organization.

You should gather information in the following areas:

• On-premises infrastructure servers and components
• Network architecture and DNS
• Authentication solutions
• Directory design
• Bandwidth
• Mail routing
• Certificates
• Hardware and software
• Mail and other client applications
• Mail archiving and compliance
Mobile devices

3.3.1 Office 365 Deployment Readiness Tool

The Office 365 Deployment Readiness Tool is available to assist you with discovery activities related to Office 365 deployments. The tool can be used to check and provide information in the following areas in your on-premises environment:

- **Domains**
  - Email domains and number of users for each domain
- **User Identity and Account Provisioning**
  - Statistical information
  - Active Directory schema data
  - Forest and domain functional data
  - Trusts and multi-forest constraints
  - Directory Synchronization pre-requisite checks and attribute assessment
  - Attribute assessment and readiness for single sign-on
- **Exchange Online**
  - Statistical information
  - Public folder, public delegates, and proxyAddresses
  - Third-party and unified proxyAddresses information
- **SharePoint Online**
  - User object count
- **Lync Online**
  - Statistical information
- **Client and end-user experience**
  - Summary of domain joined machines for rich experience and single sign-on readiness
- **Networking**
  - Port analysis on specific Office 365 endpoints
  - DNS records

You can learn more about and download the tool at Office 365 Community.
3.3.2 Microsoft Assessment and Planning Toolkit

The Microsoft Assessment and Planning (MAP) toolkit is another tool to help with planning for Office 365 deployments.

The MAP toolkit is an agentless, automated, multi-product planning and assessment tool that generates detailed readiness assessment reports with extensive hardware and software information. It provides actionable recommendations to help organizations accelerate their IT infrastructure planning process and gather more detail on assets that reside within their current environment. MAP helps make the IT planning projects faster and easier for a number of purposes including:

- Migration to Windows 7, Windows Server 2008 R2, and Microsoft Office 2010
- Migration to Windows 7 compatible versions of Internet Explorer
- Migration to cloud-based services
- Assessment of current software usage and client access history for simplified software asset management
- PC security assessment and migration to Microsoft Forefront Client Security

You can learn more about and download the MAP toolkit, see the TechNet page Microsoft Assessment and Planning Toolkit.

3.4 Pilot Deployment

Your organization may want to conduct a pilot deployment as part of its Office 365 planning and evaluation process. The pilot enables your organization to conduct its own in-house testing of Office 365 for enterprises features and functionality. It helps you to identify and assess any service issues that might affect your business prior to moving a significant number of individuals to Office 365 service offerings.

In addition, pilot deployments can help you test migration processes against the various types of mailboxes that are found within your environment. For example, if your current messaging system includes Lotus Domino and Lotus Notes, the pilot should also test access to Lotus Notes applications that may be left behind in the migration process.

---

**Note:** The Exchange Server Deployment Assistant does not support hybrid deployments with Lotus Domino and Lotus Notes.

---

In some cases, pilots may begin before and extend well past the Plan phase. You may choose to conduct a service trial prior to signing an Office 365 subscription agreement and operate your trial up until the time of full organizational deployment.
Developing a pilot plan is recommended to help keep the pilot on track. Organizations typically start with about 10 users participating in the pilot. More users are added as confidence in overall system performance is demonstrated.

To launch your pilot program, your organization simply signs up for the Office 365 in the usual manner. There is not a separate Office 365 pilot program.

For larger customers, there are special considerations related to your on-premises Active Directory size when over 10,000 objects that will impact the type of tenant provisioned for your company. Therefore it’s strongly recommended to use a test domain and company name when signing up for your pilot tenant different than the ones you plan to use in production. Please work with the Office 365 sales or support team before creating your production tenant.

3.5 Key Planning Considerations

The deployment process requires that you address several key items early in your deployment work to ensure timely completion of workstreams and avoid unnecessary deployment delays.

3.5.1 Long Lead Time Items

When deploying Office 365, you need to be aware of long lead time items. These items are tasks or milestones that have traditionally required a significant lead time to complete and have a higher risk of delaying the completion of the project if not addressed early in the implementation.

The following items are known to require significant evaluation and planning time:

- Tools and testing for mailbox migration.
- Tools and testing for SharePoint application remediation.
- Procurement and deployment of any necessary on-premises hardware and software.
- Internet and customer network capacity.
- Policies related to mobility solutions.
- Tools for provisioning and de-provisioning objects in your Active Directory.
- Preparation of your on-premises Active Directory for the initial directory synchronization with Office 365.
- Setting up the primary Simple Mail Transfer Protocol (SMTP) namespaces to be used for Office 365 and Exchange hybrid deployment.
- Encryption and encrypted email.

3.5.2 Client Hardware and Software Requirements

Office 365 for enterprises solutions allow your organization to choose either the rich experience or web experience for your users.
The rich experience requires that a user’s PC have recent versions of operating systems, desktop Office applications, and Internet browsers installed. It also requires installation of the Office 365 desktop setup, which automatically configures PCs with the required updates and service components. The web experience requires user access to a PC with a recent version of mainstream web browsers.

It is important that your organization assess the requirements highlighted in the Client and End-User Experience section of this document.

### 3.5.3 Migration Support for Existing Mail Environments

Your organization should be aware that Office 365 supports mailbox migration from the following environments:

- On-premises Microsoft Exchange Server environments
- Hosted Exchange environments
- IMAP4 servers
- Certain third-party platforms

If you have an on-premises Exchange Server environment deployed that runs Exchange Server 2010, Exchange Server 2007, or Exchange Server 2003, you can configure a hybrid Exchange deployment and then migrate your organization’s mailboxes over time.

Mail migrations from other platforms will require the use of non-Microsoft tools and processes. Each customer environment will have different requirements and the migration toolsets should be evaluated to determine if they meet the organization’s requirements.

For more information, see the Help topic Migrate Users and Get Them Connected.

### 3.6 Networking and Naming Services Planning

This section of the document presents key planning considerations about Office 365 domain and domain name service (DNS) records configuration, network bandwidth and latency, network ports and protocols, and SSL certificates.

To quickly summarize, your organization must plan in advance for configuration of internal and external (Internet-facing) DNS records, as well as the testing efforts to make sure name resolution is functioning properly. Your organization should also plan to provide the appropriate Internet bandwidth for the services you select as well when migrating data to the Office 365 data centers. It is also important to be aware that Office 365 requires specific ports and protocols to be accessible to support the use of online services and migration tools. Use of third-party SSL certificates is required to secure your organization’s Office 365 deployment.
3.6.1 Adding a Domain

When your company signs up for Office 365, you are given an initial domain name similar to the following: contoso.onmicrosoft.com.

If you want your hosted email or other services to use domains that you own rather than the one that you were given at signup, you can add these domains to Office 365. To add your domains within Office 365, you use the Microsoft Online Services Portal, verify domain ownership, and then create DNS records at your domain name registrar (or DNS hosting provider). For example, you would create the DNS records that are required to route domain traffic to your Office 365 service offerings, such as the DNS records that are required for routing inbound email to Microsoft Exchange Online.

After you add your domains to Office 365 and the domains are verified, you can then set up email, create Microsoft Lync Online accounts with the newly created domain, create distribution lists that include the domain, and use the domain for your Microsoft SharePoint Online hosted website by changing DNS records at your domain registrar.

For more information, see the Help topic Add your domain to Office 365.

3.6.1.1 Single-label Domain Support

The use of single-label domains (SLDs) is not supported in Office 365 and Exchange Online deployments. SLDs are DNS names that do not contain a suffix, such as .com, .corp, .net, or .org. For example, “contoso” is an SLD, and therefore is not supported. However, “contoso.com” and “contoso.local” are not SLDs, and therefore are supported.

For more information, see the Microsoft Support article Microsoft Online Services compatibility with single-label domains, with disjoint namespaces, and with discontiguous namespaces.

3.6.2 External DNS Records

An Office 365 for enterprises deployment requires you to configure external (Internet-facing) DNS records with your domain registrar.

Table 2 provides a summary of the external records you need to create. The Exchange Server Deployment Assistant provides more specific guidance on creating external DNS records.
### Table 2. Example External DNS Records

<table>
<thead>
<tr>
<th>DNS record</th>
<th>Purpose</th>
<th>Value to use</th>
</tr>
</thead>
</table>
| TXT (Domain Validation) | This record is used for domain validation. It proves that you own the domain but it doesn’t direct incoming mail for the domain to Office 365 service offerings. | Host: @ (domain name)  
TXT Value: <text string>  
The values that you need to enter are provided to you by the Microsoft Online Services Portal add domain wizard.  
**Note:** The wizard also gives you the option of using a MX record for domain validation. |
| **Host (A)** | This record is for the single sign-on service and indicates the end point for your off-premises users (and on-premises users if you choose) to connect to your Active Directory Federation Services (AD FS) proxy servers. | Target: sts.contoso.com |
| **CNAME (Exchange Online)** | This record allows Office Outlook clients to connect to the Exchange Online service by using the Autodiscover service. Autodiscover automatically finds the correct Exchange Server host and configures Outlook for the users. | Alias: Autodiscover  
Target: autodiscover.outlook.com  
For more information, see [Use a CNAME Record to Enable Outlook to Connect](#). |
| **SPF (TXT) (Exchange Online)** | This sender policy framework (SPF) record identifies which of your email servers are authorized to transmit email from your domain. This helps to prevent others from using your domain to send SPAM or other malicious email. | Value v=spf1 include:outlook.com ~all  
For more information, see [Use an SPF Record to Validate E-mail Sent from Your Domain](#).  
**Note:** If the firewall or proxy server blocks TXT lookups on an external DNS, this record should also be added to the internal DNS. |
| **SRV (Lync Online)** | This value is for SIP federation and allows your Office 365 domain to share instant messaging (IM) features with clients other than Windows Live Messenger. | Service: _sipfederationtls  
Protocol: TCP  
Priority: 10  
Weight: 1  
Port: 5061  
Target: Sipfed.online.lync.com  
**Note:** If the firewall or proxy server blocks SRV lookups on an external DNS, this record should also be added to the internal DNS. |
<table>
<thead>
<tr>
<th>DNS record</th>
<th>Purpose</th>
<th>Value to use</th>
</tr>
</thead>
</table>
| SRV (Lync Online) | This SRV record is used by Microsoft Lync Online to coordinate the flow of information between Lync clients. | Service: _sip  
Protocol: TLS  
Priority: 100  
Weight: 1  
Port: 443  
Target: sipdir.online.lync.com |
| CNAME (Lync Online) | This CNAME record is used by the Lync 2010 client to discover the Lync Online Service and sign in. | Alias: sip  
Target: sipdir.online.lync.com  
For more information, see [Ensuring Your Network Works With Lync Online](#) |
| MX (Exchange Online) | This value directs all incoming mail for the domain to the Exchange Online service. | Target Server &lt;MX token&gt;.mail.contoso.com  
Preference: 10 |
| Host (A) | Mail Record (A) | Target: mail.contoso.com |
| TXT (Exchange Federation) | Exchange federation for hybrid deployment | TXT record 1: contoso.com and associated custom-generated domain proof hash (ex. “Y96nu89138789315669824”)  
TXT record 2: exchangedelegation.contoso.com and associated custom-generated domain proof hash (for example, “Y3259071352452626169”) |
| SRV | Office 365 Service Record (A) | Target: service.contoso.com |

### 3.6.3 Third-Party SSL Certificates

In order to encrypt communications between your clients and the Office 365 environment, the third-party SSL certificates must be installed on your infrastructure servers.

Certificates are required for the following Office 365 components:

- Exchange on-premises
- Single sign-on service (Active Directory Federation Services)
- Federation proxy server
- Autodiscover, Outlook Anywhere, and Exchange ActiveSync services
- Exchange hybrid server
Certificates for Exchange On-Premises
For an overview of using digital certificates to secure the communication between the on-premises Exchange organization and Exchange Online, see the TechNet article Understanding Certificate Requirements.

Certificate for Single Sign-On
To provide your users with a simplified single sign-on experience that includes enterprise-class security, an identity federation third-party SSL certificate (example, common name=sts.contoso.com) using a third-party trusted root authority must be installed on all Active Directory Federation Services (AD FS) servers. For more information, see the Help topic, Plan for and deploy Active Directory Federation Services 2.0 for use with single sign-on. For additional information on ADFS 2.0 design, see the AD FS 2.0 Design Guide available on TechNet.

Federation servers require the certificates called out in Table 3.
Table 3. Federation Server Certificates

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Description</th>
<th>What you need to know before deploying</th>
</tr>
</thead>
</table>
| **SSL certificate (also called a Server Authentication Certificate)** | This is a standard Secure Sockets Layer (SSL) certificate that is used for securing communications between federation servers, clients, and federation server proxy computers. | AD FS 2.0 requires an SSL certificate when configuring federation server settings. By default, AD FS 2.0 uses the SSL certificate configured for the Default Web Site in the Internet Information Services (IIS). The Subject name of this SSL certificate is used to determine the Federation Service name for each instance of AD FS 2.0 that you deploy. For this reason, you may want to consider choosing a Subject name on any new CA-issued certificates that best represents the name of your company or organization to Office 365 and this name must be internet routable. For example, in the diagram provided earlier in this article (see “Phase 2”), the subject name of the certificate would be fs.fabrikam.com.  
**Warning:** AD FS 2.0 requires this SSL certificate to be without a dotless (short-name) Subject name.  
**Recommendation:** Because this certificate must be trusted by clients of AD FS 2.0, use an SSL certificate that is issued by a public (third-party) certification authority (CA) or by a CA that is subordinate to a publicly trusted root, for example, VeriSign or Thawte. |
| **Token-signing certificate**            | This is a standard X.509 certificate that is used for securely signing all tokens that the federation server issues and that Office 365 will accept and validate.                                                                 | The token-signing certificate must contain a private key, and it should chain to a trusted root in the Federation Service. By default, AD FS 2.0 creates a self-signed certificate. However, depending on the needs of your organization, you can change this later to a CA-issued certificate by using the AD FS 2.0 Management snap-in.  
**Recommendation:** Use the self-signed token-signing certificate generated by AD FS 2.0. By doing so, AD FS 2.0 will manage this certificate for you, by default. For example, in case this certificate is expiring, AD FS 2.0 will generate a new self-signed certificate to use ahead of time. |

**Caution:** The token-signing certificate is critical to the stability of the federation service. If the certificate is changed, Office 365 must be notified of the change. If notification is not provided, users will not be able to sign-in to their Office 365 service offerings.
Certificate for Federation Server Proxy
Federation server proxies require the certificate called out in Table 4.

Table 4. Federation Server Proxy Certificate

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Description</th>
<th>What you need to know before deploying</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL certificate</td>
<td>This is a standard SSL certificate that is used for securing communications between a federation server, federation server proxy, and Internet client computers.</td>
<td>This certificate must be bound to the Default Web Site in IIS before you can run the AD FS 2.0 Federation Server Proxy Configuration Wizard successfully. This certificate must have the same subject name as the SSL certificate configured on the federation server in the corporate network. Recommendations: Use the same server authentication certificate as is configured on the federation server that this federation server proxy will connect to.</td>
</tr>
</tbody>
</table>

Certificates for Autodiscover, Outlook Anywhere, ActiveSync
Your external facing Exchange 2010, Exchange 2007, and Exchange 2003 client access server(s) (CAS) will require a third-party SSL certificate for secure connections for Autodiscover, Outlook Anywhere, and ActiveSync services (mail.contoso.com). You may already have this certificate installed in your on-premises environment.

Certificate for Exchange 2010 Hybrid Server
Your external-facing Exchange hybrid server(s) will require a third-party SSL certificate for secure connectivity with the Exchange Online service. You will need to obtain this certificate from your third-party SSL provider.

3.6.4 Ports and Protocols
Office 365 provides services to your organization over your Internet connection and may replace applications that previously operated within your organization’s network. The traffic that previously was confined to the organization network will now travel between the organization and the Internet.

You should ensure that your organization’s connection to the Internet is configured correctly and that it has enough capacity to handle the network traffic. See Table 22. Protocol and Port Requirements for an overview of the ports and protocols involved in an Office 365 deployment.
3.6.5 Firewall Considerations

Computers on your network must be able to perform standard Internet DNS lookups. If these computers can reach standard Internet sites, your network meets this requirement.

Depending on the location of your Microsoft Online Services data center, you must also configure your network firewall devices to accept connections based on wildcard domain names (for example, all traffic from *.outlook.com or *.microsoftonline.com). If your organization’s firewalls do not support wildcard name configurations, you will have to manually determine the IP address ranges that you would like to allow and the specified ports.

Contact the Microsoft Office 365 support team for IP address ranges requirements, or refer to the Help topic IP addresses and URLs used by Office 365.

**Note:** Microsoft data center IP addresses are subject to change at any time. It is important to know that Office 365 does NOT notify customers of IP address range changes. Therefore it is highly recommended your organization configures wildcard namespaces on your firewalls.

3.6.6 WAN Accelerators

If your organization leverages wide area network (WAN) acceleration proxy appliances you may encounter issues accessing the Office 365 service offerings. You may need to optimize your network device(s) to ensure consistent experience for your end users. For example, Office 365 service offerings encrypt content and the TCP header level. Your device may not be able to handle such traffic.

Contact your appliance provider for optimization solutions.

3.6.7 Hardware and Software Load Balancing Devices

Your organization will need to either use a hardware or software-based network load balancer (NLB) solution to distribute requests to your AD FS servers and Exchange coexistence servers. Load balancing devices control the network traffic to each of the respective on-premises servers and are key to ensuring availability of single sign-on and Exchange hybrid deployment.

Microsoft provides a software-based NLB solution with Windows Server. Office 365 supports this solution to achieve load balancing.

3.6.8 Internet Bandwidth Planning

Using Office 365 service offerings may increase your organization’s Internet traffic so it is important to evaluate and assess the network impact of the services. Email traffic with Exchange
hybrid deployment and directory synchronization activity will have the most bandwidth impact, but some organizations may notice a general increase in Internet traffic after migrating users to the Office 365 suite.

3.6.8.1 Estimating Bandwidth Usage

There are many variables to consider when estimating network traffic. Some of these variables are:

- The Office 365 service offerings that your company has subscribed to.
- The number of client computers in use at one time.
- The type of task each client computer is performing.
- The performance of your Internet browser software.
- The capacity of the network connections and network segments associated with each client computer.
- Your company’s network topology and the capacity of the various pieces of network hardware.

For helpful information to estimate the network bandwidth your organization will require when using Exchange Online and SharePoint Online, see the TechNet article Company Network Requirements. For information regarding bandwidth requirements for Lync Server 2010 conferencing, review the TechNet article Defining Your Requirements for Conferencing.

3.6.8.2 Migration Velocity Testing

Testing and validating your Internet bandwidth (download, upload, and latency constraints) is vital to understanding how to achieve high-velocity migration of on-premises mailbox content to the Office 365 and Exchange Online environment. Slow or latent connectivity will reduce the number of mailbox migrations that can be completed during a migration window. Be sure to perform the following steps:

- Test and confirm if your organization’s Internet bandwidth can manage the network impact of Office 365 migrations.
- Assess internal network bandwidth availability for Office 365 migration events.
- Make use of available network tools such as ping (-I with data buffer), Tracert, and Microsoft Network Monitor.
- Determine your download, upload, and latency between your on-premises environment and the nearest Microsoft Online Services data center. The following can help with this task:
  - Ping outlook.com to determine the IP address of the nearest Microsoft Online Services data center from your location.
Consult a third-party IP mapping website (for example, iplocation.net) to determine that data center’s location.

Utilize a speed test website (for example, speedtest.net) to determine the upload, download, and latency statistics between your on-premises environment and the nearest location to the Microsoft Online Services data center.

Determine the periods in which the on-premises Exchange system is heavily used (for example, during backups).

### 3.6.8.3 Strategies to Improve Migration Velocity

To improve migration velocity as well as reduce your organization’s bandwidth constraints, you should consider the following:

- **Reduce mailbox sizes.** Smaller mailbox sizes will improve migration velocity.
- **Use the mailbox move capabilities with an Exchange hybrid deployment.** With an Exchange hybrid deployment, offline mail (.OST files) will not require re-download when migrating to Exchange Online. This will significantly reduce your download bandwidth requirements.
- **Schedule mailbox moves to occur during periods of low Internet traffic and low on-premises Exchange use.** When scheduling moves, understand that migrations requests are submitted to the mailbox replication proxy and may not take place immediately.

### 3.6.8.4 Office 365 Desktop Setup and Bandwidth Impact

Your organization must deploy and run the Office 365 desktop setup on each user PC that will use rich experience client applications such as Microsoft Outlook and Lync 2010. If you deploy the Office 365 desktop setup without first installing the necessary operating system service packs and updates, Office service packs and updates, Lync client application, and other components, there is a potential that your organization will require a significant amount of download bandwidth. More specifically, each PC would need to connect to the Internet and download and install any necessary service packs or updates. Organizations with a large number of PCs that are not patched would see the greatest bandwidth demand.

To prevent saturation of your network bandwidth, it is suggested that prior to deploying the Office 365 desktop setup that you download the necessary updates and deploy them via a package deployment tool (for example, Microsoft System Center Configuration Manager or another third-party tool) in advance to each your organization’s PCs.

Alternatively, if you do not have the infrastructure or ability to deploy the necessary updates, you may want to consider Active Directory group policy or throttling your deployment of the Office 365 desktop setup. To throttle the deployment of the Office 365 desktop setup, deploy
the setup package to a subset of your users at a time, allowing each of those users to download the necessary updates. Upon completion, deploy the setup package to another subset of users. Repeat this process until the necessary patches are deployed to all of your PCs.

For more information, see Help topic, 

**Manually update and configure desktops for Office 365** for the latest updates.

### 3.6.8.5 Port Exhaustion

Port exhaustion refers to the phenomenon of running out of TCP ports, resulting in connection failures. *If your organization has fewer than 2,000 users, you can skip this section.*

**What is Port Exhaustion?**

Most corporate networks use private (RFC1918) IP address space. Private address space is allocated by Internet Assigned Numbers Authority (IANA) and intended solely for networks that do not route directly to and from the global Internet.

To provide Internet access to clients on a private IP address space, corporations use gateway technologies like firewalls and proxies that provide network address translation (NAT) or port address translation (PAT) services. These gateways make traffic from internal clients to the Internet (including Office 365) appear to be coming from one or more publicly routable IP addresses. Each outbound connection from an internal client translates to a different source TCP port on the public IP address.

In this way, thousands of people on a corporate network can “share” a few publicly routable IP addresses.

The TCP protocol limits the number of TCP ports per IP address (approximately 64,000), and a port gets used for every active TCP connection. Port exhaustion refers to the phenomenon of running out of these ports, resulting in connection failures. This limit is rarely a problem when the only Internet usage is short-lived Web browsing connections, but Outlook maintains up to eight persistent connections per client. Additional Outlook plug-ins can add additional connection load per client.

**How to Avoid It?**

For Office 365 to function at acceptable levels, we require that companies plan for no more than 2,000 users per public IP in order to accommodate these persistent connections and leave capacity for other Internet usage. Companies with more than 2,000 users must implement methods for distributing client load across additional public IP addresses. Strategies available depend on the capabilities of the corporate gateway solution. The simplest solution is to segment your user address space and statically “assign” a number of IP addresses to each gateway. Another alternative that many gateway devices offer is the ability to use a pool of IP
addresses. Using an address pool effectively requires that your gateway solution correctly implement client source IP stickiness, as all eight of the connections from Outlook to the service must come from the same IP. The benefit of the address pool is that it is much more dynamic and less likely to require adjustment as your user base grows.

3.6.8.6 Network Device Limitations

Some network hardware may have limitations on the number of concurrent sessions it supports. We recommend that companies that have over 2,000 users monitor their network devices to ensure that they have the capability to handle the additional Office 365 service traffic. The use of SNMP monitoring software can help with the effort.

3.7 User Identity and Account Provisioning Planning

In order to use the services provided by the Office 365, user accounts or “identities” will need to be created for each user that will utilize the service. This section describes the components and configurations required to create user accounts and provision them for services. It includes discussion of Active Directory cleanup, configuration of single sign-on, and installation and configuration of the Directory Synchronization Tool.

It is important to understand from the outset that there are two options that your organization can select when planning for user access: standard or single sign-on.

- **Standard identity.** Each user in your organization requires a separate user ID and password to access the Office 365 service offerings.
- **Single sign-on.** Your users enter the same user ID and password they use to access their Active Directory corporate network to access the Office 365 service offerings. Single sign-on is also called *identity federation*.

The single sign-on model is the recommended for Office 365 for enterprises customers.

3.7.1 Adding and Provisioning User Accounts

Office 365 provides several mechanisms to add users to the service and manage user accounts. This deployment guide focuses on the directory synchronization provisioning mechanism, which is required for single sign-on and an Exchange hybrid deployment.

In addition, directory synchronization enables features and functionality in the Office 365 that are not available in the other provisioning options. Table 5 summarizes your options for creating and provisioning users.

**Table 5. User Creation and Provisioning Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Directory Synchronization      | • Allows for onboarding and offboarding of users when Exchange hybrid deployment is configured.  
• Enables single sign-on.  
• Synchronizes security and mail-enabled groups. |
| PowerShell                     | • Enables mass import of users via PowerShell scripting.  
• Does not allow for single sign-on. |
| Bulk Import                    | • Allows for an import of a CSV file to mass populate users.  
• Does not allow for single sign-on. |
| Microsoft Online Services Portal | • Provides a simple web interface to add and modify user accounts.  
• Cannot be used to modify users if directory synchronization is enabled. |

3.7.2 User License Activation

Within the Admin area of the Microsoft Online Services Portal you can enable user licenses via a simple interface. You select one or many users and then enable an Office 365 for enterprises plan license.

In addition to using the Microsoft Online Services Portal, your organization can programmatically assign user licenses by using the Windows PowerShell cmdlets for Office 365. For more information, see Help topic [Windows PowerShell cmdlets for Office 365](#).

Administrators can assign licenses to users after the directory synchronization process occurs in the deployment.

3.7.3 Active Directory Synchronization

This section describes requirements and planning considerations to implement directory synchronization between your Active Directory implementation and the Office 365 environment. As previously noted, Office 365 currently only supports directory synchronization with a single on-premises Active Directory forest.

3.7.3.1 Required Permissions

Deploying Office 365 requires high-level permissions to access your Active Directory for synchronization user data and provisioning users for Exchange Online, Lync Online, or SharePoint Online services.

The Directory Synchronization Tool requires that you are a member of the Enterprise Admins group during the initial installation. Schema Admin rights will be required to update your Active Directory forest’s schema to configure an Exchange hybrid deployment. Most other tasks will require membership in the Domain Admin group.
3.7.3.2 Schema Update

If your organization intends on implementing Exchange hybrid mode you will need to upgrade your Active Directory schema to include Exchange Server 2010 SP1 updates. This schema update is required in order to manage email attributes on-premise when using directory synchronization. You will need to obtain a user account with Schema Admin rights in order to make this change to your Active Directory forest.

You can learn about schema update risks and back out planning in the TechNet article Active Directory Schema Update.

3.7.3.3 Domain Controller Requirements

Table 6 lists the requirements for domain controllers deployed in your Active Directory forest(s) that communicate with the Office 365 environment.

Table 6. Domain Controller Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| **Schema master**          | • 32-bit or 64-bit edition of the Windows Server 2003 SP1 Standard or Enterprise operating system  
                              | • 32-bit or 64-bit edition of the Windows Server 2008 Standard or Enterprise operating system  
                              | • 64-bit edition of the Windows Server 2008 Standard R2 or Enterprise operating system |
| **Global catalog server**  | In every Active Directory site where you plan to install the Exchange 2010 SP1 hybrid server, you must have at least one global catalog server that is either:  
                              | • 32-bit or 64-bit edition of Windows Server 2003 SP2 Standard or Enterprise  
                              | • 32-bit or 64-bit edition of Windows Server 2008 Standard or Enterprise  
                              | • 64-bit edition of Windows Server 2008 R2 Standard or Enterprise |
| **Active Directory forest**| • Windows Server 2003 forest functional mode or higher                         |
| **Domain controller**      | • 32-bit or 64-bit Windows Server 2003 Standard Edition or Enterprise Edition with Service Pack 1 (SP1)  
                              | • 32-bit or 64-bit edition of the Windows Server 2008 Standard or Enterprise, Windows Server 2008 R2 Standard or Enterprise, or Windows Server 2008 Datacenter or Windows Server 2008 R2 Datacenter |

3.7.3.4 Active Directory Cleanup

It is highly recommended that you prepare your Active Directory forest prior to beginning your Office 365 deployment.

Your directory remediation efforts should focus on the following tasks:

• Remove duplicate proxyAddress and userPrincipalName attributes.
- Update blank and invalid userPrincipalName attributes with a valid userPrincipalName.
- Remove invalid and questionable characters in the givenName, surname (sn), sAMAccountName, displayName, mail, proxyAddresses, mailNickname, and userPrincipalName attributes. See Appendix F: Directory Object Preparation later in this document for details on preparing attributes.

When you deploy and configure Microsoft Online Services Directory Synchronization Tool, an email will be sent to your organization's Technical Contact with any outstanding errors that need to be corrected.

### 3.7.3.5 Active Directory Auditing

Your organization may want to use Active Directory auditing to capture and evaluate the events associated with directory synchronization such as user creation, password reset, adding users to groups, and so on.

By implementing single sign-on, Office 365 auditing will capture directory services logs on your Active Directory domain controllers. Note that security logging may be disabled by default so you will have to understand how to enable it for your organization.

For more information on configuring auditing, see the TechNet article [Audit account management](#).

### 3.7.3.6 Multi-Forest Deployment Considerations

By default, Office 365 synchronizes with a single on-premises Active Directory forest. If your organization has multiple forests for authentication (logon forests) the following is highly recommended:

- **Evaluate consolidating your forests.** In general, there is more overhead required to maintain multiple forests. Unless your organization has security constraints that dictate the need for separate forests, consider simplifying your on-premises environment in advance of deploying Office 365.
- **Use primary logon forest only.** Consider only deploying Office 365 in your primary logon forest for your initial rollout of Office 365.

> **Note:** Look for additional guidance on multi-forest deployment in future versions of this deployment guide.

### 3.7.4 Single Sign-On

With single sign-on (identity federation), your users will enter their Active Directory corporate credentials to access services from Office 365 service offerings.
Office 365 uses Active Directory Federation Services (AD FS) 2.0 to achieve single sign-on. In order to implement single sign-on, the Microsoft Online Services Directory Syncronization tool is also required.

You should review the Help topic Plan for and deploy AD FS 2.0 for use with single sign-on if your organization plans to use the single sign-on service.

3.7.4.1 Benefits of Using Single Sign-On

There is a clear benefit to users when you set up single sign-on and enable identity federation. Single sign-on allows users to use their corporate credentials to access the Office 365 service offerings that your company has subscribed to without the burden of managing additional logons and different passwords.

Figure 5 depicts the end-user experience with single sign-on.

![Figure 5](image)

Without single sign-on, an Office 365 user would have to maintain separate usernames and passwords.

Here is an example of the Office 365 sign-on name for fictional Contoso employee John Smith in federated and non-federated environments:

**Federation Environment**
- Display name: John Smith
- Username: jsmith@contoso.com
- Password: Pass1word!

**Non-federated Environment**
- Display name: John Smith
- Username: jsmith@contoso.onmicrosoft.com
• Password: Pass2word!

Configuring single sign-on also allows you to enforce your organization’s password policies and account restrictions in both the on-premises and Office 365 organizations.

In addition to the user benefits, there are considerable benefits to administrators and your organization:

• **Policy control.** The administrator can control account policies through Active Directory, which gives the administrator the ability to manage password policies, workstation restrictions, lockout controls, and more.

• **Access control.** The administrator can restrict access to Office 365 so that they can be accessed through the corporate environment, through online servers, or both.

• **Reduced support calls.** Forgotten passwords are a common source of support calls in all companies. If users have fewer passwords to remember, they are less likely to forget them.

• **Security.** User identities and information are protected because all of the servers and services used in single sign-on are mastered and controlled on-premises.

• **Support for strong authentication.** You can use strong authentication (also called two-factor authentication) with Office 365. If you use strong authentication, you must use single sign-on. There are restrictions on the use of strong authentication.

    ▶ **Note:** Strong authentication is only available using Office 365 web clients.

### 3.7.4.2 User Experience in Different Locations

A user’s experience with single sign-on varies based on how the user’s computer is connected to your organization’s network and how an administrator has configured Active Directory Federation Services. Here are some example configurations:

• **Work computer on a corporate network.** When users are at work and signed in to the corporate network, single sign-on enables them to access the services in Office 365 without signing in again.

• **Roaming with a work computer.** For users who are logged on to domain-joined computers with their corporate credentials, but who are not connected to the corporate network (for example, a work computer at home or at a hotel), single sign-on enables them to access the services in the Office 365 suite without signing in again.

• **Home or public computer.** When the user is using a computer that is not joined to the corporate domain, the user must sign in with corporate credentials to access the services in the Office 365 suite. Active Directory Federation Services Proxy servers are required in this scenario.
3.7.4.3 Identify Federation Requirements

Your organization must meet the following requirements to implement Active Directory federation:

- **Single Active Directory forest.** To use single sign-on, you must have Active Directory deployed in a single forest configuration and running in Windows 2003 or later with a functional level in mixed or native mode. If your organization has multiple Active Directory logon forests, please see the guidance provided in the Multi-Forest Deployment Considerations section of this document.

