Identity for Enterprises

Service Description

Published: June 28, 2011

Contents

Introduction

Microsoft® Office 365 for enterprises brings together cloud-based versions of trusted communications and collaboration products from Microsoft with the latest version of the Microsoft desktop suite. Office 365 is designed to meet the needs of organizations of all sizes—from sole proprietors to small, mid-sized, and large businesses to government agencies and educational institutions—helping them save time and money and free valuable resources.

Microsoft Office 365 includes:

- **Microsoft Office:** Microsoft Office Professional Plus 2010 seamlessly connects with Microsoft Office Web Apps for an exemplary productivity experience across PCs, mobile devices, and browsers.

  Note

  An appropriate device, Internet connection, and supported browser are required. Some mobile functionality requires Office Mobile 2010 which is not included in Office 2010 applications, suites, or Web Apps. There are some differences between the features of the Office Web Apps, Office Mobile 2010, and the Office 2010 applications.

- **Microsoft Exchange Online:** Exchange Online offers cloud-based email, calendar, and contacts with the most current antivirus and anti-spam solutions. Access email on virtually any mobile device and take advantage of options for voice mail, unified messaging, and archiving.
- **Microsoft SharePoint® Online:** SharePoint Online is a cloud-based service for creating sites that connect colleagues, partners, and customers using enterprise social networking and customization.
- **Microsoft Lync™ Online:** Lync Online offers cloud-based instant messaging (IM), presence, and online meeting experiences with screen sharing and voice and video conferencing.

Document Scope

This document discusses the design, policies, and best practices related to Office 365 identity, including the creation of user accounts, password policy, co-existence, directory synchronization, and single sign-on (identity federation). Users can gain access to Office 365 by authenticating to their Office 365 user accounts—either through a prompt to provide valid credentials or through a single sign-on process. Once authenticated, users' identities refer to the user names associated with the Office 365 accounts.

This document does not include information about security features that allow or prohibit access to Office 365 features or resources (for example, Role Based Access Control in Exchange Online or configuring security in SharePoint Online). For details pertaining to these and other security-related topics, refer to the help documentation and service descriptions available in each of the services.

Types of Identity in Office 365

Office 365 offers two types of identities:

- **Microsoft Online Services cloud IDs (Cloud Identity)**: Users receive cloud credentials—separate from other desktop or corporate credentials—for signing into Office 365 services. The cloud ID password policy is stored in the cloud with the Office 365 service.
- **Federated IDs (Federated Identity)**: In companies with on-premises Active Directory®, users can sign into Office 365 services using their Active Directory credentials. The corporate Active Directory authenticates the users, and stores and controls the password policy.

The type of identity affects the user experience, administrative requirements, deployment considerations, and capabilities using Office 365.

Signing In to Office 365

The sign-in experience changes depending on the type of Office 365 identity in use: Cloud Identity or Federated Identity. Table 1 details the changes for different combinations of applications and operating systems.

Table 1: Sign-in experience with Office 365

	Cloud Identity	Federated Identity
Microsoft Outlook® 2010 on Windows® 7	Sign in each session[1]	Sign in each session[2]
Outlook 2007 on Windows 7	Sign in each session[1]	Sign in each session[3]
Outlook 2010 or Outlook 2007 on Windows Vista® or Windows XP	Sign in each session[1]	Sign in each session[1]
Exchange ActiveSync®	Sign in each session[1]	Sign in each session[1]
POP, IMAP, Microsoft Outlook for Mac 2011	Sign in each session[1]	Sign in each session[1]
Web Experiences: Office 365 Portal / Outlook Web App / SharePoint Online / Office Web Apps	Sign in each browser session	Sign in each session[4]
Office 2010 or Office 2007 using SharePoint Online	Sign in each SharePoint Online session[5]	Sign in each SharePoint Online Session
Lync Online	Sign in each session[1]	No prompt
Outlook for Mac 2011	Sign in each session[1]	Sign in each session[1]

Note

[1] When first prompted, you can save your password for future use. You will not receive another prompt until you change the password.

[2] You enter your corporate credentials. You can save your password and will not be prompted again until your password changes.

[3] Outlook 2007 will be updated after Office 365 has been made generally available to have the same

experience as Outlook 2010 on Windows 7.

[4] All apps require you to enter your username or click to sign in. You are not prompted for your password if your computer is joined to the domain.

[5] If you click on "Keep me signed in" you will not be prompted again until you sign out.

Creating Office 365 User Accounts

Office 365 provides four ways to create user accounts. All user accounts hosted in Microsoft data centers are Cloud Identities unless administrators have enabled Federated Identity for their users' domain.

