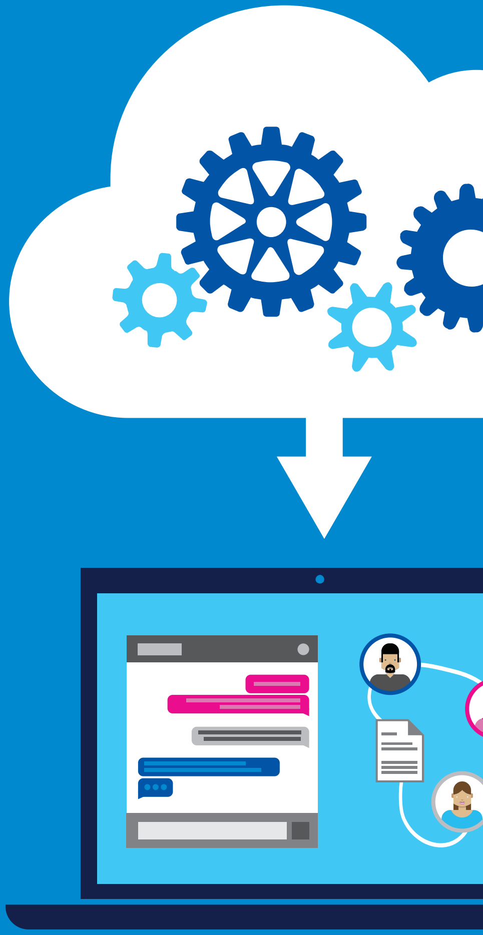
Microsoft

Cloud-Accelerated Hybrid Scenarios with SharePoint and Office 365



About this guide

This pocket guide provides an overview of Microsoft SharePoint and Microsoft Office 365 hybrid scenarios, including basic details on successfully configuring one or more hybrid workloads. For detailed documentation and support for these scenarios, refer to Microsoft TechNet.

Overview

Cloud computing has become ubiquitous, and cloud services—such as Office 365—can be an attractive alternative to on-premises SharePoint business solutions. However, for a variety of reasons, you might want or need to deploy specific solutions in the cloud while still maintaining your on-premises SharePoint Server farm. Some enterprises may wish to gradually move their existing on-premises SharePoint Server services to the cloud, using a staged migration in which SharePoint Server workloads are moved one at a time to SharePoint Online or Office 365. Hybrid functionality in on-premises SharePoint and Office 365 enables you to extend your on-premises investment to the cloud by integrating services like SharePoint Search, Office 365 Video, Microsoft Business Connectivity Services (BCS), Microsoft OneDrive for Business, Microsoft Office Delve, Microsoft Yammer, and Microsoft/SAP Duet Enterprise Online.

Learn more about SharePoint Server and SharePoint Online.

A SharePoint hybrid environment integrates features in Office 365 with SharePoint. By leveraging both systems and allowing access to both, companies can integrate their business services to create a hybrid SharePoint environment that enables secure access to applications and data from almost anywhere.

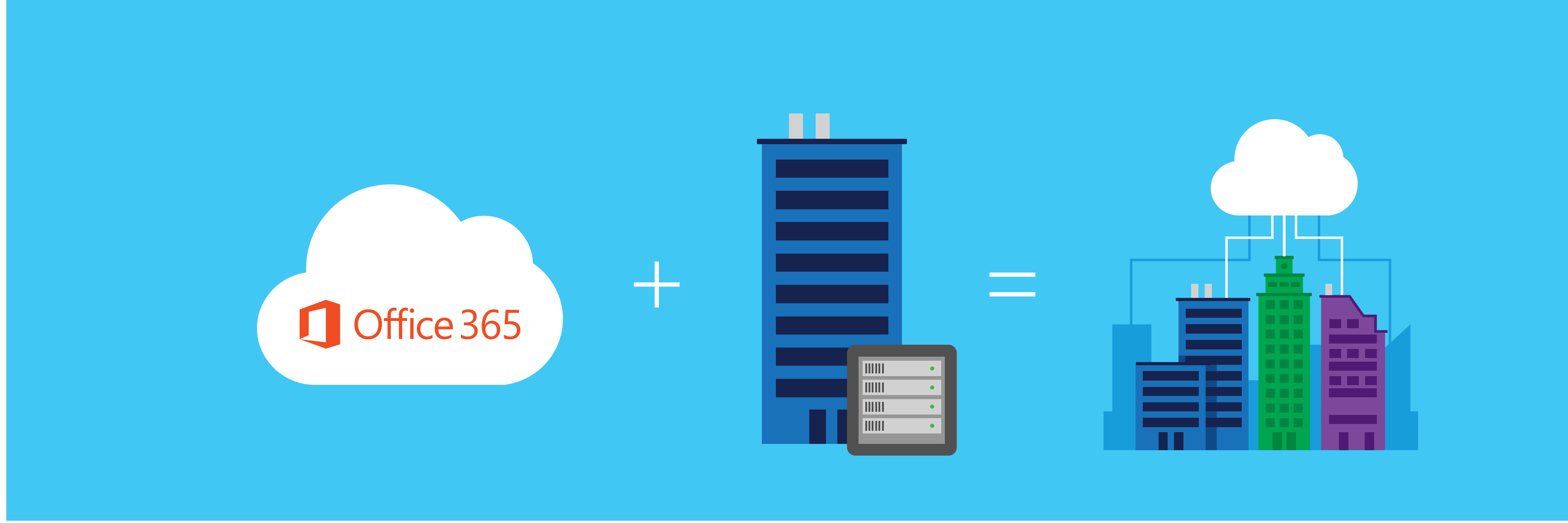
Overview

A hybrid SharePoint environment enables enterprise users to:

- Simultaneously search for content in SharePoint Server and SharePoint Online
- Interact with on-premises business data from SharePoint Online
- Access corporate SAP systems from SharePoint Online
- Seamlessly access files and data in both SharePoint Server and SharePoint Online
- Enable Office 365 cloud services—such as Office 365 Video, Delve, and the app launcher—to integrate with SharePoint Server

Additionally, a hybrid SharePoint environment can provide greater flexibility in your content management strategy by allowing you to keep sensitive data on-premises while migrating other content to the cloud.

A hybrid solution lets you explore cloud functionality on a limited scale by enabling you to take small steps at first. Some companies prefer taking this slower approach and learning what works best for them. You can use hybrid SharePoint to provide access to collaboration features and content for team projects, extranet users, and remote divisions. You can also use it to migrate team projects to SharePoint Online while maintaining connectivity to SharePoint Server 2013/2016 content and resources. A hybrid environment enables enterprise users to connected from almost anywhere to the resources and content they need.



If your on-premises SharePoint Server 2013/2016 environment contains custom code or a third-party solution package that prevents you from completely migrating from your on-premises environment, a hybrid environment enables you to retain that system and also extend it to the cloud when necessary. Many companies have sensitive data that must remain directly within the company's control or within specific geopolitical boundaries due to regulatory restrictions. Using hybrid SharePoint, private or sensitive data can stay on-premises without compromise. As a business, you can decide how to customize the experience to make sure the right people can get to the right data securely.

There are several different options for SharePoint hybrid. The hybrid SharePoint model, or topology, you choose depends on what your business needs and goals are. The size of your company and the complexity of your existing setup must be seriously considered. If you are a small or mid-sized organization, it may be more cost effective to adopt a full cloud model to reduce IT infrastructure costs and management.

Before you start planning a hybrid solution, you need to determine what exactly you want to accomplish. What business problems are you trying to solve? Do you want to find ways to make your company more flexible and mobile? Do you have most of your workloads on an on-premises SharePoint server? Do you have remote workers using the extranet who don't have access to resources on your on-premises servers? For example, maybe you have a sales representative on the road who is logged on to SharePoint Online and needs to know if an important sales document exists anywhere in the company system. A hybrid solution can make it possible for that sales representative to search and connect easily with the needed data.

Remember that a SharePoint hybrid environment isn't static. You can evolve it over time as the needs and demands of your users grow. The right hybrid environment is the one that is right for you, your business, and your customers.

Authentication and authorization

A rich hybrid implementation requires a comprehensive identity and access management cloud solution that provides a robust set of capabilities to manage users and groups. It should help secure access to on-premises and cloud applications, including Microsoft Online Services like Office 365 and many non-Microsoft software-as-a-service (SaaS) applications.