- **Active Directory Federation Services 2.0.** You must deploy AD FS 2.0 on a Windows 2008 or Windows 2008 R2 Server.

- **Latest client operating system(s) and service packs.** Your users must be running the latest updates of Windows 7, Windows Vista, or Windows XP. We strongly recommend that you install the Office 365 desktop setup to automatically get updates to the required software. The Office 365 desktop setup can be downloaded from the Home page of the Microsoft Online Services Portal, in the right pane, click **Downloads**.

- **Unique third-party SSL certificate.** When installing and configuring Active Directory Federation Services Federation and Proxy Servers you will need to provide a unique third-party certificate in the installation process (common name for your AD FS instance). Although it is possible to use a certificate that you currently own, or use a certificate that is not provided by a third party (such as Go Daddy), it is discouraged. A third-party certificate is required if your organization:
  - Allows for remote workers to access the service without a VPN.
  - Deploys ActiveSync devices to users.
  - Utilizes Outlook running on Windows XP or Windows Vista.
  - Allows for IMAP clients.
  - Allows for POP clients.

- **Windows PowerShell 2.0.** In order to run the commands to set up single sign-on, you first enable Windows PowerShell 2.0 feature, and you must have administrator privileges on the AD FS 2.0 server. You then install the Microsoft Online Services Module for Windows PowerShell. We recommend that you use remote access to the AD FS 2.0 server when you run the tool’s PowerShell commands. Remove access is available via a Windows PowerShell remote session.

After you have deployed your AD FS 2.0 production environment on-premises, you will need to establish a relying party trust relationship between the AD FS 2.0 federation server farm and Office 365. This relying party trust acts as a secure channel where authentication tokens can safely pass between your organization and Office 365 in order to facilitate single sign-on access to Office 365. Figure 6 illustrates how local Active Directory users can obtain the necessary
authentication tokens from on-premises AD FS 2.0 federation servers that can redirect the users’ requests through the relying party trust to allow them single sign-on access to Office 365 service offerings.

![Diagram](image)

**Figure 6**

### 3.7.4.4 Virtualization

AD FS 2.0 supports software virtualization of both the federation server and federation server proxy roles. To account for redundancy, we recommend that you store each AD FS virtual machine on separate physical virtual servers.

For more information about setting up a virtual server environment using Microsoft virtualization technology, see the [Step-by-Step Guide to Getting Started with Hyper-V](#).

### 3.7.4.5 Capacity Planning

Table 7 describes the recommended hardware configuration for Active Directory Federation Services based on the number of users in your organization.

**Table 7. AD FS Hardware Configuration Based on User Numbers**

<table>
<thead>
<tr>
<th>Number of users</th>
<th>Suggested hardware configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer than 1,000 users</td>
<td>• No dedicated federation server proxies&lt;br&gt; 1 dedicated NLB server</td>
</tr>
<tr>
<td>1,000 to 15,000 users</td>
<td>• 2 dedicated federation server proxies</td>
</tr>
<tr>
<td>15,000 to 60,000 users</td>
<td>• At least 2 dedicated federation server proxies</td>
</tr>
</tbody>
</table>

**Note:** If you deploy additional AD FS 2.0 servers in the future, you will not need to run the Microsoft Online Services Identity Federation Management tool again.
For more information about capacity planning, see AD FS 2.0 Capacity Planning.

3.7.4.6 Single Sign-on Infrastructure Design

Whether your organization plans on a single server deployment of Active Directory Federation Services or an Active Directory Federations Services farm, it is suggested you install your AD FS instance in farm mode. This will allow your organization the flexibility it may need if you decide to deploy multiple AD FS federation servers in the future. When deploying AD FS in a farm, the first federation server acts as the primary authentication liaison. Any additional federation servers are deployed in “read-only” mode.

Note: Up to five (5) AD FS federation servers are allowed in a farm.

Optimally, your organization should deploy at least two (2) AD FS federation servers and two (2) AD FS proxy servers at the physical location or data center nearest to the majority of your end users. You deploy the AD FS federation servers inside your on-premises data center. The AD FS proxy servers will need to be deployed in your edge/DMZ network. Communication between the federation servers and proxy servers is over port 443. It is suggested that your organization deploy a hardware-based load balancer in front of your AD FS proxy servers to balance traffic for authentication requests.

Note: Externally-facing AD FS proxy servers are required if your organization will use Outlook clients. Proxy servers are also required if you have users that will access Office 365 for enterprises services from home or public locations without setting up a VPN, or from devices such as mobile phones.

3.7.4.7 Performance

When two or more federation servers are configured in a farm using NLB technology or a third-party hardware load balancer, they can operate independently to help process the load of incoming user requests made to the AD FS 2.0 Federation Service without degrading the overall performance of the service. Therefore, there is little overhead involved with adding additional federation servers to your existing production environment after you have deployed your initial federation servers strategically in your network.

3.7.4.8 Namespace Considerations and Acceptable Domains

Active Directory Federation Services only allows for one namespace per farm/instance (for example, contoso.com). Therefore if your organization maintains multiple unique namespaces (for example, contoso.com and fabrikam.com) you would need two AD FS farms deployed in order to provide authentication for each namespace.
**Note:** If your organization owns and manages a primary domain with subdomains (contoso.com/corp.contoso.com) you will NOT require a separate AD FS farm.

Only routable domains can be used with an AD FS deployment. Examples of non-routable domains:

- .local
- .loc
- .internal

The domain extensions that use internal namespaces such as .local, .internal, and .int are not routable on the Internet and would not be acceptable domains for your AD FS deployment. If your organization implements Active Directory with an internal namespace only, you will need to add a UPN suffix in Active Directory Forests and Trusts that is routable (for example, contoso.com) as well as configure each user with that UserPrincipalName suffix. For example, johnsmith@contoso.internal would need to be modified to johnsmith@contoso.com.

**Important:** Before making any changes to your users’ userPrincipalNames attribute it is critical that you validate that there are no applications that are dependent on the existing userPrincipalName value such as smart cards, certificates, Unix, or Linux.

### 3.7.4.9 Deploying Federated and Standard Identities Together

When enabling single sign-on, you cannot mix or match users within a single namespace (contoso.com) in the manner that some users utilize single sign on while others do not. For instance, if you register the domain name contoso.com, all sub domains (for example, northamerica.contoso.com) are automatically configured as identity federated domains.

**Note:** If your organization would like to deploy a hybrid of federated and standard identities, you must configure two separate namespaces to achieve this goal. For example, contoso.com might be used for federated identities and fabrikam.com used for standard identities.

### 3.7.4.10 Microsoft Online Services Module for Windows PowerShell

The Microsoft Online Services Module for Windows PowerShell is a simple PowerShell-based application that enables single sign-on for your organization. The tool provides the following functionality:

- Adds new federated domains.
- Converts standard domain (with Microsoft Online Services user ID) to a federated domain (with single sign-on ID).
• Converts a federated domain to a standard domain.
• Manages and updates federated domain(s) including the ability to change and view federation properties and remove a federation configuration.

3.7.4.11  Server Monitoring

Monitoring your Active Directory Federation Services federation server(s) and proxy server(s) is critical in ensuring high availability of the Office 365 service offerings. If your Active Directory Federation Servers are unavailable, single sign-on users who attempt to utilize any Office 365 service offerings will be unable to authenticate and thus unable to use any of the messaging or collaboration tools.

It is highly suggested you implement Microsoft System Center Operations Manager or another third-party monitoring tool that will not only monitor the uptime of your servers and automatically restart services if they have stopped, but also attempt synthetic logons to your Active Directory federation servers. The tool you select should also include the ability to email, text, or phone people within your organization.

Microsoft provides monitoring management packs for Active Directory Federation Services. For example, you can download the Active Directory Federation Services 2.0 (ADFS) Monitoring Management Pack.

3.7.4.12  Backup and Restore

To guard against the impacts of a complete outage of your Active Directory federation servers, it is highly recommended that you have a backup and restore plan in place to allow for rapid recovery of your AD FS environment. In a catastrophic event where your servers cannot be restored, your backup and restore plan can enable you to reinstall your AD FS environment and re-enable single sign-on by following the steps provided in the Prepare phase of this document.

**Note:** You will need to run the Update-MSOLFederatedDomain PowerShell commandlet in the Microsoft Online Services Module for Windows PowerShell to restore your AD FS configuration.

3.7.4.13  Certificate Management and URLs

Because single sign-on requires SSL certificate(s), it is important that your organization devises a plan identifying who will be responsible for creating and managing your certificates. You will want to attain a certificate with an expiration that is appropriate for your organization, while also taking into consideration that each time your certificate expires you must update single sign-on with a new certificate.
Likewise, if your organization requires changing your single sign-on URL in the future it is important that you plan accordingly. You will need to update your single sign-on configuration settings with the Microsoft Online Services Module for Windows PowerShell, which you install when deploying the single sign-on service. To learn more about updating your single sign-on configuration, see the Help topic Verify and manage single sign-on.

### 3.7.4.14 Extended Protection for Authentication

If your organization’s computers are configured for the [Extended Protection for Authentication](https://docs.microsoft.com/en-us/identity/federationServices/adfs/default-configuration#adfs20-server-config) feature, and you use the Firefox, Google Chrome, or Safari browsers, your users may have difficulty signing in to Office 365 using Integrated Windows Authentication (IWA) from within the corporate network. Your users might receive repeated logon prompts in this condition exists. This is due to the default configuration (on Windows 7 and patched client operating systems) for AD FS 2.0 and Extended Protection for Authentication.

Until Firefox, Google Chrome, and Safari support Extended Protection for Authentication, the recommended option is for all clients accessing Office 365 service offerings to install and use Internet Explorer 9. If you want to use single sign-on for Office 365 with Firefox, Google Chrome, or Safari, there are two other solutions to consider. However, there may be security concerns in taking either of these approaches.

For more information, see [Microsoft Security Advisory: Extended protection for authentication](https://docs.microsoft.com/en-us/security/advisories/important) article. The solutions include:

- Uninstall the Extended Protection for Authentication patches from your computers.
- Change the Extended Protection for Authentication setting on the AD FS 2.0 server by reconfiguring the authentication settings for the web page on each federation server from Windows Integrated Authentication to forms-based authentication.

### 3.7.5 Directory Synchronization Tool

Directory synchronization is the synchronization of directory objects (users, groups, contacts) from your on-premises Active Directory environment to the Office 365 directory infrastructure. The Microsoft Online Services Directory Synchronization Tool is used to perform this synchronization. You install the tool on a dedicated computer in your on-premises environment.

Before you use the Directory Synchronization Tool, you must first edit objects you want to synchronize (user accounts and email enabled contacts and groups) using Active Directory Users and Computers MMC snap-in or via scripting.
Directory synchronization is required if you want to configure an Exchange hybrid deployment with Exchange Online. A hybrid Exchange deployment requires the use of the Directory Synchronization Tool to provide on-going synchronization of user accounts, mail-enabled contacts, and mail-enabled groups from your on-premises Active Directory to Office 365.

Directory synchronization is also required to establish single sign-on.

**Note:** When directory synchronization is enabled, identities are authoritative, managed, and mastered only on-premises.

### 3.7.5.1 About the Directory Synchronization Tool

When you first run the Directory Synchronization Tool, it writes a copy of each user account and all mail-enabled contacts and groups to the directory created for your organization in Office 365. Directory synchronization can also provide Global Address List synchronization between the on-premises Exchange Server environment and Exchange Online.

When user accounts are synchronized with the Office 365 directory for the first time, they are marked as non-activated. They cannot send or receive email and they do not consume subscription licenses. When you are ready to assign Office 365 subscriptions to specific users, you must select and activate these users by assigning a valid license.

The Directory Synchronization Tool enables the following features and functionality:

- Single sign-on.
- Lync Online coexistence.
- Exchange hybrid deployment including:
  - Fully shared global address list (GAL) between your on-premises Exchange environment and Exchange Online.
  - The ability to onboard and offboard users to and from Office 365 service offerings, which requires two-way sync (write-back) enabled in Active Directory synchronization and an Exchange hybrid server deployment on-premises.
  - The ability to move some user mailboxes to Office 365 while retaining other user mailboxes on-premises.
  - Safe senders and blocked senders on-premises are replicated and respected in Exchange Online
  - Delegation/Send on behalf of (limited)
- Synchronization of photos and thumbnails, conference rooms, security groups (rights in SharePoint Online)
Note: By design, Directory Synchronization filtering and scoping is not supported in order to prevent your organization from unintended mass deletion of accounts or attribute changes in the Office 365 service.

To learn more about the Directory Synchronization Tool, see the Help topic [Install the Microsoft Online Services Directory Synchronization tool](#).

### 3.7.5.1.1 Required Permissions for Installation

In order to install the directory synchronization tool you will need Enterprise Admin rights only during the installation process. Post-installation a non-privileged Active Directory account will be required. This account is created automatically at the time of Directory Synchronization installation.

### 3.7.5.2 Number of Objects to Synchronize

The Microsoft Online Services Directory Synchronization Tool enables you to perform directory synchronization between your on-premises Active Directory service and Microsoft Online Services. Before deploying the Directory Synchronization Tool, you need to determine how many objects in your environment will be included in synchronization with your Office 365 directory.

Note: If your Active Directory service contains more than 10,000 objects, you will need to contact the Office 365 support team, open a service request, and indicate the number of objects you need to synchronize.

The initial synchronization copies user accounts, mail-enabled contacts and groups from your on-premise Active Directory environment to Office 365. Depending on the number of objects and the available network bandwidth, you may want to schedule this first synchronization for a period of low network activity. Subsequent synchronizations copy only the incremental changes to the individual objects that have a minimal impact on network utilization.

### 3.7.5.3 Capacity Planning

The Directory Synchronization Tool setup also installs Microsoft SQL Server Express Edition by default. The Express Edition of SQL Server has a maximum file size limitation of 10 GB, sufficient for about 50,000 objects based on the data populated for on-premises Active Directory attributes.

For organizations with more than 50,000 objects to synchronize, a full version of Microsoft SQL Server 2008 is required. For more information about capacity planning, see the Office 365 Community post [Suggested hardware for the directory synchronization tool](#).
Note: The Express Edition of SQL Server is supported for Office 365 but it is recommended that your organization install the full version of SQL Server.

3.7.5.4 Two-Way Synchronization (Write-back)

Two-way synchronization (write-back) is required if your organization would like to take advantage of Office 365 features and functionality such as cloud-based archiving, configuring safe and blocked senders, and cloud voicemail. Write-back is necessary to facilitate the copying of necessary attributes to and from the Office 365 directory infrastructure and your on-premises Active Directory environment.

Table 8 shows the features enabled by two-way directory synchronization and the write-back attribute necessary to enable that feature.

**Table 8. Features Enabled by Two-Way Synchronization**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Write Back To Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filtering coexistence</td>
<td>Writes-back on-premises filtering and online safe/blocked sender data from clients.</td>
<td>SafeSendersHash, BlockedSendersHash, SafeRecipientsHash</td>
</tr>
<tr>
<td>Online archive</td>
<td>Allows your organization to archive mail in Office 365.</td>
<td>msExchArchiveStatus</td>
</tr>
<tr>
<td>Mailbox off-boarding</td>
<td>Allows your organization to complete an online mailbox move back to your on-premises environment.</td>
<td>ProxyAddresses (LegacyExchangeDN) (online LegacyDN) as X500</td>
</tr>
<tr>
<td>Enable Unified Messaging online voicemail</td>
<td>This new attribute is only used for UM-Lync integration to indicate to Lync on-premises that the user has voicemail in Office 365.</td>
<td>msExchUCVoiceMailSettings</td>
</tr>
<tr>
<td>Delegates</td>
<td>Users who manage other users’ mailboxes.</td>
<td>PublicDelegates</td>
</tr>
</tbody>
</table>

If your organization has reservations about configuring two-way synchronization, consider creating a non-privileged service account in your Active Directory service that only has rights to update the attributes defined in the Directory Synchronization Tool for the specific users that will use the service features.

3.8 Exchange Online Planning

This section of the deployment guide describes the tasks and processes associated with moving from your existing messaging system to Exchange Online. It assumes that you have
implemented the Active Directory service on-premises and have created and maintain mail-enabled user accounts.

The timeframe required to deploy Exchange Online will depend on the complexity of your existing on-premises environment. For larger companies, deployment projects can typically be completed in 8 to 12 weeks. This timeframe may be extended by service request escalations and if larger average mailboxes sizes exist in a customer’s mail environment. Customer network bandwidth can also affect this timeframe.

The Exchange Online deployment tasks are focused on two activities:

- Email coexistence
- Email migration

Each of these activities is described briefly in the sections that follow. See the Prepare section for Exchange online for more in-depth information on these key deployment tasks.

3.8.1 Email Coexistence

Email coexistence is a key feature available in the Office 365 for enterprises solution. For organizations with on-premises Exchange Server email environments, email coexistence allows administrators to establish a connection between their on-premises mail environment and the Office 365 mail environment. With coexistence configured, some users connect to Exchange Online while others continue to use the local Exchange Server environment, and all of the users can share the same email domain name.

You can set up two types of coexistence with Office 365 for enterprises:

- **Hybrid deployment.** A hybrid deployment is enabled by deploying Exchange Online together with Exchange 2010, Exchange 2007 or Exchange 2003 in the on-premises organization. A hybrid deployment also relies on deploying an Exchange 2010 hybrid server and on deploying identity federation and directory synchronization as the foundation for identity management across the on-premises and Office 365 organizations.

- **Simple coexistence.** Simple coexistence refers to the scenario where identity management is not fully deployed in the on-premises environment. The functionality that is available in the simple coexistence scenario in part depends on the version of Exchange Server you are running on-premises.
Important: The *Office 365 Deployment Guide for Enterprises* is focused on implementation of an Exchange hybrid deployment.

### 3.8.1.1 Exchange Hybrid Deployment

To provide the smoothest migration to the Office 365 environment, or to keep a mix of on-premises mail users and Office 365 mail users for an extended period of time, organizations can configure an Exchange hybrid deployment.

Hybrid mode provides a unified email experience for your Office 365 deployment. It enables users with mailboxes in your on-premises Exchange Server environment and users with Exchange Online mailboxes to find each other in the Global Address List (GAL), and to send, receive, and reply to email regardless of which system is hosting their mailbox.

A hybrid deployment provides these advantages:

- Exchange Online and on-premises users can share free/busy calendar data.
- Administrators can use the Exchange Management Console (EMC) to manage both the Exchange Online and on-premises Exchange mail environments.
- Administrators can use powerful and familiar Exchange management tools to move users to Exchange Online.
- Outlook profiles for users are automatically updated to the Exchange Online environment when the Exchange hybrid deployment and Autodiscover are configured appropriately. Administrators do not need to manually reconfigure Outlook profiles or resynchronize .OST files after moving users’ mailboxes.
- MailTips, out-of-office messages, and similar features understand that Office 365 and on-premises users are part of the same organization.
- Delivery reports and multi-mailbox search work with users who are on-premises and those working in Exchange Online.
- Authentication headers are preserved during cross-premises mail flow, so all mail looks and feels like it is internal to the company (for example, recipient names resolve in the Global Address List).
- If necessary, administrators can easily move mailboxes back to the on-premises Exchange environment.

Table 9 highlights the capabilities of an Exchange hybrid deployment compared to simple coexistence.
### Table 9. Exchange Online Simple Coexistence and Hybrid Deployment Capabilities

<table>
<thead>
<tr>
<th>Feature</th>
<th>Simple</th>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail routing between on-premises and online</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unified GAL</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Free/Busy and calendar sharing cross-premises</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Out of Office understands that cross-premises is “internal”</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Mail-tips, messaging tracking, and mailbox search cross-premises</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Outlook Web App redirection cross-premise (single Outlook Web App URL)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Can route outbound mail through on-premises (allows address rewrite, transport agents)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Secure mail routing (TLS plus Mutual Authentication) cross-premises</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Exchange Management Console (on-premises) used to manage cross-premises mailbox migrations</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Mailbox moves support for on boarding and off-boarding</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>No OST re-sync after mailbox migration</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

#### 3.8.1.2 Hybrid Deployment Considerations

You should consider the following before implementing an Exchange hybrid deployment:

- **Delegation coexistence.** Delegate permissions (such as Delegate Access, folder permissions and “Send on behalf of”) are migrated but not available after a mailbox move unless all parties are migrated at the same time. For example, if an executive in your organization is migrated to Exchange Online then his or her administrative assistant will need to be migrated at the same time in order to maintain delegate access.

- **Mailbox permissions.** On-premises mailbox permissions such as Send As, Receive As and Full Access that are explicitly applied on the mailbox are migrated. However, inherited (non-explicit) mailbox permissions as well as any permissions on non-mailbox objects—such as distribution lists or a mail-enabled user—are not migrated. Therefore, you will need to plan for configuring these permissions in Exchange Online if applicable for your organization. For example, you can use the Add-RecipientPermission and Add-MailboxPermission Windows PowerShell cmdlets to set the permissions in Office 365.

- **Cross-premises permissions.** It is important to note that we do not support cross-premises permission scenarios. Permissions are only migrated and functional when implementing an Exchange hybrid deployment if there are corresponding directory objects in Exchange Online. Additionally, all objects with special permissions such as Send As, Receive As and Full Access must be migrated at the same time. This also means
that to migrate these permissions you must ensure directory synchronization has
completed before you start moving mailboxes.

- **Offboarding.** As part of ongoing recipient management, you may have a need to move
  mailboxes back to your on-premises environment. For more information, see the
  Community Help topic Exchange Hybrid Deployment – Moving Cloud-Based Mailboxes
to the On-Premises Organization.

- **Decommissioning on-premises Exchange.** Some organizations may wish to completely
  remove their on-premises Exchange environment after all mailboxes are migrated. The
  steps to decommission on-premises Exchange should be planned carefully with the help
  of an Office 365 deployment specialist. Please contact Office 365 support for more
  information.

- **Multi-forest Active Directory environments.** If your organization implements multiple
  forests for logon or resource segmentation, Exchange hybrid deployment is not
  supported.

In addition, before you configure an Exchange hybrid deployment, your system and servers must
meet specific deployment requirements. If they do not meet these requirements, you will not be
able to configure your on-premises Exchange organization for coexistence with Exchange
Online. The Exchange Deployment Assistant outlines the hybrid deployment requirements for
the on-premises Exchange environment.

### 3.8.1.3 Hybrid Deployment Requirements

There are three key requirements for configuring an Exchange hybrid deployment with your on-
premises Exchange environment.

- **Hybrid server.** You must install a hybrid server running Exchange 2010 Service Pack 1 in
  your on-premises Exchange environment and configure Exchange coexistence between
  the on-premises Exchange environment and Exchange Online. This hybrid server acts as
  a bridge between the on-premises Exchange environment and Exchange Online.
  Organizations do not need to upgrade mailboxes to Exchange 2010 prior to moving
  them to Exchange Online. The Exchange 2010 Client Access server role on the hybrid
  server acts as a proxy between older Exchange environments and Exchange Online without
  the need to migrate on-premises Exchange mailboxes to Exchange 2010.

- **Directory Synchronization Tool.** A hybrid Exchange deployment requires the Directory
  Synchronization (DirSync) tool to be running in the local environment. DirSync write-
  back is recommended to enable smooth offboarding of users. For more details, see the
  Directory Synchronization Tool section of this document.

- **Microsoft Federation Gateway.** The Microsoft Federation Gateway is free online service
  offered by Microsoft that acts as the trust broker between your on-premises Exchange
  organization and your Exchange Online service. Organizations implementing a hybrid
Exchange deployment must create a federation trust with the Microsoft Federation Gateway.

### 3.8.1.4 Hybrid Server Requirements

Table 10 provides a detailed list of the hybrid server requirements.

**Table 10. Hybrid Server Requirements**

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating system</strong></td>
<td>• 64-bit edition of Windows Server 2008 Standard Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>• 64-bit edition of Windows Server 2008 Enterprise Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>• 64-bit edition of Windows Server 2008 Standard R2</td>
</tr>
<tr>
<td></td>
<td>• 64-bit edition of Windows Server 2008 Enterprise R2</td>
</tr>
<tr>
<td><strong>Exchange Server</strong></td>
<td>• On-premises Exchange organization: Exchange Server 2003 and later</td>
</tr>
<tr>
<td></td>
<td>• Hybrid server: Exchange Server 2010 SP1</td>
</tr>
<tr>
<td><strong>System software</strong></td>
<td>• Microsoft .NET Framework 3.5 SP1</td>
</tr>
<tr>
<td></td>
<td>• Internet Information Services (IIS)</td>
</tr>
<tr>
<td></td>
<td>• Windows Management Framework Core Package</td>
</tr>
<tr>
<td></td>
<td>• Windows Remote Management V2.0</td>
</tr>
<tr>
<td></td>
<td>• Windows6.1-KB979099-x64</td>
</tr>
<tr>
<td></td>
<td>• Windows6.1-KB979744-x64</td>
</tr>
<tr>
<td></td>
<td>• Windows6.1-KB982867-v2-x64</td>
</tr>
<tr>
<td></td>
<td>• Windows6.1-KB983440-x64</td>
</tr>
<tr>
<td></td>
<td>• Windows6.1-KB977020-v2-x64</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Filter Pack 2.0</td>
</tr>
<tr>
<td><strong>Certificates</strong></td>
<td>• Self-signed SSL certificate for federation trust</td>
</tr>
<tr>
<td></td>
<td>• Certificate Authority (CA) SSL certificate for Exchange Server 2010 SP1</td>
</tr>
<tr>
<td><strong>Autodiscover</strong></td>
<td>• Deployed on-premises and Exchange Online</td>
</tr>
<tr>
<td><strong>Active Directory</strong></td>
<td>• Schema update</td>
</tr>
<tr>
<td><strong>DNS Records</strong></td>
<td>• TXT records for proof of domain ownership with Microsoft Federation Gateway</td>
</tr>
</tbody>
</table>

### 3.8.1.5 Example Scenario: Configuring Exchange Hybrid Deployment

Figure 7 shows a typical topology for mail access in an environment where email coexistence has not been established. The customer, Contoso, Ltd., has a single forest, single domain organization with two domain controllers and one Exchange Server 2003 mail server. Contoso’s Outlook Web App users connect to Exchange 2003 over the Internet to check their mailboxes and access their Outlook calendar.
With this scenario in place, Contoso decides to configure an Exchange hybrid deployment using the Exchange Server Deployment Assistant. The Contoso administrator completes the coexistence checklist presented in the Deployment Assistant. Using the information that is generated by the Deployment Assistant, the administrator begins to work through the coexistence deployment checklist that’s tailored to Contoso. After implementing the checklist, Contoso has the coexistence configuration shown in Figure 8.

If you compare Contoso’s existing organization configuration (Figure 8) and the hybrid configuration (Figure 9), you will see that the hybrid deployment has added servers and services that support additional communication and features that are shared between the on-premises
and Office 365 organizations.

The following is an overview of the changes that a hybrid deployment has made from the initial on-premises Exchange organization.

- Users will use their existing network account credentials for logging on to the on-premises and Office 365 organizations. See the User Identity and Account Provisioning section of this document for more information.
- User mailboxes located on-premises and in the Exchange Online environment will use the same email address domain. For example, mailboxes located on-premises and mailboxes located in the Office 365 organization will both use @contoso.com in user email addresses.
- All mail is delivered to the Internet by the on-premises Exchange organization. The on-premises Exchange organization controls all messaging transport and serves as a relay for the Exchange Online service.
- On-premises and Exchange Online users can share calendar free/busy information with each other. Organization relationships configured for both organizations also enable cross-premises message tracking, MailTips, and message search.
- On-premises and Exchange Online users use the same URL to connect to their mailboxes over the Internet.

Table 11 summarizes the coexistence configuration changes.

**Table 11. Hybrid Deployment Configuration Changes**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Before hybrid deployment</th>
<th>After hybrid deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid server</td>
<td>Not applicable; single organization only.</td>
<td>Installed in the on-premises organization to deploy coexistence.</td>
</tr>
<tr>
<td>Mailbox location</td>
<td>Mailboxes on-premises only.</td>
<td>Mailboxes on-premises and with Office 365.</td>
</tr>
<tr>
<td>Message transport</td>
<td>On-premises mailbox server handles all inbound and outbound message routing.</td>
<td>On-premises hybrid server handles message inbound and outbound message routing for both the on-premises and Office 365 organization.</td>
</tr>
<tr>
<td>Outlook Web App</td>
<td>On-premises mailbox server receives all Outlook Web App requests and displays mailbox information.</td>
<td>On-premises hybrid server handles message inbound and outbound message routing for both the on-premises and Office 365 organization.</td>
</tr>
<tr>
<td>Unified GAL for both organizations</td>
<td>Not applicable; single organization only.</td>
<td>On-premises DirSync server replicates Active Directory information for mail-enabled objects to the Office 365 organization.</td>
</tr>
</tbody>
</table>
### Configuration

<table>
<thead>
<tr>
<th>Before hybrid deployment</th>
<th>After hybrid deployment</th>
</tr>
</thead>
</table>
| **Single-sign on used for both organizations** | Not applicable; single organization only. | On-premises Active Directory Federation Services (AD FS) server supports using single-sign on credentials for mailboxes located either on-premises or in the Office 365 organization. |}
| **Organization relationship established and a federation trust with Microsoft Federation Gateway** | Not applicable, single organization only. | Free/busy sharing between both on-premises and Office 365 users. |

---

### 3.8.1.6 Exchange Server Deployment Assistant

It is strongly recommended that you use the Microsoft [Exchange Server Deployment Assistant](#) wizard to assist your organization in configuring a hybrid deployment of Exchange Online. Shown in Figure 9, the Deployment Assistant is an online tool available from TechNet.

---

**Figure 9**

The Deployment Assistant is especially useful as it generates detailed configuration instructions for organizations deploying email coexistence scenarios. Customers submit specific information about their on-premise Exchange Server organization and the Deployment Assistant produces a customized checklist with configuration details.
3.8.2 Email Migration

Email migration is the process of moving your existing mailbox content to Office 365 and Exchange Online. Migration can occur as quickly or as slowly as your organization wants. Small organizations may be able to migrate mailbox content to Exchange Online overnight or over a weekend. Larger or more complex organizations typically prefer to establish email and directory coexistence for a longer period of time and perform a controlled migration in logical stages. The ultimate goal of the migration process is to have a unified migration experience for end users with minimal impact to their daily routines.

Office 365 for enterprises supports five types of mailbox migrations:

- Exchange Server mailbox migrations
- Hosted Exchange mailbox migrations
- IMAP4 mailbox migrations
- Lotus Notes mailbox migrations
- Novell GroupWise mailbox migrations

Each type of mailbox migration is briefly discussed below.

3.8.2.1 Exchange Server Migrations

If your organization is using Exchange Server 2010, Exchange Server 2007, Exchange Server 2003, or Hosted Exchange, you have several ways to migrate mailbox data. Table 12 describes them. The Microsoft Office 365 Deployment Guide for Enterprises is primarily focused on mailbox migrations for Exchange hybrid deployments.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Tools/Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Simple Exchange Migration</strong></td>
<td>Intended for small organizations that desire a quick cutover, with no coexistence, from their existing Exchange mail environment to Exchange Online. All on-premises mailboxes are migrated in preparation for moving your entire email organization to Exchange Online. You can migrate a maximum of 1,000 mailboxes from your on-premises Exchange organization to Exchange Online. User identities are automatically provisioned by the tool. After cutover, identity federation may be deployed.</td>
<td>Email Migration tool via the Exchange Control Panel. For step-by-step instructions, see Migrate All Exchange Mailboxes to the Cloud.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
<td>Tools/Methods</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Staged Exchange Migration</strong></td>
<td>Intended for organizations that desire a shorter period of coexistence from their existing Exchange mail environment to Exchange Online. User identities will automatically be provisioned by the Directory Synchronization Tool. After all users are migrated to Exchange Online, identity federation may be deployed. This type of migration allows you to maintain coexistence between your on-premises and Office 365 email organizations. In this scenario, you can move some mailboxes to Exchange Online while maintaining the rest of the mailboxes in your on-premises mail environment.</td>
<td>Email Migration tool via the Exchange Control Panel and a CSV file; Directory Synchronization Tool (DirSync) to keep your on-premises Active Directory synchronized with Office 365 and Exchange Online. For step-by-step instructions, see <a href="#">Migrate a Subset of Exchange Mailboxes to the Cloud with a Staged Migration</a>. <strong>Note:</strong> On-premises Exchange decommissioning after a staged migration should be planned carefully with the help of an Office 365 deployment specialist. Please contact Office 365 support for more information.</td>
</tr>
</tbody>
</table>

| **Hybrid Deployment Migration** | This type of migration enables on-premises users can see calendar or free/busy information for Exchange Online users. You must add a hybrid server to your on-premises Exchange environment. | Install and configure Exchange Server 2010 SP1. Directory Synchronization Tool (DirSync) to keep your on-premises Active Directory synchronized with Office 365 and Exchange Online. For step-by-step instructions, use the [Exchange Server Deployment Assistant](#). |

---

**Note:** The migration velocity, especially if any third-party tools are involved, may be impacted by the Exchange Web Services (EWS) limits for Exchange Online. For more information, see the blog entry [Exchange Online Throttling and Limits FAQ](#).
3.8.2.1.1 Hybrid Reverse Proxy Configuration

The Exchange Mailbox Replication Proxy (MRSPProxy) service may not work properly if a reverse proxy, such as Microsoft ISA Server or Microsoft Forefront Threat Management Gateway(TMG), is publishing Exchange services in the perimeter network and requires pre-authentication. You should perform the following steps if this is your scenario:

1. Create an additional ISA/TMG rule that uses the same listener as the original Exchange 2010 rule that already allows pre-authenticated traffic to the internal Exchange server(s).
2. Configure the new rule as follows:
   - Authentication Delegation: No delegation, but client may authenticate directly.
   - Users: All Users
   - Paths:
     - /ews/mrsproxy.svc
     - /ews/exchange.asmx/wssecurity
     - /autodiscover/autodiscover.svc/wssecurity
     - /autodiscover/autodiscover.svc
   - Rule Priority: This rule must be set to a higher priority than the other Exchange publishing rules.