- **Office 365 administration console**: You can manually create user accounts and assign licenses in the Office 365 administration console. The type of license you assign determines which services the user can access. When you assign the license, a temporary logon password is generated. After creating a user account, you can enter user details, including job title, department, phone numbers, and other properties that appear in the Global Address List.
- **Bulk upload using .csv files**: The Bulk add users wizard in the Office 365 administration site helps you upload existing .csv files or edit a blank .csv template in a text editor (for example, Notepad). The wizard also includes a sample .csv file that provides a correctly formatted example containing sample user data. To import .csv files, you must assign licenses to new users. You can then view the new users' passwords and optionally send them to users' email addresses
- **Active Directory Synchronization Tool**: You can use the Active Directory Synchronization Tool to replicate Active Directory user accounts (and other Active Directory objects) in Office 365. Unlike manually created accounts, accounts created by the Directory Synchronization Tool are fully populated with user account information from Active Directory (for example, department, phone number). When using Directory Synchronization, users are mastered on-premises—that is, the online account is a copy of the on-premises user account and cannot be edited online. Directory Synchronization Tool accounts remain inactive until you activate them. As a result, Office 365 licenses are not consumed when user accounts are created by the tool. When you activate user account from the Office 365 administration site (or using Microsoft Windows PowerShell™), a service license is assigned and an initial password is generated.
- **Microsoft Online Services Module for Windows PowerShell**: This tool installs a set of Office 365 cmdlets to Windows PowerShell that you can use to create users and accomplish many administrative tasks.
- **Exchange simple migration**: Simple migration is also called a cutover migration because all on-premises mailboxes are migrated to prepare for moving the entire email organization (including contacts and distribution groups) to the cloud. Using the simple migration method, you can migrate a maximum of 1,000 mailboxes from on-premises Exchange 2010 and Exchange 2007 servers to the cloud. During the process, all user accounts and mailboxes are created automatically. Accounts must be licensed within 30 days to continue with uninterrupted use.

Assigning a Custom Domain to Users

When you create a new user, the user's sign-in name and email address are assigned to the default domain as set in the Office 365 administration console. By default, the Office 365 account uses the <company name>.onmicrosoft.com domain that was created with the Office 365 account. When you create the account, you provide your company's name for the domain prefix (for example, contoso.onmicrosoft.com). This company name must be unique and not claimed by any other Office 365 customer. The custom domain cannot be removed or renamed.

Note

We recommend that you do not remove the default administrator account provided when your account was provisioned.

However, you can assign custom domains to email addresses instead of retaining the *onmicrosoft.com* domain. For example, a user can have the email address bill@contoso.com rather than bill@contoso.onmicrosoft.com. To assign the custom domain to the address, add the custom domain to Office 365. All custom domains go through the domain ownership verification process that is documented in the Office 365 Online Help topic Manage domains and domain properties.

Once the custom domain name is verified, you can set the custom domain as the default domain. When set, new users created in Office 365 are assigned to the new default domain (that is, the custom domain) instead of the *onmicrosoft.com* domain. Users that already exist when you validate the custom domain will not be automatically changed to use the new domain.

You can add more than one custom domain to Office 365 and can assign users to sign in with any of the validated domains. Each user's assigned domain is the email address that will appear on sent and received email messages.

Note

Before users can sign in with and use the custom domain for email, you must verify ownership of the custom domain and change the domain in the users' Properties pages in the Office 365 administration site.

Mailbox Aliases

Users' mailboxes can receive mail for multiple alias names (for example, mrina@contoso.com can also receive mail for sales@contoso.com or info@contoso.com). Each domain used for an alias must be a validated domain, and alias addresses do not require additional mailbox licenses.

Authentication and Office 365

With the exception of internet sites for anonymous access created with SharePoint Online, Users must be authenticated when accessing Office 365 services (except when using Internet sites created by SharePoint Online for anonymous access). Office 365 Cloud Identities are authenticated using traditional challenge/response, where users type in their user name and password. Users with Federated Identities are authenticated transparently using Active Directory Federation Services.

Office 365 Desktop Setup

To ensure proper discovery and authentication of Office 365 services, administrators must apply a set of components and updates to each workstation that uses rich clients (such as Microsoft Office 2010) and connects to Office 365. Rather than manually installing the updates, Microsoft provides an automated setup package—the Office 365 desktop setup—that automatically configures workstations with the required updates. This application replaces the Microsoft Online Services Connector.

The Office 365 desktop setup provides multiple benefits, including:

- Automatically detecting necessary updates.
- Installing updates and components upon approval or silently from a command line.
- Automatically configuring Internet Explorer and Lync for use with Office 365.

A list of these update requirements will be published for companies that want to use an alternative method of deploying the updates.

The Microsoft Online Services Sign In client previously used with Business Productivity Online Suite (BPOS) is no longer required with Office 365.

System Requirements

Installing Office 365 desktop setup requires one of the following operating systems.

- Windows 7 (32-bit or 64-bit edition)
- Windows Vista with Service Pack 1 (SP1) (32-bit and 64-bit editions)
- Windows XP with Service Pack 2 (SP2) (32-bit edition and 64-bit editions)
- Microsoft Windows Server® 2008
- In addition, each of the services has requirements that should be reviewed before you deploy Office 365. For more information, see the Office 365 Online Help topic Software requirements for Office 365.

Note

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

For more information about the Office 365 desktop setup, see the Office 365 online help topic Set up your desktop for Office 365.

Network Considerations

Office 365 uses forms-based authentication, and authentication traffic over the network is always encrypted with TLS/SSL using port 443. Authentication traffic uses a negligible percentage of bandwidth for Office 365 services.

Types of Authentication

This section discusses the types of user authentication that work with Office 365.