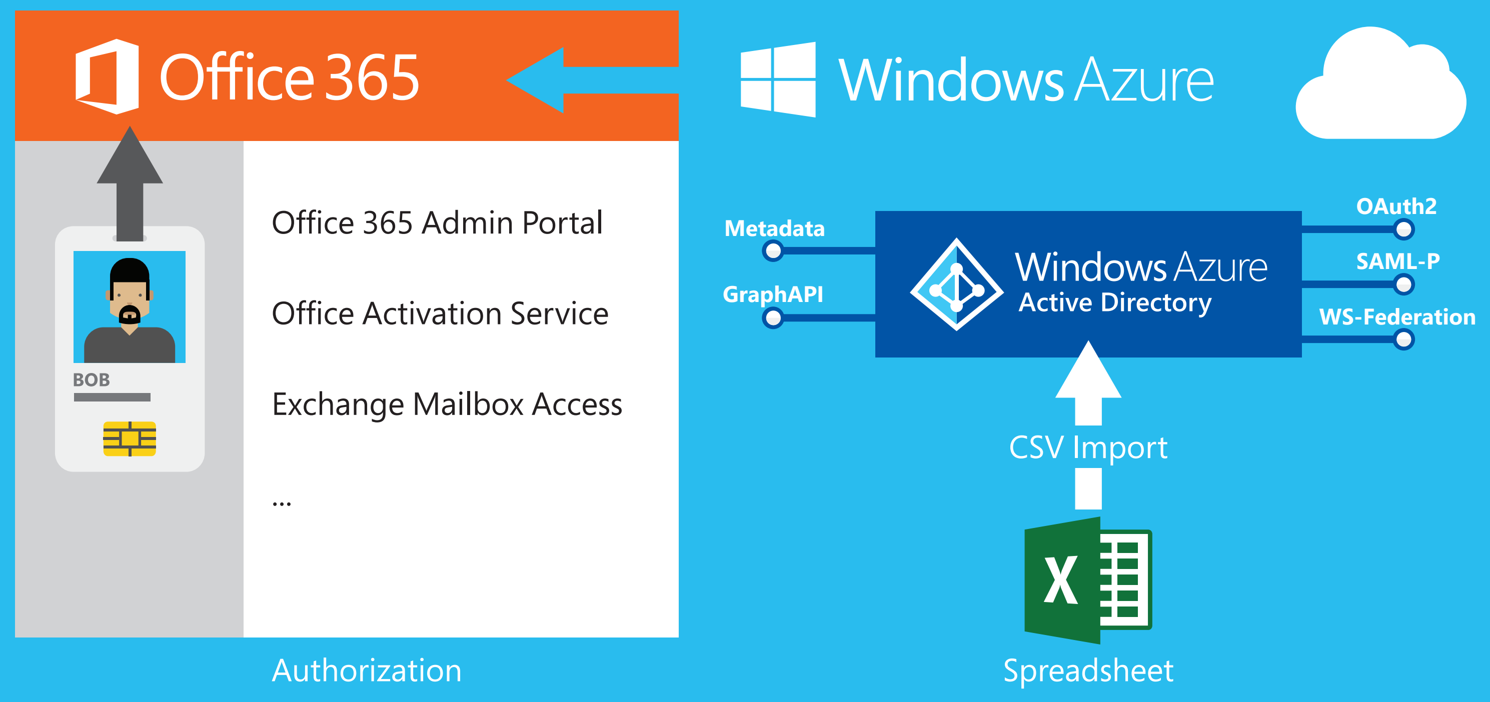
How identity is managed is the first step in preparing your SharePoint and Office 365 hybrid scenario; it defines how users will authenticate and authorize against Office 365 resources and what their ultimate experience will be. A properly planned identity scenario can reduce user friction and abstract cloud resources for greater adoption of Office 365 services.

When you integrate with directory services, you can synchronize and manage user accounts for both environments. You can also add password synchronization or single sign-on (SSO) so users can log on to both environments with their on-premises credentials.

When you integrate with on-premises server products, you create a hybrid environment. A hybrid environment can help you migrate users or information to Office 365, or you can keep some users and information on-premises and some in the cloud.

Getting started with identity integration

The initial prerequisite step to implementing a hybrid scenario is choosing the most effective identity management/federation options to suit your business needs. At a minimum, cloud identity is required to enable most hybrid scenarios with Office 365. Otherwise, organizations seeking a more integrated, seamless experience should consider using Directory Synchronization with Password Sync or Microsoft Active Directory Federation Services (AD FS) with SSO for integrated authentication and authorization experiences.



Cloud identity

Cloud identities provide the most rapid solution to provisioning users in Office 365. Cloud identity is based on a separate, discrete set of credentials established in Azure Active Directory (Azure AD); however, no correlation exists between the cloud identity and the organization's primary identity provider, such as Microsoft Active Directory Domain Services (AD DS).

Cloud identity provides a rapid, easy-to-configure scenario for smaller organizations: businesses can quickly establish, manage, and authenticate users with no change to their existing identity management systems or practices. In a cloud identity scenario, users are discretely managed through a web portal and Azure AD in the Microsoft cloud.

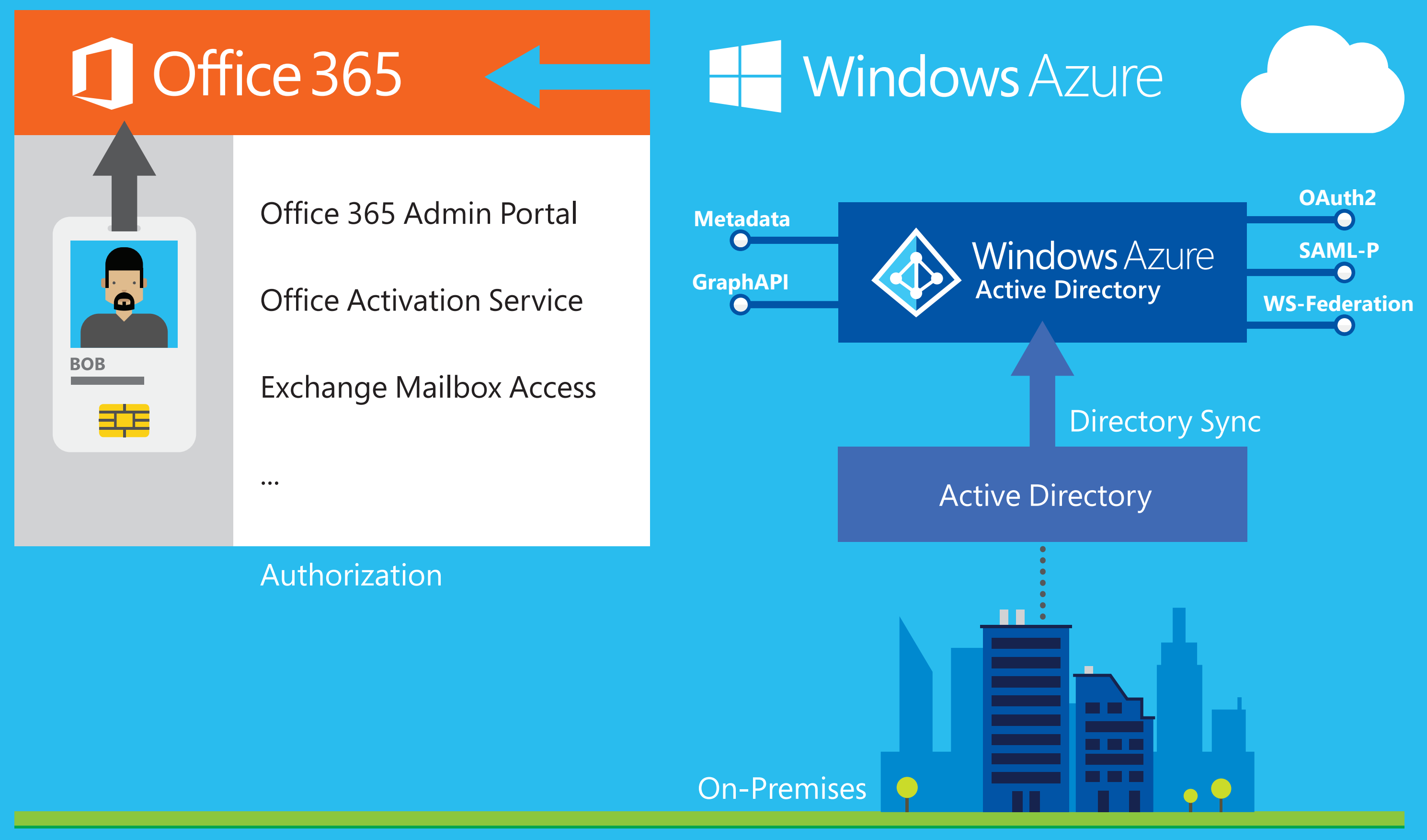
Authentication and authorization

Advantages

- Requires no additional hardware or change to existing identity management infrastructure
- Simple management and control of user identity—suitable for organizations with 0-50 users