3.8.2.2 IMAP Migration

An IMAP migration is used by small organizations that desire a quick cutover, with no coexistence, to Exchange Online services from their existing mail environment by leveraging the IMAP protocol. User identities are automatically provisioned with the IMAP migration tool within the Exchange Control Panel. Note that you will need to create Exchange Online mailboxes before beginning this process. See the Help topic Migrate E-Mail from an IMAP Server to Cloud-based Mailboxes for more information. After cutover, identity federation may be deployed.

You can use the Email Migration tool in the Exchange Control Panel and a CSV file to migrate the contents of users’ mailboxes from an IMAP messaging system to their Exchange Online mailbox. Supported IMAP servers include the following:

- Courier-IMAP
- Cyrus
- Dovecot
- UW-IMAP
- Exchange 2010
- Exchange 2007
- Exchange 2003
During the migration, to avoid overusing the remote server’s resources and bandwidth, Exchange Online creates fewer than 10 connections to the IMAP server.

3.8.2.3 Lotus Notes and Novell GroupWise Migrations

If your organization is migrating to Exchange Online from a non-Microsoft platform such as Lotus Notes and Novell GroupWise, you may want to evaluate migration solutions offered by consulting services and third party software providers.

The Recommended Deployment Partners area of the Microsoft Online Services deployment site can help you find technology consultants and partners with expertise in Office 365 migration services and solutions.

3.8.2.4 Reducing Mailbox Size

The size of a mailbox, along with available bandwidth to the Internet, is a limiting factor in achieving a high migration velocity.

A common practice to reduce the size of the mailbox is to move mail items out of the mailbox to an archive (for example, a .PST file) either manually or with auto archive functionality. This practice is discouraged because when the user moves the mail items back to the new Exchange Online mailbox after migration, the Exchange Online mailbox will not allow the user to reply to the mail.

When attempting to reduce mailbox size, consider doing the following:

- Delete or archive mail in the Sent Items folder
- Delete or archive all Calendar attachments
- Delete or archive Calendar items over 30 days old
- Delete or archive Inbox items over 30 days old
- Search for and delete attachments over 5 MB
- Disable Journaling
- Empty the Deleted Items folder
- Enable AutoArchive via Group Policy
- Run the Mailbox Cleanup wizard from the Outlook Tools menu (Outlook only)

**Note:** The number of days and file sizes are recommendations only. They may not be suitable for your organization.

3.8.2.4.1 Mailbox Assessments

Your organization will need to assess the number of mailboxes, mailbox size, and the rate of mailbox size growth in your existing environment. This information will help you evaluate the
impact of migration traffic on your network, which must be considered when scheduling migrations.

If your organization enforces maximum mailbox size limits, this information is also important to consider when you define Exchange Online storage capacities. Your new Exchange Online environment should let all users store the same amount of data or more in their Exchange Online mailboxes. It may be necessary for users with extra-large mailboxes to move some of that content from their mailboxes to some form of offline storage, such as a Microsoft Office Outlook .PST file to facilitate timely mailbox migrations.

In addition, when evaluating your existing mailbox inventory be aware that your organization receives 25 GB of mailbox space for each Exchange Online (Plan 1) and Exchange Online (Plan 2) user license purchased. Each Exchange Online Kiosk user receives 500 MB of mailbox storage. Administrators can use Remote PowerShell to reduce maximum mailbox sizes for some or all of their users.

3.8.3 Certificates

Secure Sockets Layer (SSL) digital certificates play a significant role in deploying email coexistence. They help to secure communications between the on-premises hybrid server and your Office 365 organization. If you are already using digital certificates in your Exchange organization, you may have to modify the certificates to include additional domains or purchase additional certificates from a trusted certificate authority (CA). If you aren’t already using certificates, you will need to purchase one or more certificates from a trusted CA. Certificates are needed early in the hybrid deployment checklist and are a requirement to configure several types of services.

For more information, see the TechNet article Understanding Certificate Requirements.

3.8.4 Bandwidth

As discussed earlier, your network connection to the Internet will directly impact the communication performance between your on-premises organization and your Office 365 organization. This is particularly true when moving mailboxes from your on-premises Exchange 2003 server or later to Exchange Online. The amount of available network bandwidth, in combination with mailbox size and the number of mailboxes moved in parallel, will result in varied times to complete mailbox moves. Additionally, other Office 365 service offerings, such as SharePoint Online and Lync Online, may also impact the available bandwidth for messaging services.

Before moving mailboxes to Exchange Online, you should:
• Determine the average mailbox size for mailboxes that will be moved to your Office 365 organization.
• Determine the average connection and throughput speed to the Internet from your on-premises organization.
• Calculate the average expected transfer speed, and plan your mailbox moves accordingly.

For more information, see the TechNet article Company Network Requirements.

3.8.5 Public Folders

Public folders are not supported in Office 365 and Exchange Online mailboxes won't have access to public folders located in the on-premises Exchange organization. Existing on-premises public folder configuration and access for on-premises mailboxes will not be changed in a hybrid deployment.

To learn about strategies for transitioning away from public folders as part of a migration to Exchange Online and Office 365, see the Migrate from Exchange Public Folders to BPOS whitepaper.

3.8.6 Email Client Software

You should have a clear picture of email client applications used in your current environment. For most deployments, the following clients are suggested:

• Microsoft Outlook 2010
• Microsoft Office Outlook 2007 with SP2
• Outlook Web App
• Microsoft Outlook for Mac 2011
• Microsoft Entourage 2008 Web Services Edition

**Note:** Outlook for Mac 2011 and Entourage 2008 use Exchange Web Services to communicate with Exchange Server.

If end users are not familiar with these client applications, training may be required.

For additional information, see the following Help topics:

• Supported E-Mail Programs and Features
• Access Your Account Using IMAP or POP E-Mail Programs
• License requirements for Personal Archive and retention policies

The Client and End-User Experience section of this document also has more information.
3.8.7 Mobile Devices

Mobile devices are supported in a coexistence deployment. The Microsoft Exchange ActiveSync® protocol is enabled by default on the coexistence server and will automatically redirect requests from mobile devices to mailboxes located in Exchange Online or the on-premises mailbox server. All mobile devices that support Exchange ActiveSync should be compatible with a coexistence deployment. For more information, see the Help topic Mobile Phones.

Exchange Online includes support for mobile devices—in particular devices that use the Exchange ActiveSync protocol, such as Windows Mobile 6.0 and later devices, Nokia E and N series devices, Android, and iPhone. BlackBerry® device users are also able to access Exchange Online via the BlackBerry Internet Service. The following sections provide additional information about Exchange Online device support.

**Note:** It is your organization's responsibility to procure, deploy, manage, and support mobile client software and compatible devices, and manage relationships with wireless carriers. Microsoft does not provide end-user device support.

3.8.7.1 ActiveSync Devices

Exchange ActiveSync is a Microsoft Exchange Server synchronization protocol that is optimized to work with high-latency and low-bandwidth networks. The protocol, based on HTTP and XML, lets devices such as browser-enabled mobile phones or Windows Mobile-powered devices access organization information on a Microsoft Exchange Server. Exchange ActiveSync enables mobile device users to access their email, calendar, contacts, and tasks and to continue to be able to access this information while they are working offline.

The default mailbox policies for all Exchange ActiveSync devices are provisioned according to the “Default Exchange ActiveSync settings” table found in the TechNet article Understanding Exchange ActiveSync Mailbox Policies.

**Note:** Not all mobile devices support all the Exchange ActiveSync policy settings. If a policy setting is not supported on a particular device, the device may not apply the setting. You can control whether devices that do not support specific policies are allowed to connect in the General settings for the policy. For more information, see the TechNet article Exchange ActiveSync Mobile Phones and Compatible Features.

For more information about Exchange ActiveSync solutions, see Mobility Solutions for Microsoft Online Services.
3.8.7.2 BlackBerry Devices

Users of Research In Motion Limited (RIM®) BlackBerry devices can connect their devices to Exchange Online using the BlackBerry Internet Service (BIS). This service allows BlackBerry users to access their email accounts without connecting through a BlackBerry Enterprise Server (BES). It does not provide the same capabilities as a BES server or a hosted BES service. Exchange Online (Plan 1) and Exchange Online (Plan 2) users can configure BIS to access their mailboxes via IMAP. Exchange Online (Kiosk) users can configure BIS to access their mailboxes via POP.

RIM will introduce a new hosted BES service for Exchange Online customers later this year. RIM will host, license and support the service. See the Office 365 blog Office 365 and BlackBerry for additional details.

For additional information on BlackBerry support, review the Exchange Online Service Description.

3.8.8 Mail-Enabled Applications

Your organization should take inventory of any mail-enabled applications used in your on-premises environment. If you have mail-enabled applications, your organization should determine whether they can be modified to work with Exchange Online using Exchange Web Services (EWS).

Some examples of mail-enabled applications are:

- An application that sends a reorder request via email when inventory levels fall below a certain level.
- A report automatically generated by a line-of-business application that is emailed to an email address or a distribution group.

In some cases, it may be necessary for you to keep your existing email environment on-premises in order to support mail-enabled applications until you can make the necessary modifications. The Exchange Legacy API scanner is an excellent tool to help you analyze mail-enabled applications with legacy APIs in your on-premises environment.

In some scenarios, the Microsoft Forefront® Online Protection for Exchange (FOPE) configuration (white list, block list, and policy filtering) must be managed in order to permit potentially blocked emails generated by mail-enabled applications.

3.8.9 Service Limits

You should be aware of the limitations that apply to Exchange Online messaging services. The Exchange Online Service Description describes limits that apply to the following:
- Email messages
- Mailboxes
- Mailbox size
- Mailbox capacity alerts
- Recipients and senders (to protect against spam, mass mailings and malware)
- Mail item retention
- Distribution groups
- Transport rules
- Moderation settings

**Note:** The migration velocity, especially if any third-party tools are involved, may be impacted by Exchange Web Services (EWS) limits for Exchange Online. For more information, see the blog entry [Exchange Online Throttling and Limits FAQ](#).

### 3.8.9.1 Thresholds for Mail Items in Folders

For certain types of mail items, Office 365 limits the number of items that Exchange Online users can have in mail folders. These limitations are set to mitigate service performance issues.

The following thresholds are applied:

- Inbox folder: 20,000 items
- Sent Items folder: 20,000 items
- Deleted Items folder: 20,000 items
- Calendar: 5,000 items
- Contacts: 5,000 items

If there are users that exceed these thresholds, the Office 365 support team will contact the customer to request that the user reduce the high item counts. For additional information, see the TechNet article [Understanding Performance Impact of High Item Counts and Restricted Views](#).

### 3.8.10 Exchange Online Administration

Your Office 365 administrator has a number of tools available to manage your Exchange Online services. These tools are described in this section.

#### 3.8.10.1 Microsoft Online Services Portal

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

### 3.8.10.2 Exchange Control Panel

The Exchange Control Panel (ECP) allows administrators to configure and manage the Exchange Online environment from a web browser.

Administrators can access the Exchange Control Panel by choosing one of the following options:

- Via the Microsoft Online Services Portal.
- Opening the URL http://www.outlook.com/ecp/\(<\text{customer domain}>\).
- Opening the Outlook Web App Options page and selecting My Organization.

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

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

Administrators can give users access to selected features in the Exchange Control Panel, using the granular Role-Based Access Control User Editor.

### 3.8.10.3 Forefront Online Protection for Exchange Administration Center

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

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

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

Administrators can access the FOPE Administration Center via the Microsoft Online Services Portal.
3.8.10.4  Remote PowerShell

With Windows PowerShell Remote—better known as Remote PowerShell—administrators can connect to Exchange Online to perform management tasks that are not available or practical in the web management interface. For example, they can use Remote PowerShell to automate repetitive tasks, extract data for custom reports, customize policies, and connect Exchange Online to existing infrastructure and processes.

To use Remote PowerShell, administrators’ computers must be running the Windows Management Framework, which contains Windows PowerShell v2 and WinRM 2.0. These components are already installed in computers running Windows 7 or Windows Server 2008 R2. Administrators can manually download these components for computers running other operating systems. Administrators do not need to install any Exchange Server management or migration tools in order to use Remote PowerShell.

Exchange Online uses the same PowerShell cmdlets as Exchange Server 2010 Service Pack 1, with certain commands and parameters disabled because these features do not apply in the data center environment.

For a list of the cmdlets available to Exchange Online administrators, see the Help topic Reference to Available PowerShell Cmdlets.

3.8.10.5  Roles-Based Access Control (RBAC)

Exchange Online uses a role-based access control (RBAC) model that allows administrators to finely control access to Office 365 service offerings. Using RBAC, administrators can delegate tasks to employees in the IT department as well as to non-IT employees. For example, if a compliance officer is responsible for mailbox search requests, the administrator can delegate this administrative feature to the officer.

Exchange Online uses the same flexible RBAC framework as Exchange Server 2010 SP1. Administrators can use the Exchange Control Panel to assign users to built-in roles and role groups. Alternatively, they can use Remote PowerShell to create custom RBAC roles. For example, an administrator can create a custom role to let the help desk team manage mailboxes only for users in a certain subsidiary or geographic region. To learn more about managing administrator roles, see the Help topic Create Exclusive Write Scopes.

The following role groups are available by default in Exchange Online:
- Organization Management
- View-Only Organization Management
- Recipient Management
- Unified Messaging Management
- Help Desk
- Records Management
Discovery Management
For more information, see the Help topic Administrator Role Groups in Exchange Online.

The Office 365 platform has an implementation of RBAC that is separate from Exchange Online RBAC. Users who are Global Administrators in Office 365 are assigned organization administrator permissions by default in Exchange Online; otherwise, the two security models are managed separately. To learn more about configuring RBAC, see the Help topic Role Based Access Control in Exchange Online.

3.8.10.6 Message Tracking
Administrators can use delivery reports to view detailed reporting on email messages within the Exchange Online environment. Using the Exchange Control Panel, they can search for messages and view information such as time and date of delivery, reasons for non-delivery, and policies applied. Users can also view delivery report information for the emails they have sent. See the Help topic Search for Message Delivery Reports for more information.

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

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

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

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

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

- **Administrator audit logging.** Allows customers to track changes made by their administrators in the Exchange Online environment, including changes to RBAC roles or Exchange policies and settings.
- **Mailbox audit logging.** Allows customers to track access to mailboxes by users other than the owners, including access by delegates and access to shared mailboxes.
Several predefined audit reports are available in the Exchange Control Panel, including Administrator Role Changes, Litigation Hold, and Non-Owner Mailbox Access. Administrators can filter reports by date and role, and can export all audit events for specified mailboxes in XML format for long-term retention or custom reporting.

Administrator audit logging is on by default. Mailbox audit logging is off by default. Administrators can use Remote PowerShell to enable mailbox audit logging for some or all mailboxes in their organization as described in the Help topic Use Auditing Reports in Exchange Online.

3.8.10.9 Mail Archiving and Compliance

Exchange Online administrators have the ability to manage mail archiving and compliance features available with the service.

3.8.10.9.1 Disclaimers

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

For more information about adding disclaimers, see the Help topic Add Disclaimers to Messages.

3.8.10.9.2 Transport Rules

Transport rules are used to inspect emails in transit (inbound, outbound, and internal) and take actions such as applying a disclaimer, blocking messages, or sending a blind carbon copy to a mailbox for supervisory review. Transport rules use a set of conditions, actions, and exceptions similar to inbox rules.

Exchange Online supports the transport rule functionality of Exchange Server 2010 SP 1 including the following:

- **Granular transport rule conditions.** Administrators can create transport rules to inspect messages for a variety of email attributes, such as specific senders, recipients, distribution lists, keywords, and regular expressions (for common patterns like those associated with credit card numbers or social security numbers). Administrators can also include users’ Active Directory attributes (for example, department, country, or manager) and distinguish by message types (such as automatic replies, meeting requests, and voicemail messages). See the Office 365 topic Conditions and Exceptions for Transport Rules for more information.
- **Ability to moderate.** Administrators can use transport rules to route email messages to a manager or trusted moderator for review. Reviewers can then approve or block the message and, if blocked, provide an explanation to the sender. See the Help topic Use Transport Rules to Silently Copy Messages to an Auditor for more information.

- **Message classifications.** Administrators can use transport rules to apply metadata to messages, describing the intended use or audience (for example, attorney–client privileges). Users can also apply classifications manually and have transport rules check messages when they enter the transport pipeline. If messages do not meet the conditions of the classification, an action can be applied to modify, protect, or block the messages.

- **Attachment inspection.** Administrators can create transport rules based on content in a Microsoft Office attachment. However, file types such as Adobe PDF files that require installation of third-party IFilters on the email server cannot be inspected in Exchange Online.

Administrators can manage transport rules using the Exchange Control Panel or Remote PowerShell. Using transport rules to copy messages to an Exchange Online mailbox for the purposes of archiving is not permitted.

For more information, see the Help topic Create a New Rule.

### 3.8.10.9.3 Personal Archive

Exchange Online offers archiving through the personal archive capabilities of Exchange 2010. A personal archive is a specialized mailbox that appears alongside users’ primary mailbox folders in Outlook or Outlook Web App. Users can access the archive in the same way they access their primary mailboxes. In addition, users can search both their personal archives and primary mailboxes.

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

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

Outlook 2007 provides basic support for the personal archive, but not all archiving and compliance features are available in Outlook 2007. For example, with Outlook 2007, users cannot apply retention or archive policies to items in their mailboxes. They must rely on administrator-provisioned policies instead. Outlook 2007 users require the Office 2007 Cumulative Update for February 2011 to access the personal archive.
**Note:** The personal archive has specific Outlook licensing requirements, which are described at the [License requirements for Personal Archive and retention policies](#) page.

Administrators can use the Exchange Control Panel or Remote PowerShell to enable the personal archive feature for specific users. Users with Exchange Online mailboxes cannot have personal archives in on-premises Exchange Servers.

See the Help topic [Enable an Archive Mailbox](#) for more details.

**Personal Archive Size**

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

An Exchange Online (Plan 2) user receives 25 gigabytes of storage in the primary mailbox, plus unlimited storage in the personal archive. A quota is set on the personal archive for Exchange Online (Plan 2) users that is large enough to accommodate reasonable use, including the import of one user’s historical email.

**Note:** During the Office 365 365, the default quota for the personal archive is 100 GB for Exchange Online (Plan 2) users.

In the unlikely event that a user reaches these archive quotas, a call to Office 365 support is required. Administrators cannot adjust this quota upward or downward.

**Importing Data to the Personal Archive**

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

- Drag email messages from .PST files into the archive.
- Drag email messages from the primary mailbox into the archive.
- Let retention policies automatically move email messages from the primary mailbox, based on the age of the messages.

**Note:** Administrator-driven import of .PST files using the `new-mailboximportrequest` PowerShell cmdlet introduced in Exchange Server 2010 SP 1 is not available in Exchange Online.

**3.8.10.9.4 Journaling**

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

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

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

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

The retention policy capabilities offered in Exchange Online are the same as those offered in
Exchange Server 2010 Service Pack 1. Administrators can use Remote PowerShell to migrate
retention policies from on-premises Exchange Server 2010 environments to Exchange Online.
Managed Folders, an older approach to messaging records management that was introduced in
Exchange 2007, are not available in Exchange Online. For more information, see the Help topic
Set Up and Manage Retention Policies in Exchange Online.

3.8.10.9.6 Legal Hold
Exchange Online provides legal hold capabilities to preserve users’ deleted and edited mailbox
items (including email messages, appointments, and tasks) from both their primary mailboxes
and personal archives. Administrators can use the Exchange Control Panel or Remote PowerShell
to set legal holds on individual mailboxes or across an organization. This feature also includes an
option that sends an email notification to users or automatically alerts them through Outlook
2010 that a hold has been placed on their mailboxes.
3.8.10.9.7 Multi Mailbox Search/Cross-Premises

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

For legal discovery purposes, you can copy and move email messages located through search to a specified mailbox for further investigation. Administrators can connect Outlook to this mailbox, and export the search results to a .PST file.

**Note:** In Exchange Online, administrators cannot directly export mailbox search results to a .PST file.

For more information, see the Help topic Multi-Mailbox Searches.

3.8.11 Application Interoperability

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

The following conditions apply to hosted applications:

- The application vendor must provide support for the application and perform all related application compatibility testing.
- Custom applications cannot be hosted in a Microsoft data center unless they are hosted on the Windows Azure™ platform.
- Exchange Online does not host custom code or third-party applications including DLL files, custom code packaged in transport agents, or modifications to files on servers in the data center.

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

3.8.11.1 Exchange Web Services

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

### 3.8.11.2 SMTP Relay

Exchange Online can be used as an SMTP delivery service to relay email messages sent from fax gateways, network appliances, and custom applications. For example, if a line-of-business application sends email alerts to users, it can be configured to use Exchange Online as the mail delivery system. The application or service must authenticate to a valid, licensed Exchange Online mailbox and connect over TCP port 587 using TLS. Applications that use SMTP relay are subject to the same message size and rate limits as regular users.

See [TechNet](https://docs.microsoft.com) for details on how to configure SMTP Relay with Exchange Online. Note that you will need to provide the SMTP server name that is specific to the mailbox used for relay. The Help article [Set Up Outlook 2007 for IMAP or POP Access to Your E-Mail Account](https://docs.microsoft.com) includes the steps to find the server settings.

### 3.8.11.3 Outlook Web App Web Parts

Exchange Online supports Outlook Web App Web Parts, which provide access to content in Outlook Web App directly from a URL. Web Parts are usually embedded in a custom application or a web-based portal, such as Microsoft SharePoint Online or Microsoft SharePoint Server.

See the TechNet article [Using Outlook Web App Web Parts](https://docs.microsoft.com) for more details.

### 3.8.11.4 Outlook Add-Ins and Outlook MAPI

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

Applications that use the Outlook MAPI library to connect to Exchange Online usually work, but those that use the Exchange Server MAPI library will not work (see the next subsection for details). If an application requires Outlook to be installed in order to function, it probably uses the Outlook MAPI library.

### 3.8.11.5 Exchange Server MAPI/CDO

Some third-party applications use Exchange Server MAPI client and Collaboration Data Objects (MAPI/CDO) for server-to-server communication with Exchange. These applications need to be installed within the same local network as Exchange and will not connect over the Internet to Exchange Online.
3.8.11.6  **Lync Server 2010 and Office Communications Server 2007 R2**

Lync Online can be configured for domain federation with an on-premise Microsoft Office Communications Server 2007, Office Communications Server 2007 R2, or Lync Server 2010 as long as Lync Online and the on-premise system are using different SIP domains.

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

- IM and presence interoperability in Outlook Web App.
- Voicemail interoperability (see the [Unified Messaging Services](#) section of this document for details).

3.8.11.7  **WebDAV**

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

3.8.12  **Security**

Exchange Online security components are described in the sections that follow.

3.8.12.1  **Anti-Spam and Antivirus Filtering**

Exchange Online uses Microsoft Forefront Online Protection for Exchange (FOPE)—an enterprise-level email filtering technology—to help protect incoming, outgoing, and internal messages from malicious software transferred through email. All messages transported through the Exchange Online service are scanned for viruses and malicious software.

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

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

---

**Note:** Microsoft Forefront Protection 2010 for Exchange Server (FPE) is configured on internal Exchange servers within the Office 365 environment. FPE is not configurable or manageable by customer administrators.

3.8.12.2  **Safe and Blocked Senders**

Users can manage their safe and blocked senders from within their inboxes in Outlook or Outlook Web App. They can right-click any message and specify several actions, including:
- Block the sender.
- Never block the sender.
- Never block the sender’s domain.
- Never block this group or mailing list.

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

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

See the Help topic Learn about Junk E-Mail Messages for more information.

**Junk Mail and Spam Quarantine**

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

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

3.8.12.3 **Use of Other Filtering Services for Inbound Email**

An on-premises appliance or another hosted service can be used to filter email before it reaches Exchange Online. In this scenario, the email domain’s MX record is pointed to the appliance or service, which then relays the email to Exchange Online. This same configuration can also be used in email coexistence, when some users have mailboxes in an on-premises email server while others are hosted in Exchange Online.

3.8.12.4 **Custom Routing of Outbound Email**

Exchange Online provides the ability to route outbound mail through an on-premises server or a hosted service (sometimes called “smart hosting”). This capability allows organizations to utilize data loss prevention (DLP) appliances, perform custom post-processing of outbound email, and deliver email to business partners via private networks.
Administrators configure custom email routing within the Forefront Online Protection for Exchange (FOPE) Administration Center. For additional information, consult the Forefront Online Protection for Exchange (FOPE) 11.1 Product Documents available from the Microsoft Download Center.

3.8.12.5 Address Rewrite for Outbound Email

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

3.8.12.6 Encryption Between Email Servers

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

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

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

3.8.12.7 Encryption Between Clients and Exchange Online

Client connections to Exchange Online use SSL encryption to enhance security for securing Outlook, Outlook Web App, Exchange ActiveSync, and Exchange Web Services traffic using TCP port 443.

Client connections to IMAP use SSL over TCP port 995.

3.8.12.8 Third-party Encryption Solutions

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

Exchange Online will transport and store Secure/Multipurpose Internet Mail Extensions (S/MIME) messages. However, Exchange Online does not host S/MIME functions, nor does it provide key repository, key management, or key directory services.

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

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

3.8.12.10 Information Rights Management

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

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

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

Support for IRM in Outlook Web App

Users can read and create IRM-protected messages natively in Outlook Web App, just like in Outlook. IRM-protected messages in Outlook Web App can be accessed through Internet Explorer, Firefox, Safari, and Google Chrome (with no plug-in required) and include full-text search, conversation view, and the preview pane.
Support for IRM in Exchange ActiveSync
Users with mobile devices that support the IRM features of the Exchange ActiveSync protocol can open and work with IRM-protected messages with the appropriate rights—and without tethering the phone or installing additional IRM software. Administrators can control the use of this feature using Role-Based Access Control (RBAC) and Exchange ActiveSync policies.

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

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

3.8.12.10.1 Protected Voicemail
Either senders or administrators can apply Do Not Forward permissions to voice messages to prevent protected voicemail from being forwarded to unauthorized persons, regardless of the email client. To apply these permissions, senders must mark the message as private.

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

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

3.8.13 Unified Messaging Services
Exchange Online offers hosted Unified Messaging services, which provide:
- Call answering (voicemail)
- Dial-in user interface to Exchange (Outlook Voice Access)
- Dial-in interface for callers (Automated Attendant)

**Note:** Currently, organizations with services hosted from data centers in the Asia-Pacific and Europe regions cannot integrate on-premises Lync Server 2010 with hosted voicemail services because the hardware for Lync Server integration has not yet been deployed in those data centers. Integration with other on-premises PBX systems is supported.

Exchange Online Unified Messaging allows a company to connect its on-premises phone system to voicemail services provided by Exchange Online. Voicemails are recorded and stored in the Exchange Online infrastructure, allowing users to access their voice messages from Outlook, Outlook Web App, IMAP clients, Exchange ActiveSync devices, mobile and other types of devices.

All telephony connections to Exchange Online require voice-over-IP (VoIP) protocols. Administrators can connect an on-premises PBX to Exchange Online using VoIP media gateways, or an IP-PBX directly to Exchange Online UM through a session border controller (SBC). SBCs are deployed in the perimeter of the customer network and help secure the communications (and the customer network) against eavesdropping and intrusion. Interoperability with the voice capabilities of Lync Server 2010 is also supported.

For more information, see the Help topic [Set Up Unified Messaging](#) and TechNet article [Connect Lync Server 2010 to Exchange Online UM](#)

**Note:** A VoIP media gateway is not required if the PBX supports VoIP directly and is interoperable with Exchange Unified Messaging.

### 3.8.13.1 Telephony Solutions Details

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

For more information, see the Help topic [Differences Between an On-Premises Deployment of UM and UM Deployment in the Cloud](#).

The following Unified Messaging features work similarly online and on-premises:

- “Play on Phone” from Outlook and Outlook Web App
- Missed call notifications
- Caller ID (using information in the Global Address List and users’ Outlook contacts)
- Voicemail PIN reset from Outlook Web App and Outlook
- Message waiting indicator
- Call answering rules
- Protected voicemail (requires implementation of Information Rights Management and Windows Rights Management Services)

The Exchange Control Panel includes screens to configure and manage Unified Messaging interoperability.

**Interoperability with On-Premises Voicemail Systems**

On-premises voicemail solutions from third-party providers can interoperate with Exchange Online if they can forward voicemails through SMTP or if they support Microsoft Exchange Web Services. If the voicemail system does not natively support forwarding voicemails through SMTP, an email server can be kept on-premises to receive messages from the voicemail system and then forward them to the Office 365 using SMTP. Because many third-party voicemail systems use MAPI/CDO to interoperate with Exchange Server for advanced Unified Messaging features, the full capabilities of these systems may not be available when SMTP is used for interoperability with Exchange Online.

**Fax Interoperability**

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

Inbound fax solutions can interoperate with Exchange Online via SMTP. If a company uses a third-party fax solution that is capable of receiving faxes and forwarding them to recipients via email, the administrator can specify Exchange Online mailboxes as a destination. If the company has deployed Unified Messaging in Exchange Online, advanced interoperability with inbound fax solutions is available. This interoperability enables features such as one-number fax receiving (a single phone number for voice calls and fax), rich caller-ID information through Active Directory and Exchange personal contacts, and identification of fax messages as a special message class in Exchange and Outlook.

**3.8.13.2 Unified Messaging Migration Support**

Office 365 for enterprises offers Unified Messaging functionality, but migration is only supported for customers running Exchange 2007 Unified Messaging or Exchange 2010 Unified Messaging on-premises. Customers with other on-premises Unified Messaging products who wish to move to Office 365 Unified Messaging will need to enable the Exchange Online users’ mailboxes as new mailboxes for Unified Messaging.
3.8.14 Contacts and Distribution Groups

This section addresses the Exchange Online functionality with respect to contacts, distribution groups, and Global Address List.

3.8.14.1 Distribution Groups

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

Exchange Online supports advanced distribution group capabilities, including:

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

Restricted Distribution Groups

By default, anyone can send emails to a distribution group. However, administrators can change the permissions of a distribution group to allow only specific individuals to send emails to that group. This restriction can discourage inappropriate use of large distribution lists. Administrators can also provide only internal access to distribution groups to prevent spam from external sources. The Exchange Control Panel includes a web-based GUI for managing distribution group permissions. For distribution groups that are synchronized from on-premises Active Directory using the Directory Synchronization Tool, the attributes for restriction are synchronized to Exchange Online automatically.

Dynamic Distribution Groups

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

The Office 365 Directory Synchronization Tool ignores dynamic distribution groups in on-premises Active Directory, and does not synchronize these to Exchange Online. Organizations that use the Directory Synchronization Tool should use a naming convention that avoids conflicts between the regular distribution groups managed on-premises and the dynamic distribution groups that are managed in Exchange Online.
See the Help topic Dynamic Distribution Groups for more details.

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

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

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

Administrators can also disable these features and let the IT department manage distribution groups.

---

**Note:** Self-service capabilities are not available for distribution groups that are mastered in on-premises Active Directory and synchronized to Exchange Online via directory synchronization.

---

### 3.8.14.2 Global Address List
Exchange Online supports the Global Address List, a company’s directory of all mail-enabled users, distribution groups, and external contacts.

Administrators can hide users, distribution groups, and contacts from the Global Address List by setting the `msExchHideFromAddressLists` attribute for the object in their on-premises Active Directory (if using the Directory Synchronization Tool and the on-premises schema is extended for Exchange) or through Remote PowerShell.

For more information, see the Help topic Hide a User from the Shared Address Book in Office 365.

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

**Global Address List Photos**

Outlook 2010 includes new features that incorporate photos of users stored in Active Directory. For example, when users receive emails from coworkers, they can see the senders’ photos in the upper right corner in Outlook. When users search for coworkers in the Global Address List using Outlook, the coworkers’ photos are displayed. Mobile devices that support the latest version of Exchange ActiveSync can also display photos from Active Directory. Global Address List photos are not available in Outlook Web App.

There are two ways for organizations to load user photos into the Exchange Online environment and enable these features:

- End users can upload their photos manually through the User Settings screen in the Microsoft Online Services Portal.
- Administrators can populate the `ThumbnailPhoto` user attribute in on-premises Active Directory; the Directory Synchronization Tool will automatically synchronize the user photo to Exchange Online, SharePoint Online, and Lync Online.