Authentication from a Web Browser

Office 365 offers several services that you can access using a web browser, including include Outlook Web App, SharePoint Online, and the Office 365 administration portal. When you access these services, your browser is redirected to a sign-in page where you provide your sign-in credentials. The sign-in experience varies depending on the kind of authentication enabled for the sign-in domain:

- **Cloud Identity**: The web browser is redirected to the Office 365 sign-in service, where you type your Microsoft Online Services ID and password. The sign-in service authenticates your credentials and generates a service token, which the web browser posts to the requested service and logs you in.
- **Federated Identity**: The web browser is redirected to the Office 365 sign-in service, where you type your corporate ID in the form a user principal name (UPN; for example, isabel@contoso.com). The sign-in service determines that you are part of a federated domain and offers to redirect you to the on-premises Active Directory Federation Server 2.0 for authentication. If you are logged on to the desktop (domain joined), you are authenticated (using Kerberos or NTLMv2) and Active Directory Federation Services 2.0 generates an SAML logon token, which the web browser posts to the Office 365 sign-in service. Using the logon token, the sign-in service generates a service token that the web browser posts to the requested service and logs you in.

Authenticating from Rich Client Applications

Rich clients include Microsoft Office desktop applications that are typically installed on a PC. Authentication from these types of applications can occur in two ways:

- **Basic/proxy authentication over SSL**: The Outlook client passes basic authentication credentials over SSL to Exchange Online. Exchange Online proxies the authentication request to the Office 365 Identity Platform, and then to on-premises Active Directory Federation Server 2.0 (for single sign-on).

  Note

  If you have set up single sign-on, then this authentication **requires** deployment of a proxy server or an Active Directory Federation Services 2.0 proxy server in your perimeter network (also known as demilitarized zone, DMZ, and screened subnet).

- **Microsoft Online Services Sign-In Assistant**: The Microsoft Online Services Sign-In Assistant, which is installed by the Office 365 desktop setup, contains a client service that obtains a service token from the Office 365 sign-in service and returns it to the rich client. If you have a Cloud Identity, you receive a prompt for credentials, which the client service sends to the Office 365 sign-in service for authentication (using WS-Trust). If you have a Federated Identity, the client service first contacts the Active Directory Federation Services 2.0 server to authenticate the credentials (using Kerberos or NTLMv2) and obtain a logon token that is sent to the Office 365 sign-in service (using WS-Federation and WS-Trust).

Table 2: Authentication mechanisms in Office 365

Application	Type of Identity	Authentication Mechanism
Web browser	Cloud Identity	Web sign in and WS-Trust
	Federated Identity	Web sign in, WS-Trust and WS-Federation (Active Directory Federation Services 2.0)
Outlook 2010 on Windows 7	Cloud Identity	WS-Trust (Sign-in Assistant)
	Federated Identity	Basic over SSL, authenticated via the Active Directory Federation Services 2.0 proxy
Outlook 2007 on Windows 7	Cloud Identity	Basic over SSL, authenticated at Office 365
	Federated Identity	Basic over SSL, authenticated via the Active Directory Federation Services 2.0 proxy
Outlook 2010 and Outlook 2007 on Windows Vista or Windows XP	Cloud Identity	Basic over SSL, authenticated at Office 365
	Federated Identity	Basic over SSL, authenticated via the Active Directory Federation Services 2.0 proxy
Exchange ActiveSync	Cloud Identity	Basic over SSL, authenticated at Office 365
	Federated Identity	Basic over SSL, authenticated via the Active Directory Federation Services 2.0 proxy
POP/IMAP/SMTP client	Cloud Identity	Basic over SSL, authenticated at Office 365
	Federated Identity	Basic over SSL, authenticated via the Active Directory Federation Services 2.0 proxy
Microsoft Office 2010 and Office 2010 on Windows 7, Windows Vista, or Windows XP	Cloud Identity	Web sign in and WS-Trust
	Federated Identity	Web sign in, WS-Trust, and WS-Federation (Active Directory Federation Services 2.0)
Lync Online	Cloud Identity	WS-Trust (Sign In application)
	Federated Identity	WS-Trust and WS-Federation (Sign In application and Active Directory Federation Services 2.0)

Two-Factor Authentication for Office 365

Two-factor authentication (also called strong authentication) provides improved security by requiring users to meet two authentication criteria such as a user name/password combination *and* a token or certificate.

Planning for Two-Factor Authentication with SSO

To use two-factor authentication, you must implement an single sign-on strategy using Active Directory Federation Services 2.0 with Office 365. When planning your implementation, consider whether users have a supported operating system, are inside or outside the corporate network, and are using rich clients or web browsers. Also consider the ability of your authentication provider to interoperate with other services.

Table 3 shows supported and unsupported scenarios.

Table 3: Supported and unsupported scenarios

Scenario	Supported/Unsupported	
Domain joined PC	Supported for Lync and SharePoint Not supported for Outlook	Allows users to log onto the corporate Active Directory from either inside or outside the corporate network. The existing infrastructure supports domain-joined PCs, but you must configure Office 365 for Federated Identities using single sign-on.
Non-domain joined PC with web application	Limited Support See the **Error! Reference source not found.** section	Requires two-factor authentication when users sign in to web applications from a non-domain joined computer, such as a home PC or Internet kiosk.

Note

Two-factor authentication for Lync and SharePoint can be supported if the PC is domain joined and the action of joining the machine to the corporate network requires two-factor authentication.