Disadvantages

- Identity and authentication are managed completely in the cloud without affinity to an on-premises Active Directory store
- Discrete credentials across SharePoint Server on-premises and Office 365
- Disconnected user experiences
- Cannot be combined/used with hybrid SharePoint 2013/2016 and Office 365 hybrid topologies

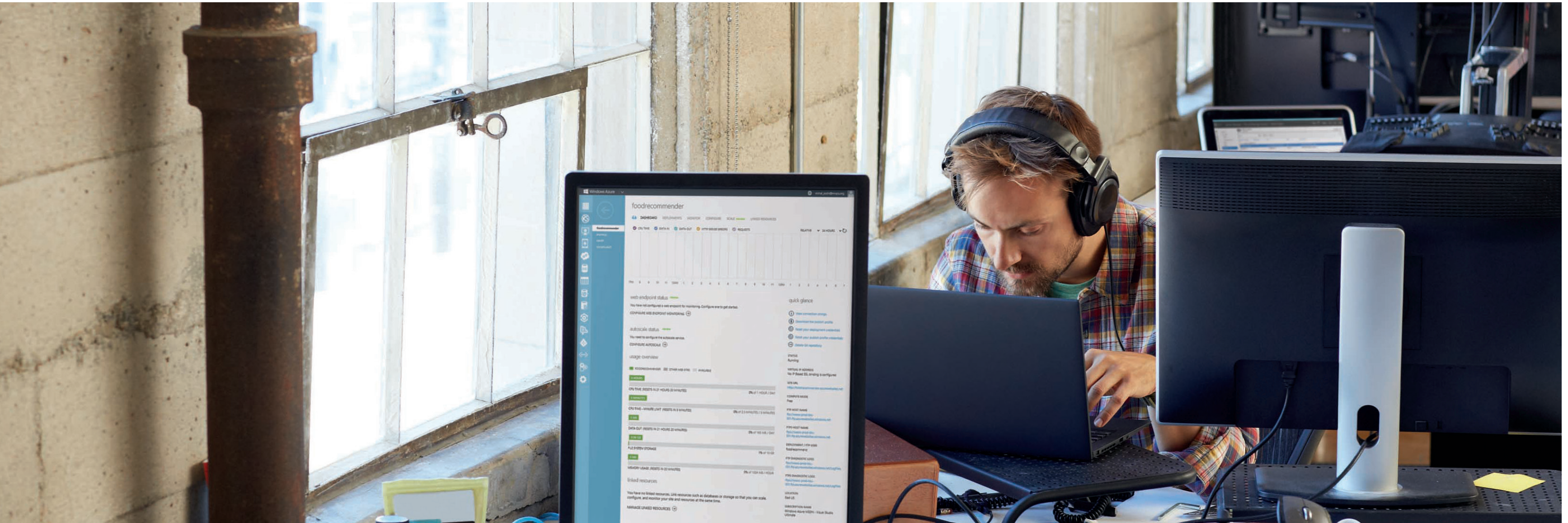


Directory Synchronization with Password Sync

Directory Synchronization enables an organization with an established on-premises Active Directory environment to leverage their existing on-premises and user and group accounts in Office 365. This reduces overall operational costs and provides easier user access to cloud services, such as OneDrive for Business. Directory Synchronization continuously synchronizes on-premises user and group accounts with Azure AD. By combining Directory Synchronization with Password Sync, user passwords and user and group accounts are synchronized to Azure AD. This enables users to log on to cloud services using the same credentials they use to log on to their corporate network.

Advantages

- Requires no additional hardware or change to existing identity management infrastructure
- Eliminates the need to manually manage user and group accounts in Azure AD
- Enables an integrated user authentication experience across on-premises and cloud services



Disadvantages

- Somewhat disconnected user experience (users are required to log on to cloud services)
- If a user is in the scope of Password Sync, the cloud account password is set to "Never Expire." This means that it is possible for a user's password to expire in the on-premises environment, but they can continue logging on to cloud services using this expired password.
- Users are authenticated against cloud services as opposed to on-premises Active Directory

Learn more about directory synchronization.

Microsoft Azure Active Directory Connect

Azure AD Connect integrates your on-premises identity system, such as Windows Server Active Directory, with Azure AD, and it connects your users to Office 365.

Why use Azure AD Connect

Integrating your on-premises directories with Azure AD increases productivity by providing a common identity for accessing both cloud and on-premises resources. This integration gives users and organizations the following advantages:

- Users can use a single identity to access on-premises applications and cloud services
- A single tool delivers an easy deployment experience for synchronization and sign-in
- It provides the newest capabilities for your scenarios and replaces older versions of identity integration tools. Read the directory integration tools comparison to learn more.

How Azure AD Connect works

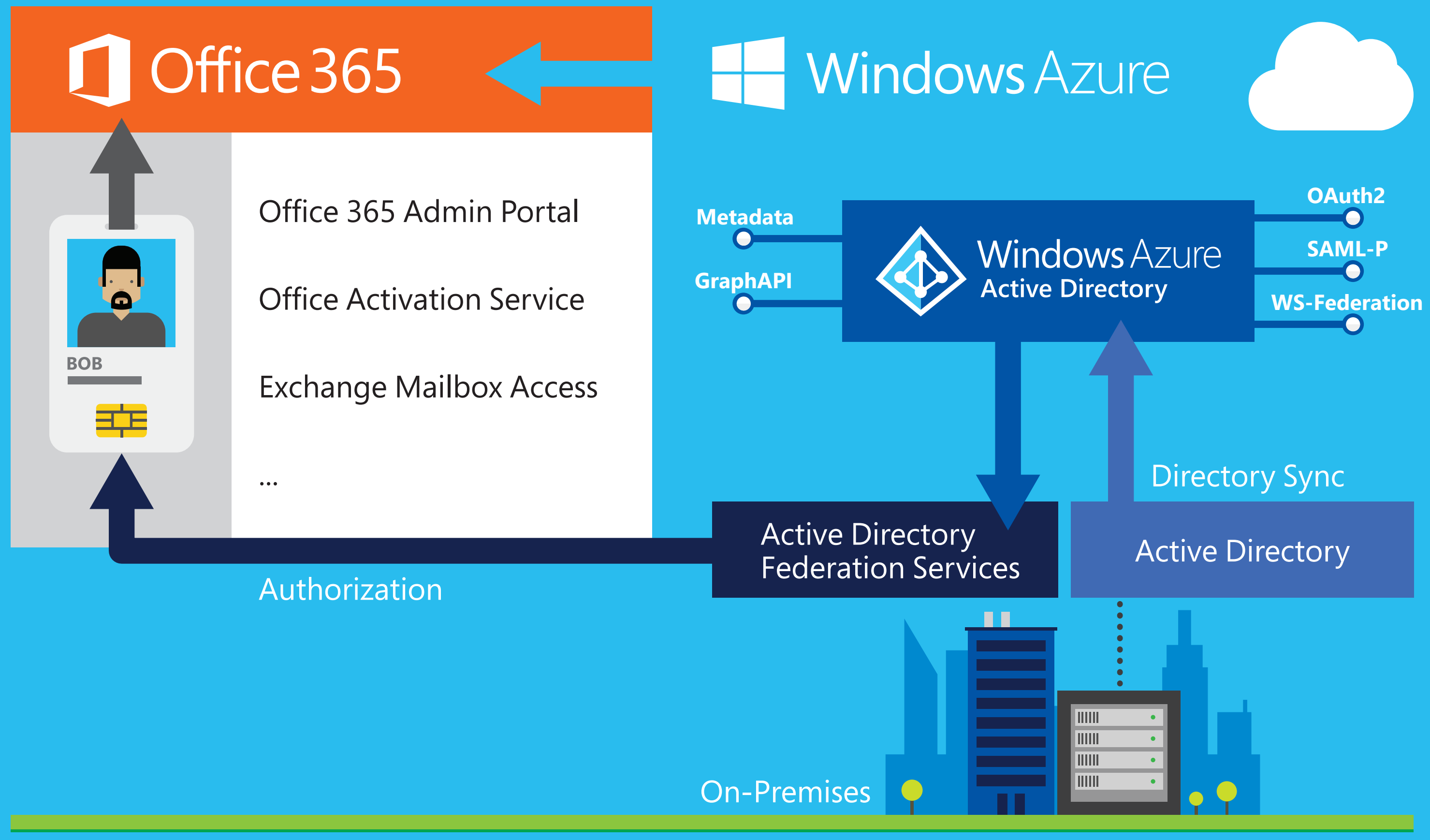
Similar to DirSync, Azure AD Connect is made up of three primary parts: the synchronization services, the optional AD FS piece, and the Azure AD Connect Health tool.