**Note:** During the Office 365 period, the ability to upload a photo from the User Settings screen is not available.

**External Contacts**

An external contact is a record with information about a person who works outside of a specified company. External contacts are available to all users in the company, which makes external contacts different from the personal contacts that individuals create in Outlook. External contacts are created in the Exchange Control Panel or synchronized from on-premises Active Directory, and appear in the Global Address List in Outlook. External contacts require an SMTP address in order to be synchronized to Exchange Online.

---

### 3.8.15 Calendar Sharing

This section describes the different kinds of calendar sharing available with Exchange Online.

#### 3.8.15.1 Federated Calendar Sharing

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

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

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

For more details, see the TechNet article Understanding Federated Delegation.

### 3.8.15.2 Calendar Sharing Using iCal

Exchange Online allows users to publish their calendars using the iCal format for anonymous access by other users. Users can also subscribe to calendars that others have published to Internet locations through iCal. This personal calendar sharing is different than federated calendar sharing, which is configured by an administrator and provides organization-to-organization free/busy sharing. Administrators can disable iCal publishing and iCal subscriptions for users in an organization through Remote PowerShell.

### 3.8.16 Conference Rooms and Resource Mailboxes

Conference room mailboxes represent a company's meeting rooms or other facilities. Users can reserve rooms by adding the conference room email alias to meeting requests in Outlook or Outlook Web App. Conference rooms appear in the Global Address List in Outlook and Outlook Web App, and administrators can create conference rooms in the Exchange Control Panel or through Remote PowerShell. Administrators can also use the Directory Synchronization Tool to synchronize conference rooms from on-premises Active Directory. The mailbox quota for conference rooms is 250 MB. Conference rooms do not require a user subscription license.

For more information, see the Help topic Create a New Room Mailbox.

### 3.8.16.1 Resource Booking Attendant

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

For more information, see the Help topic Configure Resource Mailbox Options.

3.8.16.2 Outlook 2010 Room Finder

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

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

3.9 SharePoint Online Planning

This section of the deployment guide describes the SharePoint Online deployment planning tasks and processes. Information in this section comes largely from the SharePoint Online Planning Guide for Office 365 for enterprises, which you may want to review in its entirety.

The SharePoint Online Planning and Administration site also provides useful information for small and enterprise organizations. Refer to this site for additional information related to SharePoint Online.

For planning information about developing custom solutions for SharePoint Online, see the following resources:

- SharePoint Online Developer Resource Center
- SharePoint Online: An Overview for Developers

Note: SharePoint Online is currently not available for purchase by Office 365 customers with more than 20,000 users in their Active Directory. This temporary limitation on the number of users applies to organization purchasing SharePoint Online as part of the Office 365 service suite or as a standalone service. An updated to the SharePoint Online service is planned that will enable SharePoint Online provisioning for organizations with up to 100,000 users in their Active Directory.

3.9.1 About SharePoint Online

Built on Microsoft Office SharePoint Server 2010, SharePoint Online provides a single, integrated
location where users can efficiently collaborate on tasks, share documents, create project-focused sites, manage content and workflow, search for and find organizational resources, and leverage business insight to make better-informed decisions. For additional details, see the Microsoft SharePoint Online Service Description.

Figure 10 illustrates the capabilities (also known as work areas) of SharePoint 2010.

![Figure 10](image)

Details about the SharePoint 2010 capabilities are presented in Table 13.

**Table 13. SharePoint Capability Descriptions**

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td>SharePoint 2010 Sites provides a single infrastructure for your business websites. This capability allows for sharing information with colleagues, manage projects with partners, and publish information to customers.</td>
</tr>
<tr>
<td>Communities</td>
<td>SharePoint 2010 Communities provides a full set of collaboration tools—from wikis to workflows and team sites to tagging. A single, flexible platform makes it easy to manage these tools and design the right collaborative experiences for different business needs.</td>
</tr>
<tr>
<td>Content</td>
<td>SharePoint 2010 is designed to simplify content management with features like content types, retention policies, and automatic content sorting—and then let people work naturally in Microsoft Office.</td>
</tr>
<tr>
<td>Search</td>
<td>SharePoint 2010 Search provides a unique combination of relevance, refinement, and social cues helps people find the information and contacts they need to get their jobs done.</td>
</tr>
<tr>
<td>Insights</td>
<td>SharePoint 2010 Insights gives everyone access to the information in databases, reports, and business applications. Help people locate the information they need to make good decisions</td>
</tr>
<tr>
<td>Composites</td>
<td>SharePoint 2010 Composites offers tools and components for creating do-it-yourself business solutions. Build no-code solutions to rapidly respond to</td>
</tr>
</tbody>
</table>
3.9.2 Available Features

In your planning, it is important to consider the available SharePoint Online features and how they may differ from those available in an on-premises implementation of SharePoint Server 2010. For a comprehensive comparison of feature availability between Office SharePoint Server 2010 and SharePoint Online solutions, see Appendix B of the Microsoft SharePoint Online Service Description. Features are compared across the major SharePoint work areas: Sites, Communities, Content, Search, Insights, and Composites.

Table 14 offers a high-level comparison of SharePoint Online features across Office 365 user subscription plans.

**Table 14. Feature Comparison of SharePoint Online User Subscriptions**

<table>
<thead>
<tr>
<th>Capability</th>
<th>For Small Businesses SharePoint Online in P1</th>
<th>For Kiosk Workers SharePoint Online in K1/K2</th>
<th>For Information Workers SharePoint Online Plan 1 in E1/E2</th>
<th>For Information Workers SharePoint Online Plan 2 in E3/E4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team Sites</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Simple Public-Facing Site</td>
<td>1 Basic Public facing site included</td>
<td>No</td>
<td>1 Basic Public facing site included</td>
<td>1 Basic Public facing site included</td>
</tr>
<tr>
<td>Site Designer</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SharePoint Designer 2010</td>
<td>Yes, for Intranet sites</td>
<td>Yes, for Intranet sites</td>
<td>Yes, for Intranet sites</td>
<td>Yes, for Intranet sites</td>
</tr>
<tr>
<td>Custom Workflows</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sandbox Solutions (PTC)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>My Site</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enterprise Features (Forms Services, Excel Services, Visio Services)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Services</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### 3.9.3 Service Limitations

Before you begin your SharePoint Online configuration, you should be aware of the following limitations:

- **Migration of existing SharePoint data.** Office 365 does not migrate data from your organization’s existing on-premises SharePoint sites to SharePoint Online. Third-party products are available to help with this task.

- **Mail-enabled lists.** SharePoint Online does not support mail-enabled lists due to the multi-tenant architecture of the service. Mail can be sent from SharePoint Online as a result of a workflow or other event, but not to SharePoint Online. As a result, mail-enabled list usage should be reviewed in a pre-provisioned environment for solution alignment.

---

<table>
<thead>
<tr>
<th></th>
<th>For Small Businesses SharePoint Online in P1</th>
<th>For Kiosk Workers SharePoint Online in K1/K2</th>
<th>For Information Workers SharePoint Online Plan 1 in E1/E2</th>
<th>For Information Workers SharePoint Online Plan 2 in E3/E4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Connectivity Services (BCS)</strong></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Site Collections</strong></td>
<td>Single Site Collection</td>
<td>N/A</td>
<td>Up to 300</td>
<td>Up to 300</td>
</tr>
<tr>
<td><strong>Office Web Apps</strong></td>
<td>View &amp; Edit</td>
<td>View only for K1</td>
<td>View only for E1</td>
<td>View &amp; Edit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View &amp; Edit for K2</td>
<td>View &amp; Edit for E2</td>
<td>View &amp; Edit</td>
</tr>
<tr>
<td><strong>Search (across Site Collections)</strong></td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Basic External Document Sharing</strong></td>
<td>Yes</td>
<td>N/A</td>
<td>Yes, add-on</td>
<td>Yes, add-on</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>10GB + 500MB per USL</td>
<td>10GB + 0MB per USL</td>
<td>10GB + 500MB per USL</td>
<td>10GB + 500MB per USL</td>
</tr>
<tr>
<td><strong>Buy additional storage</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Max Org Users</strong></td>
<td>Up to 50</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td><strong>Administrator</strong></td>
<td>Yes. Within Single Site Collection</td>
<td>No</td>
<td>Yes. Tenant level.</td>
<td>Yes. Tenant level.</td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td>Community</td>
<td>24x7 phone support for Admin</td>
<td>24x7 phone support for Admin</td>
<td>24x7 phone support for Admin</td>
</tr>
</tbody>
</table>
• **Search restrictions.** Microsoft Office document file types and .ZIP and .PDF files are enabled for search in the SharePoint Online environment. It is not possible to extend Search to support new file types. A best practice is to review Office document meta tags and search taxonomy for search requirements prior to migration.

### 3.9.4 Capacity Planning

Table 15 describes the SharePoint Online feature specifications that you should consider for capacity planning in your SharePoint Online deployment.

**Table 15. SharePoint Online feature specifications**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage (pooled)</strong></td>
<td>10 gigabytes (GB) base customer storage plus 500 megabytes (MB) per enterprise user</td>
</tr>
<tr>
<td><strong>Storage per Kiosk Worker</strong></td>
<td>Zero (0). Licensed Kiosk Workers do not bring additional storage allocation.</td>
</tr>
<tr>
<td><strong>Storage per external user</strong></td>
<td>Zero (0). Licensed external users do not bring additional storage allocation.</td>
</tr>
<tr>
<td><strong>Additional storage</strong></td>
<td>Available per GB per month; no minimum purchase</td>
</tr>
<tr>
<td><strong>Site collection storage quotas</strong></td>
<td>Up to 100 GB per site collection</td>
</tr>
<tr>
<td><strong>My Site storage allocation</strong></td>
<td>500 megabytes (MB) of personal storage per My Site (once provisioned)</td>
</tr>
<tr>
<td><strong>Site collections per tenant</strong></td>
<td>Up to 300 (non-My Site site collections)</td>
</tr>
<tr>
<td><strong>Total storage per tenant</strong></td>
<td>Up to 5 terabyte (TB) per tenant</td>
</tr>
<tr>
<td><strong>Storage per external user</strong></td>
<td>Zero (0). Licensed external users do not bring additional storage allocation.</td>
</tr>
</tbody>
</table>

For additional information on SharePoint Online capacity planning, see [SharePoint Online: software boundaries and limits](#).

### 3.9.5 SharePoint Online Planning Guide

The best way to learn how to use SharePoint Online in your organization is to review the [SharePoint Online planning guide for Office 365 for enterprises](#). This comprehensive planning guide consists of a series of articles that guide site collection administrators and site owners through the steps involved in setting up and using SharePoint Online sites. The guide is divided into the following seven sections or “steps.”

- Step 1: Plan to manage SharePoint Online by using the Administration Center
• Step 2: Plan sites and manage users
• Step 3: Plan content on sites
• Step 4: Plan customizations and solutions
• Step 5: Create and customize the public-facing website
• Step 6: Train and support users
• Step 7: Plan to monitor and maintain site collections and sites

We recommend that you read all of the articles in this guide before you proceed with setting up SharePoint Online. You will need to know how SharePoint features work together in order to make decisions about setting up your sites.

3.10 Lync Online Planning

Lync Online provides real-time communications capabilities including text-based instant messaging and integrated audio and video communication. With Lync Online, your organization can check the presence information of coworkers, regardless of their location or time zone, and choose the best way to communicate with them (IM and presence is also available in Outlook Web App).

Important: You should review the Microsoft Lync Online Service Description for complete details about features and limitations of Lync Online.

The features provided by the Lync Online service include:

• **Presence information.** You can see the availability status and other presence-related information for users displayed in Lync Online and other Microsoft Office applications such as Microsoft Office Outlook, enabling you to choose the best method for communicating with them. (Outlook Web App also provides presence and IM capabilities).

• **Instant messaging (IM).** You can perform traditional text-based IM communications in real time with one or more people in the organization. You can also transfer files to the people you are messaging.

• **Audio and video communication.** The Lync Online service delivers person-to-person (1:1) audio and video conversations for users equipped with a headset device and Web camera.

• **Online meetings.** Your organization’s online conferencing experience is simple and integrated with the Office 365.

• **Application and Desktop Sharing.** Allows your users to share their computer desktop and applications that they are running in PC-to-PC and multiparty conferences.
• **Lync domain federation.** You can enable collaboration with your on-premises Microsoft Lync 2010 Server and Microsoft Office Communications Server 2007 users (using a different domain for Lync Online than any currently used on-premises), other organizations utilizing Lync Online (outside your organization), or Windows Live users.

• **Unified Lync client.** The collaborative features of instant messaging, presence and audio/video conferencing are all integrated into the Lync 2010 client.

• **Lync web application.** The Lync Web App provides the ability to attend Lync Online meetings with a web-based client.

**Notes:**

- Feature availability varies by usage location. Some features may not be available at general availability.
- PBX replacement/integration is *not* available in Lync Online—only Lync on-premises.
- Lync users can only be homed on-premises or to Lync Online—you cannot split features (IM, conferencing, voice) between on-premises and Lync Online.
- In the supported scenario, Lync on-premises with Exchange Online, the SMTP address and SIP URI must be the same.

### 3.10.1 Lync Domain Federation

If you are an Office 365 administrator, you can enable domain federation in Lync Online so users in your company can connect to other Lync 2010 users in other companies. If you want to establish Lync domain federation with your own on-premises implementation of Office Communications Server 2007, Office Communications Server 2007 R2, or Lync 2010, Lync Online and your on-premises system must be using different SIP domains. After you have enabled domain federation, users can exchange peer-to-peer instant messages (IM), initiate peer-to-peer audio and video calls, and view presence information. You can also enable public IM connectivity, so that users can add contacts from Windows Live Messenger and communicate with them by using Lync 2010.
Note: Lync domain federation is not the same as Lync coexistence. Coexistence with Lync Server will become available at a later time and will provide additional functionality such as the ability to share the same SIP domain between Lync Online and Lync Server on-premises, the ability to split features between Lync Online and Lync Server on-premises, and the use of an integrated searchable address book.

3.10.2 Federation Settings
By default, domain federation is disabled for all domains except those that you explicitly block. Disabling federation allows you the option to add only the domains you would like to enable federation with.

If you do not want to utilize federation, you may choose to leave federation disabled.

3.10.3 Public IM Connectivity
Allowing instant messaging (IM) communication with external users who use a public IM service provider may be useful for the employees in your company. For example, if your company does business with another company that uses Windows Live, you might want employees of both companies to be able to communicate freely with IM.

To allow this type of communication, you can enable public IM connectivity for Lync Online users. Enabling public IM connectivity will allow communications with members of the Windows Live messenger network.

Note: Public IM connectivity is supported with Windows Live Messenger. Public IM connectivity with AOL Instant Messenger (AIM) and Yahoo! Messenger is not supported.

You may choose to enable or disable all of your organization from public IM connectivity. Public IM connectivity (PIC) is disabled by default.

It is important to note that you cannot configure block lists or edit which public IM connectivity you allow for.

3.10.4 Lync Coexistence
Lync technology does not support coexistence between Lync Online and Lync Server using a single domain. Therefore, it is not possible to deploy a subset of users in Lync Online and other users on-premises using a single domain name. Lync federation can be used to enable users to communicate between Lync Online and Lync on-premises deployments, using different domain names.

If you would like to deploy Lync features to both on-premises users and to Office 365 users, you

Lync Online users can be homed to either Lync Online or Lync Server on-premises—you cannot split some of the features to users on-premises (for example, conferencing and voice services) with some of the features available in Lync Online. Therefore, it is important that you determine what features your organization will need in your Office 365 deployment and assess which users will need to be homed to Lync Server on-premises and which users should be homed to Lync Online.

Voicemail support in Office 365 requires deployment of Lync Server 2010 on-premises. Note that in the Exchange Online and Lync on-premises scenario, the SMTP address and SIP URI must be the same.

Note: Coexistence between Lync Server on-premises and Lync Online will become available at a later time. If you are interested in taking advantage of Lync coexistence functionality when it becomes available, and you currently have Office Communications Server 2007 implemented on-premises, you may want to start planning to upgrade your on-premises system to Lync Server 2010.

3.10.5 Client Requirements and Limitations

The following Lync Online clients can be used with Office 365:

- **Microsoft Lync 2010 client.** Users must install the Lync 2010 client to use all of the Lync Online features. A promotional version of Lync 2010 client can be downloaded from the [Microsoft Online Services Portal download page](#).

- **Outlook Web App.** The web-based Outlook Web App client provides Lync Online IM and presence features to users.

- **Lync Web App.** The web-based Lync Web App client experience enables IM in meetings, high-fidelity desktop, application and presentation viewing, desktop sharing, whiteboard, lobby, and presenter access controls. In addition, the web client supports phone dial-out after joining the meeting, which requires a third-party dial-in audio conferencing service. For more information on third-party audio conferencing, see the Help article [Configure dial-in conferencing](#).

- **Lync 2010 Attendee.** This client allows external or anonymous users join a scheduled online meeting with full fidelity PC-audio, video, and data sharing.

The Microsoft Office Communicator 2007 client and other instant messaging program clients cannot be used to connect to Lync Online.
3.10.5.1  

**Network Port Configuration**

The Lync 2010 client typically uses port 5061 (TCP) for network communications. However, after the client is configured for Lync Online, it uses port 443 (TCP). Port 443 is more available port on customer firewalls, routers, and proxy devices. See the [Networking and Naming Services](#) section for details on ports and IP ranges for Lync Online.

3.11  

**Client and End-User Experience**

Office 365 for enterprises allow your organization to choose either rich experience or web experience for your users. The web experience requires a recent version of Internet web browsers. The rich experience requires recent versions of operating systems, Microsoft Office software, Internet browsers, Office 365 desktop setup, and some updates to your computers.

3.11.1  

**Rich Experience Clients**

Rich experience clients provide users with full-featured desktop applications for email, instant messaging, and business productivity and require methods for distributing, configuring and updating clients.

Rich experience clients include the following desktop applications:

- Microsoft Office 2010 (including Outlook)
- Microsoft Office 2007 SP2 (including Outlook)
- Microsoft Office 2008 for Mac and Microsoft Entourage® 2008 Web Services Edition
- Microsoft Office 2011 for Mac
- Office Web Apps
- Microsoft Lync 2010
- Office 365 desktop setup

3.11.1.1  

**Rich Experience Hardware Requirements**

Table 16 shows the hardware requirements for operating systems installed on client computers.
### Table 16. Operating System Requirements for Rich Experience Clients

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Hardware Requirements</th>
</tr>
</thead>
</table>
| Windows XP (SP3) or later                | • 500 megahertz (MHz) Pentium processor or faster; 1 gigahertz (GHz) recommended  
                                        | • 256 megabytes (MB) or more of system RAM                  |
| Windows Vista SP2 or later               | • 1 GHz Pentium processor or faster                         |
|                                         | • 1 gigabyte (GB) or more of system RAM                     |
| Windows 7 Enterprise, Professional, Ultimate RTM and later | • 1 GHz or faster 32-bit (x86) or 64-bit (x64) processor  
                                        | • 1 GB RAM (32-bit) or 2 GB RAM (64-bit)                    |
| Windows Server 2008 R2                  | • 2 GHz or faster 64-bit (x64) processor                    |
|                                         | • 4 GB RAM                                                  |

### 3.11.1.2 Rich Experience Software Requirements

Table 17 shows rich experience software requirements for client computers

### Table 17. Software Requirements for Client Computers

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating systems</strong></td>
<td>• Windows 7 Enterprise, Professional, Ultimate RTM and above</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista Business, Enterprise, Ultimate Service Pack 2 and above</td>
</tr>
<tr>
<td></td>
<td>• Windows XP Professional Service Pack 3 and above with RPC over HTTP Update</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.6 (Snow Leopard)</td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.5 (Leopard)</td>
</tr>
<tr>
<td><strong>Note:</strong> Windows versions that do not allow for machines to be domain joined (for example, Home or Media Center editions) can be used with Office 365 suite. However, identity federated users will be prompted for credentials each time to use each of the services with Office 365.</td>
<td></td>
</tr>
<tr>
<td><strong>System software</strong></td>
<td>• Microsoft .NET Framework 3.0+ (Windows XP)</td>
</tr>
<tr>
<td></td>
<td>• Java client 1.4.2 (for Macintosh OS X)*</td>
</tr>
<tr>
<td><strong>Microsoft Office/email</strong></td>
<td>• Office 2010</td>
</tr>
<tr>
<td></td>
<td>• Office 2007 (SP2) or later</td>
</tr>
<tr>
<td></td>
<td>• Office for Mac 2011</td>
</tr>
<tr>
<td></td>
<td>• Office 2008 for Mac and Microsoft Entourage® 2008 Web Services Edition</td>
</tr>
<tr>
<td></td>
<td>• Mainstream IMAP client for low fidelity experience</td>
</tr>
<tr>
<td><strong>Note:</strong> Some features, such as Archiving and Retention, requiring specific versions of Outlook. See License requirements for Personal Archive and retention policies.</td>
<td></td>
</tr>
<tr>
<td>Scenario</td>
<td>Supported Version</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Browsers** *(for SharePoint Online, Microsoft Online Services Portal, Outlook Web App)* | • Internet Explorer 7 or later  
• Firefox 3 or later  
• Safari 4 or later for PCs  
• Safari 3 or later for Macintosh OS 10.5  
• Google Chrome 3 or later                                                                      |
| **Instant messaging and presence**           | • Lync 2010 desktop client  
• Lync Attendee client (This is a free download that can be used by external users join Lync Online meetings. It is available from the Microsoft Download Site.) |
| **Audio, video, web conferencing**           |                                                                                                                                                   |
| **Enterprise single sign-on**                | • Domain joined Windows computer  
• Macintosh users will be prompted for credentials                                                                                           |
| **Client applications**                      | • Windows Live ID components  
• Windows Live Sign-In Assistant  
• Office 365 desktop setup                                                                                                                          |

**Notes:**

- Only Windows versions that can be joined to a domain are able to utilize identity federation with single sign-on. (For example, Windows Professional, Business, and Enterprise editions.)
- Outlook 2003 (or earlier editions of Outlook) and Office Communicator clients are not supported.

### 3.11.1.3 Outlook Client

Microsoft Office Outlook 2010 and Microsoft Outlook 2007 with Service Pack (SP) 2 are the supported Outlook clients for Office 365.

The features only available with Outlook 2010 include:

- Conversation View
- MailTips
- Find a room
- Text message integration with Windows mobile phone
- Ability to remove (mute) yourself from conversations.

For a complete description of Outlook 2010 features, see [Top 10 reasons to try Outlook 2010](#).

Although Office 365 supports Outlook 2007 SP2, some functions available in Outlook 2010 may not be available in Outlook 2007 SP2.
Note: Identity federated users will be required to check the “save my password” option when initially configuring Outlook 2007 SP2. If a user changes their password, they may be required to reenter their password Outlook and check the box again.

3.11.1.4 Microsoft Office Professional Plus Subscriptions

With Microsoft Office Professional Plus, Office 365 provides organizations with the ability to use Microsoft Office 2010 and Microsoft Office for Mac 2011 on a subscription basis.

Subscriptions are managed in the Microsoft Online Services Portal. Users will need to download and install Microsoft Office on their computers prior to being granted a subscription.


You can review the Office Professional Plus Service Description for a comprehensive description of Microsoft Office Professional Plus.

3.11.1.5 Lync 2010 Client

The Lync 2010 desktop client should be deployed on each PC that will connect to Lync Online. You may choose to have your users install the application themselves or deploy via software distribution. For full functionality with Lync Online, the Lync Cumulative Update 2 (CU2) or later should be used, and it can be downloaded from the Microsoft Online Services Portal download page.

Note: Lync has specific client system requirements. See Lync 2010 System Requirements.

3.11.1.6 Manual Distribution of Client Updates

Before rolling out the necessary software and patches in your organization, it is important for large enterprise organizations to determine how to install the following client applications:

- Microsoft Office 2010
- Microsoft Office 2007 SP2
- Microsoft Lync 2010 client
- Internet Explorer 7.0 or later
- Outlook add-ins
- Service packs,
- Hotfixes
- Office 365 desktop setup

Depending on your organization’s infrastructure and lock-down policies, you may need to push
this software to users’ computers through Microsoft Systems Management Server (SMS) or Microsoft System Center Configuration Manager (SCCM), group policy, or another software distribution tool.

All of the updates and patches that are required for Office 365 client setup are listed and described in the Help topic Manually update and configure desktops for Office 365 for the latest patches.

3.11.1.7 Client Updates with Office 365 Desktop Setup

For smaller deployment projects, Microsoft at no charge provides the Office 365 desktop setup, an application which installs a set of required components and updates to each PC that uses rich clients (such as Microsoft Office 2010) and connects to the Office 365 service.

After the Office 365 desktop setup is installed, it automatically detects when new updates are necessary and installs them on the PC.

**Note:** The Office 365 desktop setup package is not an authentication or sign-in service and should not be confused with single sign on.

3.11.2 Web Experience Clients

The web experience is suitable for users in larger businesses do not have a dedicated computer. Office 365 has solutions for these “kiosk workers,” giving them access to email and company information via a web browser.

3.11.2.1 Web Experience Client Requirements

Table 18 summarizes the client requirements required for Office 365 web experience users.

**Table 18. Web Experience Client Requirements**

<table>
<thead>
<tr>
<th>Experience</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Systems</td>
<td>• Windows XP, Windows Vista, Windows 7</td>
</tr>
<tr>
<td></td>
<td>• Macintosh OS X</td>
</tr>
<tr>
<td>Instant Messaging and Presence</td>
<td>• IM and presence within the Outlook Web App</td>
</tr>
<tr>
<td>Conferencing</td>
<td>• Lync Attendee web client (for joining meetings only)</td>
</tr>
<tr>
<td>Email Instant Messaging and Presence</td>
<td>• Outlook Web App</td>
</tr>
<tr>
<td>Experience</td>
<td>Requirement</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| SharePoint Online and Microsoft Online Services Portal | • Internet Explorer 7 or higher  
• Firefox 3  
• Firefox 2  
• Safari (on Macintosh OS X)                  |
| Office Suite (Word, Excel, PowerPoint)          | • Office Web Apps                                                            |

### 3.11.2.2 Internet Browsers

The web experience requires a recent version of many of the following main stream web browsers:

- Internet Explorer 7 or later
- Firefox 3 or later
- Safari 3 or later on Macintosh OS 10.5

### 3.11.2.3 Office Web Apps

Office Web Apps give you more flexibility to stay connected to your work over the Web. Even when working away from the office, you will still have online access to your work and a core set of Microsoft Office functionality.

**Note**: The Office Web Apps Service Description is available at the [Microsoft Download Center](https://www.microsoft.com/download) and provides more details about Office Web Apps.

### 3.11.2.4 Outlook Web App

Outlook Web App is a powerful web-based version of the Outlook client that provides most of the same features and functionality of Outlook 2010. In addition to email, Outlook Web App provides:

- Integrated instant messaging and presence
- Delegate mailbox access
- Search filters and favorites
- Side by side calendar view
- Shared nickname cache with mobile device
- Inbox rules

Although Outlook Web App includes a number of features, some features are **not** available:

- Rich integration experience with SharePoint Online.
- Integrated experience with Office Web Applications.
**Note:** Any Outlook Web App customizations you may have made on-premises will not be migrated into the Exchange Online service. If you require a custom logon page, it is recommended that you deploy customization to your AD FS proxy servers.

3.11.3  **Web Conferencing**

Lync Online replaces the Office Live Meeting service as the web conferencing solution in Office 365. The Live Meeting service is available for existing BPOS customers during the transition to Lync Online.

3.11.4  **Browser Issues with Extended Protection for Authentication**

If your computers have Extended Protection for Authentication, and you use the Firefox, Google Chrome, or Safari browsers, you may not be able to sign on to Office 365, depending upon your operating system. Instead, you will get an access denied message. This is due to the default configuration for AD FS 2.0 and Extended Protection for Authentication.

Unless and until Firefox, Google Chrome, and Safari support Extended Protection for Authentication, the best option is to install and use Internet Explorer 8 (recommended).

If you want to use single sign-on for Office 365 with Firefox, Google Chrome, or Safari, there are two other solutions:

- Uninstall the Extended Protection patches from your computer.
- Change the Extended Protection setting on the Active Directory Federation Services 2.0 server. See “ExtendedProtectionTokenCheck” on the Set-ADFSProperties page for details.

Note that there may be security concerns in taking either of these approaches. See Microsoft Security Advisory: Extended protection for authentication for more details.

3.11.5  **Mobile Devices**

Microsoft Exchange ActiveSync lets users synchronize their mobile phones with their Microsoft Exchange mailboxes. You can manage what devices users can use to synchronize with Exchange, and manage how those devices synchronize to control long-distance and data charges.

Exchange ActiveSync is offered on many mobile devices and can provide different levels of security for your organization’s data and experiences for your users. As an administrator, in the Exchange Control Panel, you can specify which devices your users can use to synchronize, and how you want your organization’s data to be safeguarded on your user’s devices.

The following Office 365 Help articles provide additional information on mobile device management:
• **Manage Access for Mobile Devices.** Device access rules control which devices your users can use to synchronize with Exchange. This functionality may involve ongoing maintenance and may thus require making an action plan prior to instituting access rules.

• **Manage Data Protection on Mobile Devices.** Exchange ActiveSync device policies provide you a way to require that your users use a PIN on their mobile devices and have the emails and Exchange data encrypted on the devices. They also let you decide how to handle devices that don’t support your organization policies.

• **Troubleshoot Exchange ActiveSync Synchronization Problems.** Troubleshoot common synchronization problems that users might experience.

### 3.11.5.1 BlackBerry Support

For information about planning and support for BlackBerry devices with Office 365 for enterprises, review the [Exchange Online Service Description](#).
4 Prepare Phase

In the Prepare phase of your deployment project, you will begin to take the steps to configure your organization’s environment for integration with the Office 365 environment.

Figure 11 illustrates the high-level sequence of tasks that you will carry out during this phase to set up Exchange hybrid deployment.

1. **Add Your Domain(s)**
   Add your organization's domain via the Microsoft Online Services Portal.

2. **Add TXT Record**
   Add a TXT record in your domain registrar’s DNS database.

3. **Directory Cleanup**
   Clean up your on-premises Active Directory and update schema (if necessary).

4. **Single Sign-On**
   Install and configure identity federation servers on-premises and activate the single sign-on service.

5. **Directory Sync**
   Install and configure directory synchronization server(s) on-premises and activate directory synchronization.

6. **Hybrid Servers**
   Install and configure Exchange hybrid servers on-premises, configure DNS records and certificates, and enable rich coexistence.

7. **Assign Licenses**
   Assign licenses to users and enable Exchange Online, Lync Online, and SharePoint Online for users.

8. **Migrate Mailboxes**
   Migrate user mailboxes with Exchange tools or third-party solutions.

9. **Install Client Apps**
   Install client software before or during deployment.

### 4.1 Key Activities Summary

The following are the key deployment tasks and events that your carry out in the Prepare phase:

- **Add and verify your domain name with Office 365**
  You must add your domain to Office 365 and then create the DNS records to route domain traffic to your Office 365 service.
• **Prepare your on-premises Active Directory for directory synchronization**
  Successful directory synchronization between your on-premises Active Directory environment directory and Office 365 requires that your on-premises directory objects and attributes are properly prepared.

• **Enable single sign-on (identity federation)**
  To enable single sign-on, you must deploy and configure Active Directory Federation Services servers on-premises.

• **Install the Directory Synchronization Tool and perform synchronization**
  Directory synchronization enables you provision user accounts for an Exchange hybrid deployment.

• **Configure email coexistence**
  You install and configure an Exchange 2010 hybrid server on-premises to enable communication between your existing Exchange servers and Exchange Online.

• **Configure Lync Online**
  You optimize your network for Lync conferencing, configuring domain federation and public IM connectivity settings.

• **Configure SharePoint Online**
  You prepare for deployment of any custom SharePoint solutions and migration of existing SharePoint content.

• **Deploy client applications and the Office 365 desktop setup**
  A hybrid deployment requires that rich client applications are deployed and installed on users’ PCs. The Office 365 desktop setup is deployed to ensure that client applications are properly updated and configured for Office 365.

• **Perform mailbox size reduction**
  To improve migration velocity of mailbox content, you may need to reduce the size of user mailboxes.

• **Prepare customer service desk**
  Your service desk must be trained to support Office 365 service offerings.

• **Test and validate email migration and coexistence**
  Prior to velocity migrations, you set up test user accounts to validate that migration processes and that the Exchange hybrid deployment are properly functioning.

• **Complete the migration groups and migration schedule**
  Finalize the groups of users, resources, and shared mailboxes that will be moved at each migration window.

### 4.2 Network and Naming Services Tasks

This section describes the tasks you must perform to configure networking and DNS components for an Exchange hybrid deployment.
4.2.1 Add Domain and Verify Ownership

This topic describes the process of adding a domain that you already own to Office 365. When you add a domain to Office 365 you can create email addresses, Microsoft Lync Online accounts, and distribution lists that use your own domain name. You can also use your domain to host a website on Microsoft SharePoint Online.

To add a domain, you do the following:

- Add and verify your domain name with Office 365
- Create the DNS records that are required to route domain traffic to your Office 365 service. These are the DNS records that are required for routing inbound email to Microsoft Exchange Online.

Office 365 offers domain verification procedures that are specific to some of the most popular domain registrars. Visit the Microsoft Online Services Forums or contact the Office 365 support team to see if there is a procedure for your domain registrar. However, the procedure in this section can be used with any domain registrar.