Deploying Two-Factor Authentication with Single Sign-on for Web Applications

Two options exist for enforcing two-factor authentication with single sign-on for users accessing Office 365 web applications outside the corporate network (for example from a home PC or Internet kiosk):

- **Integrate the Active Directory Federation Services 2.0 proxy logon page with your strong authentication provider**: Customize the Active Directory Federation Services 2.0 proxy logon web page to introduce the extra fields needed to gather information for the two-factor authentication. Further customize the page to interact with two-factor authentication servers or services to authenticate users.
- **Use the Microsoft Forefront® Unified Access Gateway SP1 server**: Use a Microsoft Forefront Unified Access Gateway (UAG) SP1 server to support a wide range of two-factor authentication providers as well as direct access to an expanded set of scenarios that involve two-factor authentication. For more information, see Deploying Forefront UAG with AD FS 2.0.

Password Management

The policies and procedures for password management depend on the kinds of identity in use with Office 365. When using Cloud Identities, passwords are automatically generated when the account is created. When using Federated Identities, passwords are managed in Active Directory.

Managing Passwords for Cloud Identities

Table 5 describes the password policies and options for Cloud Identities.

Table 4: Password policies and options for Cloud Identities

Property	Description
Password restrictions	8 characters minimum and 16 characters maximum Allowed values: • A – Z • a – z • 0 – 9 • ! @ # $ % ^ & * - _ + = [ ] { } | \ : ' , . ? / ` ~ " < > ( ) ; Disallowed values: • UNICODE • Username alias (part before @ symbol)
Password expiry duration	90 days (non-configurable)
Password expiry	Password expiry is enabled by default. When enabled, users are forced to change their passwords after 90 days. Users do not receive any form of password expiry notification. Administrators are able to enable and disable the password expiry setting at the user level through the Microsoft Online Services Module for Windows PowerShell.
Password strength	Strong passwords require 3 out of 4 of the following: • Lowercase characters • Uppercase characters • Numbers (0-9) • Symbols (see password restrictions above) Users by default are required to create strong passwords when they change their passwords. Administrators are able to enable and disable this setting at the user level through the Microsoft Online Services Module for Windows PowerShell.
Password history	Last password cannot be used again.
Password history duration	None
Account lockout	After 10 unsuccessful sign-in attempts with the wrong password, the user must solve a CAPTCHA dialog as part of the sign-in process. After 10 unsuccessful additional sign-in attempts with the wrong password and correct solving of the CAPTCHA dialog, the user is locked out of their account for a time period. Additional incorrect passwords results in an increase in the lockout time.

Changing Initial Passwords

To increase security, users must change their passwords when they first access the Office 365 services. As a result, before users can access Office 365 services, they must sign into the Office 365 portal, where they

are prompted to change their passwords. If users do not change their passwords when they first access Office 365, they will receive Access Denied messages.

Resetting Passwords

If users lose or forget their passwords, administrators with the **Global Administrator, Password Administrator, or User Management Administrator** role can reset users' passwords in the Office 365 administration site or through Windows PowerShell. Users cannot change their own passwords without providing their existing passwords.

If administrators lose or forget their passwords, a different administrator with the **Global Administrator** role can reset administrators' passwords in the Office 365 administration site or through Windows PowerShell.

If no administrators are available to reset passwords, users must contact Office 365 support to request a reset password.

Changing Passwords with Outlook Web App

With on-premises Exchange Server, users can change their passwords using Outlook Web Access (in Exchange Server 2007) or Outlook Web App (in Exchange Server 2010). With Office 365 and Exchange Online, the specific behavior of the change password feature in Outlook Web App depends on the type of identity in use (that is, Cloud Identity or Federated Identity):

- **Cloud Identity**: The Outlook Web App options page features a **Change password** hyperlink, which redirects users to the Change Password screen in the Microsoft Online Portal.
- **Federated Identity**: Outlook Web App does not feature a **Change Password** hyperlink. Users can change their passwords using standard, on-premises tools or through their desktop PC logon options.

Note

Unlike the on-premises Exchange Server 2010 version of Outlook Web App, the Office 365 version of Outlook Web App does not include a Password tab.

Authenticating After a Password Change

After users' passwords are changed, users are prompted to authenticate when they try to access a Office 365 service and Office 365 web portal. After they are authenticated to one service, they are authenticated to any others they use. In general, subsequent access to the same service or web portal doesn't require re-authentication; however, some factors—such as the browser or client in use or the time since last access—may require re-authentication.

Delegating the Reset Password User Right

With role-based access control in Exchange Online, users can be assigned the Reset Password user right by predefined or custom roles without becoming full services administrators. Assigning the following predefined roles to users (as listed in the Exchange Online Roles and Auditing) will give users the ability to reset passwords:

- Help Desk
- Organization Management
- Recipient Management

In addition, you can assign users the right to change passwords in the Office 365 Administration website

by assigning one of the following roles in the users' Settings pages:

- Global Administrator
- Password Administrator
- User Management Administrator (does not include the ability to reset passwords for billing, global, and service administrators)

Partners who are certified for providing support for Office 365 customers can reset passwords on behalf of their customers when authorized.