- **Synchronization:** This part includes the components and functionality previously released as Directory Sync and Azure AD Sync. It is responsible for creating users and groups as well as making sure the information on users and groups in your on-premises environment matches the cloud.
- **AD FS:** This is an optional part of Azure AD Connect that can be used to set up a hybrid environment using an on-premises AD FS infrastructure. It can be used to address complex deployments that include such things as domain join SSO, enforcement of Active

Directory logon policy, and smart card or third-party multi-factor authentication (MFA).

- **Azure AD Connect Health:** This can provide robust monitoring of your AD FS servers and a central location in the Azure portal for viewing this activity.

Learn more about Azure AD Connect.



Active Directory Federation Services and SSO

AD FS makes it possible for local and federated users to use claims-based SSO to access websites and services, including cloud services such as Office 365. AD FS enables your organization to collaborate securely with other external organizations across Active Directory domains by using identity federation. This reduces the need for duplicate accounts, management of multiple logons, and other credential management issues that can occur when establishing cross-organizational trusts.

Advantages

- Complete SSO experience with minimal-to-no credential prompts
- Improved security over Directory Synchronization (users are authenticated against on-premises Active Directory)
- Required for complex hybrid scenarios

Disadvantages

- Additional infrastructure required (federation services)
- Added operational complexity

Learn more about Office 365 Single Sign-On with AD FS 2.0.

Getting started with directory synchronization

If your company has existing user and group accounts in an on-premises Active Directory environment at the time you subscribe to a Microsoft cloud service, you can use Microsoft tools to synchronize those accounts to Azure AD where a copy of those accounts are stored in the cloud.

By using Azure AD Sync, your company's administrators can keep your on-premises Active Directory continuously synchronized with Azure AD. Directory synchronization is intended as an ongoing relationship between your on-premises environment and Azure AD.

Active Directory synchronization should be considered a long-term commitment to coexistence scenarios between your on-premises Active Directory and the cloud. Note that after you activate directory synchronization, you will be limited to editing synchronized objects only in your on-premises environment.

Activate directory synchronization

Follow these steps to activate directory synchronization:

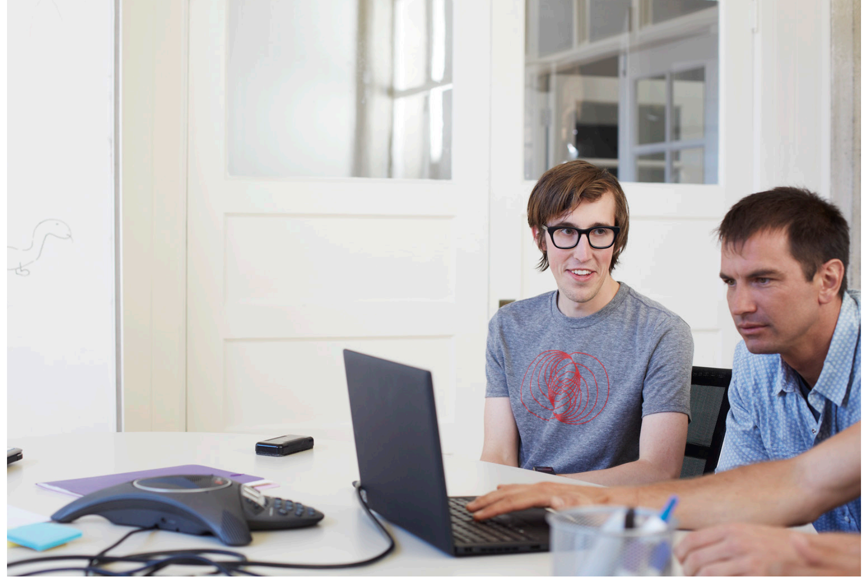
1. Install and run the Microsoft Office 365 Deployment Readiness Tool.
2. Depending on which portal you use, do one of the following:
   - If you are using Office 365 or another account portal, click **Users** and then click **Set up** located next to **Active Directory synchronization**. Proceed to the next step.
   - If you are using the Azure portal, click **Active Directory**, click your directory name on the **Enterprise Directory** page, and then click **Directory Integration**. Proceed to the next step.
   - If you are using the Azure AD Preview Portal, click **Integration** in the left pane and then click **Deploy directory sync**. Proceed to the next step.
3. Click **Activate**.

Learn more about activating directory synchronization.

Follow these steps to configure directory synchronization:

1. Download and install the Azure AD Sync tool on your computer.
2. Follow the instructions in the setup wizard.
3. On the last page of the setup wizard, select **Start Configuration Wizard now**. Then click **Finish**.
4. Provide the Enterprise Administrator and Azure AD credentials as prompted.
5. Enable the optional features that are required.
6. When prompted, select **Synchronize your directories now** to start synchronization.

Learn more about configuring directory synchronization.



Synchronize directories

Follow these steps to configure directory synchronization:

1. To start the configuration wizard, do one of the following:
   - If you are setting up directory synchronization for the first time, select **Start Configuration Wizard now** on the last page of the Azure AD Sync setup wizard, and then click **Finish**.
   - If you are updating the configuration of directory synchronization, click **Start** and then click **All Programs**. Click **Microsoft Azure Active Directory**, click **Directory Synchronization**, and then click **Directory Sync Configuration**. Read [Manage directory synchronization]() to learn more.
2. On the **Microsoft Azure Active Directory Credentials** page, type your cloud administrator credentials and then click **Next**.
3. On the **Active Directory Credentials** page, type your Active Directory Enterprise admin credentials and then click **Next**.
4. On the **Exchange hybrid deployment** page, you can activate the Exchange hybrid deployment features if you have already installed Exchange Server 2010 Service Pack 1. If you activate the Exchange hybrid deployment features, the Directory Sync tool will write attribute data back into your on-premises Active Directory.

Force directory synchronization

If you don't want to wait for the recurring synchronizations that occur every three hours, you can force directory synchronization at any time. For example, if an employee is terminated, you may want to immediately disable or delete their Active Directory account in the cloud if the account was created there, or on-premises if the account was created locally. Then you would force directory synchronization to prevent that employee's continued access to your email system and network resources. For more information, watch How to force directory synchronization.

Force directory synchronization using Windows PowerShell

You can use the directory synchronization Windows PowerShell cmdlet (command-let lightweight script) to force synchronization. The cmdlet is installed when you install the Directory Sync tool.

1. On the computer that is running the Directory Sync tool, start PowerShell, type **Import-Module DirSync**, and then press **ENTER**.
2. Type `Start-OnlineCoexistenceSync` and then press **ENTER**.

Learn more about synchronizing directories.

Getting started with Azure Active Directory Connect

This guide describes the basic steps required to configure Azure AD Connect. For detailed documentation on additional scenarios, read Custom installation of Azure AD Connect.

Express installation of Azure AD Connect

Express installation is the default option and is one of the most common scenarios. When using this option, Azure AD Connect deploys sync with the password sync option. This is for a single forest only and allows your users to use their on-premises password to sign in to the cloud. Using the express settings will automatically initiate a synchronization once the installation is complete. With this option, there are only a few short clicks to extending your on-premises directory to the cloud.

To install Azure AD Connect using the express settings, follow these steps:

1. Download and install Microsoft Azure Active Directory Connect on the designated server for synchronization tasks.
2. On the **Welcome** page, select the check box to agree to the licensing terms. Then click **Continue**.
3. On the **Express Settings** page, click **Use express settings**.
4. On the **Connect to Azure AD** page, enter the username and password of an Azure global administrator for your Azure AD. Click **Next**.
5. On the **Connect to AD DS** page, enter the username and password for an enterprise admin account. Click **Next**.
6. On the **Ready to Configure** page, click **Install**.
    - Optionally, on the **Ready to Configure** page, you can clear the **Start the synchronization process as soon as configuration completes** check box. The wizard will then configure sync but will not run until you manually enable it in the Task Scheduler. Once the task is enabled, synchronization runs every three hours.

- Also optionally, you can choose to configure sync services for Exchange hybrid deployment by selecting the corresponding check box. If you don't plan to have Exchange mailboxes both in the cloud and on-premises, you do not need this.