You only need to add and verify a domain once. If someone else in your organization has already added and verified the same domain, you will receive a message noting this.

To add a domain to Office 365, you use the domain wizard at the Microsoft Online Services Portal.

**To add a domain and verify domain ownership**

1. Log on to the Microsoft Online Services Portal with your Office 365 administrator credentials.
2. In the portal header, click Admin.
4. Click Add a domain.
5. Type the name of the domain you would like to add (for example, contoso.com).
6. Click Next.
7. Click Verify domain.
8. From the table on the Verify domain page, record the following information:
   - Alias or Host Name
   - Destination or Points to Address

Now you will add the DNS record for your domain name at your domain registrar.

4.2.2 Change DNS Records at Domain Registrar

The following procedure describes the process to register a TXT or MX record for your company.
Note: This process requires you to access the domain account with your domain registrar. Contact the domain registrar if you need help accessing your domain account. You may notice differences between your domain name registrar’s process and those described in these instructions.

To change your DNS records at your domain registrar

1. Sign in to your domain name registrar’s website, and then select the domain that you are verifying.
2. In the DNS management area for your account, select the option to add a **TXT** record for your domain.
3. In the **TXT** box for the domain, type or paste the alias or host name that you recorded in the previous Add Domain and Verify Ownership section.
4. In the **Fully qualified domain name (FQDN)** or **Points to** box, type or paste the Destination or Points To Address that you recorded in the Add Domain and Verify Ownership section.
5. Where it asks for TTL information, type **1** to set TTL to **1 hour**.
6. Save your changes, and then sign out of your domain name registrar’s website.
7. Wait 15 minutes. If you are still signed in to the Microsoft Online Services Portal, click Verify.
8. After your domain is verified, click Close.

If you prefer, you can use the following procedure to instead create an MX record to verify your domain in Office 365.

1. Sign in to your domain name registrar’s website, and then select the domain that you are verifying.
2. In the DNS management area for your account, select the option to add a **MX** record for your domain.
3. In the **MX** box for the domain, type or paste the alias or host name that you recorded in the previous Add Domain and Verify Ownership section.
4. In the **Fully qualified domain name (FQDN)** or **Points to** box, type or paste the Destination or Points To Address that you recorded in the Add Domain and Verify Ownership section.
5. Where it asks for TTL information, type **1** to set TTL to **1 hour**.
6. Where it asks for a priority (or preference), type a number that is larger than the number you’ve specified for existing MX records. This can help prevent the new MX record from interfering with mail routing for the domain. Instead of a priority, you may see the following options: **Low, Medium, High**. In this scenario, choose **Low**.
7. Save your changes, and then sign out of your domain name registrar’s website.
8. Wait 15 minutes. If you are still signed in to the Microsoft Online Services Portal click Verify.
9. After your domain is verified, click Close.

If you are no longer signed in:

1. Log on to the Microsoft Online Services Portal with your Office 365 administrator credentials.
2. Click Domains.
3. Select the Pending Verification link next to your domain you added in the earlier step.
4. Click Verify.
5. After your domain is verified, click Close.

Repeat the above steps for any other domains you intend on registering with Office 365.

4.2.3 Create Autodiscover and Sender Policy Framework Records

After you have added and verified a domain, you can enable the Autodiscover service to help your users configure the Office Outlook messaging client. In order to ensure the successful delivery of your email to outside partners, it is also highly recommended that you create a sender policy framework (SPF) record to make sure that other email environments recognize Office 365 and your on-premises email system as valid sources of email from your company.

- **Autodiscover.** Automatically finds the correct Exchange Server host and configures Outlook 2010, Outlook 2007, and Windows Phone and Windows Mobile devices for your users. It also includes an offline address book and the Free-Busy availability service that provides availability information for your users.

- **SPF.** Lets you specify which computers are authorized to transmit email from your domain. This helps to prevent others from using your domain to send SPAM or other malicious email. As more email environments query for Simple Mail Transfer Protocol (SMTP) domain SPF records, you must create or modify your SPF records to allow Exchange Online and your on-premises email system to successfully send email from your domain.

4.2.3.1 Create Sender Policy Framework Record

This procedure modifies records at your domain registrar to include a sender policy framework (SPF) record to allow Microsoft Exchange Online and your on-premises email system to successfully send email from your domain. This procedure is highly recommended, and it is required if your ISP has implemented SPF.
To create an SPF record

1. Log on to your domain registrar. The interface for the registrar Go Daddy (Figure 12) is referenced in the remaining steps.
2. Click to access your account information (for example, My Account).
3. Click the domain that you want to register with Office 365.
4. Click to access details for the domain (for example, Advanced Details).
5. Open the DNS management console (for example, Launch DNS Manager).
6. In TXT or Text section, click Add (for example, Quick Add).
7. Under Host, type @.
8. For the TXT value, type v=spf1 include:outlook.com ~all.
   
   If there is an existing SPF record, you must update it to include the “include: outlook.com” statement in addition to your already declared legitimate hosts.
9. For TTL/time to live, type 1 Hour.

![Figure 12](image)

**Note:** SPF is a relatively new feature and may not be implemented by your ISP. Even if your ISP has not implemented SPF, we recommend that you create an SPF record to make sure your domain is compatible with future enhancements at your ISP.

4.2.4 Create Autodiscover Record

This procedure modifies records at your domain registrar feature to help your users configure Outlook. The interface for the registrar Go Daddy is referenced in procedure and in Figure 13.
To create an external Autodiscover record

1. Log on to your domain registrar.
2. Click on your account information.
3. Click on the domain that you want to register with Office 365.
4. Click on the details for that domain.
5. Open the DNS management.
6. In CNAME or Alias section, click Add.
7. Under Host, type Autodiscover.
8. For the Points to/Destination field, enter autodiscover.outlook.com.
9. In TTL (time to live), type 1 Hour.
10. Click Save.

![Figure 13](image)

11. Wait 15 minutes for the Autodiscover record to register.

Note: Outlook can use either a domain alias (CNAME) or an SRV record to locate Exchange Autodiscover service. You should not add both types of record to the domain. For more information about how to use SRV records for Autodiscover, see the Microsoft Support article [A new feature is available that enables Outlook 2007 to use DNS Service Location (SRV) records to locate the Exchange Autodiscover service](http://support.microsoft.com/kb/958461).

4.2.5 Create Internal Autodiscover Record

If your organization has a split-brain DNS configuration and does not have an Autodiscover record in its internal DNS environment, it is recommended that you create one.

The following procedure demonstrates how to create an Autodiscover record in your internal DNS environment on your Windows DNS Server.
To create an internal Autodiscover record

1. Log on to your internal DNS server or domain controller.
2. Click Start, click Administrative Tools, and then click DNS.
3. Click to expand <yourservername>.
4. Click to expand Forward Lookup Zones.
5. Select the domain for which you would like to create an Autodiscover record.
6. Right-click the domain name and select New Alias (CNAME)....
7. In the Alias Name field, type Autodiscover.
8. Type the fully qualified domain name (FQDN) for the target host (Exchange Server).
9. Click OK.

4.3 User Identity and Account Provisioning Tasks

This section describes the tasks you must perform to prepare your Active Directory environment for establishing directory synchronization with Office 365 service and to install and configure Active Directory Federation Services for single sign-on. For an overview of the single sign-on feature, review the Help topic Prepare for single sign-on.

4.3.1 Update Schema for Exchange Hybrid Deployment

If your organization is implementing an Exchange hybrid deployment, you will need to upgrade your Active Directory schema to the Exchange Server 2010 SP1 version. Before you begin, ensure you have the Exchange Server 2010 SP1 media available, or have downloaded the Exchange Server 2010 SP1 files to an available location.

Note: The domain controller on which you update your schema must be a 64-bit machine and included in the same Active Directory site as the schema master.

To update your Exchange schema for hybrid deployment

1. Log on to your domain controller with an account that has schema administrative rights.
2. Click Start.
3. Click Run.
4. Type CMD.
5. Click OK.
6. Navigate to the location of the Exchange Server 2010 SP1 media or downloaded files.
7. Extract the executable. Note the location where you extract the files.
8. Type CD <space> <directory location of Exchange Server 2010 SP1 binaries>.
   Example: cd c:\exchangeserver2010sp1
10. Type `setup /preparead`.
11. Wait for the tool to copy files, perform pre-requisite checks, and complete the organizational preparation.
12. When complete you should see a message The Microsoft Exchange Server setup operation completed successfully.

### 4.3.2 Clean Up Active Directory

Your organization will need to prepare or “clean up” your Active Directory environment prior to the initial directory synchronization with the Office 365 environment.

**Important:** If Active Directory cleanup is not performed before the deployment process, there can be a significant negative impact to the on-boarding process. It could take days, or even weeks, to iterate through the cycle of syncing, identifying syncing errors, and re-syncing.

In your organization’s Active Directory forest, perform the following clean-up tasks:

- Ensure each user that is assigned Office 365 service offerings has a valid and unique email address. Remove any duplicate ProxyAddress and UserPrincipalName that exists in your forest.
- Populate the following username attributes:
  - First Name
  - Last Name
  - Display Name

**Note:** For a better user experience and more complete global address list (GAL), do not leave these Username attributes blank.

- For optimal use of the Global Address List (GAL), populate the following GAL attributes:
  - Job Title
  - Department
  - Office
  - Office Phone
  - Mobile Phone
  - Fax Number
  - Street Address
  - City
  - State or Province
  - Zip or Postal Code
  - Country or Region
4.3.2.1 Directory Object Preparation

Successful directory synchronization between your on-premises Active Directory environment directory and Office 365 requires that your on-premises directory objects and attributes are properly prepared. For example, you will need to ensure that specific characters are not used in certain Active Directory objects and attributes that are synchronized with the Office 365 environment. These objects and attributes include:

- userPrincipalName
- sAMAccountName
- proxyAddresses
- givenName
- sn (surname)
- displayName
- mailNickname (Exchange alias)
- mail

For details about valid characters associated with these attributes and about additional attribute requirements, see Appendix F: Directory Object Preparation later in this document.

4.3.2.2 Prepare UPN Attribute

Your Active Directory environment must be properly configured in order to work with single sign-on. In particular, the user principal name (UPN) attribute, also known as a user logon name, must be set up for each user in a specific way.

4.3.2.2.1 Add Alternative UPN Suffix to Active Directory

You must add an alternative UPN suffix to associate the user’s corporate credentials with the Office 365 environment. A UPN suffix is the part of a UPN to the right of the @ character. UPNs that are used for single sign-on can contain letters, numbers, periods, dashes, and underscores, but no other types of characters.

**Note:** If you use of more than one UPN, you will require an additional AD FS instance per UPN. See the Office 365 Identity Service Description for more information.

**To add an alternative UPN suffix**

1. Log on to one your organization’s Active Directory domain controllers.
2. Click Start, Administrative Tools, and then click Active Directory Domains and Trusts.
3. In the console tree, right-click Active Directory Domains and Trusts and then click Properties.
4. Select the **UPN Suffixes** tab, type an alternative UPN suffix for the forest, and then click **Add**.

5. Repeat step 3 to add additional alternative UPN suffixes.

**Note:** If your Active Directory domain name ends with a ".local" suffix, you will need to set a UPN that can be registered with Office 365. It is recommended that you use something familiar to the user, such as his or her email domain.

4.3.2.2.2 Match On-Premise UPN with Office 365 UPN

If you have not yet set up Active Directory synchronization, you can skip this task and continue with the next section.

If you have already set up Active Directory synchronization, the user’s UPN for Office 365 may not match the user’s on-premises UPN defined in Active Directory. This can occur when a user was assigned a license before the domain was verified. To remedy this issue, use Windows PowerShell to update users’ UPNs to ensure that their Office 365 UPN matches their corporate user name and domain.

4.3.3 Deploy Federation Server Farm

After your Active Directory environment is properly prepared, you deploy and configure Active Directory Federation Services on-premises to create single sign-on access for your Office 365 users.

The most important operation you need to perform to provide your users with single sign-on access to Office 365 is to deploy a new AD FS 2.0 federation server farm. We recommend that you deploy at least two federation servers and two federation proxy servers in order to provide fault tolerance, load balancing, and scalability to your organization’s AD FS 2.0 production environment.

You should review the Help topic [Plan for and deploy AD FS 2.0 for use with single sign-on](#) before you begin your single sign-on deployment.

4.3.3.1 Pre-Installation Requirements

During the AD FS 2.0 installation process, the setup wizard attempts to automatically check for and, if necessary, install prerequisite applications and dependent hotfixes. In most cases, the setup wizard will install all of the prerequisite applications necessary for AD FS 2.0 to operate and install.

When installing AD FS 2.0 on the Windows Server 2008 platform, you will first need to make sure that Microsoft .NET Framework 3.5 Service Pack 1 (SP1) is installed on the servers running
Windows Server 2008. This is a prerequisite of AD FS 2.0. If .NET Framework 3.5 SP1 is not installed, the AD FS 2.0 Setup Wizard will prevent installation of the AD FS 2.0 software.

You may need to install AD FS 2.0 hotfixes after you have installed AD FS 2.0. For more information, see the TechNet article Install the AD FS 2.0 Software.

You must complete the following tasks before you set up the single sign-on feature.

- Deploy on-premises Active Directory Federation Services federation and proxy servers. Proxy servers are necessary for remote access for users without a VPN.
- Add your Active Directory Federation Services server(s) to your Active Directory forest.
- Create a service account in Active Directory to deploy Active Directory Federation Services in a farm.
- Download the Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0).
- Download Active Directory Federation Services 2.0 installation package. The following roles and features will be automatically be installed in the process:
  - Windows PowerShell
  - .NET Framework 3.5 SP1
  - Internet Information Services (IIS) 7
  - Windows Identity Foundation
- Download and install the Microsoft Online Services Module for Windows PowerShell.
- Download the Office 365 desktop setup.
- Install and configure SQL Server 2008 (Standard or Enterprise) if your organization has more than 30,000 users who will use Office 365 service offerings.
- Configure an external DNS Host (A) Record for your AD FS Proxy (example sts.contoso.com).
- Prepare for trusted third-party SSL certificate (for example, Go Daddy or VeriSign) with AD FS instance name (example, sts.contoso.com).

The instructions in the next sections include how to obtain your certificate and configure it for AD FS.

**Note:** Certificates are an integral part of deploying AD FS with Office 365 identity federation. It is highly suggested that you attain a separate certificate with the name of your AD FS endpoint (sts.contoso.com) with a trusted third-party SSL provider. Additionally, if your organization leverages wildcard certificates (*.contoso.com), review your third-party SSL providers documentation on creating and exporting wildcard certificates prior to proceeding on with this document.
4.3.3.2 Join Federation Servers to Your Domain

You must join your federation servers to the Active Directory domain where you authenticate users.

Note: You can ignore this step if you will use existing domain controllers for federation.

► To join your federation servers to the domain

1. On the computer that you want to join to a domain, click Start, click Control Panel, and then double-click System.
2. Under Computer name, domain, and workgroup settings, click Change settings.
3. On the Computer Name tab, click Change.
4. Under Member of, click Domain and type the name of the domain that the computer will join.
5. Click OK.

4.3.3.3 (Optional) Add Resource Record to Corporate DNS for NLB Cluster

For clients on your corporate network to successfully access the federation service, you must first create a host (A) resource record in the corporate DNS that resolves the cluster DNS name of the federation service (for example, fs.fabrikam.com) to the cluster IP address in the corporate network (for example, 172.16.1.3). You can use the following procedure to add a host (A) resource record to the corporate DNS for the NLB cluster.

Note: This procedure is optional if you are not using a hardware network load balancer (NLB).

► To add a resource record to corporate DNS for the cluster DNS name configured on the corporate NLB host

1. On a DNS server for the corporate network, open the DNS snap-in.
2. In the console tree, right-click the applicable forward lookup zone (for example, fabrikam.com), and then click New Host (A or AAAA).
3. In the Name box, type only the computer name of the federation server or federation server cluster; for example, for the fully qualified domain name (FQDN) fs.fabrikam.com, type fs.
4. In the IP address box, type the IP address for the federation server or federation server cluster (for example, 172.16.1.3).
5. Click Add Host.
Important: It is assumed that you are using a DNS server running Windows 2000 Server, Windows Server 2003, or Windows Server 2008 with the DNS Server service to control the DNS zone.

4.3.3.4 Request and Import Server Authentication Certificate to Default Web Site

This section describes the tasks you perform to request a certificate and import it to the Default Web site on your AD FS server.

You will later export this certificate and import it to all computers that you configure to be part of the federation server farm.

4.3.3.4.1 Active Directory Federation Services Certificate

After Active Directory Federation Services is installed, you will need to request a certificate.

Note: The common name of your certificate will match the URL that will point your users to AD FS. For example, sts.contoso.com will route your users to https://sts.contoso.com/adfs/ls. It is very important that the common name value matches the name of the AD FS website for Office 365. If the value does not match, users will be prompted with a certificate warning.

To request an AD FS certificate

1. Log on to your AD FS server.
2. Click Start.
3. In the search dialog box, type Internet Information Server.
4. Click Internet Information Server (IIS) Manager in the search results.
5. Click to expand your <servername>.
6. Double-click Server Certificates.
7. Under the Actions choices, click Create Certificate Request.
8. In the Request Certificate dialog box, populate the fields listed.
   - Common name: sts.<yourcompany>.com (suggested value)
   - Organization: Your organization's name
   - Organizational Unit: Value you may designate
   - City/locality: City/locality location of your organization
   - State/province: State/province of your organization
   - Country/region: Country/region of your organization
9. Click Next.
10. Select Microsoft RSA SChannel Cryptographic Provider (default).
11. For bit length, choose 2048, then click Next.
12. In the **Specify a file name for the certificate request** window, type a file name (for example, C:\adfsCertificateRequest.txt).
13. Click **Finish**.

4.3.3.4.2 Create Certificate Request with Third-Party SSL Certificate Provider

**Note:** You may skip this step if you already have multiple domains Unified Communications Certificates (UCC) or wildcard certificates with your third-party SSL certificate provider.

If this is the first time that your organization has attained third-party SSL certificates, consider using either a UCC or a wildcard certificate for your organization if you need to have multiple certificates under the same domain name as shown in the following example:

- sts.contoso.com (AD FS)
- mail.contoso.com (Exchange)
- contoso.com (website)

Be sure to review your third-party SSL provider’s documentation for more information on creating a certificate request. If you are unsure on what type(s) of certificates to attain for your organization, a single domain SSL is suggested for each name space for which you desire a certificate.

**Note:** In the procedures that follow, the steps reference the web interface of the domain registrar GoDaddy for example purposes.

► **To create a third-party SSL certificate request**

1. Log on to your AD FS server.
2. Open Internet Explorer.
3. Enter the URL of your preferred third-party SSL certificate provider (for example, http://www.godaddy.com).
4. Create an account with the third party SSL certificate provider if you do not have one already.
5. Sign in to your account with your username and password.
6. To purchase an SSL certificate, choose **SSL & Security**.
7. Chose **Single Domain SSL**.
8. Complete the purchase of your certificate (if applicable).
9. On the right hand side of the screen, click **My Account**.
10. Under My Products, select **SSL Certificates**.
11. Select your new certificate.
12. Choose **Request Certificate** in the bottom right corner.
13. Click **Start** and type `C:\adfs.certificaterequest.txt` (or the file location and name you provided in your certificate request).
14. Press **Enter**. The certificate text file will open in Notepad.
15. In Notepad, click **Edit**.
16. Choose **Select All**.
17. Click **Edit**.
18. Choose **Copy**.
19. In Internet Explorer, on your domain registrar page, choose **Third Party or Dedicated Server or Virtual Dedicated Server without Simple Control Panel**.
20. Under **Enter your Certificate Signing Request (CSR) below**, right-click on the blank portion of the screen.
21. Chose **Paste**.
22. Click **OK**.
23. Verify the domain name is correct. The domain name `sts.contoso.com` should match your AD FS website URL (for example, `https://sts.contoso.com/adfs/ls`).
24. Click **Next**.
25. Click **Finish**.

**4.3.3.4.3 Download Certificate from Third-Party SSL Certificate Provider**

Now you will download the certificate that you created with your domain registrar.

► **To download a third-party SSL certificate**

1. Log on to your AD FS server.
2. Open the Internet Explorer browser.
3. Enter the URL of your preferred third-party SSL certificate provider (for example, `http://www.godaddy.com`).
4. Log on with your username and password.
5. Under My Products, select **SSL Certificates**.
6. Check the box next to the name of your certificate you created earlier (for example, `sts.contoso.com`).
7. Check **Manage Certificate**.
8. Check the box next to the name of your certificate.
9. Choose **Download**.
10. In **Select your server type**, select **IIS**.
11. Click **Download**.
12. In the **File Download** dialog box, choose **Save**.
13. Type the name of the certificate. Be sure to include the file extension (for example, `c:\sts.contoso.com.zip`). You may choose a different folder location to save the file.
14. Double-click on the file you just saved (for example, c:\sts.contoso.com.zip).
15. At the top of Windows Explorer window, click Extract all files.
16. Choose the default directory or a different directory.
17. Click Extract.

4.3.3.4.4 Install Third-Party SSL Certificate

After you have downloaded your certificate, you install it on your AD FS server.

► To install a third-party SSL certificate

1. Log on to your AD FS server.
2. Click Start.
3. In the search dialog box, type Internet Information Server.
4. In the search results, click Internet Information Server (IIS) Manager.
5. Click to expand <servername>.
6. Double-click Server Certificates.
7. Under the Actions pane, click Create Certificate Request.
9. Click the Browse button.
10. In the file name containing the certification authority’s response, type the path of the certificate you created with your domain registrar (for example, c:\sts.contoso.com) (for example, c:\sts.contoso.com).
11. Next to the File Name field, choose *. *
12. Select the name of your certificate (for example, c:\sts.contoso.com\) and click Open.
13. Type a friendly name for the certificate (for example, AD FS Certificate or sts.contoso.com).
14. Click OK.

4.3.3.4.5 Configure Third-Party SSL Certificate

After you install the certificate on your AD FS server, you must configure it.

► To configure the third-party SSL certificate

1. Log on to your AD FS server.
2. Click Start.
3. In the search dialog box, type Internet Information Server.
4. In the search results, click Internet Information Server (IIS) Manager.
5. Expand your <servername> folder.
6. Expand the Sites folder.
7. Click Default Web Site.
8. In the Actions pane, click Bindings.
9. Click https.
10. Click Edit.
11. Select your certificate (for example, sts.contoso.com) in the SSL certificate dialog box.
12. Choose the IP address for which IIS will listen to the request for https://sts.contoso.com, or leave the default setting.
13. Click OK.

4.3.3.5 Create Dedicated Service Account

Before you install Active Directory Federation Services, you must first create a service account for the federation server farm.

► To create an ADFS service account

1. Log on to a domain controller in your Active Directory forest.
2. Click Start, select All Programs, and click Administrative Tools.
3. Click Active Directory Users and Computers.
   (Optional) Right-click Active Directory Users and Computers and select the domain you would like to create the service account.
4. Right-click the Organizational Unit you would like to create your ADFS service account in (for example, Users) and select New, and then User.
5. Enter the values in the required fields (First Name, Initial, Last Name, Full Name, User logon name, and User logon name (pre-Windows 2000). (An example of a User logon name is svc_adfs).
6. Click Next.
7. Enter a Password and re-enter password in the Confirm Password field.
8. In the checkboxes, the following is recommended:
   o Select User cannot change password.
   o Select Password never expires.
   o Deselect User must change password at next logon.
9. Click Next.
10. Click Finish.

4.3.3.6 Install AD FS 2.0 Software

After you have created an AD FS service account you can install Active Directory Federation Services. You will need to download the AD FS software package at Active Directory Federation Services 2.0 RTW to perform this step.

► To install AD FS 2.0

1. Download the AD FS 2.0 software package for your operating system (either Windows Server 2008 or Windows Server 2008 R2) and save the AdfsSetup.exe setup file to the computer.
2. Navigate to and double-click AdfsSetup.exe.
3. On the Welcome to the AD FS 2.0 Setup Wizard page, click Next.
4. On the End-User License Agreement page, read the license terms.
5. If you agree to the terms, select the I accept the terms in the License Agreement check box, and then click Next.
6. On the Server Role page, select Federation server, and then click Next.
7. On the Completed the AD FS 2.0 Setup Wizard page, click Finish.

In some instances, the AD FS 2.0 installation may require a restart (for example, when dependent hotfixes have been installed).

4.3.3.7 Configure First Federation Server in Federation Server Farm

After you have installed AD FS on the computer, you can set up the computer to become the first federation server in a new federation server farm. You do this using the AD FS 2.0 Federation Server Configuration Wizard. Membership in Domain Admins or a delegated domain account that has been granted write access to the Program Data container in Active Directory is the minimum requirement to complete this procedure.

►To create the first federation server to the federation server farm
1. Click Start, Administrative Tools, AD FS 2.0 Management and open the AD FS 2.0 Management snap-in.
2. On the Overview page, click the AD FS 2.0 Federation Server Configuration Wizard link.
3. On the Welcome page, verify that Create a new Federation Service is selected, and then click Next.
4. On the Select Stand-Alone or Farm Deployment page, click New federation server farm, and then click Next.
5. On the Specify the Federation Service Name page, verify that the SSL certificate that is showing matches the name of the certificate that was imported into the Default Web Site in IIS previously. If this is not the correct certificate, select the appropriate certificate from the SSL certificate list.

Note: The configuration wizard will not allow you to override the certificate if an SSL certificate is configured for IIS. This ensures that any intended prior IIS configuration for SSL certificates is preserved. To work around this issue, you can go back and import the certificate to the Default Web Site of IIS again.

6. If you have previously reinstalled AD FS on this computer, then the Existing AD FS Configuration Database Detected page appears. If that page appears, click Delete database, and then click Next.
7. On the **Specify a Service Account** page, click **Browse**. In the Browse dialog box, locate the domain account that will be used as the service account in this new federation server farm, and then click **OK**. Type the password for this account, confirm it, and then click **Next**.

8. On the **Ready to Apply Settings** page, review the details. If the settings appear to be correct, click **Next** to begin configuring AD FS 2.0 with these settings.

9. On the Configuration Results page, review the results. When all the configuration steps are finished, click **Close** to exit the wizard.

When you finish the steps in this procedure, the AD FS 2.0 Management snap-in will automatically open and a message will display indicating that the required configuration is incomplete and that you should add a trusted relying party. You can disregard this message. A relying party trust for Office 365 will be added in a later step and the message will no longer display in the AD FS 2.0 Management snap-in.

### 4.3.3.8 Add Federation Server to Federation Server Farm

To add another federation server to the server farm, you install the AD FS 2.0 software and configure the required certificates on a computer. You can then configure the computer to become a federation server in the federation server farm.

### 4.3.3.8.1 Export and Import AD FS Federation Server Certificate

Before you configure computers as federation farm servers, you need to export the certificate from the first federation server and import it to any computer you want to add to the federation server farm.

**To export the AD FS federation server certificate**

1. Log on to the first AD FS federation server that you deployed on-premises.
2. Click **Start**, type **Internet Information Services (IIS) Manager**, and click **Internet Information Services (IIS) Manager**.
3. On the **Home** page, click to expand `<servername>`.
4. In **Features View**, double-click **Server Certificates**.
5. Right-click your third-party SSL server certificate (for example, `sts.contoso.com`) and select **Export**.
6. In the **Export to** field, enter a path on your local computer (for example, `\sts.contoso.com`). A .pfx extension will automatically be added to the file you create.
7. In the **Password** field, enter a password.
8. In the **Confirm** password field, enter the same password.
9. Locate the file you created (for example, `c:\sts.contosto.com.pfx`).
10. Copy the file to the computers that you will add to AD FS federation server farm.
4.3.3.8.2 Configure Federation Server Farm Computer

You join a computer to a farm with the AD FS 2.0 Federation Server Configuration Wizard. When you use this wizard to join a computer to an existing farm, the computer is configured with a read-only copy of the AD FS configuration database and it must receive updates from a primary federation server.

► To configure a federation server to the federation server farm

1. To open the AD FS 2.0 Management snap-in, click Start, Administrative Tools, and then AD FS 2.0 Management.
2. On the Overview page or in the Actions pane, click AD FS 2.0 Federation Server Configuration Wizard.
3. On the Welcome page, verify that Add a federation server to an existing Federation Service is selected, and then click Next.
4. If the AD FS 2.0 database that you selected already exists, the Existing AD FS Configuration Database Detected page appears. If that occurs, click Delete database, and then click Next.

⚠️ Caution: Select this option only when you are sure that the data in this AD FS 2.0 database is not important or that it is not used in a production federation server farm.

5. On the Specify the Primary Federation Server and Service Account page, under Primary federation server name, type the computer name of the primary federation server in the farm, and then click Browse.
6. In the Browse dialog box, locate the domain account that is used as the service account by all other federation servers in the existing federation server farm, and then click OK.
7. Type the password and confirm it, and then click Next.

⚠️ Note: For more information about creating this service account, see the Create Dedicated Service Account procedure provided earlier in this document. Each federation server in the federation server farm must specify the same service account for the farm to be operational. For example, if the service account created was contoso\svc_adfs, each computer you configure for the federation server role and that will participate in the same farm must specify contoso\svc_adfs at this step in the Federation Server Configuration Wizard for the farm to be operational.

8. On the Ready to Apply Settings page, review the details. If the settings appear to be correct, click Next to begin configuring AD FS 2.0 with these settings.
9. On the **Configuration Results** page, review the results. When all the configuration steps are finished, click **Close** to exit the wizard.

### 4.3.3.9 Verify Federation Server Is Operational

You can use either of the following procedures to verify that a federation server is operational; that is, that any client on the same network can reach a new federation server.

**► Procedure 1: To verify that the federation server is operational**

1. Log on to a client computer that is located in the same forest as the federation server.
2. Open a browser window, in the address bar type the federation server’s DNS host name, and then append `/adfs/fs/federationserverservice.asmx` to it for the new federation server, for example:

   ```
   https://fs1.contoso.com/adfs/fs/federationserverservice.asmx
   ```
3. Press ENTER, and then complete the next procedure on the federation server computer.

   **Note:** If you see the message **There is a problem with this website’s security certificate**, this is because the FQDN used is different from the names registered in the certificate; however, this issue will be resolved with farm configuration and DNS record creation. Click **Continue to this website**.

**► Procedure 2: To verify that the federation server is operational**

1. Log on to the new federation server as an Administrator.
2. Click **Start**, point to **Administrative Tools**, and then click **Event Viewer**.
3. In the Details pane, double-click **Applications and Services Logs**, double-click **AD FS 2.0 Eventing**, and then click **Admin**.
4. In the **Event ID** column, look for event ID 100. If the federation server is configured properly, you see a new event—in the **Application** log of Event Viewer—with the event ID 100. This event verifies that the federation server was able to successfully communicate with the Federation Service.

### 4.3.3.10 Install Microsoft Online Services Sign-In Assistant

The Microsoft Online Services Sign-In Assistant must be installed on federation server. The Sign-In Assistant can be downloaded at the [Microsoft Online Services Portal](https://portal.microsoftonline.com).

**► To install the Microsoft Online Services Sign-In Assistant**

1. Log on to your AD FS federation server.
2. Click **Start**.
3. In the search dialog box, type the location where you saved the Sign-In Assistant installation package.
4. Double-click the .msi file for the package and then click Run.
5. At the Welcome screen, click Next.
6. Select the default directory for installation (you may change this if needed) and click Install.
7. When the installation is complete, click Finish.
8. Allow the tool to find any necessary patches to install and then restart the server.

4.3.3.11 Install Microsoft Online Services Module for Windows PowerShell

In order to configure single sign-on, you must install the Microsoft Online Services Module for Windows PowerShell. You can download the tool at the Microsoft Office 365 Help site.

► To install the Microsoft Online Services Module for Windows PowerShell

1. Log on to your AD FS server.
2. Click Start.
3. In the search dialog box, type the location where you downloaded and saved the installer file for the Microsoft Online Services Module for Windows PowerShell (for example, c:\FederationConfig.msi).
4. Double-click the installer file.
5. Click Run.
6. Click Next.
7. Review and accepts the license terms and click Next.
8. Select the default directory and options and click Next.
9. Click Install.
10. Click Finish.

4.3.3.12 Enable Single Sign-On

After you have installed the Microsoft Online Services Module for Windows PowerShell, you run a series of commands in the Windows PowerShell command-line interface to enable the single sign-on feature.

► To enable single sign-on with Office 365

1. Log on to your AD FS server.
2. Open Microsoft Online Services Module for Windows PowerShell. PowerShell will open.
3. Type cd\ and press Enter.
4. Type $cred=Get-Credential and press Enter.
5. Enter your Office 365 administrator name and password and click OK.
6. Type `Connect-MsolService -Credential $cred` and press **Enter**.
7. Type `Set-MsolAdfscontext -Computer <AD FS 2.0 primary server>`
   
   *Note:* `<AD FS 2.0 primary server>` is the internal FQDN name of the primary AD FS 2.0 server. This cmdlet creates a context that connects you to AD FS 2.0.
8. Press **Enter**.
9. Type `New-MsolFederatedDomain -DomainName <domain>`
   
   *Example:* `New-MsolFederatedDomain -DomainName contoso.com`
10. Press **Enter**.
11. Using the information provided by the results of the `New-MsolFederatedDomain` cmdlet, contact your domain registrar to create the required DNS record. This record verifies that you own the domain.
12. Type `New-MsolFederatedDomain` a second time, specifying the same domain name to finalize the process and press **Enter**.