Resetting Passwords Using Windows PowerShell

In Office 365, service administrators can use Windows PowerShell to reset passwords, which can help script bulk password resets, create utilities for help-desk personnel, and control migration. Administrators who have the rights to reset passwords can reset passwords with Windows PowerShell.

Synchronizing Passwords

Office 365 does not support synchronizing local Active Directory passwords with Office 365 Cloud Identities.

Managing Passwords for Federated Identities

When you use Federated Identities with Office 365, Active Directory Federation Services negotiates the authentication with Office 365 Federation Gateway without passing users' local Active Directory passwords over the Internet to Office 365. When local users attempt to access Office 365 services, Active Directory Federation Services generates a signed token based on the user's Kerberos ticket. This token is accepted by the Office 365 service. As a result, users are logged onto Office 365 transparently and securely when they authenticate to Active Directory (for example, logging onto a local workstation).

In federated environments, users don't use Office 365 passwords; therefore, Office 365 password policy does not apply. Users are required only to authenticate to Active Directory. However, local password policies or two-factor authentication for Active Directory authentication will apply.

For more details, see the Federated Identities section.

Identity and Email Coexistence

In on-premises Exchange Server email environments, Exchange Online allows administrators to establish email coexistence between the on-premises environment and the Office 365 environment. During coexistence, some users connect to Exchange Online while others continue to use the local Exchange Server environment; all of the users can share the same email domain name.

For more details on Exchange coexistence, see the Exchange Online Service Description.

Companies that implement directory synchronization also employ a form of identity coexistence by integrating users, security groups, distribution lists, and other Active Directory objects into Office 365. For example, companies can use the security groups from Active Directory when applying SharePoint Online security settings.

Office 365 does not support Lync Online coexistence with on-premises Lync 2010. Instant messaging federation between different domains is supported as described in the Lync Online Service Description.

Active Directory Synchronization and Identity

When companies with users in local Active Directory environments initially subscribe to Microsoft Office 365 for enterprises, they can synchronize those users to the Office 365 directory. Using the Microsoft Online Services Directory Synchronization Tool, service administrators can keep Office 365 users, contacts, and groups updated with changes made in the local Active Directory.

Before implementing Active Directory synchronization, consider the following:

- **Email migration**: Active Directory synchronization is intended for ongoing relationships between your local environment and Office 365. If you want to migrate your users to Office 365 and stop using your local Active Directory, you must use other tools. For more information, see Migrate on-premises Exchange mailboxes to Exchange Online: Roadmap.
- **Single sign-on**: Before you set up directory synchronization, we strongly recommend that you set up single sign-on (identity federation).The single sign-on feature lets your users to sign in to Office 365 using their corporate credentials. To get started, see Prepare for single sign-on. If you decide not to set up single sign-on, you must add and verify your company's domains. For more information, see Manage domains and domain properties.
- **Local user management**: Active Directory manages Office 365 users that were created by the Directory Synchronization Tool. When you update details about users in Active Directory, that information is automatically updated in the users' Office 365 accounts at the next synchronization interval. When you add new users in Active Directory, new users are automatically created in Office 365. For more information, see Directory Synchronization Details and Managing Office 365 Users in Active Directory in this document.
- **Compliance**: Determine whether you require directory auditing to capture events such as creating users, resetting passwords, and adding users to groups. Security logging may be disabled by default; you might have to enable it for your organization. For more information on auditing, see Audit account management.

When to Use Directory Synchronization

Table 6 shows specific scenarios where directory synchronization is required or not supported.

Table 5: Directory synchronization in specific scenarios

Scenario	Required/Not Supported
Rich coexistence with on-premises Exchange Server	Required
Simple coexistence	Required
Staged migration with simple coexistence	Required
Federation and single sign-on	Required
Directory synchronization to create users in Office 365, then disabling directory synchronization.*	Not Supported
Multiple on-premises forests	Not Supported
Scoping or filtering (that is, limiting to a domain, organizational unit, or other container or group)	Not Supported

Note

* Some companies need to create a large number of users in Office 365 but do not want to implement directory synchronization long term. Using directory synchronization as means to simply create users in Office 365 and then decommissioning directory synchronization is not supported.

Authentication and Directory Synchronization

Directory synchronization has no direct impact on authentication. Users created by directory synchronization are not activated by default, and users cannot authenticate to inactive accounts. If administrators activate the accounts, users can then authenticate with their user names and passwords (if using Cloud Identities) or with their workstation identities (if using Federated Identities).

Directory Synchronization Details

The Directory Synchronization Tool was designed to serve a specialized purpose and has specific capabilities and limitations. Before implementing Directory Synchronization, become familiar with how the service works and its core requirements.

One-Way Push

The Directory Synchronization Tool replicates objects from the local Active Directory into Office 365. For example, if you add a user to Active Directory, that user will appear in Office 365 at the next synchronization interval. This allows the Global Address List for Office 365 to be populated with the full list of users in Active Directory. When Office 365 users search for names in Outlook, Outlook Web App, Lync Communicator, or another service that uses the Global Address List, they see additional details about the users they are searching for. In this way, Office 365 users have experiences almost identical to those of on-premises users. Users created by the Directory Synchronization Tool must be activated before they can sign into the service. Office 365 licenses are not automatically consumed when users are first created, either after deploying directory synchronization or adding users to Active Directory when the Directory Synchronization tool is running.