7. Once the installation completes, click **Exit**.

8. Log off and log on again before you use Synchronization Service Manager or Synchronization Rule Editor.

Assigning licenses to Azure AD Premium and Enterprise Mobility users

Now that your users have been synchronized to the cloud, you will need to assign them a license so they can begin using cloud apps, such as Office 365.

Follow these steps to assign an Azure AD Premium or Enterprise Mobility Suite License:

1. Sign in to the Azure portal as an administrator.

2. Select **Active Directory**.

3. On the **Active Directory** page, double-click the directory that holds the users you wish to enable.

4. At the top of the **Directory** page, select **Licenses**.

5. On the **Licenses** page, select **Active Directory Premium** or **Enterprise Mobility Suite** and then click **Assign**.

6. In the dialog box, select the **users** you want to assign licenses to and then click the **check mark icon** to save the changes.

Verifying the scheduled synchronization task

You can view the current status of a synchronization task in the Azure portal.

To verify the scheduled synchronization task:

1. Sign in to the Azure portal as an administrator.
2. Select **Active Directory**.
3. On the **Active Directory** page, double-click the directory that holds the users you wish to enable.
4. At the top of the **Directory** page, select **Directory Integration**.
5. Under **Integration with Local Active Directory**, note the last sync time.

Starting a scheduled synchronization task

If you need to run a synchronization task, you can run through the Azure AD Connect wizard again. You will need to provide your Azure AD credentials. In the wizard, select the **Customize synchronization options** task. Next, click through the wizard. At the end, ensure that the **Start the synchronization process as soon as the initial configuration completes** check box is selected.

Upgrade from DirSync to Azure AD Connect

Do not uninstall DirSync before the upgrade to Azure AD Connect. Azure AD Connect will read and migrate the configuration from DirSync and will uninstall it after inspecting the server.

Different options for the upgrade are available depending on your current DirSync deployment. If the expected upgrade time is less than three hours, an in-place upgrade is your best option. If the expected upgrade time is more than three hours, a parallel deployment on another server would be the better choice.

Note: If you have more than 50,000 objects, the upgrade is likely to take more than three hours.

Scenario	
In-place upgrade	Preferred option if the upgrade is expected to take less than three hours.
Parallel deployment	Preferred option if the upgrade is expected to take more than three hours.

In-place upgrade

The expected time to complete the upgrade is displayed by the wizard. This estimate is based on the assumption it will take three hours to complete an upgrade for a database with 50,000 objects (users, contacts, and groups). Azure AD Connect will analyze your current DirSync settings and will recommend an in-place upgrade if the number of objects in your database is below 50,000. If you decide to continue, your current settings will be applied automatically during the upgrade and your server will automatically resume active synchronization.

If you want to do a configuration migration and do a parallel deployment, you can override the in-place upgrade recommendation. For example, you might take the opportunity to refresh the hardware and operating system. Learn more about parallel deployment.

Parallel deployment

Using a parallel deployment is recommended if you have more than 50,000 objects. This will help you and other users avoid any operational delays. The Azure AD Connect installation will attempt to estimate the downtime for the upgrade.

The following configuration changes are supported with DirSync and will be upgraded:

- Domain and organizational unit (OU) filtering
- Alternate ID (UPN)
- Password sync and Exchange hybrid settings
- Your forest/domain and Azure AD settings

Some changes cannot be upgraded from an existing DirSync configuration. If you have made any of these changes, the upgrade will be blocked (see below).

- Unsupported DirSync changes (for example, removed attributes and using a custom extension DLL)
- Filtering based on user attributes

In the event changes are detected that cannot be upgraded, install a new Azure AD Connect server in staging mode and verify the old DirSync and new Azure AD Connect configuration. Reapply any changes using custom configuration, as described in Azure AD Connect Sync custom configuration.

The passwords used by DirSync for the service accounts cannot be retrieved and will not be migrated. These passwords will be reset during the upgrade.

Authentication and authorization

The following are basic steps for upgrading from DirSync to Azure AD Connect:

1. Analyze current DirSync configuration.
2. Collect Azure AD global admin password.
3. Collect credentials for an enterprise admin account (used only during the installation of Azure AD Connect).
4. Install Azure AD Connect (Uninstall DirSync, install Azure AD Connect, and optionally begin synchronization).

Additional steps are required in the following circumstances:

- You're currently using Full SQL Server (local or remote).
- You have more than 50,000 objects in scope for synchronization.

In-place upgrade

1. Download and install Microsoft Azure Active Directory Connect on the designated server for synchronization tasks.
2. Review and agree to the license terms and privacy notice.
3. Select **begin analysis of your existing DirSync installation**.
4. At the completion of the analysis, Azure AD Connect will recommend how to proceed.
5. Provide the password for the account you currently use to connect to Azure AD. This must be the account currently used by DirSync.
6. Provide an enterprise admin account for Active Directory.
7. You’re now ready to configure. When you click **Upgrade**, DirSync is uninstalled, and Azure AD Connect is configured and begins synchronizing.

Parallel deployment

Export the DirSync configuration

Parallel deployment with more than 50,000 objects

If you have more than 50,000 objects, Azure AD Connect will recommend a parallel deployment.

- Click **Export settings**. When you install Azure AD Connect on a separate server, these settings are imported to migrate any settings from your current DirSync to your new Azure AD Connect installation.

Once your settings have been successfully exported, you can exit the Azure AD Connect wizard on the DirSync server. Continue with the steps to install Azure AD Connect on a separate server.

Parallel deployment with fewer than 50,000 objects

If you have fewer than 50,000 objects but still want to do a parallel deployment, follow these steps:

1. Download and install Microsoft Azure Active Directory Connect on the designated server for synchronization tasks.
2. When you see the **Welcome to Azure AD Connect** screen, exit the installation wizard.
3. Open a command prompt.
4. From the install location of Azure AD Connect (Default: C:\Program Files\Microsoft Azure Active Directory Connect), execute the following command: **AzureADConnect.exe /ForceExport**.
5. Click **Export settings**. When you install Azure AD Connect on a separate server, these settings are imported to migrate any settings from your current DirSync to your new Azure AD Connect installation.

Once your settings have been successfully exported, you can exit the Azure AD Connect wizard on the DirSync server. Continue with the steps to install Azure AD Connect on a separate server.

Install Azure AD Connect on separate server

When you install Azure AD Connect on a new server, it assumes that you want to perform a clean install of Azure AD Connect. If you want to use the DirSync configuration, there will be some additional steps.

1. Download and install Microsoft Azure Active Directory Connect on the designated server for synchronization tasks.
2. When you see the **Welcome to Azure AD Connect** screen, exit the installation wizard.
3. Open a command prompt.
4. From the install location of Azure AD Connect (Default: C:\Program Files\Microsoft Azure Active Directory Connect), execute the following command: **AzureADConnect.exe /migrate**.

5. Select the settings file that was exported from your DirSync installation.
6. Configure any advanced options, including:
   - A custom installation location for Azure AD Connect.
   - An existing instance of SQL Server (default: Azure AD Connect installs SQL Server 2012 Express). Do not use the same database instance as your DirSync server.
   - A service account used to connect to SQL Server. If your SQL Server database is remote, this account must be a domain service account.
7. Click **Next**.
8. On the **Ready to configure** page, keep the **Start the synchronization process as soon as the configuration completes** option selected. The server will be in staging mode, so changes will not be exported to Azure AD.
9. Click **Install**.

Verify that Azure AD Connect is ready to begin synchronization

In order to verify that Azure AD Connect is ready to take over from DirSync, open **Synchronization Service Manager** in the **Azure AD Connect** group from the **Start** menu.

Within the application, view the **Operations** tab to confirm that the following operations have been completed:

- Import on the AD Connector
- Import on the Azure AD Connector
- Full Sync on the AD Connector
- Full Sync on the Azure AD Connector

Review the results from these operations and ensure there are no errors.

If you want to review which changes are about to be exported to Azure AD, follow the instructions for verifying the configuration under staging mode. Make required configuration changes to resolve any remaining issues.

If you are satisfied with these changes, you can proceed to uninstall DirSync and enable Azure AD Connect synchronization. Perform the following steps to complete the migration.

Uninstall DirSync (old server)

1. From **Programs and features**, locate **Windows Azure Active Directory sync tool**.
2. Uninstall **Windows Azure Active Directory sync tool**. Note that it might take up to 15 minutes to completely uninstall the sync tool.

With DirSync uninstalled, there is no active server exporting to Azure AD. The next step must be completed before any changes in your on-premises Active Directory will continue to be synchronized to Azure AD.

Enable Azure AD Connect (new server)

1. Select **Configure staging mode**.
2. Turn off staging by clearing the **Enabled staging mode** check box.
3. Click **Next**.
4. On the confirmation page, click **Install**.