### 4.3.3.13 Verify Single Sign-on Functionality

After setting up single sign-on, you should verify that it is working correctly.

**To verify single sign-on functionality**

1. Sign in to the [Microsoft Online Services Portal](https://portal.microsoftonline.com).
2. In the portal header, click **Admin**.
3. Under **Management**, click **Users**.
4. Select your Microsoft User ID or a test User ID that has been synchronized into the Office 365 service. Ensure you know the username and password in your on-premises Active Directory and that the user you have selected has a username (UserPrincipalName) that matches the domain you have federated.
5. Select the check box beside the test user.
6. Click the user’s Display Name. (For example, *John Smith*).
7. On the **Licenses** page for the user, select a license for the user (for example, *Microsoft Office 365 (Plan X)*).
8. Click **Save**.
9. Select the location of the user (for example, *United States*).
10. Click **Save**.
11. Now log on to a PC.
12. Open Internet Explorer.
14. In the **Microsoft Online Services ID** field, type the user name for the user you assigned a license to (for example, `jsmith@contoso.com`).
15. The web page should display with **You are now required to sign in at**
<yourdomainname.com>.

16. Click the sign-in link and enter your on-premises Active Directory credentials for the account you chose (for example, username jsmith@contoso.com and password Orang312).

17. If the home screen to the Microsoft Online Services Portal is displayed (Figure 14) after signing in, it indicates that single sign-on is working properly.

![Figure 14](image)

### 4.3.4 Deploy Federation Proxy Server

You deploy AD FS 2.0 federation servers in the proxy role to act as a proxy for client logons to a federation server that is located in the corporate network. The federation server proxy also facilitates the distribution of security tokens for remote clients that are attempting to access Office 365 service offerings.

Before you get started, note the following:

- It is recommended that you deploy at least two federation proxy servers in order to provide fault tolerance and deploy an NLB host or third-party hardware load balancer for fault tolerance and load balancing.
- You can also use third-party HTTP reverse proxies solutions to publish AD FS to the extranet.
- To complete all of the tasks using the procedures in this section you must log on to the computers as a member of the Administrators group, or have been delegated equivalent permissions.

Table 19 and 20 are checklists of the deployment tasks that are necessary to deploy two federation server proxies that will redirect authentication requests to a federation server in your new federation server farm.
Table 19. Checklist: Prepare Network Infrastructure for Federation Server Proxies

<table>
<thead>
<tr>
<th>Deployment task</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare two computers running either the Windows Server 2008 or Windows Server 2008 R2 operating system to be set up as federation server proxy. Depending on the number of users you have, you can use existing web or proxy servers or use a dedicated computer.</td>
<td>☐</td>
</tr>
<tr>
<td>Add the name of the Federation Service in the corporate network (the cluster DNS name you created earlier on the NLB host in the corporate network) and its associated cluster IP address to the hosts files on each federation server proxy machine in the perimeter network.</td>
<td>☐</td>
</tr>
<tr>
<td>Create a new cluster DNS name and cluster IP address on the NLB host in the perimeter network and then add the federation server computers to the NLB cluster. If you are using Windows Server technology for your current NLB hosts, choose the appropriate link to the right based on your operating system version.</td>
<td>☐</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td></td>
</tr>
<tr>
<td>The cluster DNS name used for this new NLB cluster must match the name of the Federation Service in the corporate network.</td>
<td></td>
</tr>
<tr>
<td>Create a new resource record for the NLB cluster in the perimeter network DNS that points the cluster DNS name of the NLB cluster to its cluster IP address.</td>
<td>☐</td>
</tr>
<tr>
<td>Use the same server authentication certificate as the one used by the federation servers in the corporate network and install it in IIS on the Default Web Site of the federation server proxy.</td>
<td>☐</td>
</tr>
</tbody>
</table>

Table 20. Deploy Federation Server Proxies

<table>
<thead>
<tr>
<th>Deployment task</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the AD FS 2.0 software on the computer that will become the federation server proxy.</td>
<td>☐</td>
</tr>
<tr>
<td>Configure the AD FS 2.0 software on the computer to act in the federation server proxy role by using the AD FS 2.0 Federation Server Proxy Configuration Wizard.</td>
<td>☐</td>
</tr>
<tr>
<td>Using Event Viewer, verify that the federation server proxy service has started.</td>
<td>☐</td>
</tr>
</tbody>
</table>

4.3.4.1 Export and Import AD FS Federation Server Certificate

To start the your AD FS proxy server deployment, you export your AD FS federation server certificate and then import it to the Default Web Site for each federation server proxy in your organization.

►To export the AD FS federation server certificate

1. Log on to your AD FS federation server that you deployed on-premises.
2. Click Start, type Internet Information Services (IIS) Manager, and click Internet Information Services (IIS) Manager.
3. On the Home page, click to expand <servername>.
4. In Features View, double-click Server Certificates.
5. Right-click your third-party SSL server certificate (for example, sts.contoso.com) and select Export....
6. In the Export to: field, enter a path on your local computer (for example, c:\sts.contoso.com). A .pfx extension will automatically be added to the file you create.
7. In the Password field, enter a password.
8. In the Confirm password field, enter the same password.
9. Locate the file you created (for example, c:\sts.contoso.com.pfx).
10. Copy the file to your AD FS proxy server.

Import Server Authentication Certificate to Default Web Site

After you obtain a server authentication certificate used by one of the federation servers in your corporate network, you must manually install that certificate on the Default Web Site for each federation server proxy in your organization.

Because this certificate must be trusted by clients of AD FS 2.0, use an SSL certificate that is issued by a public certificate authority (CA) that is subordinate to a publicly trusted root (for example, VeriSign or Thawte). For information about installing a certificate from a public CA, see the TechNet article Request an Internet Server Certificate.

Note: The subject name of this server authentication certificate must match the FQDN of the cluster DNS name (for example, fs.contoso.com) that you created earlier on the NLB host. If Internet Information Services (IIS) has not been installed on the proxy server, you must install IIS first in order to complete this task. When installing IIS for the first time, we recommend that you use the default feature options when prompted during the installation of the server role.

To import a server authentication certificate to the Default Web Site on the proxy server

1. Click Start, point to All Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. In the console tree, click ComputerName.
3. In the center pane, double-click Server Certificates.
4. In the Actions pane, click Import.
5. In the Import Certificate dialog box, click the ... button.
6. Browse to the location of the Personal Information Exchange (.pfx) certificate file, highlight it, and then click Open.
7. Type a password for the certificate, and then click OK.
4.3.4.2 Add Cluster DNS Name and IP Address to Hosts File

In order for the federation server proxy to work as expected in the perimeter network, you must add an entry to the hosts file on each federation server proxy computer that points to the cluster DNS name hosted by the NLB in the corporate network (for example, fs.fabrikam.com) and its IP address (for example, 172.16.1.3). Adding this entry to the hosts file enables the federation server proxy to properly route a client-initiated call to a federation server either within the perimeter network or outside the perimeter network.

To add the cluster DNS name and IP address to the hosts file on the proxy server

1. Navigate to the %systemroot%\Winnt\System32\Drivers directory folder and locate the hosts file.
2. Start Notepad, and then open the hosts file.
3. Add the IP address and the host name of a federation server in the account partner to the hosts file, as shown in the following example:
   
   172.16.1.3   fs.fabrikam.com

4. Save and close the file.

Caution: If the cluster IP address ever changes on the NLB host in the corporate network, you must update the local hosts file on each federation server proxy.

4.3.4.3 Add Resource Record to Perimeter DNS for Cluster DNS Name

To service authentication requests from clients either in the perimeter network or outside the perimeter network, AD FS 2.0 requires name resolution to be configured on external-facing DNS servers that host the organization’s zone (for example, fabrikam.com).

To do this, add a Host (A) Resource Record to the external-facing DNS server that serves only the perimeter network for the cluster DNS name (for example, “fs.fabrikam.com”) to point to the external cluster IP address that has just been configured.

To add a resource record to the perimeter DNS for the cluster DNS name configured on the perimeter NLB host

1. On a DNS server for the perimeter network, click Start, point to Administrative Tools, and then click DNS.
2. In the console tree of the DNS snap-in, right-click the applicable forward lookup zone (for example, fabrikam.com), and then click New Host (A or AAAA).
3. In the Name box, type only the name of the cluster DNS name you specified on the NLB host in the perimeter network (this should be the same DNS name as the name of the Federation Service). For example, for the FQDN fs.fabrikam.com, type fs.
4. In the **IP address** box, type the IP address for the new cluster IP address you specified on the NLB host in the perimeter network (for example, **192.0.2.3**).
5. Click **Add Host**.

### 4.3.4.4 Install the AD FS 2.0 Software on Proxy Computer

You must install the AD FS 2.0 software on any computer that you are preparing for the federation server proxy role. You can install this software by either using the AD FS 2.0 Setup Wizard or by using a command line parameter. For more information about this parameter, see the [AD FS 2.0 Deployment Guide](#).

Make sure to complete the installation process by installing all of the required hotfixes on each federation proxy server, as indicated by the last step in this procedure.

► **To install the AD FS 2.0 software on the proxy computer**

1. Download the AD FS 2.0 software package for your specific operating system version (either Windows Server 2008 or Windows Server 2008 R2) by saving the **AdfsSetup.exe** setup file onto the computer. To download this file, go to [Active Directory Federation Services 2.0 RTW](#).
2. Locate and double-click the **AdfsSetup.exe** setup file that you downloaded to the computer.
3. On the **Welcome to the AD FS 2.0 Setup Wizard** page, click **Next**.
4. On the **End-User License Agreement** page, read the license terms.
5. If you agree to the terms, select the **I accept the terms in the License Agreement** check box, and then click **Next**.
6. On the **Server Role** page, select **Federation server proxy**, and then click **Next**.
7. On the **Completed the AD FS 2.0 Setup Wizard** page, verify that the **Start the AD FS 2.0 Federation Server Proxy Configuration Wizard when this wizard closes** check box is selected, and then click **Finish** to restart the computer.

### 4.3.4.5 Configure Federation Server Proxy Role

After you configure the computer with the required certificates and have installed the AD FS 2.0 software, you are ready to configure the computer to become a federation server proxy. You can use the following procedure so that the computer acts in the federation server proxy role.

⚠️ **Important**: Before you use this procedure to configure the federation server proxy computer, make sure that you have completed your federation server farm deployment as described in the [Server Farm Deployment Checklists](#) section. Make sure that at least one federation server is deployed and that all the necessary credentials for authorizing a federation server proxy configuration are implemented. You must also configure Secure Sockets Layer (SSL)
bindings on the Default Web Site, or this wizard will not start. All these tasks must be completed before this federation server proxy can function.

After you finish setting up the computer, verify that the federation server proxy is working as expected. For more information, see the Verify Federation Server Proxy Is Operational section of the document.

To configure the computer for the federation server proxy role

1. On the Completed the AD FS 2.0 Setup Wizard page in the AD FS 2.0 Setup Wizard, the check box Start the AD FS 2.0 Federation Server Proxy Configuration Wizard when this wizard closes is selected by default.
2. Start the wizard, and on the Welcome page, click Next.
3. On the Specify Federation Service Name page, under Federation Service name, type the name that represents the Federation Service for which this computer will act in the proxy role (for example, fs.contoso.com).
4. Based on your specific network requirements, determine whether you will need to use an HTTP proxy server to forward requests to the Federation Service. If so, select the Use an HTTP proxy server when sending requests to this Federation Service check box, under HTTP proxy server address type the address of the proxy server, click Test Connection to verify connectivity, and then click Next.
5. When you are prompted, specify the credentials that are necessary to establish a trust between this federation server proxy and the Federation Service.

By default, only the service account used by the Federation Service or a member of the local BUILTIN\Administrators group can authorize a federation server proxy.

6. On the Ready to Apply Settings page, review the details. If the settings appear to be correct, click Next to begin configuring this computer with these proxy settings.
7. On the Configuration Results page, review the results. When all the configuration steps are finished, click Close to exit the wizard.

4.3.4.6 Verify Federation Server Proxy Is Operational

You can use the following procedure to verify that the federation server proxy can communicate with the Federation Service in AD FS 2.0. You run this procedure after you run the AD FS 2.0 Federation Server Proxy Configuration Wizard to configure the computer to run in the federation server proxy role.

Important: The result of this test is the successful generation of a specific event in Event Viewer on the federation server proxy computer.
To verify that the federation server proxy is operational

1. Log on to the federation server proxy as an Administrator.
2. Click Start, point to Administrative Tools, and then click Event Viewer.
3. In the details pane, double-click Applications and Services Logs, double-click AD FS 2.0 Eventing, and then click Admin.
4. In the Event ID column, look for event ID 198.

If the federation server proxy is configured properly, you will see a new event in the Application log of Event Viewer, with the event ID 198. This event verifies that the federation server proxy service was started successfully and now is online.

4.3.4.7 Testing Naming Services

You now can test network connectivity to your AD FS federation and proxy servers.

Internal Network Test

In your DNS environment, you should have an entry for your AD FS instance (sts.contoso.com), or your local hosts file should be modified to point to your AD FS instance, (sts.contoso.com) to your AD FS federation server.

1. Log on to your AD FS proxy server you deployed on-premises in your edge network.
2. Click Start, and then click Run.
3. Type CMD and then click OK.
4. Type ping <space> and then your federation name (for example, sts.contoso.com).
5. Press Enter.

For example, the response you receive is 167.2.2.1, a reply from your internal network.

External Network Test

You should be able to ping sts.contoso.com from a computer and reach the externally facing AD FS proxy server.

1. Log on to a computer.
2. Click Start, and then click Run.
3. Type CMD and then click OK.
4. Type ping <space> and the name of your federation name (for example, sts.contoso.com).

For example, the response you receive is a reply from 65.64.63.123 (your external network).
4.3.4.8 Post Installation Validation

You can verify that single sign-on was set up correctly by testing it further. This topic also gives you information about optional maintenance tasks to keep identity federation running smoothly.

1. Log on to a computer.
2. Open Internet Explorer and type https://portal.microsoftonline.com in the address bar.
3. In the Microsoft Online Services ID field, type your user name (for example, jsmith@contoso.com).
4. The web page should update with You are now required to sign in at <yourdomainname.com>.
5. Click the sign-in link and, in the Sign In page (Figure 15), enter your on-premises Active Directory credentials for the account you chose (for example, username jsmith@contoso.com and password Orang312).

![Figure 15](image)

6. If you are presented with the Microsoft Online Services Portal home screen (Figure 16), this indicates that your proxy server with identity federation is working properly.
4.3.5 Advanced Option: Deploy Federation Services with SQL Server

The AD FS configuration database stores all the configuration data that represents a single instance of AD FS 2.0 (also known as the Federation Service). You can store this configuration data in either a Microsoft SQL Server® database or using the Windows Internal Database (WID).

As indicated in the Capacity Planning section of this document, customers with 15,000-60,000 users or more and multiple federation servers in the farm may want to consider using a SQL Server-based policy store. An AD FS 2.0 federation server farm configured to use WID supports a maximum of five federation servers. If you need more than five federation servers, you need to configure a SQL Server database to store the AD FS 2.0 configuration database.

4.3.5.1 Installation Steps

These steps provide a high-level instruction on how to install AD FS for use with SQL Server.

► To install SQL Server AD FS configuration database

1. Install the full version (not Express version) of SQL Server 2005 or higher in your on-premises environment. Note whether you install using the default instance or with an instance name as this is important later during the configuration process.
2. Install the AD FS Core Services onto a machine designated to run this service. Best practice is to install on a Windows Server 2008 R2/x64 with plenty of memory.
3. After the AD FS Core Services installation stops, do not d to Configuration when asked. Uncheck the configuration option and close the application.
4. Now navigate to the following location: c:\program files\Active Directory Federation Services 2.0
5. Run the following command:

```
FSConfig.exe CreateSQLFarm /ServiceAccount "domain\user" /ServiceAccountPassword "password" /SQLConnectionString "database=AdfsConfigurationServer;server=MSSQLSERVER\Instance [as needed];integrated security=SSPI" /port 443 /FederationServiceName "sts.contoso.com" /AutoCertRolloverEnabled
```

Notes:
• `/ServiceAccount`: Must be created before this command is run
• `Server`: Should either be the MSSQLSERVER which is the default install for SQL or MSSQLSERVER\Instance if an instance has been created for use with the AD FS Services.
• `/FederationServiceName`: Should refer to the Common Name of your certificate used for your AD FS Services

### 4.3.5.2 Configure Communication with Federation Gateway
After the AD FS server has been configured to use SQL, use the following steps to configure the server to communicate with the Microsoft Federation Gateway.

1. Download and install the Microsoft ID components.
2. Run the following PowerShell cmdlets to create your custom federated domain:

   ```
   $cred = Get-Credential [Enter your Online Admin Account]
   Connect-MsolService -Credential $cred
   Set-MsolAdfscontext -Computer <AD FS 2.0 primary server internal FQDN>
   New-MsolFederatedDomain -DomainName <domain>
   ```

#### 4.3.5.2.1 Install Second or future AD FS Core Services with Full SQL
1. Follow the above steps but change the command to Join the SQL Farm instead of creating, as it has already been created.
2. After the initial SQL Database has been created, use the following command on any AD FS Servers wanting to use Full SQL:

   ```
   FSConfig.exe JoinSQLFarm /ServiceAccount "domain\user"
   /ServiceAccountPassword "password" /SQLConnectionString "database=AdfsConfigurationServer;server=MSSQLSERVER\Instance [as needed];integrated security=SSPI"
   ```

**Note:** For more information, see AD FS 2.0: How to Perform an Unattended Installation of an AD FS 2.0 STS or Proxy.

### 4.3.5.3 Converting from Windows Internal Database to SQL Database
The Windows Internal Database is a Windows Server feature that is automatically installed on the computer after you complete the AD FS 2.0 Federation Server Configuration Wizard for the first time. Because the wizard does not provide an option to choose SQL Server as the store for the AD FS configuration database, your organization may simply continue to use the wizard defaults to see if they work well for your infrastructure.
However, it is highly possible that in time you will want to scale out your federation server farm to use more than five federation servers by migrating the configuration database to SQL Server. By migrating to SQL you will obtain scale, high availability and also be able to use SQL’s backup mechanisms.

This topic is provided for just this situation and will walk you through all the steps necessary to migrate your existing AD FS configuration data from your current Windows Internal Database store (in a production environment) to a new SQL Server store.

4.3.5.3.1 AD FS 2.0: Migrate Your AD FS Configuration Database to SQL Server

In the steps that follow, use steps 1, 2, 3, and 5 on the primary federation server. Follow steps 1, 2, 4, and 5 on each of the secondary federation servers in the farm. These steps include:

1. Backing up the federation server
2. Temporarily disable the computer in the load balancer
3. Performing steps on the primary federation server
4. Performing steps on all of the secondary federation servers
5. Enabling the computer on the load balancer

For more information about the pros and cons of using either Windows Internal Database or SQL Server to store AD FS 2.0 configuration data, see the TechNet article The Role of the AD FS Configuration Database in the AD FS 2.0 Design Guide.

**Step 1: Backing up the federation server**

Use Windows Server Backup to back up the entire federation server computer including the AD FS configuration database stored in Windows Internal Database. You can also use Windows Server Backup to restore the AD FS configuration database.

More information about how to back up the AD FS configuration database will be out soon. Once this content is provided we will update this link.

**Step 2: Temporarily remove server from load balancer**

If your federation server is running in a farm and you have a load balancer, temporarily remove this machine from the load balancer configuration.

**Step 3: Performing steps on the primary federation server**

1. On the primary federation server in the farm, download the SQL Server 2008 Management Studio Express software and install it on the primary federation server. The software is available from the Microsoft Download Center.

   **Note:** This software is necessary in order to install and register the SQLCMD command-line tool, which is used in an upcoming step.
2. Stop the AD FS 2.0 Windows Service on the primary federation server.

3. Open an elevated command prompt, type the following command-line to stop the AD FS 2.0 Windows Service and then press ENTER.

```
net stop adfssrv
```

4. Connect to the Windows Internal Database that currently stores the AD FS configuration database and then detach both the AD FS configuration and artifact databases. In the command prompt window, type the following SQLCMD command-line syntaxes in order, and then press ENTER after each one.

```
sqlcmd -S \\.\pipe\MSSQL$MICROSOFT##SSEE\sql\query
use master
go
sp_detach_db 'adfsconfiguration'
go
sp_detach_db 'adfsartifactstore'
go
```

5. Connect to SQL server and attach the configuration and artifact database from the primary federation server. In the command prompt window, type the following SQLCMD command-line syntaxes in order, and then press ENTER after each one. In SQLServer\SQLInstance below, type in the appropriate SQL Server and SQL Server instance name where you are migrating the configuration data to. For example, contosasrv01\adfs.

```
sqlcmd -S <SQLServer\SQLInstance>
use master
go
sp_attach_db 'adfsconfiguration',
  'c:\windows\sysmsi\ssee\mssql.2005\mssql\data\adfsconfiguration.mdf',
  'c:\windows\sysmsi\ssee\mssql.2005\mssql\data\adfsconfiguration_log.ldf'
go sp_attach_db 'adfsartifactstore',
  'c:\windows\sysmsi\ssee\mssql.2005\mssql\data\adfsartifactstore.mdf',
  'c:\windows\sysmsi\ssee\mssql.2005\mssql\data\adfsartifactstore_log.ldf'
go
alter database AdfsConfiguration set enable_broker with rollback immediate
go
```

6. Change the configuration database connection string to point to the new SQL Server-based AD FS configuration database. Open a Windows PowerShell command-line, type
the following command-line syntaxes in order, and then press ENTER after each one. In SQLServer\SQLInstance below, type in the appropriate SQL Server and SQL Server instance name where you are migrating the configuration data to. For example, contososrv01\adfs.

```
$temp= Get-WmiObject -namespace root/AD FS -class SecurityTokenService
$temp.ConfigurationdatabaseConnectionstring="data source=<SQLServer\SQLInstance>; initial catalog=adfsconfiguration;integrated security=true"
$temp.put()
```

7. Open an elevated command-line prompt, type the following command-line syntax to start the AD FS 2.0 Windows Service, and then press ENTER.

```
Net start adfssrv
```

8. Change the artifact connection string to point to the new SQL Server-based artifact data location. Open a Windows PowerShell command-line, type the following command-line syntaxes in order, and then press ENTER after each one. In SQLServer\SQLInstance below, type in the appropriate SQL Server and SQL Server instance name where you are migrating the artifact data to. For example, contososrv01\adfs-artifact.

```
Add-pssnapin microsoft.adfs.powershell
Set-adfsproperties -artifactdbconnection "data source=<SQLServer\SQLInstance>; initial catalog=adfsartifactstore;integrated security=true"
```

9. Stop and restart the AD FS 2.0 Windows Service to refresh the new settings. Open a regular command-line prompt, type the following command-line syntaxes to stop and start the AD FS 2.0 Windows Service, and then press ENTER after each one.

```
Net stop adfssrv
Net start adfssrv
```

**Step 4: Performing steps on the secondary federation server**

Make sure the primary federation server has been added back to the load balancer before proceeding with this section.

1. Make sure the secondary federation server has been temporarily removed from the load balancer before proceeding.

2. On a secondary federation server in the farm, open an elevated command prompt, type the following command-line to stop the AD FS 2.0 Windows Service, and then press ENTER.

```
net stop adfssrv
```
3. Change the configuration database connection string to point to the new SQL Server-based AD FS configuration database. Open a Windows PowerShell command-line, type the following command-line syntaxes in order, and then press ENTER after each one. In SQLServer\SQLInstance, type in the appropriate SQL Server and SQL Server instance name where you are migrating the configuration data to. For example, contososrv01\adfs.

```
$temp= Get-WmiObject -namespace root/AD FS -class SecurityTokenService
$temp.ConfigurationdatabaseConnectionstring="data source=<SQLServer\SQLInstance>; initial catalog=adfsconfiguration;integrated security=true"
$temp.put()
```

4. Open a regular command-line prompt, type the following command-line syntax to start the AD FS 2.0 Windows Service, and then press ENTER:

```
Net start adfssrv
```

5. Change the artifact connection string to point to the new SQL Server-based artifact data location. Open a Windows PowerShell command-line, type the following command-line syntaxes in order, and then press ENTER after each one. In SQLServer\SQLInstance below, type in the appropriate SQL Server and SQL Server instance name where you are migrating the artifact data to. For example, contososrv01\adfs-artifact.

```
Add-ps snapin microsoft.adfs.powershell
Set-adfsproperties -artifactdbconnection “data source=<SQLServer\SQLInstance>; initial catalog=adfsartifactstore;integrated security=true”
```

6. Stop and restart the AD FS 2.0 Windows Service to refresh the new settings. Open a regular command-line prompt, type the following command-line syntaxes to stop and start the AD FS 2.0 Windows Service, and then press ENTER after each one:

```
Net stop adfssrv
Net start adfssrv
```

7. Verify that the service starts up successfully.

8. Repeat these steps for every federation server in this Windows Internal Database-based farm.

**Step 5: Enabling this computer on the load balancer**

Enable the computer in the load balancer so that requests are sent to it.
4.3.6 Deploy Directory Synchronization

After you have completed Active Directory clean up, reduced user mailbox sizes if necessary, and implemented Active Directory Federation Services, you can move forward with the steps to synchronize information from your on-premises Active Directory to the Office 365 directory service.

Synchronization is performed with the Microsoft Online Services Directory Synchronization Tool. By default, the Directory Synchronization Tool will install Microsoft SQL Server 2008 Express for database purposes. If your organization has more than 50,000 objects to synchronize, your organization should install the full version of SQL Server 2008.

For additional information, see the following Help topics:

- Activate Directory Synchronization
- Suggested Hardware for Running the Microsoft Online Services Directory Synchronization Tool

4.3.6.1 Install and Configure Directory Synchronization Tool (Fewer Than 50,000 Objects)

The following steps are recommended for organizations with fewer than 50,000 Active Directory objects to synchronize and require only SQL Server 2008 Express Edition. When you install and set up of the Directory Synchronization Tool on a dedicated computer, SQL Server 2008 Express Edition is also installed. Before beginning the installation process, refer to the deployment plan and verify that you have met the computer requirements and that you have the necessary permissions.

The first step is to activate the directory synchronization in the Microsoft Online Services Portal.

▸ To activate directory synchronization

1. Sign in to the Microsoft Online Services Portal with your Office 365 administrator credentials.
2. In the portal header, click Admin.
4. Next to Active Directory synchronization (Deactivated), click Activate.
6. When the Are you sure you want to activate message is displayed, click Yes.

After activating directory synchronization, you install the Directory Synchronization Tool and SQL Server Express Edition on its own member server or install the tool on its own member
server and point to a SQL Server cluster. See the guidance that follows on using a separate SQL Server with the Directory Synchronization Tool.

You should have downloaded and saved the Microsoft Online Directory Synchronization Tool package to your computer before you start.

► To install the Directory Synchronization Tool

1. Log on to the computer that will run the Directory Synchronization Tool.
2. Click Start, click Run, type the path to where you saved the Directory Synchronization Tool package, and then click OK.
3. Double-click DirSync.exe.
4. Click Run.
5. At the Welcome screen, click Next.
6. Review and accept the license terms, and then click Next.
7. At the Installation Folder screen, click Next.
   You may consider installing the tool in a directory different from the default location.
   There is the potential for better tool performance if installed on a separate physical disk.
8. At the Installation Complete screen, click Next.
9. Leave the Start Configuration Wizard now box checked and click Finish.
10. At the Configuration Wizard Welcome page, click Next.
11. Enter your Office 365 administrator account credentials at the Microsoft Online Services credentials screen and click Next. (For example, user name: johnsmith@contoso.com; password: Orang312.)
12. Enter your Active Directory enterprise administrator account credentials at the Active Directory Enterprise Admin Credentials screen and click Next. (For example, username: administrator@contoso.com; password: Appl312.)
13. At the Configuration Complete screen, click Next.
14. Leave the Synchronize directories now box checked, and click Finish.
15. At the final screen that highlights the information on verifying directory synchronization, click OK.

4.3.6.2 Install Directory Synchronization Tool (More Than 50,000 Objects)

These procedures describe the Directory Synchronization Tool installation with SQL Server 2008 Full Edition for organizations with more than 50,000 Active Directory objects.

You begin by activating directory synchronization in the Microsoft Online Services Portal.

► To activate directory synchronization

1. Sign in to the Microsoft Online Services Portal with your Office 365 administrator credentials.
2. In the portal header, click Admin.
4. Next to Active Directory synchronization (Deactivated), click Activate.
6. When the Are you sure you want to activate message is displayed, click Yes.

After activating directory synchronization, you install the Directory Synchronization Tool on the SQL Server or install on its own member server and point to a SQL cluster.

You should download and save the Microsoft Online Directory Synchronization Tool package to your computer before you start.

► To install the Directory Synchronization Tool using a separate SQL Server

1. Log on to the computer that will run the Directory Synchronization Tool.
2. Click Start and click Run.
3. Type CMD and click OK.
4. Type the path of where you saved the Microsoft Online Directory Synchronization Tool package.
5. Type DirSync.exe /fullsql and press Enter.
   If prompted with a User Account Control prompt, and click Continue, or enter the username and password of an administrator account, and click OK.
6. At the Welcome screen, click Next.
7. Review and accept the license terms, and click Next.
8. At the Installation Folder screen, click Next.
   You may consider installing the tool in a directory different than the default location.
   There is the potential for better tool performance if installed on a separate physical disk.
9. At the Installation Complete screen, click Next.
10. Click Finish.

Now you install the Directory Synchronization Tool using Windows PowerShell.

► To configure the Directory Synchronization Tool using Windows PowerShell

1. On the computer on which the Directory Synchronization Tool was installed, open Windows PowerShell by opening the command-line tool and entering the command Powershell.exe –noexit.
2. Press Enter.
3. At the Windows PowerShell prompt, type Add-PSSnapin Coexistence-Install.
4. To install the Directory Synchronization Tool onto the same system as SQL Server 2008, type Install-OnlineCoexistenceTool –UseSQLServer –Verbose.
   -OR-
To install the Directory Synchronization Tool using a remote installation of SQL Server 2008, type `Install-OnlineCoexistenceTool –UseSQLServer –SqlServer <SQLServerName> -ServiceCredential (Get-Credential) –Verbose`.

5. At the Windows PowerShell Credential Request prompt, type the username and password of the domain account that will be used to run the Microsoft Identity Integration Server service and the Microsoft Online Directory Services Synchronization Service.

6. Run the Microsoft Online Services Directory Synchronization Configuration Wizard to complete the installation.

### 4.3.6.2.1 Complete Directory Synchronization Tool Configuration

After installing SQL Server 2008, you must complete the Microsoft Online Services Directory Synchronization Tool Configuration Wizard before synchronization will occur.

**To complete the Directory Synchronization Tool installation**

1. If you are working through the Directory Synchronization Tool Installation Wizard, on the Finish page, select **Start Configuration Wizard now**, and then click **Finish**.
   - OR -
   Click **Start, All Programs, Microsoft Directory Sync**, and then click **Directory Sync Configuration**.

2. On the **Microsoft Online Services Credentials** page of the Microsoft Online Services Directory Synchronization Configuration Wizard, provide the user name and password for a user account with Administrator permissions in your organization.

3. On the **Active Directory Credentials** page, provide the user name and password for an account with Enterprise Admin permissions on the on-premises Active Directory service.

4. On the **Finish** page, select **Synchronize directories now**, and then click **Finish**.

**Important** The Microsoft Online Services credentials that were provided are used to synchronize information from the on-premises Active Directory to the Office 365 directory service. If you change the password associated with this account, you must rerun the configuration wizard and provide the updated credentials.

The Enterprise Admin credentials that were provided are not saved. They are used to create the MSOL_AD_Sync directory synchronization service account. This service account is used to read the changes from the on-premises Active Directory.

### 4.3.6.3 Verify Directory Synchronization

Verifying directory synchronization from your on-premises Active Directory to Office 365 requires testing both forced (manual) synchronization and automatic synchronization. Because
the Directory Synchronization Tool performs an automatic one-way synchronization between the on-premises Active Directory and the Office 365 directory once every three hours, completion of this procedure may take up to three hours. You can also force directory synchronization at any time using PowerShell.

The Directory Synchronization Tool writes entries to an event log. These entries indicate the start and end of a synchronization session. When you review the event log, look for entries where the source is "Directory Synchronization." An entry that is designated “Event 4” and that has the description "The export has completed” indicates that the directory synchronization is complete. Directory synchronization errors are also sent via email to your designated technical contact.

After the Directory Synchronization Tool is installed and configured, your on-premises Active Directory is the master for all changes to the synchronized mail-enabled objects in Office 365. The following procedures show how both forced and automatic verification work and you should perform them in sequence. You make changes to mail-enabled objects in the on-premises Active Directory and verify that those changes are synchronized with Office 365.

### 4.3.6.4 Forced Directory Synchronization

The following procedure describes how to force immediate directory synchronization and verify the synchronization changes are made. Forcing directory synchronization bypasses the replication window of three hours and applies incremental changes immediately.