When you add changes to Office 365, they are not moved into the local Active Directory by default. For example, if you validate a new domain in Office 365, that domain will not appear automatically in your local Exchange environment. However, you can write (and update) a limited set of Active Directory attributes from Office 365 to the local Active Directory if the directory synchronization write-back feature is enabled. For more information, see the **Error! Reference source not found.** section in this document.

Unsynchronized Passwords

Passwords stored in Active Directory are not replicated to Office 365, and passwords created in Office 365 are not moved to Active Directory. When using Cloud Identities, you must manage Office 365 passwords in addition to local sign-in credentials. If you implement single sign-on with your deployment, you do not need to manage Office 365 passwords.

Replicated Objects

Directory synchronization replicates the following objects into Office 365. The list of objects is not customizable:

- Users
- Mail-enabled groups

- Security groups
- Contacts

All Replicated Objects in a Single Forest

All replicated objects in Active Directory are copied into Office 365. Office 365 does not support multiple forests, which limits the scope to a group, domain, organizational unit, or other subset.

Write-Back Capabilities

Directory synchronization in Office 365 includes an optional write-back capability for rich coexistence scenarios. This feature is included to improve the ability to manage Office 365 and your local Active Director as a single entity. For example, if you make an entry to block a domain when logged into the Exchange Management Console of Office 365, that information is written back to the local Active Directory so it can also be implemented in the local Exchange server. For details about what objects are written back to the local Active Directory, see Synchronized attributes that are written back to the on-premises Active Directory directory service (Write-Back).

When write-back is enabled, the following capabilities are activated:

- Cloud data regarding safe and blocked senders is shared with on-premises Exchange Server.
- Mail can be archived in Exchange Online.
- Users can reply to historical messages in their mailboxes.
- Administrators can easily move mailboxes back on-premises.

Object Limit

The Directory Synchronization Tool is limited to replicating 10,000 objects (see the **Error! Reference source not found.** section in this document). If your forest contains more than 10,000 replicated objects, contact Microsoft Support before you enable directory synchronization.

Synchronization Frequency

After you install, a full synchronization begins immediately. After the initial synchronization, a "delta" synch occurs every three hours. The replication period is not configurable.

Forced Synchronization

You can force replications by using the Windows PowerShell command *Start-OnlineCoexistenceSync*, or by running the Microsoft Online Services Directory Synchronization Tool Configuration Wizard. For details on these methods, see the Office 365 online help topic Synchronize your directories.

Synchronization Time

The actual time required for synchronization is influenced by the bandwidth available for your organization's Internet connection, the hardware used to host the directory synchronization service, and the current load on the directory synchronization service in the Microsoft Data Center. Table 7 provides estimated synchronization times based on experience with the directory synchronization service.

Table 6: Estimated synchronization time

Objects	Estimated first synchronization	Subsequent synchronizations
500	6 minutes	35 seconds
1,000	12 minutes	1.5 minutes
5,000	55 minutes	6 minutes

Objects	Estimated first synchronization	Subsequent synchronizations
15,000	3 hours	12 minutes

Note

Objects that have been synchronized from your on-premises Active Directory service will appear immediately in the Global Address List (GAL); Objects may not appear in the Offline Address Book (OAB) or in Microsoft Lync Online for up to 24 hours.

Throughput may be affected by throttling in place when the service is experiencing a high transaction volume.

Installation Requirements

Installing the Directory Synchronization Tool starts with a prompt for Active Directory Enterprise administrator credentials and the sign-in credentials for an Office 365 service administrator. The Active Directory credentials are not retained, as they are required only for correctly installing the service so it can read Active Directory.

For detailed installation requirements and procedures see the Office 365 online help topics Prepare for Directory Synchronization and Install the Microsoft Online Services Directory Synchronization tool.

Directory Synchronization Best Practices

Prepare your Active Directory by deleting unused accounts, locating duplicate Proxy-Addresses and User-Principle-Name entries, and inspecting the contents of the attributes for completeness and validity.

Note

When you deploy and configure Microsoft Online Directory Synchronization, your service administrator will receive an email message with recommendations for cleaning Active Directory.

If your organization uses federation, you should set it up before your first directory synchronization. Disabling directory synchronization after it has been enabled is not supported and may make it difficult for users to access Office 365 services.

Before running Directory Synchronization, you must validate your custom domains. User accounts without validated domains in Office 365 will be assigned to the default *onmicrosoft.com* domain.

For more information about Directory Synchronization, see the Office 365 online help topic Active Directory synchronization: Roadmap.

Managing Office 365 Users in Active Directory

After you deploy the Directory Synchronization tool, you can manage your Office 365 user accounts with your local Active Directory. Changes to properties of the user objects are automatically transferred to Office 365, including changes to user account statuses such as deleting or disabling user accounts.

Adding Active Directory User Accounts

When you add new users to Active Directory, you automatically create identical users in Office 365. You can then activate and assign licenses to users so they can access Office 365. If the license includes Exchange Online, a mailbox is automatically created. You can activate users with directory synchronization

either automatically using Windows PowerShell or manually in the Office 365 administration web application.

Deleting Active Directory User Accounts

When you delete user accounts in Active Directory, the matching Office 365 user accounts are also deleted. As a result, the associated mailboxes and their contents are deleted automatically. Information in SharePoint Online associated with deleted user accounts is preserved.