Azure AD Connect is now your active server. After installation, you can make additional configuration changes by re-opening Azure AD Connect.

Getting started with AD FS

For a more seamless authentication experience, AD FS can be implemented. However, the implementation is out of scope for this guide.

The option to configure AD FS 2.0 is up to each individual company. With the exception of Internet sites for anonymous access created with SharePoint Online, users must be authenticated when accessing services in Office 365.

For that purpose, Office 365 offers two types of identities, as described earlier in this guide:

- **Microsoft Online Services cloud IDs (Cloud Identity):** For signing in to services in Office 365, users receive cloud credentials that are separate from other desktop or corporate on-premises credentials. Cloud IDs are mastered in the service/cloud.

  Note: With the optional directory synchronization, the user IDs mastered on-premises can be synchronized to the service/cloud in the form of Cloud Identities.

- **Federated IDs (Federated Identity):** SSO can be leveraged in companies with on-premises Active Directory. Users can then sign in to services in Office 365 using their own Active Directory corporate credentials. Their IDs are mastered on-premises in Active Directory and synchronized to the service in the form of Federated IDs.

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 SSO. Once authenticated, users' identities refer to the usernames associated with the Office 365 accounts. Three authentication types are available:

- Cloud Identities
- Cloud Identities plus Directory Synchronization (DirSync)
- Federated Identities plus Directory Synchronization (DirSync)

The type of identity (cloud versus federated) affects the user experience, administrative requirements, deployment considerations, and capabilities using Office 365.

The following is a simplified breakdown of the experience:

- **User experience with Cloud Identities:** Users sign in with their cloud IDs, which are authenticated using traditional challenge/response, where users type in their username and password. Authentication happens in the cloud. Users are always prompted for credentials.

As mentioned above, users have two IDs: one to access on-premises services and one for the services in Office 365. Consequently, users are prompted for credentials even when logged in to their Active Directory domain when accessing Office 365 services. This can be mitigated by selecting the **save password** option when you are prompted.

- **User experience with Federated Identities:** Users sign in with their corporate ID for access to online and corporate services; they are authenticated transparently using AD FS 2.0 when accessing Office 365 services. Authentication happens on-premises against the organization's Active Directory, and users get true SSO. Furthermore, 2-Factor Authentication (2FA) can be utilized if it is deployed on-premises.

- **Administrator experience with Cloud Identities:** Organization administrators manage the password policy both in the cloud and on-premises. The password policy is stored in the cloud with the Office 365 service. Password reset must be managed for on-premises and Microsoft Online Services cloud IDs; consequently, users have to change the password according to the policy for both. Finally, there is no 2FA integration.
- **Administrator experience with Federated Identities:** Organization administrators manage the password policy on-premises only and do not need to worry about password reset for Federated Identities. The organization's Active Directory stores and controls the password policy. Password reset occurs for on-premises IDs only.

After the most appropriate identity integration solution for your business has been determined, you need to evaluate your on-premises identity infrastructure. This evaluation is important for defining the technical requirements to integrate your current identity solution to the cloud identity management system.

You also need to be aware of the cloud services your company might have, so it is important to perform an assessment to understand the current integration with SaaS, IaaS, or PaaS models in your environment. Answer the following questions during this assessment: Does your company have any integration with a cloud service provider? If yes, which services are being used? Is this integration currently in production or is it a pilot?

Note: If you don't have an accurate mapping of all your apps and cloud services, you can use the Cloud App Discovery tool. This tool provides your IT department with visibility into all your organization's business and consumer cloud apps. This makes it easier to discover shadow IT in your organization, including details on usage patterns and any users accessing your cloud applications.

To learn more about configuring Azure AD and Office 365 SSO with AD FS, read the Active Directory from on-premises to the cloud whitepapers. These papers provide an understanding of the different SSO deployment options with Azure AD/Office 365, how to enable SSO using corporate AD credentials and AD FS to Azure AD/Office 365, and the different configuration elements for such deployment. It also provides an end-to-end walkthrough to set up an Azure-based lab environment.

Learn more about supported scenarios for using AD FS to set up SSO in Office 365, Azure, or Microsoft Intune.

Choosing between directory integration with DirSync and Azure AD Connect and AD FS

The decision to implement directory integration with DirSync and/or AD FS depends on several factors, including the desired user experience and available infrastructure.

For organizations with a mature AD FS infrastructure, the option to extend AD FS to Office 365 may be a viable option. On the other hand, organizations seeking to reduce IT complexity and minimize operational costs may elect to leverage DirSync or Azure AD Connect.

Read more about hybrid identity management.

Comparing directory integration solutions

Use the following key for each of the following tables:

● = Available now

FR = Future release

PP = Public preview

On-premises to cloud synchronization

Feature	Azure Active Directory Connect	Azure Active Directory Synchronization Services	Azure Active Directory Synchronization Tool (DirSync)	Forefront Identity Manager 2010 R2 (FIM)v
Connect to single on-premises AD forest	●	●	●	●
Connect to multiple on-premises AD forests	●	●		●
Connect to multiple on-premises Exchange orgs	●	●		
Connect to single on-premises LDAP directory	FR			●
Connect to multiple on-premises LDAP directories	FR			●
Connect to on-premises AD and on-premises LDAP directories	FR			●
Connect to custom systems (such as SQL, Oracle, MySQL)	FR			●

Cloud to on-premises synchronization

Feature	Azure Active Directory Connect	Azure Active Directory Synchronization Services	Azure Active Directory Synchronization Tool (DirSync)	Forefront Identity Manager 2010 R2 (FIM)v
Write back of devices	●		●	●
Attribute write back (for Exchange hybrid deployment)	●	●	●	●
Write back of users and groups objects	●			
Write back of passwords (from self-service password reset and password change)	●	●		●

Authentication feature support

Feature	Azure Active Directory Connect	Azure Active Directory Synchronization Services	Azure Active Directory Synchronization Tool (DirSync)	Forefront Identity Manager 2010 R2 (FIM)v
Password sync for single on-premises AD forest	●	●	●	
Password sync for multiple on-premises AD forests	●	●		
SSO with federation	●	●	●	●
Write back of passwords (from self-service password reset and password change)	●	●		

Setup and installation

Feature	Azure Active Directory Connect	Azure Active Directory Synchronization Services	Azure Active Directory Synchronization Tool (DirSync)	Forefront Identity Manager 2010 R2 (FIM)v
Supports installation on a Domain Controller	●	●	●	
Supports installation using SQL Express	●	●	●	
Easy upgrade from DirSync	●			
Localization Windows Server languages	FR	●	●	
Support for Windows Server 2008 and Windows Server 2008 R2	● Yes for DirSync; No for federation	●	●	●
Support for Windows Server 2012 and Windows Server 2012 R2	●	●	●	Only 2012

Filtering and configuration

Feature	Azure Active Directory Connect	Azure Active Directory Synchronization Services	Azure Active Directory Synchronization Tool (DirSync)	Forefront Identity Manager 2010 R2 (FIM)v
Filter on domains and organizational units (OU)	●	●	●	●
Filter on objects' attribute values	●	●	●	●
Allow minimal set of attributes to be synchronized (MinSync)	●	●		
Allow different service templates to be applied for attribute flows	●	●		
Allow removing attributes from flowing from AD to Azure AD	●	●		
Allow advanced customization for attribute flows	●	●		●

SharePoint Server 2013/2016 prerequisites

A hybrid SharePoint and Office 365 environment requires several services to be provisioned on your server farm environment. These services include:

- Managed metadata service application
- User Profile service application
    - My Sites

These are the baseline services necessary to configure OneDrive for Business redirection as described later in this guide. Additional configuration is required for other hybrid scenarios, including Search and Business Connectivity Services, and those configurations are described in their respective sections of this guide.

In a SharePoint environment where these services have been previously provisioned, no additional instances are required; however, specific configurations for hybrid scenarios may be required.

Managed metadata service application

The managed metadata service application makes it possible to use managed metadata and share content types across site collections and web applications.

A managed metadata service publishes a term store and, optionally, content types; a managed metadata connection consumes these. To learn more, read the overview of managed metadata in SharePoint 2013. Before reading it, however, you may want to review the concepts it presents.

Learn more about managed metadata service applications.

To create a managed metadata service application:

1. In SharePoint Central Administration, under **Application Management**, click **Manage service applications**.
2. Click **New** and then click **Managed Metadata Service**.
3. In the **Name** box, type a name for the service application.
4. In the **Database Name** box, type a name for the database.
5. Under **Application Pool**, choose **SharePoint Web Services Default** from the **Use existing application pool** list**.**
6. Click **OK**.