1. Sign in to the [Microsoft Online Services Portal](https://portal.office.com) using your administrator user name and password.
2. Ensure that the Technical Contact information contains a valid email address that is monitored by the technical contact.
3. Verify the address properties of a user account that is being synchronized from the on-premises Active Directory to the Microsoft Online Services Portal.
4. Verify that you cannot edit the address properties of that user account using the Microsoft Online Services Portal.
5. On your domain controller, open Active Directory Users and Computers and target the on-premises Active Directory forest/domain with permissions to edit user accounts, contacts, and distribution groups.
6. Make a simple but obvious change to one of the email address properties of the user account that you verified in step 2.
7. Open the Microsoft Online Services Directory Synchronization Configuration Wizard, provide the information requested on the wizard pages, and on the **Finish** page, select **Synchronize directories now**, and then click **Finish**.
8. When the synchronization is complete, view the address properties of the user in the Microsoft Online Services Portal and verify that the changes you made in the on-premises Active Directory have been synchronized to Office 365.

Next you will see how automatic directory synchronization works using the Directory Synchronization Tool.

4.3.6.5 Automatic Directory Synchronization

The Directory Synchronization Tool synchronizes changes to user accounts and mail-enabled contacts and groups from your on-premises Active Directory to your Office 365 directory service every three hours, beginning at the time of the initial synchronization.

► To verify automatic directory synchronization

1. Sign in to the Microsoft Online Services Portal using your administrator user name and password.
2. Ensure your Technical Contact information contains a valid email address that is monitored by the technical contact on a daily basis.
3. In the Microsoft Online Services Portal, verify the address properties of a specific user account, contact, and distribution group that are being synchronized from your on-premises Active Directory to Office 365.
4. In Microsoft Online Services Portal, modify the address properties of the contact and distribution group that you verified in step 3 of the forced directory synchronization procedure.
5. On your domain controller, open Active Directory Users and Computers and target your on-premises Active Directory forest/domain with permissions to edit user accounts, contacts, and distribution groups.
6. In the on-premises Active Directory, make a simple but obvious change to one of the address properties of the user account that you verified in step 3 of the forced directory synchronization procedure.
7. In the on-premises Active Directory, make simple but obvious changes to the contact and the distribution group that you modified in step 4.
8. Check the directory synchronization event log to determine when directory synchronization is complete. This may take up to three hours.
9. When synchronization is complete, view the properties of the user, contact, and distribution list in the Microsoft Online Services Portal and verify that the changes you made in the on-premises Active Directory now appear in Office 365.

In this procedure, the changes you made to the contact and distribution group in Office 365 have been overwritten by the changes you made to the same contact and distribution group in the on-premises Active Directory.
4.3.6.6 Maintain Authentication to On-premises Resources

After your organization has established email coexistence between its on-premises Exchange Server environment and Exchange Online, and established directory synchronization of user accounts and mail-enabled contacts and groups from the on-premises Active Directory to Office 365, you may want to continue using Active Directory authentication to control access to on-premises printers, file shares, and other network resources.

In this scenario, leave directory synchronization running to continue to synchronize user accounts and mail-enabled contacts and groups from the on-premises Active Directory to Office 365. Continue to edit the properties of these objects in the on-premises Active Directory.

4.4 Implement Password Policies for Non-Federated Identities

Your organization may choose not to federate your on-premises Active Directory for single sign-on functionality. If so, it is important to understand the Office 365 password policies. Below are the password requirements for Microsoft Online Identities:

The following rules and restrictions apply to passwords for Microsoft Online IDs.

- **Password rules**
  - The password is case-sensitive.
  - The password can contain uppercase letters and lowercase letters.
  - The password can contain numbers.
  - The password can contain the following ASCII text characters: ` ~ ! @ # $ % ^ & * () _. + = { } | \ [ ] : ; " ' < > ? , /
  - The minimum password length is 8 characters.
  - The maximum password length is 16 characters.

- **Password restrictions.** The password cannot contain any of the following items:
  - Spaces
  - Non-English characters
  - The account name part of the email address. For example, if the email address is user@contoso.com, the password cannot contain user. This restriction is not case-sensitive. Therefore, USER or User cannot be used in the password for user@contoso.com.

For more information about password policies, see [Change your password](#).
4.5 Activate User Licenses

Your organization cannot enable Exchange Online without first activating user licenses. The procedure that follows shows the steps to activate licenses for groups of users from the Admin area within the Microsoft Online Services Portal.

There are several strategies to consider when activating groups of users at the same time:

- Activating groups of users who require the same type of license.
- Activating groups of users who share the same location.

**To activate user licenses**

1. Sign in to the Microsoft Online Services Portal with your Office 365 administrator credentials.
2. In the portal header, click Admin.
4. From the list of users, determine which licenses you want to assign to specific users and then select the check box next to each user’s name.
5. Click Activate Synced Users.
6. Select the location for the group of users (example: United States).
7. Check the license you would like to assign these users.
8. Click Next.
9. Click Activate.
10. Click Finish.

4.6 Exchange Online Preparation

This section provides deployment instruction to enable moving user mailboxes to Microsoft Exchange Online in a hybrid deployment. It is assumed that your organization is running Exchange Server 2003 or later, so that you can configure hybrid deployment between the on-premises Exchange Server environment and Exchange Online.

**Note:** Configuring an Exchange hybrid deployment requires directory synchronization. For more information, see the Install and Configure Directory Synchronization section of this document.

Many of the steps required to enable email coexistence are performed by selecting the E-Mail Hybrid mode page from the Migration tab in the Microsoft Online Services Portal.

4.6.1 Deployment Pre-requisites

Ensure you have performed all the procedures in the Networking and Names Services Tasks and
User Identity and Provisioning Tasks sections of this document before you start with your Exchange Online preparation steps.

4.6.1.1 Upgrade Active Directory Schema

To implement email coexistence, you will need to upgrade your Active Directory schema to Exchange Server 2010 SP1 version. If you have not already completed the Active Directory scheme upgrade, review the Update Schema for Hybrid Deployment section found earlier in this document.

4.6.1.2 Install Update Rollup

We recommend installing the latest update rollup for Exchange 2010 on all your servers. Microsoft releases update rollup packages approximately every six to eight weeks. The rollup packages are available via Microsoft Update and the Microsoft Download Center. In the Search box on the Microsoft Download Center, type "Exchange 2010 update rollup" to find links to the rollup packages.

4.6.2 Establish Email Coexistence

After you have completed the hybrid deployment prerequisites, you can begin to configure the Exchange hybrid deployment. The Exchange Server Deployment Assistant is the recommended tool to use for this multi-step process, which include installation of the hybrid server.

After you launch the web-based Deployment Assistant, click the Hybrid button. The Deployment Assistant asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your hybrid deployment. The checklist (Figure 17) provides a prioritized list of tasks and steps you need to complete to configure your Exchange hybrid deployment and provides references TechNet documentation
In addition to English, the Deployment Assistant is also available in Chinese (Simplified), Chinese (Traditional), French, German, Italian, Japanese, Korean, Portuguese (Brazil), Russian, and Spanish.

### 4.6.3 Testing Exchange Online with Remote Connectivity Analyzer

To verify that inbound mail, Exchange ActiveSync, Autodiscover, Outlook Anywhere (RPC/HTTP), and other connections are properly configured, you should consider using the [Exchange Remote Connectivity Analyzer](https://aka.ms/ExchangeRemoteConnectivityAnalyzer). The Remote Connectivity Analyzer is a Web-based tool that is designed to help you troubleshoot connectivity issues by testing your Exchange on-premises and on-premises configuration.

You may want to become familiar at this tool in advance of your deployment to understand its capabilities and usage. Additionally, if you already have ActiveSync, Outlook Anywhere, and Autodiscover enabled in your on-premises environment we highly recommend you run through the tests provided to ensure your on-premises environment is functioning appropriately.

See the Help article [DNS Troubleshooting for Exchange Online](https://docs.microsoft.com/en-us/Exchange/troubleshoot/dns-troubleshooting) for more information about the Remote Connectivity Analyzer.
4.7 SharePoint Online Preparation

When planning your Office 365 deployment you should evaluate which of the SharePoint capabilities you will implement in your Office 365 environment.

4.7.1 Analysis of Existing SharePoint environment

Before deciding on a migration strategy it is vital that you perform an analysis of your current environment. This analysis should focus on those SharePoint workloads and content that you plan to move to SharePoint Online.

As an outcome of the analysis you should have a clear understanding on the content and the customizations you have in your On-Premises environment.

You should then create a content and customization roadmap that covers what content and customizations that will be moved to SharePoint Online and how they will be moved.

For each customization you will need to decide if you want to provide that functionality in your SharePoint Online environment. As the next step you will need to validate if the customizations can be implemented as sandboxed solutions.

4.7.2 Preparing for Customizations

Once you have an inventory of all the customizations that you want to move to SharePoint Online you need to decide the right packaging and deployment mechanisms. Generally, it is recommended to package all the customization in Web Solution Packages (WSPs). This will allow the site collection administrators to upload these to the Solution Gallery of each Site Collection that needs the customization. After the upload the solutions need to be activated.

Figure 18 shows the Solution Gallery.
If you have design artifacts such as master pages or page layouts that only need to be deployed to one Site Collection you can upload them manually to the Master Page Gallery of the Site Collection however if you need them in multiple site collections it is beneficial to package them as WSPs as well.

### 4.7.3 Content Migration

Office 365 does not provide SharePoint content migration support for customers. If you plan to migrate SharePoint content from an on-premises or hosted service to SharePoint Online, your organization will either use a manual approach or to use a third-party SharePoint migration tool.

One way to manually move content to SharePoint Online is by connecting the SharePoint Library to SharePoint Workspace. You can then upload content to SharePoint Workspace and it will automatically synchronize these files to SharePoint Online. Another manual approach is to use the capability of SharePoint to upload multiple files. This will allow you to upload batches of files at once.

**Note:** If you use the manual migration methods described above, the uploaded files will appear as being created by the user who uploaded them. Also the timestamp of the file will be the upload time and not the original creation time.

Before choosing the migration tool to migrate your SharePoint content, be sure to verify that the tool meets your migration requirements and that it supports all of the SharePoint artifacts you want to migrate. Refer to the third-party tool’s documentation and evaluate what preparation steps your organization will need to implement.

Microsoft partners are also available to assist with migrating your SharePoint content to SharePoint Online using third-party tools. For assistance with SharePoint content migration, see
the “Recommended Deployment Partners” area at the Microsoft Online Services deployment page. The Office 365 Marketplace also provides names of recommended deployment partners that can assist with SharePoint content migrations.

4.8 Lync Online Preparation

Key tasks in preparing your organization for Lync Online include optimizing your network for Lync conferencing, configuring domain federation and public IM connectivity settings, and ensuring the Lync 2010 client is installed on Lync Online user’s computers.

For additional information, see the Help topic Set up Microsoft Lync Online.

4.8.1 Network Preparation for Conferencing

You can optimize your network environment for use with Lync conferencing by performing the following configurations:

- Enabling the required firewall ports to access the Lync conferencing servers.
- Disabling authentication for Lync Online audio and video traffic when an authenticating HTTP proxy is employed.
- Configuring the network to allow User Datagram Protocol (UDP) traffic for better audio and video performance.
- Adjusting internal routers and optimizing internal network paths for audio and video traffic (optional).
- Filtering traffic (if required by the service provider SLA)

As a hosted service, Lync Online conferencing can operate in a large variety of network topologies. Typically, your network administrator is able to make minor configuration changes to routers and firewalls to provide an optimized user experience that does not interfere with your organization’s ability to secure its network. For information regarding bandwidth requirements for Lync Server 2010 conferencing, see the TechNet article Defining Your Requirements for Conferencing.

4.8.2 Enable and Disable Federation

If you are an Office 365 for enterprises administrator, you can enable domain federation in Microsoft Lync Online so users in your company can connect with users in other companies that have deployed Microsoft Office Communications Server 2007, Office Communications Server 2007 R2, or Microsoft Lync Server 2010. If you want to establish Lync domain federation with your own on-premise implementation of Office Communications Server 2007, Office Communications Server 2007 R2, or Microsoft Lync Server 2010, Lync Online and your on-
premise system must be using different SIP domains. Note that none of your Lync Server 2010 on-premises SIP domains should be in the list of active domains for your Office 365 tenant.

Once you have enabled domain federation, users can exchange peer-to-peer instant messages (IM), initiate peer-to-peer audio and video calls, and view presence information. You can also enable public IM connectivity, so that users can add contacts from Windows Live Messenger and communicate with them by using Lync 2010. Note that domain federation does not create an integrated, searchable address book.

► To disable federation with other Office 365 organizations using Lync Online

1. Log on to the Microsoft Online Services Portal with your Office 365 administrator credentials. portal
2. In the portal header, click Admin.
3. Under Lync Online, click Manage.
4. In the Microsoft Lync Online Control Panel, click Domain federation.
5. Click Edit.
7. Click OK.

4.8.3 Enable Federation with Windows Live Messenger

If your organization would like to establish federation with Windows Live Messenger you may enable these features through the Microsoft Online Services Portal.

► To enable Lync Online federation with public IM services

1. Log on to the Microsoft Online Services Portal with your Office 365 administrator credentials.
2. In the header, click Admin.
3. Under Lync Online, click Manage.
4. In the Microsoft Lync Online Control Panel, click Public IM.
5. Click Enable.
6. Click OK.

4.9 Client and End-User Experience

As discussed earlier in the Plan section this deployment guide, your organization will potentially need to upgrade client hardware and software when moving to Office 365. For client software, consider using Microsoft Update or an enterprise software deployment solution (such as Microsoft System Center Configuration Manager) to ensure that the requirements are met for the Office 365 web or rich client experience.
4.9.1 Rich Client Experience

For users to experience the highest fidelity with the Office 365, your organization will need to deploy install rich experience clients to users' computers and provide for ongoing patches and updates.

Rich experience clients provide users with full-featured desktop applications for email, instant messaging, and business productivity and require methods for distributing, configuring and updating clients.

Office 365 for enterprises solutions make use of the following rich clients:

- Microsoft Office 2010 and Office 2007 SP2 (including Outlook)
- Microsoft Office 2008 for Mac
- Microsoft Entourage® 2008 Web Services Edition
- Microsoft Office 2011 for Mac
- Office Web Apps
- Microsoft Lync 2010

When using rich experience clients, you need to install the Office 365 desktop setup package on user’s computers. This application ensures that the required components and updates are installed for rich clients. The Office 365 desktop setup package automatically configures Outlook and Microsoft Lync for use with Microsoft Online Services. Administrators can allow enterprises users to update their desktops on their own using Office 365 desktop setup, or can choose to deploy the updates remotely by using Active Directory.

4.10 Create Migration Groups

Migration groups are the set of users that you migrate to Office 365 during each migration window. Depending on the number of users you have, your organization will likely require multiple migrations to move all your users to the Office 365 environment.

When defining migration groups, you will want to consider more than just the total size of the included mailboxes. Here are some additional things to keep in mind:

- **Bandwidth considerations.** All of the mailbox content must travel from the on-premises mail environment over the Internet to Office 365. You can use the migration tools to determine how much data should be migrated once mailbox reduction has been performed. Based on this information, you should scope the size of your migration groups and schedule migration times to work with your existing network and Internet bandwidth.

- **User groups.** When migrating groups of users, it is a best practice to migrate users who communicate with each other frequently. For example, if an executive team uses email to
communicate vital information, you should migrate the members of the executive team at the same time. Schedule your migration groups to ensure that the owners of the mailboxes that are migrated will be available immediately after the migration to validate the success of the migration. This is especially imperative for organizations that have end of month financial, inventory, or other reporting mechanisms that cannot be disrupted. Keep in mind the mailbox and calendaring requirements of shared/delegate mailboxes for executives and other key customer personnel and their assistants. It is important that assistants are able to access the calendars of executives and key staff without delay.

- **User locations.** In addition, be sure to migrate users in accordance with the physical buildings they occupy. It makes sense to migrate fourth floor Conference Rooms with users on the fourth floor. For smaller buildings with limited meeting space it may become necessary to survey the rooms that are used on other floors as well to ensure these resources are available as soon as possible.
5 Migrate Phase

The Migrate phase is primarily focused on the steps required to move user mailbox content from on-premises to Exchange Online.

5.1 Key Activities Summary

The following are the key deployment tasks and events that your carry out in the Migrate phase:

- **Assign licenses to users**
  To access Office 365 service offerings, assign licenses to users through the Microsoft Online Services Portal. If you have not already done so, review the [Activate User Licenses](#) topic presented in the Prepare section of this guide.

- **Issue final communications to end users**
  Prior to the start of velocity migrations, send all users moving to Office 365 the necessary notifications and instructions they need to make the transition to the new hosted services platform.

- **Migrate mailbox data**
  Proceed with velocity mailbox migrations from on-premises mailboxes to Exchange Online using your selected migration tools and migration group schedule.

- **Migrate existing collaboration documents**
  Using third-party migration tools, move files and folders from your existing SharePoint environment to SharePoint Online.

- **Change DNS records**
  When all migrations are completed, change your DNS records (for example, MX and TXT records) to at your domain registrar.

- **Configure mobile phones and devices for Office 365**
  Set up user mobile phones to access your email using the Exchange ActiveSync protocol. Exchange Online

- **Perform post-migration service testing**
  After migrations are completed, perform full-scale testing of Office 365 service functionality.

5.2 Send Final End User Communications

Prior to the start of velocity migrations, you should send your final notifications and instructions to users moving to Office 365 service offerings. See [Appendix G: Sample Email Migration End User Communications](#) for an example of messaging used in these communications.
5.3 Migrate Mailboxes

You can use the New Remote Move Request wizard in the Exchange Management Console (EMC) on the hybrid server to move existing user mailboxes in the on-premises organization to the Office 365 organization.

By default, the Mailbox Replication Proxy service (MRSProxy) running on the hybrid server automatically throttles the mailbox move requests when you select multiple mailboxes to move to Office 365. The total time to complete the mailbox move depends on the total number of mailboxes selected, the size of the mailboxes, and the properties of the MRSProxy.

Steps for migrating mailboxes are provided in the “Move or create a mailbox” topic in the Exchange Server Deployment Assistant and the Help topic Move or create a mailbox for shared domains.

5.4 Change MX Record

When you are ready to put your coexistence server into production, you will need to change your MX record to redirect inbound mail flow to your hybrid server or Exchange server deployed in an Edge Transport server role.

The Exchange Server Deployment Assistant will provide detail steps for how to change the MX record in the topic “Redirect mail flow to coexistence server.”

5.5 Set Up Mobile Phones and Devices

Information about setting up mobile phones and devices for your Office 365 users is available at http://help.outlook.com.

You can find specific instructions for setting up many popular mobile phones at Mobile Phone Features.

- For instructions for the Apple iPhone, iPod, or iPad see Set Up Microsoft Exchange E-Mail on an Apple iPhone.
- For instructions for the BlackBerry Curve™, see Set Up POP or IMAP E-Mail on a BlackBerry Curve.
- For instructions for the BlackBerry Pearl™, see Set Up POP or IMAP E-Mail on a BlackBerry Pearl.

5.5.1 ActiveSync Devices

To set up your mobile phone to access your email using the Exchange ActiveSync protocol, you will need the Exchange ActiveSync server name as well as your user name and password.
5.5.1.1 Set Up Windows Phone and Windows Mobile Devices

If a Windows Mobile device is already set up to synchronize with another computer running Microsoft Exchange Server, you must delete that email account from your mobile device before your device can sync with Microsoft Exchange Online.

The following procedures describe how your Exchange Online administrator can do the following:

- Delete an existing relationship between a Windows Mobile 6.5, 6.1, and 6.0 device and Exchange Server
- Set up a new Windows Mobile and Windows Phone relationship with Exchange Online.
- Use the remote wipe feature.

**Note:** The menu options displayed on your device may be different from those described in the procedures that follow. If you have questions, refer to your mobile device documentation.

**To delete an existing Windows Mobile relationship**

1. From the Windows Mobile Start menu on the mobile device, tap Programs, and then tap ActiveSync.
2. Tap Menu, and then tap Options.
3. Tap Microsoft Exchange, and then tap Delete to delete the existing relationship.

**To configure a Windows Mobile device connection**

1. On the mobile device, tap Start, tap Programs, and then tap ActiveSync.
2. Tap Menu, tap Add Server Source, and then enter the mobile device address for your organization’s data (example:outlook.com)
3. Select the This server requires an encrypted (SSL) connection check box, and then tap Next.
4. In User name, enter your Office 365 email address.
5. In Password, enter your password, select Save Password, and then tap Next. Leave the domain box blank.
6. Select the check boxes for the types of data you want to synchronize, and then tap Finish.

Use the following steps to configure your connection on a Windows Phone 7.

**To configure a Windows Phone 7 connection**

1. Press the Windows button to return to home.
2. Slide right and then up, and select Settings.
3. Select email & accounts.
4. Click **add an account**.
5. Select **Outlook**.
6. Enter your email address (for example, **johnsmith@contoso.com**).
7. Enter your password (with single sign-on this would be the same as your Active Directory password).
8. Click **sign in**.

### 5.5.1.2 Configure Remote Device Wipe Option

Administrators in your organization have the ability to remotely erase data from an Exchange ActiveSync mobile device in the event that an Exchange Online user’s device is lost, stolen or otherwise compromised.

**To remotely erase data from an Exchange ActiveSync device**

1. Log on to Microsoft Outlook Web App at [https://outlook.com](https://outlook.com) using the email address and password of the user account that the mobile device synchronizes with.
2. In the Outlook Web App window title bar, click **Options**.
3. In the navigation pane, click **Mobile Devices**.
4. Click the ID of the device you want to remotely erase, click **Wipe All Data from Device**, and then click **OK**.
5. Click **Remove Device from List**.

### 5.6 Perform Post-migration Service Testing

After user provisioning and mailbox migrations are completed, you should perform comprehensive testing of the Office 365 service offerings for which your organization has subscribed to ensure the services operate as described in the Office 365 for enterprises service descriptions.

See **Appendix H: Post-deployment Service Test Plan** for an example test plan.
6 Feature Enablement

This section describes Office 365 for enterprises features that are available to your organization but outside the scope of the deployment tasks described in this deployment guide. Many of these features are described in the Office 365 for enterprises service descriptions, which are available at the Microsoft Download Center.

Examples of user account and provisioning features that are available to enable include:

- Multi-factor authentication with Active Directory Federation Services
- Active Directory Federation Services custom log on page

Examples of Exchange Online features that are available to enable include:

- **Disclaimers.** Exchange Online enables administrators add disclaimers to messages in transit using transport rules. See the Help topic [Add Disclaimers to Messages](#) for details.
- **Transport rules.** Transport rules are used to inspect emails in transit (including inbound, outbound, and internal messages) and take actions, such as applying a disclaimer, blocking messages, or sending a blind carbon copy to a mailbox for supervisory review. See the Help topic [Organization-Wide Rules](#) for details.
- **Personal archive.** Exchange Online offers archiving through the personal archive capabilities of Exchange 2010. A personal archive is a specialized mailbox that appears alongside users’ primary mailbox folders in Outlook or Outlook Web App. See the Help topic [Enable an Archive Mailbox](#) for details.
- **Journaling.** Administrators can configure Exchange Online to journal copies of emails to any external archive that can receive messages via SMTP. See the Help topic [Journal Rules](#) for details.
- **Retention policies.** Exchange Online offers retention policies to help organizations reduce the liabilities associated with email and other communications. With these policies, administrators can apply retention settings to specific folders in users’ inboxes. The retention policy capabilities offered in Exchange Online are the same as those offered in Exchange Server 2010 Service Pack 1. See the Help topic [Set Up and Manage Retention Policies in Exchange Online](#) for details.
- **Legal hold.** Exchange Online provides legal hold capabilities to preserve users’ deleted and edited mailbox items (including email messages, appointments, and tasks) from both their primary mailboxes and personal archives. See the Help topic [Put a Mailbox on Litigation Hold](#) for details.
- **Rolling legal hold (single item recovery).** Some organizations want to preserve users’ mailbox contents for archiving and eDiscovery purposes, but only for a specific amount of time, such as one year. The single item recovery feature in Exchange Online can be used to meet this need, by providing rolling legal hold capabilities.
- **Multi-mailbox search.** Exchange Online provides a web-based interface for searching the contents of mailboxes in an organization. Through the Exchange Control Panel, administrators can search a variety of mailbox items—including email messages, attachments, calendar appointments, tasks, and contacts. See the Help topic [Create a New Multi-Mailbox Search](#) for details.
Appendix A: Key Deployment Resources

The following resources can provide additional help with deployment questions and tasks.

**Office 365 Community**  
The Office 365 Community site posts the latest developments and information related to Office 365. It includes a discussion area where site members post questions and answers. You can also access the Blogs, Forum, and Wiki pages from this site.

*Available at [http://community.office365.com](http://community.office365.com)*

**Office 365 Help**  
This extensive set of Help topics provides guidance to administrators and users working with Exchange Online, SharePoint Online, Lync Online, and Office Professional Plus.


**Office 365 Deployment Readiness Tool**  
The Office 365 Deployment Readiness Tool is available to assist you with discovery activities related to Office 365 deployments. The tool can be used to check and provide important information about your on-premises environment.


**Microsoft Assessment and Planning Toolkit**  
The Microsoft Assessment and Planning (MAP) toolkit generates detailed readiness assessment for migration to cloud-based services such as Office 365 for enterprises.


**MOSDAL (Microsoft Online Services Diagnostics and Logging) Support Toolkit**  
The MOSDAL Support Toolkit collects system, network, service-based application configuration and logging data along with performing network diagnostics. The toolkit can be used for a variety Office 365 troubleshooting issues.

8 Appendix B: Deployment Planning Template

Table 21 provides a high-level planning template for Office 365 for enterprises deployments. The sequence of tasks and events describe the typical workflow for deployments and serve as a guide for an orderly and efficient rollout of Office 365.

Key stakeholders in your organization should feel free to modify this template and workflow to meet your needs and requirements.

**Table 21. Office 365 for Enterprises Deployment Template**

<table>
<thead>
<tr>
<th>Deployment Tasks /Events</th>
<th>Start Date</th>
<th>Finish Date</th>
<th>Resources</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. PLAN PHASE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hold project kickoff meeting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Build risk and issue tracking system</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop migration strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify mailbox size and item counts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan for mail-enabled applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify options for user identity and account provisioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify Active Directory preparation and remediation requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify your email coexistence strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify current network links, user concentration, and current utilization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify on-premises infrastructure server requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify the operating systems and client applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify the mobile platform that your organization will use</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop an end user and administrator training schedule and delivery mechanism</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop end-user communications strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2. PREPARE PHASE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deployment Tasks /Events</td>
<td>Start Date</td>
<td>Finish Date</td>
<td>Resources</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>-------------</td>
<td>-----------</td>
<td>---------------</td>
</tr>
<tr>
<td>Add and verify your domain name with Office 365</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare your on-premises Active Directory for directory synchronization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable single sign-on (identity federation)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install the Directory Synchronization Tool and perform synchronization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure email coexistence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure Lync Online</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure SharePoint Online</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploy client applications and the Office 365 desktop setup</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform mailbox size reduction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare customer service desk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test and validate email migration and coexistence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complete the migration groups and migration schedule</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**3. MIGRATION PHASE**

<table>
<thead>
<tr>
<th>Deployment Tasks /Events</th>
<th>Start Date</th>
<th>Finish Date</th>
<th>Resources</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign licenses to users</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue final communications to end users</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Migrate mailbox data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Migrate existing collaboration documents</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change DNS records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure mobile phones and devices for Office 365</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform post-migration service testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9 Appendix C: Customer Deployment Checkpoints

To ensure a successful Office 365 deployment, you should periodically review and assess the key milestones within the deployment project. The following checkpoints are sample entrance and exit criteria to use while moving through the deployment process. If your deployment has not completed all exit criteria tasks included in a checkpoint, the deployment should not move forward on the project until all those tasks are completed.

9.1 Office 365 Deployment Entrance Requirements

Prior to moving forward with your Office 365 for enterprises deployment, you should ensure your organization has completed the following entrance criteria:

- **Review of Office 365 service descriptions to ensure solution alignment.** Your organization should not move forward with its deployment until all aspects of the service have been evaluated for alignment with your existing business and IT requirements.

- **Review of your Active Directory environment.** Your organization should ensure that your Active Directory complies with the requirements for Office 365. During your review, you should keep in mind that hybrid deployments only support email coexistence with a single Active Directory forest and that the directory synchronization service requires a support exception for synchronization of more than 20,000 users.

- **Purchase of Office 365 for enterprises user licenses.** To provision users for Office 365 services, your organization will need to have valid user licenses available to assign to users.

9.2 Checkpoint 1: Planning Complete

**Objectives**

Ensure that the deployment project scope and schedule are well understood by all your project team members from the Project Manager to the Executive Sponsor.

**Checkpoint Exit Criteria**

1. **Identified plans for the following items:**
   
   - Migration
   - Mail-enabled applications
   - User identity and account provisioning options
   - On-premises infrastructure and hardware requirements
   - Network bandwidth requirements
   - Client operating systems and client applications
• Service desk training
• End user and administrator training
• End user communication strategy

2. Completed the following activities:

• Customer kickoff meeting with agreement on the following:
  o Dedicated deployment project management team
  o Review of each workstream, milestone activities, and timelines
  o Commitment from all workstream owners on milestone timelines and dates
• Customer sign-off on Plan Complete milestone.

9.3 Checkpoint 2: Preparation Complete

Objectives
Ensure all configuration and preparation tasks are completed.

Checkpoint Exit Criteria
• Remediation of directory synchronization errors.
• Specific service configurations are completed.
• Office 365 Desktop Setup package is deployed.
• Email migration and coexistence is tested and validated.
• Service desk integrated
• Migration schedule is completed.

9.4 Checkpoint 3: Migration Complete

Objectives
• Velocity mailbox migrations begin.
• Criteria to stop the deployment is defined and agreed upon.

Checkpoint Exit Criteria
• Mailbox migration is completed.
• Plan is in place for deprovisioning of on-premises services (unless hybrid scenarios exist).
This compilation of URLs, ports and IP addresses provides a resource for customers when configuring firewall access during an Office for 365 for enterprises deployment project. Contact the Microsoft Office 365 support team if you need more information, or refer to the Help topic IP addresses and URLs used by Office 365.

10.1 URLs

**General Service URLs**
- Microsoft Online Services Portal
  [https://portal.microsoftonline.com](https://portal.microsoftonline.com)
- PowerShell Connection URI for Office 365 PowerShell
  [https://ps.microsoftonline.com](https://ps.microsoftonline.com)
- Community Portal for Office 365 Customers
  [https://community.office365.com](https://community.office365.com)
- Active Directory Federation Services End Point
  [https://nexus.microsoftonline-p.com](https://nexus.microsoftonline-p.com)
- Directory Synchronization End Point
  [https://adminwebservice.microsoftonline.com](https://adminwebservice.microsoftonline.com)

**Exchange Online URLs**
- Exchange Online PowerShell Connection URI
  [https://ps.outlook.com](https://ps.outlook.com)
- Outlook Web App address for a specific customer
  [https://outlook.com/<domain>.onmicrosoft.com](https://outlook.com/<domain>.onmicrosoft.com)
- Outlook Web App address for a customer specific domain
  [https://www.outlook.com/<companyname>.com](https://www.outlook.com/<companyname>.com)

**SharePoint Online URLs**
- *.sharepoint.com
- *.sharepointonline.com
- Default Root SharePoint site for customer
  `<domain>.SharePoint.com`
- Site Settings for the Root Site Collection
  `<domain>.sharepoint.com/_layouts/settings.aspx`
- SharePoint Online Administration Center for customer
  \(<domain>\)-Admin.SharePoint.com

**Lync Online URLs**
- *.online.lync.com
- *.infra.lync.com
- *.lync.com

Additional URLs that require firewall access include:
- *.microsoftonline.com
- *.onmicrosoft.com
- *.microsoftonlinesupport.net
- *.microsoftonline-p.com
- *.microsoftonline-p.net
- *.microsoftonlineimages.com
- *.live.com
- admin.messaging.microsoft.com

**10.2 IP Address Ranges**

To help ensure that network traffic from the Microsoft data centers is accepted, you may need to open ports in your on-premises firewall so network traffic originating from the Microsoft data center IP addresses is allowed to enter your on-premises organization.

Contact the Microsoft Office 365 support team for IP address ranges requirements, or refer to the Help topic [IP addresses and URLs used by Office 365](#).