Managing Account Passwords

Active Directory passwords are not synchronized with Office 365. Changing a password in Active Directory modifies the password only in Active Directory; changing a password in Office 365 modifies the password only in Office 365. If your organization uses federation, there are no Office 365 passwords to manage. If users can successfully authenticate to their local Active Directory, their sign-in credentials will be accepted in Office 365.

Disabling Accounts

When you disable accounts in Active Directory, the corresponding user accounts in Office 365 will also be disabled at the next replication interval. Users will no longer have access to Office 365, but their mailboxes and SharePoint Online content are preserved.

Single Sign-On

When you set up single sign-on (identity federation), users automatically sign into Office 365 for enterprises by logging onto a domain-joined local workstation with their Active Directory corporate credentials.

Note

Single sign-on in Office 365 requires Active Directory Federation Services 2.0.

Benefits of Using Single Sign-On

When you set up single sign-on, you can eliminate the need to manage passwords specifically for Office 365. In addition to benefitting users, single sign-on can benefit administrators in the following ways:

- **Policy control**: Administrators can control account policies through Active Directory, which lets administrators manage password policies, workstation restrictions, and lock-out controls without needing to perform additional tasks in the cloud.
- **Access control**: Administrators can restrict access to Office 365 so that users can access it through the corporate environment, through online servers, or through both methods.
- **Reduced support calls**: Users often call for support because they have forgotten their passwords. If users have fewer passwords to remember, they are less likely to forget them.
- **Improved security**: Servers and services used in single sign-on are mastered and controlled on-premises, which can improve protection of user identities and information.
- **Cross-trust federation**: Using Active Directory Federation Services, you can establish trusts with other organizations, Active Directory Federation Services, or other services using WS-*, SAML1.1, or SAML2.0 services.
- **Two factor authentication**: You can use two-factor authentication systems that protect local resources to better protect access to Office 365 services.

User Experience in Different Locations

User experience with single sign-on varies based on computer connection to the network and configuration of Active Directory Federation Services 2.0.

- **Work computer on a corporate network**: When users are at work and logged on to the corporate network, single sign-on enables them to access the services in Office 365 without additional sign in.
- **Work computer off of a corporate network**: When users are logged on to domain-joined computers with their corporate credentials but 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 Office 365 without additional sign in.
- **Home or public computer**: When users are logged on to a computer that is not joined to the corporate domain, they must log on with corporate credentials to access the services in Office 365.

Requirements

The following programs, tools, and capabilities are required to implement single sign-on with Office 365:

- **Active Directory**: Deploy and run Active Directory in Windows Server 2003 or later with a functional level in mixed or native mode.
- **Active Directory Federation Services 2.0**: Deploy Active Directory Federation Services 2.0 on a Windows Server 2008 or Windows Server 2008 R2.
- **Latest client operating systems and service packs**: Run the latest updates of Windows 7, Windows Vista, or Windows XP. We strongly recommend that you install the Office 365 Desktop Setup to properly configure the client operating system for use with Office 365.
- **Windows PowerShell 2.0 and Federation Configuration Tool**: Install Windows PowerShell 2.0 with administrator privileges on the Active Directory Federation Services 2.0 server to run the commands to set up single sign-on. We recommend that you use remote access to the Active Directory Federation Services 2.0 server when you run these commands; to do this you must use Windows PowerShell remote commands. For more information, see Running Remote Commands.
- **Trusted third-party SSL certificates:** Acquire a certificate from a trusted certificate authority that contains a Common Name issued to your local Active Directory domain namespace. This certificate will allow you to set up an Active Directory Federation Services Proxy.
- **Internet access to Active Directory Federation Services Proxy servers**: Ensure Internet access for servers that host the Active Directory Federation Services Proxy services. If you deploy Active Directory Federation Services proxies, the internal Active Directory Federation Services servers are connected to the internet by way of the Active Directory Federation Services Proxy servers.

Creating and Converting Domains

New domains in Office 365 use are set to use Microsoft Online Services Cloud Identities. When you federate a domain that uses Cloud Identities, you use Windows PowerShell commands that are installed by the Microsoft Online Services Module for PowerShell. User accounts are converted to Federated Identities when the users next log on. We recommend that you wait 24 hours for the Office 365 identity system to fully update.

After making the conversion to federated identities, you must use Active Directory Federation Services to access Office 365 sites and services. We recommend that you stage your federated rollout to proof your setup plans before you fully deploy federation. If you are unable to access the services after converting to federated identities, you can still manage Office 365 using the default admin@<domain>.onmicrosoft.com account.

Note

Office 365 allows you to host multiple domains. Any hosted domain can be either a Cloud Identity or a Federated Identity domain. Users within a single domain cannot be split into Cloud Identities and Federated Identities.

You can also convert domains from federated identities to cloud identities. After you issue the proper Windows PowerShell commands, Office 365 will begin to convert the accounts and create new passwords. We recommend performing this conversion when it will least affect operations.