My Sites

In SharePoint Server 2013/2016, a “My Site” is a personal site for a user in an organization. Although it appears as a single site to the user, the My Sites architecture consists of a web application, a My Site host site collection, an individual site collection, and several SharePoint service applications and features. Except for the individual site collection, all other parts of this infrastructure are configured once and shared among all the users who are part of the My Sites deployment.

Learn more about My Sites.

To create a My Site web application:

1. In SharePoint Central Administration, in the **Application Management** section, click **Manage web applications.**
2. On the ribbon, click **New**.
3. On the **Create New Web Application** page, in the **Authentication** section, select the authentication mode that will be used for this web application.
4. In the **IIS** (Internet Information Services) **Web Site** section, configure the settings for your new web application by selecting one of the following two options:
    - Click **Use an existing web site** and then select the website on which to install your new web application.
    - Click **Create a new IIS web site** and then type the name of the website in the **Name** box. You can also provide the port number, host header, or path for the new IIS website.
5. In the **Security Configuration** section, select an authentication provider. Then, choose whether to allow anonymous access and whether to use Secure Sockets Layer (SSL).
6. In the **Application Pool** section, do one of the following:
    - If you want to use an existing application pool, click **Use existing application pool** and select the application pool from the drop-down menu.
    - If you want to create a new application pool, click **Create a new application pool**, type the name of the application pool, and either select the account that the application pool will run under or create a new managed account for the application pool to run under.
7. In the **Database Name and Authentication** section, select the database server, database name, and authentication method for your new web application.
8. If you use database mirroring, go to the **Failover Server** section. In the **Failover Database Server** box, type the name of the specific failover database server that you want to associate with a content database.

9. In the **Service Application Connections** section, select the service application connections that will be available to the web application.

10. In the **Customer Experience Improvement Program** section, click **Yes** or **No**.

11. Click **OK** to create the new web application.

12. When the **Application Created** page appears, click **OK**.

Create a My Site Host site collection with the following steps:

1. In SharePoint Central Administration, click **Create site collections** in the **Application Management** section.

2. On the **Create Site Collection** page, in the **Web Application** section, select the web application that you just created for My Sites.

3. In the **Title and Description** section, type the title and a description for the site collection.

4. In the **Web Site Address** section, select the path of the URL for the My Site host. In most cases, you can use the root directory (/).

5. In the **Template Selection** section, click the **Enterprise** tab and then select **My Site Host.**

6. In the **Primary Site Collection Administrator** section, type the username (in the form **<DOMAIN>\<username>**) for the user who will be the site collection administrator.

7. In the **Secondary Site Collection Administrator** section, type the username for the secondary administrator of the site collection.
8. If you are using quotas to manage storage for site collections, in the **Quota Template** section, click a template in the **Select a quota template** list.
9. Click **OK**.

User Profile service application

The User Profile service application stores information about users in a central location. Social computing features use this information to enable productive interactions so users can collaborate efficiently. You must enable the User Profile service application to provision My Sites, enable social computing features such as social tagging and newsfeeds, and create and distribute profiles across multiple sites and farms.

Learn more about the User Profile service application.

Use the following steps to create a User Profile service application:

1. In SharePoint Central Administration, under **Application Management**, click **Manage service applications**.
2. Click **New** and then click **User Profile Service Application.**
3. In the **Name** box, type a name for the service application.
4. Under **Application Pool**, choose **SharePoint Web Services Default** from the **Use existing application pool** list.

5. In the **Profile Synchronization Instance** drop-down list, choose the server where you want to run the User Profile Synchronization Service.

   Note: Make note of the server that you choose here. You will need it when you start the service.

6. In the **My Site Host URL** box, type the URL of the My Site Host that you created.
7. Optionally, change other settings to meet your needs. The default settings work fine for hybrid environments.
8. Click **OK**.

Hybrid SharePoint environments rely on the App Management and Microsoft SharePoint Foundation Subscription Settings service applications. These applications use multitenancy features to provide app permissions and create the subdomains for apps. Therefore, even if you are not hosting multiple tenants, you must still establish a name for the default tenant for your environment. (Any SharePoint site that is not associated with a tenant will be in the default tenant.)

App Management service

Use the following steps to create an App Management service application in SharePoint Server 2013/2016:

1. In Central Administration, on the **Application Management** page, click **Manage service applications.**
2. On the ribbon, click **New** and then click **App Management Service.**
3. In the **New App Management Service Application** page, in the **Service Application Name** box, type the name for the service application.
4. In the **Database** section, in the **Database Server** box, type the instance of SQL Server where you want to store the database, or use the default server.
5. In the **Database Name** box, type a database name, or use the default name.
6. Under **Database authentication**, select the authentication that you want to use by doing one of the following:
   - If you want to use Windows authentication, keep this option selected. This option is recommended because Windows authentication automatically encrypts the password when it connects to SQL Server.
   - If you want to use SQL authentication, click **SQL authentication**. In the **Account** box, type the name of the account that you want the service application to use to authenticate to the SQL Server database. Then type the password in the **Password** box.

   Note: In SQL authentication, an unencrypted password is sent to SQL Server. We recommend that you use SQL authentication only if you force protocol encryption to SQL Server or encrypt network traffic by using IPsec.

7. In the **Failover Database Server** section, specify the server name if you want to use a failover database server.
8. In the **Application Pool** section, do one of the following:
   - Click **Use existing application pool.** Then, from the drop-down list, select the application pool you want to use.

- Click **Create a new application pool** and type the name of the new application pool. Then, under **Select a security account for this application pool**, do one of the following:
  - ◦ Click **Predefined** to use a predefined security account and then select the account from the drop-down list.
  - ◦ Click **Configurable** to specify a new security account. You can create a new account by clicking the **Register new managed account** link.

9. In the **Create App Management Service Application Proxy** section, keep the **Create App Management Service Application Proxy and add it to the default proxy group** check box selected.
10. Click **OK**.

Subscription Settings service application

Use the following steps to start the Subscription Settings and App Management services:

1. Verify that you are a member of the farm administrators group in SharePoint Central Administration.
2. In Central Administration, click **System Settings**.
3. On the **System Settings** page, under **Servers**, click **Manage services on server**.
4. On the **Services on Server** page, next to **App Management Service**, click **Start**.
5. On the **Services on Server** page, next to **Microsoft SharePoint Foundation Subscription Settings Service**, click **Start**.

Use the following steps to start the Subscription Settings and App Management services:

1. In Central Administration, under **System Settings**, click **Manage services in this farm**.
2. For the **Microsoft SharePoint Foundation Subscription Settings Service**, click **Enable Auto Provision**.

A hybrid configuration also requires profile synchronization. You can configure a synchronization connection in SharePoint Server 2013/2016 by following these steps:

1. In Central Administration, under **Application Management, click Manage service applications**.
2. Click the **User Profile service application**.
3. Click **Configure Synchronization Connections**.
4. Click **Create New Connection** and type a name for the connection in the **Connection Name** box.
5. In the **Forest name** box, type the name of your domain (for example, contoso.com).
6. Type the username and password of your domain administrator.
7. Click **Populate Containers**.
8. Expand the domain node, and select the check box that indicates where your users are located.
9. Click **OK**.

Validate user profile properties

The **Work email** user property needs to contain the email address that you configured for each user in AD DS. Also, the **User Principal Name** property must be mapped to the **userPrincipalName** attribute.

Use the following steps to verify both of these mappings:

1. In Central Administration, under **Application Management**, click **Manage service applications**.
2. Click the **User Profile** service application.
3. Click **Manage User Properties**.
4. In the **Property Name** column, confirm that **User Principal Name** is mapped to **userPrincipalName** in the **Mapped Attribute** column.
5. In the **Property Name** column, confirm that **Work email** is mapped to **mail** in the **Mapped Attribute** column.

If either of these properties is not mapped as described, you need to update the mapping.

Synchronize user profiles

After you verify the user property mappings, you need to synchronize the User Principal Name domain suffix and email address that you configured in AD DS. Use the following steps to start a profile synchronization manually:

1. In Central Administration, in the **Application Management** section, click **Manage service applications**.
2. Click the **User Profile** service application.
3. On the **Manage Profile Service** page, in the **Synchronization** section, click **Start Profile Synchronization**.
4. On the **Start Profile Synchronization** page, select **Start Incremental Synchronization**.
5. Click **OK**.

Search

Federated search

Federated search is a traditional hybrid experience offered in SharePoint Server 2013/2016. Federated search distributes users' queries across both a local SharePoint Server and a remote SharePoint Online index, returning the results in discrete result blocks.