**10.3 Required Ports**

Table 22 lists the protocol and port requirements for Office 365 for enterprises deployments.
### Table 22. Protocol and Port Requirements

<table>
<thead>
<tr>
<th>Protocol /Port</th>
<th>Applications</th>
</tr>
</thead>
</table>
| TCP 443       | • Active Directory Federation Services (federation server role)  
               | • Active Directory Federation Services (proxy server role)  
               | • Microsoft Online Services Portal  
               | • My Company Portal  
               | • Microsoft Outlook 2010 and Outlook 2007  
               | • Microsoft Entourage 2008 EWS/Outlook 2011 for Mac  
               | • Outlook Web App  
               | • SharePoint Online  
               | • Lync 2010 client (communication to Lync Online from on-premises Lync Server) |
| TCP 25        | • Mail routing |
| TCP 587*      | • SMTP relay |
| TCP 143/993   | • Simple IMAP4 migration tool |
| TCP 995**     | • POP3 |
| TCP 80 and 443* | • Microsoft Online Services Directory Synchronization Tool  
               | • Simple Exchange Migration Tool  
               | • Simple IMAP Migration Tool  
               | • Staged Exchange Migration Tool  
               | • Exchange Management Console  
               | • Exchange Management Shell |
| PSOM/TLS 443  | • Lync Online (outbound data sharing sessions) |
| STUN/TCP 443  | • Lync Online (outbound audio, video, application sharing sessions) |
| STUN/UDP 3478 | • Lync Online (outbound audio and video sessions) |
| RTC/UDP 50000-59999 | • Lync Online (outbound audio and video sessions) |

*SMTP Relay with Exchange Online requires port 587(TCP) and requires TLS. See TechNet for details on how to configure SMTP Relay with Exchange Online. Note: you will need to provide the SMTP server which is specific to the mailbox used for relay. Please see the TechNet article Set Up Outlook 2007 for IMAP or POP Access to Your E-Mail Account.

** POP3 access with Exchange Online requires port 995 TCP) and requires SSL. See TechNet for details on how to configure POP3 with Exchange Online.
11  Appendix E: Exchange Hybrid Deployment Domain and Host Names Worksheet

Configuring an Exchange hybrid deployment, email coexistence, and directory integration between your on-premises environment and the Office 365 environment requires that you provide appropriate domain and host names. Table 23 provides a sample list and examples of domain and host names used in the deployment process. You are strongly encouraged to use the Exchange Deployment Assistant to generate specific examples for your organization.

Table 23. Host Names Worksheet

<table>
<thead>
<tr>
<th>Description</th>
<th>Example value</th>
<th>Value in your organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Forest</td>
<td>corp.contoso.com</td>
<td></td>
</tr>
<tr>
<td>Internal Exchange Server 200X server hostname</td>
<td>DEN-SRV-EXCH-2K3</td>
<td></td>
</tr>
<tr>
<td>Exchange External 200X server FQDN</td>
<td>mail.contoso.com</td>
<td></td>
</tr>
<tr>
<td>Proposed internal coexistence server host</td>
<td>DEN-SRV-EXCH-2K10</td>
<td></td>
</tr>
<tr>
<td>Proposed external coexistence server FQDN</td>
<td>mail.contoso.com</td>
<td></td>
</tr>
<tr>
<td>Outlook Web App URL</td>
<td>owa.contoso.com</td>
<td></td>
</tr>
<tr>
<td>Primary SMTP namespace</td>
<td>Contoso.com</td>
<td></td>
</tr>
<tr>
<td>UserPrincipalName domain</td>
<td>Contoso.com</td>
<td></td>
</tr>
<tr>
<td>Microsoft Online ID domain</td>
<td>Contoso.com</td>
<td></td>
</tr>
<tr>
<td>Service SMTP namespace</td>
<td>service.contoso.com</td>
<td></td>
</tr>
<tr>
<td>Important: You must not use the service tenant FQDN, specified below, as the service SMTP namespace. We recommend that you use &lt;service, your domain&gt;.</td>
<td>service.contoso.com</td>
<td></td>
</tr>
<tr>
<td>Internal Active Directory Federation Services (AD FS) server hostname</td>
<td>DEN-SRV-AD FS-FED1</td>
<td></td>
</tr>
<tr>
<td>External AD FS server FQDN</td>
<td>sts.contoso.com</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Example value</td>
<td>Value in your organization</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td><strong>Internal directory synchronization server host name</strong></td>
<td>DEN-SRV-DIRSync</td>
<td></td>
</tr>
<tr>
<td><strong>Exchange federation trust namespace</strong></td>
<td>Exchangedelegation.contoso.com</td>
<td></td>
</tr>
<tr>
<td><strong>On-premises Autodiscover FQDN</strong></td>
<td>Autodiscover.contoso.com</td>
<td></td>
</tr>
<tr>
<td><strong>Service Autodiscover FQDN</strong></td>
<td>Autodiscover.&lt;value&gt;.contoso.com</td>
<td></td>
</tr>
<tr>
<td><strong>Service tenant FQDN</strong></td>
<td>contoso.onmicrosoft.com</td>
<td></td>
</tr>
</tbody>
</table>

*Note: You can only choose the subdomain portion of this FQDN. The domain portion must be "onmicrosoft.com".*
12 Appendix F: Directory Object Preparation

Successful directory synchronization between your on-premises Active Directory environment directory and Office 365 requires that your on-premises directory objects and attributes are properly prepared.

If your organization intends on implementing an Exchange hybrid deployment, you will need to upgrade your Active Directory schema to include Exchange Server 2010 SP1 updates. This is required in order to manage email attributes on-premise when using directory synchronization.

Apply the following requirements for user object attributes in preparing your Active Directory for directory synchronization.

**sAMAccountName**

- Maximum number of characters: 20
- Invalid Active Directory characters: !#\$%^&*()_+`~","\;\[\]::@<>\+=\?*'
- If a user has an invalid sAMAccountName but a valid userPrincipalName, the user account is created in Office 365.
- If both the sAMAccountName and userPrincipalName are invalid, the on-premises Active Directory userPrincipalName must be updated.

**givenName**

- Maximum number of characters: 64
- Questionable characters: ?@\+

  *Note: The Deployment Readiness Tool checks for questionable characters.*

**sn (surname)**

- Maximum number of characters: 64
- Questionable characters: ?@\+

  *Note: The Deployment Readiness Tool checks for questionable characters.*

**displayName**

- Maximum number of characters: 256
- Questionable characters: \?@\+

  *Note: The Deployment Readiness Tool checks for questionable characters.*

**mail**

- Maximum number of characters: 256
- Invalid characters: [ ! # $ %&*+/ = ? ^ ` { ]
- Duplicate values: The mail attribute cannot contain any duplicate values.

  *Note: If there are duplicate values in mail field, the first user with the value is
synchronized to the Office 365 environment. Subsequent users will not appear in the Microsoft Online Services Portal. You must modify the value not found the portal, or modify both of the values in the on-premises directory, in order for both users to appear in the Office 365 service.

**mailNickname**
- Maximum number of characters: 64
- Invalid characters: """-

**proxyAddresses**
- Maximum number of characters: 256
- Invalid characters: \\; > \n
**userPrincipalName**
- Maximum number of characters for username: 64
- Maximum number of characters for domain name: 256
- Invalid characters: }{ # ' $ % ~ * + ) ( > < / \ = ?`
- & character: Automatically changed to underscore:
- ^ character: No email will be sent, or an error report sent, and the value is automatically removed.
- ( ) character: remains the same.
- Duplicate proxies will be emailed as an error before any notification errors.

*Additional requirements for a valid userPrincipalName:*
- @ character is required in each userPrincipalName value.
- @ character cannot be first character in each userPrincipalName value.
- Username cannot end with a period (.) an ampersand (&) a space ( ), or at sign (@)
- Username cannot have a space ( ).
- Routable domains must be used (for example, .local or .internal cannot be used)
- Unicode is converted to underscore characters.
- userPrincipalName may not contain any duplicate values in the forest.

**Groups**
- Mail-enabled character check: All mail-enabled groups must follow the pattern of *@*.
- Administrators can hide users, distribution groups, and contacts from the Global Address List by setting the msExchHideFromAddressLists attribute for the object in on-premises Active Directory

**Contacts**
- Mail-enabled character check: All mail-enabled contacts must follow the pattern of *@*. 
13 Appendix G: Sample Email Migration End User Communications

The following is a communication timeline and sample emails that your Office 365 administrator can use to inform managers and employees about the email migration to Exchange Online.

5 Weeks Prior to Migration Date: Send Manager Email
Notify all managers that your organization is migrating to Microsoft Exchange Online. Tell your managers when it is going to happen. Provide an overview of the process. Explain why you are migrating. Give your managers tools to promote your organization’s decision to make this change. Give them information to communicate to their employees so that their employees know the migration is coming.

4 Weeks Prior to Migration Date: Send General Email
The following is a sample email for the administrator to send to all organization mail users at four weeks prior to the email migration.

Subject: ACTION REQUIRED: We are migrating your mailbox to Microsoft Exchange Online!

This email is your first notice that your mailbox will be migrated to Microsoft Exchange Online on <Date>. There are many tasks that you must perform before your email can be migrated. There are also several actions you can take before migration to improve your Exchange Online experience.

See ACTION REQUIRED BEFORE MIGRATION <insert link to before-migration instructions on your Microsoft SharePoint Online site>to prepare for your migration.

You can also preview what you will need to do after your mailbox has been migrated. See ACTION REQUIRED AFTER MIGRATION <insert link to after-migration instructions on your SharePoint site>to preview this information.

If you have any questions, check the Exchange Online FAQ <insert link to Microsoft Online FAQ> and the Exchange Online Known Issues <insert link to Microsoft Online Known Issues>, or contact support <insert your support contact information>.

Thank you,

<Your Migration or Support Contact Alias>
2 Weeks Prior to Migration Date: Send Manager Email

The following is a sample email for the administrator to send to all managers at two weeks prior to the email migration.

Subject: ACTION REQUIRED: Do you approve mailbox migration for these employees?

We need your approval to migrate your employees’ mailboxes to Microsoft Exchange Online on <Date>. If we do not receive your approval, the following employees will not be migrated.

**ACTION REQUIRED**

Review the list of your employees and respond to this email to let us know if they can be migrated.

<table>
<thead>
<tr>
<th>Employee</th>
<th>Migrate? (yes/no)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aaron Con</td>
<td></td>
</tr>
<tr>
<td>Coby Thomas</td>
<td></td>
</tr>
</tbody>
</table>

In the “Migrate?” column next to the employee, please indicate “Yes” to approve mailbox migration. If someone’s mailbox cannot be migrated, or if you do not want them to be migrated at this time, include that information in the “Migrate?” column.

If you have any questions, check the Microsoft Exchange Online FAQ <insert link to Microsoft Exchange Online FAQ> and the Exchange Online Known Issues <insert link to Microsoft Online Known Issues>, or contact support <insert your support contact information>.

Thank you,

<Your Migration or Support Contact Alias>

2 Weeks Prior to Migration Date: Send User Email

The following is a sample email for the administrator to send to all mail users at two weeks prior to the email migration.

Subject: ACTION REQUIRED: We are migrating your mailbox to Microsoft Exchange Online!

Your mailbox will be migrated to Microsoft Exchange Online on <Date, Day, and Time>. Please complete the tasks that you must perform before your email can be migrated.
There are also several actions you can take before migration to improve your Exchange Online experience.

See ACTION REQUIRED BEFORE MIGRATION <insert link to before-migration instructions on your SharePoint site> to prepare for your migration.

You can also preview what you will need to do after your mailbox has been migrated. See ACTION REQUIRED AFTER MIGRATION <insert link to after-migration instructions on your SharePoint site> to preview this information.

If you have any questions, check the Exchange Online FAQ <insert link to Microsoft Online FAQ> and the Microsoft Online Known Issues <insert link to Microsoft Online Known Issues>, or contact support <insert your support contact information>.

Thank you,

<Your Migration or Support Contact Alias>

1 Week Prior to Migration Date: Send User Email
The following is a sample email for the administrator to send to all mail users at one week prior to the email migration.

Subject: IMPORTANT! - ACTION REQUIRED: We are migrating your mailbox to Microsoft Exchange Online!

We are migrating our mailboxes to Microsoft Exchange Online on <Date>. If you do not complete the required actions by <Date – today’s date + 1 day> your mailbox will not be migrated.

If you have already completed the actions required before migration, please ignore this email.

See ACTION REQUIRED BEFORE MIGRATION <insert link to before-migration instructions on your SharePoint site> to prepare for your migration.

You can also preview what you will need to do after your mailbox has been migrated. See ACTION REQUIRED AFTER MIGRATION <insert link to after-migration instructions on your SharePoint site> to preview this information.

If you have any questions, check the Microsoft Exchange Online FAQ <insert link to Microsoft Online Exchange FAQ> and the Microsoft Exchange Online Known Issues <insert link to Exchange Online Known Issues>, or contact support <insert your support contact information>.
Thank you,

<Your Migration or Support Contact Alias>

1 Week Prior to Migration Date: Send General Email
The following is a sample email for the administrator to send to everyone who has completed the migration survey and is ready to migrate. Instructions for taking the migration survey are included in the ACTION REQUIRED BEFORE MIGRATION.

Subject: NOTIFICATION: We are migrating your mailbox to Microsoft Exchange Online!
Congratulations! Your mailbox is ready to be migrated on <Date>.

You can continue to use your current mailbox as usual until your mailbox is migrated to Exchange Online. After your mailbox has been migrated, you will receive a Welcome email with your Office 365 logon credentials and a link to instructions describing how to set up and use your new Microsoft Online mailbox. For a preview of those instructions, see ACTION REQUIRED AFTER MIGRATION <insert link to after-migration instructions on your SharePoint site>.

If you have any questions, check the Microsoft Exchange Online FAQ <insert link to Exchange Online FAQ> and the Exchange Online Known Issues <insert link to Microsoft Online Known Issues>, or contact support <insert your support contact information>.

Thank you,

<Your Migration or Support Contact Alias>

1 Week Prior to Migration Date: Send Manager and Support Mail
The following is a sample email for the administrator to send to the managers of the employees whose mailboxes are being migrated, and the designated migration administrators and support people.

Subject: NOTIFICATION: These people will be migrated to Microsoft Exchange Online on <Date>.

The following people will be migrated to Microsoft Exchange Online on <Date>:

<table>
<thead>
<tr>
<th>Employee</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shola Aluko</td>
<td></td>
</tr>
<tr>
<td>Jesper Hess</td>
<td></td>
</tr>
</tbody>
</table>
Migration will begin at <Time> on <Day> and is expected to be completed by <Time>, <Day>.

The employees whose mailboxes are being migrated will receive a reminder email the day before their migration. When their migration is complete, they will receive a Welcome email with instructions describing how to use their Microsoft Exchange Online mailbox.

The following people will be performing the migration:

Administrator 1: <Name>

Administrator 2: <Name>

Administrator 3: <Name>

The following Support people will be available by phone, <phone number> and by email <Support Alias>.

Support Person 1: <Name>

Support Person 2: <Name>

Support Person 3: <Name>

Support coverage will begin at <Start Time> and run through <End Time> until this group has been successfully migrated.

If you have any questions, check the Microsoft Exchange Online FAQ <insert link to Exchange Online FAQ> and the Exchange Online Known Issues <insert link to Exchange Online Known Issues>, or contact support <insert your support contact information>.

Thank you,

<Your Migration or Support Contact Alias>

1 Day Prior to Migration Date: Send General Mail

The following is a sample email for the administrator to send to everyone who has completed the migration survey and is ready to migrate. Instructions for taking the migration survey are included in the ACTION REQUIRED BEFORE MIGRATION document.

Subject: REMINDER: We will migrate your mailbox to Microsoft Exchange Online tomorrow!
Migration will begin at <Time> and is expected to be completed by <Time>. Support will be available by phone, <phone number> and by email <Support Alias>.

You can continue to use your current mailbox as usual until your mailbox is migrated to Exchange Online. After your mailbox has been migrated, you will receive a Welcome email with your Microsoft Online logon credentials and a link to the instructions describing how to set up and use your new Microsoft Online mailbox. For a preview of those instructions, see ACTION REQUIRED AFTER MIGRATION <insert link to after-migration instructions on your SharePoint site>.

If you have any questions, check the Exchange Online FAQ <insert link to Exchange Online FAQ> and the Exchange Online Known Issues <insert link to Microsoft Online Known Issues>, or contact support <insert your support contact information>.

Thank you,

<Your Migration or Support Contact Alias>

**After Migration: Send User Welcome Email**

The following is a sample email for the administrator to send to everyone who has been successfully migrated after the migration team has verified that the mailbox migration and forwarding has been successfully accomplished. It can be emailed or printed and distributed by hand.

Subject: ACTION REQUIRED: Get connected to Microsoft Exchange Online!

Congratulations! Your mailbox has been successfully migrated to Microsoft Exchange Online.

Your new logon credentials are:

User name: <username>@example.com
Temporary password: <password>

There are many tasks that you must perform now that your email has been migrated. We recommend setting aside two or three hours to complete them. To review the instructions and perform the tasks, see ACTION REQUIRED AFTER MIGRATION <insert link to after-migration instructions>.

If you have any questions, check the Exchange Online FAQ <insert link to Microsoft Online FAQ> and the Exchange Online Known Issues <insert link to Exchange Online Known Issues>, or contact support <insert your support contact information>.

Thank you,

<Your Migration or Support Contact Alias>
14 Appendix H: Post-deployment Services Test Plan

The following is an example of a post-deployment test plan that you can use to verify the functionality of Office 365 service offerings.

**Post-Migration Services Test Plan**

<table>
<thead>
<tr>
<th>Status</th>
<th>Directory Synchronization (DirSync) Tool Functionality</th>
<th>Owner</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Started</td>
<td>Create user object to verify DirSync account creation</td>
<td></td>
<td>3 hour replication interval or force DirSync</td>
</tr>
<tr>
<td>Not Started</td>
<td>Modify user object to verify DirSync attribute modification</td>
<td></td>
<td>3 hour replication interval or force DirSync</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>End-User Acceptance</th>
<th>Owner</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Started</td>
<td>Install the Services Connector application</td>
<td>Download from Microsoft Online</td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Configure Outlook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Open Outlook and verify connectivity to Exchange Online</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Launch customer online portal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Authenticate using Outlook Web App verifying URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Launch customer online portal verifying URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Launch customer SharePoint verifying URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Perform necessary updates to internal URLs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Individual User Mailbox Migration</th>
<th>Owner</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Started</td>
<td>Create user’s profile and point to the Office 365 service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Permission to their own mailbox post-migration and can read/send email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Permission to Shared Mailboxes post-migration and can read/send email</td>
<td>Send-As only available with post-migration script</td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>User has ability to sync their BlackBerry device post-migration via BlackBerry Enterprise Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Migration of delegate permissions</td>
<td>Applicable based on migration tool capabilities</td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>No unexpected NDRs for user post-</td>
<td>Scope will need to be defined as some NDRs</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Email</td>
<td>Owner</td>
<td>Notes</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Not Started</td>
<td>Send and receive email messages to migrated users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Send and receive email messages to non-migrated users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Send and receive email messages to external users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Send email to Distribution List</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Reply to email from migrated users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Reply to email from external users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Non-migrated user reply to email</td>
<td></td>
<td>Sent from migrated user prior to migration</td>
</tr>
<tr>
<td>Not Started</td>
<td>Recover deleted item from the Recycle Bin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Email access with Outlook Web App</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Reply to an email with a Distribution List</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Incoming mail from an external user</td>
<td></td>
<td>To both Distribution List and User</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Calendaring</th>
<th>Owner</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Started</td>
<td>Meetings have been migrated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Book a meeting in a migrated conference room</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Meeting request can be accepted for an available conference room</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Meeting request is not accepted for a pre-booked conference room</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Remote booking agent is functional where appropriate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Updated meeting requests notify all attendees</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>View details of free/busy information for those permitted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>View secondary calendar side-by-side for those permitted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Mobile Devices</td>
<td>Owner</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Not Started</td>
<td>Email sent from Exchange arrives at BlackBerry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Email sent from BlackBerry arrives in Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Email sent from Exchange arrives at a Windows Mobile device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Email sent from a Windows Mobile/ActiveSync device arrives in Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Delete mail item from supported mobile devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Create calendar item from supported mobile devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Message Archiving (Optional)</td>
<td>Owner</td>
<td>Notes</td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify inbound emails are archived</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify outbound emails are archived</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify internal emails are archived</td>
<td></td>
<td>With emails which do not contain any external recipients in To/CC/BCC fields.</td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify the members of Archive Group DL</td>
<td></td>
<td>The number of users should be the same with the number of users in Administration Center if you archive all.</td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify search functionality is present and works correctly for title, message body</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify email is encrypted in transit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify authorized export users can export to .PST file</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify ad hoc searches work</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify nightly harvest is occurring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify keyword and percentage sampling work</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Verify message review and escalation process work</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Lync Online Conferencing</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Create a Conference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Invite people to a conference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Initiate a Conference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>SharePoint</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Site collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Create site</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Create site collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Add user to site collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Remove user from a site collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Create new group for a site collection and add user</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Users and groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Add user to site</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Remove user from a site</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Create new group for a site and add user</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Publishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Publish a blog</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Publish an RSS feed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Remove RSS viewer Web part</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Create document library</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Create document</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Upload document to library</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Lists</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Create list</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Add list items</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Add approval workflow to list, library, or content type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Remove approval workflow from above list</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Searches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Perform document search</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Perform people search</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Bulk Upload content</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Upload calendar information from Outlook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Upload Contacts from Outlook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Started</td>
<td>Upload document libraries</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
15 Appendix I: Glossary

**Active Directory Federation Services (AD FS):** AD FS provides the various end-points that the Microsoft Federation Gateway uses to redirect clients to the AD FS server for different types of authentication. AD FS must be installed on a separate physical server that is a part of your on-premises network organization.

**Active Directory Federation Services configuration database:** A database used to store all configuration data that represents a single AD FS 2.0 instance or Federation Service. This configuration data can be stored using the Windows Internal Database (WID) feature included with Windows Server 2008 and Windows Server 2008 R2 or using a SQL Server® database.

**Autodiscover:** The Exchange Autodiscover service automatically finds the correct Microsoft Exchange Server host and configures Microsoft Office Outlook or Outlook 2007 for your users. It also includes an offline address book and the Free-Busy availability service that provides availability information for your users.

**BPOS (Business Productivity Online Standard Suite):** This is the acronym for the first version of the cloud-based, multi-tenant productivity suite from Microsoft Online Services. The BPOS service offering is being replaced by Office 365 service offerings.

**Comma separated value (CSV) file:** A text file in which each value is separated by a comma. It is typically used as an input file for a software program or script.

**CNAME record:** A Canonical Name (CNAME) record is a type of resource record in the Domain Name System (DNS) that is an alias for the Address (A) record that maps an IP address to the target server. The target server does not have to exist in the same domain as the CNAME record itself. You can define an alias in one domain to point to a target server in a completely different domain. Many organizations use CNAME records with web servers. An organization might point the alias www to a Web server that is hosted by a dedicated Web hosting company. For example, requests for www.contoso.com can be redirected to webserver1.fabrikam.com

**Deployment Consultant:** The Deployment Consultant (Microsoft or partner) is the primary resource for customers to work with on technical and project related items. The Deployment Consultant is the primary contact for your Technical Lead.

**Directory synchronization:** Active Directory synchronization (DirSync) replicates an organization’s on-premises Active Directory information for mail-enabled objects to the Office 365 environment. Using the Microsoft Online Services Directory Synchronization Tool, your company’s administrators can keep your local Active Directory continuously synchronized with Office 365. This not only allows you to create synchronized versions of each user account and group, but also allows global address list (GAL) synchronization from your local Microsoft
Exchange Server environment to Microsoft Exchange Online. Organizations deploying coexistence must deploy DirSync on a separate, on-premises server. The synchronization from your on-premises Active Directory to the Office 365 Active Directory environment is one way.

**Domain registrar:** A domain name registrar is an organization or commercial entity, accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) or by a national country code top-level domain (ccTLD) authority, to manage the reservation of Internet domain names in accordance with the guidelines of the designated domain name registries and offer such services to the public.

**Email coexistence:** Email coexistence enables organizations with on-premises Exchange Server email environments to establish a connection between their on-premises mail environment and the Office 365 Exchange Online mail environment. With coexistence configured, some users connect to Exchange Online while others continue to use the local Exchange Server environment, and all of the users can share the same email domain name. Email coexistence can be configured as either simple coexistence or as a hybrid deployment.

**Exchange Management Shell:** The command-line interface for Exchange 2010.

**Exchange Control Panel (ECP):** This Web-based console is used to manage the Exchange Online environment. The ECP can be accessed through the Admin area of the Microsoft Online Services Portal.

**Exchange Hosted Archive:** Part of the Exchange Hosted Services (EHS) network, EHA provides a repository that stores email. Using EHA, organizations can manage increasingly complex retention, compliance, and regulatory requirements. The EHA systems receive a message and after being filtered the clean message is delivered to the corporate mail server. A copy is made and stored in a security-enhanced online message repository.

**Exchange Online:** A hosted email and messaging service built on Microsoft Exchange Server and offered by Office 365. For organizations using on-premises Exchange Server and Exchange Online, Exchange Online is sometimes referred to as their “cloud-based Exchange organization.”

**External relay:** A configuration option in Microsoft Online Services Portal when mailboxes for a domain are hosted outside of Exchange Online and the MX record points to an email server outside of Exchange Online. Selecting this option requires disabling of inbound messaging.

**Federation Service:** A logical instance of AD FS 2.0. A Federation Service can be deployed as a stand-alone federation server or as a load-balanced federation server farm. You can configure the name of the Federation Service using the AD FS 2.0 Management snap-in. The DNS name of the Federation Service must be used in the Subject name of the SSL certificate.

**Federation server:** A computer running Windows Server 2008 or Windows Server 2008 R2 that has been configured to act in the federation server role. A federation server serves as part of a
Federation Service that can issue, manage, and validate requests for security tokens and identity management. Security tokens consist of a collection of claims, such as a user's name or role.

**Federation server farm:** Two or more federation servers in the same network that are configured to act as one Federation Service instance.

**Federation server proxy:** A computer running Windows Server 2008 or Windows Server 2008 R2 that has been configured to act as an intermediary proxy service between a client on the internet and a Federation Service that is located behind a firewall on a corporate network. In order to allow remote access to the services in Office 365, such as with a smart phone, home computer, or Internet kiosk, you need to deploy a federation server proxy.

**FOPE Administration Center:** The service management site for Microsoft ForeFront Online Protection for Exchange.

**Hybrid Deployment:** A hybrid deployment is an email coexistence configuration offers Exchange organizations the ability to extend the feature-rich messaging experience and administrative control they have with their existing on-premises Exchange Server organization to Office 365 and Exchange Online. A hybrid deployment provides the seamless look and feel of a single Exchange organization between an on-premises organization and an Office 365 organization. In addition, a hybrid deployment can serve as an intermediate step to moving completely to Exchange Online. A hybrid deployment offers a unified global address list (GAL) and mail routing between the on-premises and Office 365 organizations plus additional messaging features typically available in an on-premises Exchange deployment, including sharing free/busy and calendar information between the organizations and the ability to move mailboxes from the on-premises organization to the Office 365 organization.

**Hybrid Server:** A hybrid server is an Exchange Server 2010 SP1 server that is installed in your existing Exchange organization. It is required for hybrid deployments. The hybrid server enables messaging features and messaging delivery between your existing Exchange organization and the Office 365-based Exchange organization.

**Identity federation:** Identity federation provides a true single sign-on (SSO) experience for users to access both the on-premises and Office 365 service offerings with a single user name and password. Additionally, identity federation allows administrators to easily control account policies for Office 365 mailboxes by using on-premises Active Directory management tools.

**Internet Message Access Protocol (IMAP):** This is an application-layer Internet standard protocol used by on-premises email clients to retrieve email from a remote server over a TCP/IP connection. Microsoft Online supports email data migration from IMAP4 environments.

**Journaling:** A feature of Office 365 that enables Exchange to record all email communications in an organization. The feature can be enabled by opening a service request with the support team.
**Lync Online**: The Office 365 solution for instant messaging, audio and video calling, and online meetings. The Lync Online service is built on Microsoft Lync 2010 Server.

**Mailbox size reduction**: The tasks associated with reducing the overall mailbox size for all users to allow for an increase in the total number of mailboxes that can be migrated in a single migration event.

**Microsoft Federation Gateway**: The Microsoft Federation Gateway is a free cloud-based service offered by Microsoft that acts as the trust broker to establish federation between your on-premises Exchange 2010 organization and Exchange Online.

**Microsoft Forefront Online Protection for Exchange (FOPE)**: FOPE consists of layered technologies to actively help protect your organization’s inbound and outbound email from spam, viruses, phishing scams, and email policy violations.

**Microsoft Premier Deployment (MPD)**: This deployment consulting service is provided by Microsoft to large organizations seats for delivery of Office 365 for enterprises solutions.

**Microsoft Online Services Module for Windows PowerShell**: This tool installs a set of cmdlets to Windows PowerShell that you use to set up single sign-on for Office 365.

**Microsoft Online Services ID**: When you first sign up for Microsoft Office 365, you create a new email address and password, known as a Microsoft Online Services ID, as part of the sign-up process. You use this email address and password every time you sign in to use Microsoft Office 365 service offerings. With your Microsoft Online Services ID, you sign in to perform administrative tasks, view billing and account information, and use any of the services, including Microsoft Exchange Online, Microsoft SharePoint Online, and Microsoft Lync Online.

**Microsoft Online Services Portal**: Web portal that the designated service administrator for a customer subscribing to Microsoft Online Services uses to manage settings for the organization. You can also manage your active subscriptions: for example, you can increase the number of user licenses, change billing details, or select a Microsoft Authorized Partner to help with your subscription.

**MX record**: A mail exchanger record (MX record) is a type of resource record in the Domain Name System that specifies a mail server responsible for accepting email messages on behalf of a recipient’s domain and a preference value used to prioritize mail delivery if multiple mail servers are available.

**Network load balancer (NLB)**: A dedicated application (such as Microsoft Network Load Balancing) or hardware device (such as a multilayer switch) used to provide fault tolerance, high availability, and load balancing across multiple nodes. For AD FS, the cluster DNS name that you create using this NLB must match the Federation Service name that you specified when you deployed your first federation server in your farm.
**Office 365 desktop setup package:** This application is installed on workstations that use rich clients (such as Microsoft Office 2010) and connect to Office 365 service offerings. It automatically configures rich clients for use with Office 365 and manages and installs client updates.

**Office Professional Plus:** Microsoft Office applications that connect to Office 365 service offerings and provide access to documents, email, and calendars from a variety of clients. Office Professional Plus includes Office Web Apps, online companions to Word, Excel, PowerPoint, and OneNote, which let you review and make light edits to documents directly from a browser.

**Office Web Apps.** Online companions to Word, Excel, PowerPoint, and OneNote, which let you review and make light edits to documents directly from a browser.

**Outlook Web App:** This is the browser based email client used to access Exchange Online. Formerly known as Outlook Web Access.

**Relying party:** A federation service or application that consumes claims in a particular transaction.

**Relying party trust:** In the AD FS 2.0 Management snap-in, a relying party trust is a trust object that is created to maintain the relationship with another Federation Service, application, or service (in this case Office 365) that consumes claims from your organization’s Federation Service.

**Remote PowerShell:** A Windows PowerShell feature that allows scripting of routine tasks and access to raw data for reports.

**RSS feed:** A frequently updated communication channel for announcements from Microsoft Online Services. Announcements come in the form of service alerts, planned and unplanned outages, and maintenance.

**Security Token Service (STS):** The Web service that authenticates clients by validating credentials that are presented by a client. The STS can issue to a client a security token for a successfully authenticated client.

**Service continuity:** The process and procedures required to maintain or recover critical services during a business interruption.

**Service interruption:** Any event, whether anticipated (for example, a public service strike) or unanticipated (for example, a power outage), which disrupts the normal course of business operations at the organization’s location. Similar terms: outage, service interruption.

**Service request:** A service request (SR) is how customers engage Office 365 support for reactive and proactive issues.
**Service Support Admin:** Customer role that has read only permissions to all company objects. Also has the ability to manage individual services.

**SharePoint Online:** The Office 365 solution for collaboration. The SharePoint Online service is built on Microsoft SharePoint Server 2010.

**Simple coexistence:** Simple coexistence is an email coexistence configuration that offers only the basic feature of a unified global address list (GAL) and mail routing between the on-premises and Exchange Online organizations.

**Single-label domain (SLD):** SLDs are DNS names that do not contain a suffix, such as .com, .corp, .net, or .org. SLDs are not supported in Office 365 and Exchange Online deployments. For example, “contoso” is an SLD, and therefore is not supported. However, “contoso.com” and “contoso.local” are not SLDs, and therefore are supported.

**Single sign-on:** See Identify Federation.

**SMTP relay:** Allows organizations to use Exchange Online as an SMTP service for mail originating outside of the Exchange Online environment, for example SMTP-enabled applications such as fax servers.

**SPF record:** The Sender Policy Framework (SPF) record specifies which computers are authorized to transmit email from a domain. This helps to prevent others from using your domain to send SPAM or other malicious email. If your ISP has implemented SPF, you must create an SPF record to allow Microsoft Exchange Online to send email from your domain.

**User Principal Name (UPN):** A user account name (sometimes referred to as the user logon name) and a domain name identifying the domain in which the user account is located. This is the standard usage for logging on to a Microsoft Windows domain. The format is user@microsoft.com (similar to an e-mail address).

**User Principal Name (UPN) suffix:** The part of the UPN to the right of the @ character. The default UPN suffix for a user account is the Domain Name System (DNS) domain name of the domain that contains the user account. Alternative UPN suffixes may be added to simplify administration and user logon processes by providing a single UPN suffix for all users. The UPN suffix is used only within the Active Directory forest, and it does not have to be a valid DNS domain name.

**Velocity migrations:** Bulk migrations of user mailboxes from an on-premise messaging system to the Exchange Online system. Each bulk migration occurs within a scheduled migration window.