Piloting Federation

Domains in Office 365 use either Cloud Identities or Federated Identities, but not both. As a result, federated identity with Office 365 is easiest to pilot when you begin with a federated domain. In this case, you can start by deploying Federated Identities to a designated group of users and then deploy to other users when ready. If your organization has users in Office 365 using Cloud Identities, you cannot deploy

federation to subset of users. Instead, you can add an additional UPN suffix to your forest for the pilot. You must also update the UPNs of users in the pilot in Active Directory to reflect the test domain name.

For detailed instructions on piloting Federated Identities, see the Office 365 Community Wiki.

Active Directory Considerations

To successfully deploy Office 365 Federated Identities, you must prepare the structure and use of your existing Active Directory domain name.

- **UPNs**: Federated Identities require users to have UPNs, though Active Directory does not. UPNs associate users' identities in Microsoft Office 365 for enterprises with the identity in the cloud; without this value, users may not be able to sign into Office 365 with their corporate credentials. UPNs that are used for Federated Identities can contain letters, numbers, periods, dashes, and underscores; no other types of characters are permitted. In addition, UPNs cannot end in a period before the at sign (@). For more information on creating UPNs, see Add User Principal Name Suffixes.
- **Matching domains**: When Office 365 domain names match the domain names for the local Active Directory, no special considerations regarding the name space are required.
- **Sub domains**: Configure top-level domains first, and then configure sub-domains.
- **Local Domains**: Local domains that are configured as .local (for example, contoso.local) cannot be used for federation because they cannot be accessed from the Internet (that is, they are not publicly routable or identifiable in DNS). You can register public domains with your registrar and then federate that domain with Office 365. Then add the new domain as a UPN domain suffix to your forest, and specify UPNs under the new domain. This will ensure that your federated users' UPN domain suffix is under the domain that you federated with Office 365.
- **Multiple distinct logon domains**: You must deploy an Active Directory Federation Services server for each unique domain.
- **Multiple forests**: Multiple forests are not currently supported for Federated Identities.

Network Architecture and Active Directory Federation Services Overview

To authenticate on-premises users to Office 365 using Federated Identities , you must install Active Directory Federation Services (AD FS) 2.0 on a local server that users can access. To provide high availability, install Active Directory Federation Services in a load-balanced design, selecting the Farm option. By selecting the Farm option, you can later add more servers without rerunning the Microsoft Online Identity Federation Management tool, even if you start with only one Active Directory Federation Services 2.0 server role.

The Office 365 online help article Plan for and deploy Active Directory Federation Services 2.0 for use with single sign-on provides additional information on building out your AD FS infrastructure. Table 8 shows recommended hardware configurations based on the number of users.

Table 7: Recommended hardware configurations

Number of users	Recommended hardware configuration
Fewer than 15,000 users	Use existing Active Directory domain controllers for the Active Directory Federation Services 2.0 server role if external access isn't required. If external access is required, use existing web servers or proxy servers. All of these servers must use either Windows Server 2008 or Windows Server 2008 R2. We recommend the use of two servers in a load-balanced configuration, because if no servers are available, then users can't access Office 365.
15,000 to 30,000 users	Use two dedicated servers for the Active Directory Federation Services 2.0 primary federation server and an additional Active Directory Federation Services 2.0 federation server. If users need to access services remotely, you should also install the Active Directory Federation Services federation server proxy role on externally facing servers.

Notes

If you deploy Active Directory Federation Services 2.0 for single sign-on, you must install one of following components so users can connect to Exchange Online:

- Active Directory Federation Services 2.0 proxy
- A proxy that can publish Active Directory Federation Services 2.0 endpoints to the Internet (for example, Internet Security and Acceleration Server, Forefront Threat Management Gateway)

Without a proxy in place, users will be unable to connect to Exchange Online using Federated Identities. This is true regardless of the connection method (for example, Outlook, Outlook Web App, Exchange ActiveSync, POP, IMAP, or Exchange Web Services).

For more details on using Active Directory Federation Services with Office 365, see the Office 365 online help topic Prepare for single sign-on.

Delegated Administration and Support for Partners

Office 365 includes a delegated administration features designed specifically to allow you to administer accounts on behalf of customers. You can submit an authorization request to the customer, which, when approved, allows you to administer Office 365 on behalf of the customer. The customer does not require a user account for your use and does not consume an Office 365 license when granting delegated administration authority.

You can manage your customers directly in your Office 365 administration site. Because your customer's administrative settings are managed within your Office 365 administration site, users within your organization who can sign into the site can view or edit customer settings. (Only companies that have approved your access can be seen).

To provide additional security, you can assign full or limited access to users within your organization.

- **Full administration**: Access to all features in the administration center and ability to assign other administrator roles.
- **Limited administration**: Rights to reset passwords, manage service requests, and monitor service health.

SharePoint Online External Sharing

Content collaboration and document management often involves multiple individuals across multiple companies. Editors, designers, partners, customers, and other workers both inside and outside your organization may be actively involved in the life cycles of documents or information. To help people share simply and more securely, SharePoint Online enables external sharing and collaboration with all stakeholders as a part of the overall value of Office 365.

You can invite up to 50 external users to access a SharePoint Online site. You can purchase additional external sharing licenses to invite an additional 50 external users.

You first have to activate the external sharing feature . Once enabled, your named SharePoint Online Administrator can invite external users to the desired site collections using the built-in wizard. External users will then receive email messages that direct them to sign in with their Office 365 credentials to gain access.