How do you decide whether to set up hybrid search in the SharePoint Server 2013/2016 farm (outbound hybrid search), or in SharePoint Online (inbound hybrid search), or both? That can depend in part on which deployment users are working in, what content they will need, and where that content is stored.

Outbound hybrid search is generally the simplest hybrid search solution to configure, primarily because it doesn't require configuration of a reverse proxy device. It is also generally the safest hybrid search solution because, unlike inbound hybrid search, it doesn't involve receiving unsolicited calls from the Internet.

For the convenience of users, it can be beneficial to set up hybrid search in the deployment where most users are working. That way, users don't have to go to the remote deployment to search for content.

For performance reasons, it can be beneficial to set up hybrid search in the deployment where most of the content is stored. If most of the search results are from the local deployment, the overall query latency is likely to be less (all other things being equal) than if many results are from the remote deployment. Also, in general, when a user clicks a search result for local content, the response time to open that content will be faster than it would be to open content that is stored remotely. This is especially true for large files.

It can be reasonable to set up hybrid search in both deployments under any of the following circumstances:

- Many users are working in one deployment, and many other users are working in the other deployment
- Much of the content is in one deployment, and much is in the other deployment
- Most users are working in one deployment, and most of the content is in the other deployment

Outbound topology

A one-way outbound hybrid authentication topology enables hybrid service integration in a single direction. In a one-way outbound hybrid topology, SharePoint Server 2013/2016 on-premises consumes content and resources from Office 365. For example, a search can be configured to allow federated users to see both local and remote search results in a SharePoint Server 2013/2016 search portal. An outbound search topology is implemented where SharePoint Online results should appear in a separate result block in SharePoint Server 2013/2016 on-premises. Outbound topologies are the most effective for use with OneDrive for Business redirection because they require minimal configuration and infrastructure requirements.

Learn more about planning a one-way outbound hybrid topology.

Worksheets

Use the following worksheets if you are deploying a SharePoint hybrid environment using a one-way outbound authentication topology.

User accounts

Information needed	Description	Value
Global Administrator	Office 365 account that has been assigned to the **Global Administrator** role for Office 365	
AD Domain Administrator	AD account in the **Domain Admins** group of the on-premises domain	
AD Enterprise Administrator	AD account in the **Enterprise Admins** group of the on-premises domain	
SharePoint Farm Administrator	Member of the **Farm Administrators** group of the on-premises SharePoint farm	
Federated Users	AD accounts that have been synchronized with Office 365	

Authentication and topology choices

Information needed	Choice
Authentication topology Choose the following: • One-way outbound	
Identity management type Choose one of the following: • AD FS with SSO • DirSync with Password Sync	

Public domain information

Information needed	Description	Value
Public Internet Domain name	Domain name of the public-facing corporate DNS domain (such as, adventureworks.com)	
UPN Domain Suffix	The UPN domain suffix in your on-premises AD domain that matches the public domain (such as, sharepoint. adventureworks.com)	

STS Certificate information

Information needed	Value
STS Certificate friendly name	
STS Certificate path\filename (*.pfx file)	
STS Certificate password	
STS Certificate path\filename (*.cer file)	
Subject name	
STS Certificate start date (the date the certificate was issued)	
STS Certificate end date (the certificate expiration date)	

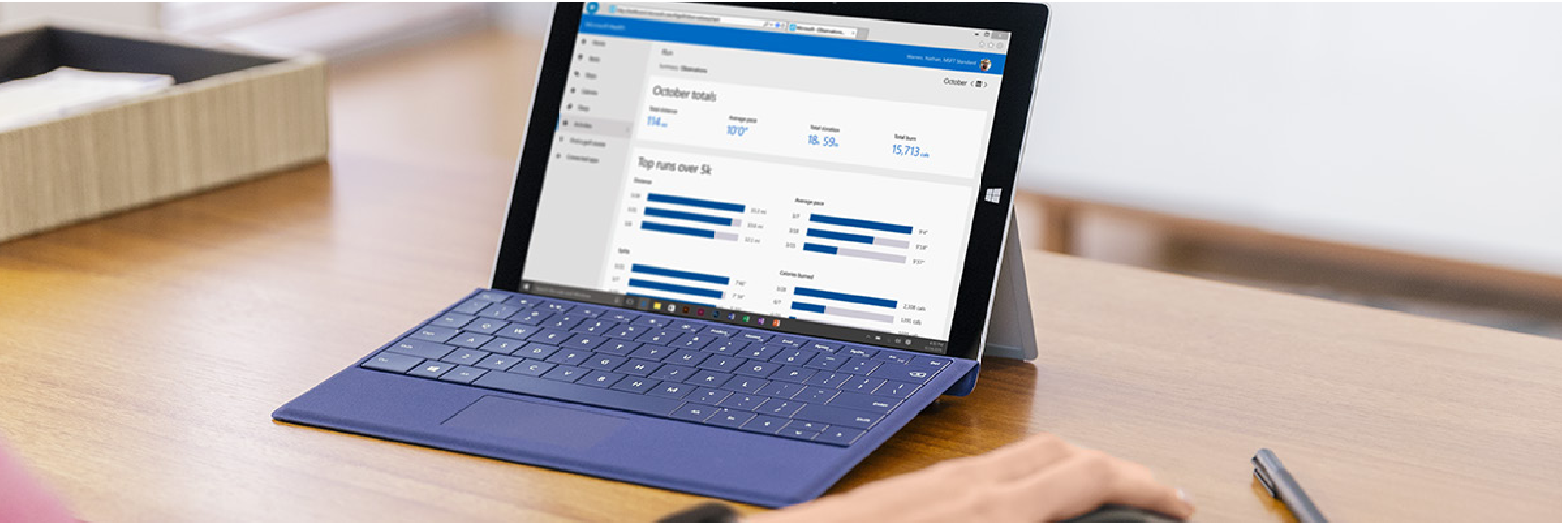
Inbound topology

A one-way inbound hybrid authentication topology enables hybrid service integration in a single direction. In a one-way inbound hybrid topology, Office 365 consumes content and resources from SharePoint Server 2013/2016 on-premises. For example, a search can be configured to allow federated users to see both local and remote search results in an Office 365 search portal. An inbound search topology is implemented where SharePoint Server 2013/2016 on-premises results should appear in a separate result block in SharePoint Online. Inbound topologies, unlike outbound topologies, require additional infrastructure and are least commonly implemented when redirecting OneDrive for Business to Office 365 because both local and remote results are available only in SharePoint Online.

Learn more about planning a one-way inbound hybrid topology.

Worksheets

Use the following worksheets if you are deploying a SharePoint hybrid environment using either a one-way inbound or a two-way authentication topology.



User accounts

Information needed	Description	Value
Global Administrator	Office 365 account that has been assigned to the **Global Administrator** role for Office 365	
AD Domain Administrator	AD account in the **Domain Admins** group of the on-premises domain	
AD Enterprise Administrator	AD account in the **Enterprise Admins** group of the on-premises domain	
SharePoint Farm Administrator	Member of the **Farm Administrators** group of the on-premises SharePoint farm	
Federated Users	AD accounts that have been synchronized with Office 365	

Authentication and topology choices

Information needed	Choice
Authentication topology Choose one of the following: • One-way outbound • Two-way	
Site collection strategy Choose one of the following: • Host-named site collection • Path-based site collection (with AAM) • Path-based site collection (without AAM)	
New or existing web application Choose one of the following: • New • Existing	
Identity management type Choose one of the following: • AD FS with SSO • DirSync with Password Sync	

Public domain information

Information needed	Description	Value
Public Internet Domain name	Domain name of the public-facing corporate DNS domain (such as, adventureworks.com)	
IP Address of the external endpoint	IP address of the external endpoint of the reverse proxy device that faces the Internet; this is used to create an A host record in your public domain (such as, 10.10.10.13)	
External URL	The endpoint URL of the reverse proxy device that faces the Internet (such as, https://spexternal.adventureworks.com)	
UPN Domain suffix	The UPN domain suffix in your on-premises AD domain that matches the public domain (such as, sharepoint. adventureworks.com)	

STS Certificate information

Information needed	Value
STS Certificate friendly name	
STS Certificate path\filename (*.pfx file)	
STS Certificate password	
STS Certificate path\filename (*.cer file)	
Subject name	
STS Certificate start date (the date the certificate was issued)	
STS Certificate end date (the certificate expiration date)	

Secure Channel SSL Certificate information

Information needed	Description	Value
Secure Channel SSL Certificate location and filename	Provides a secure communication channel between the reverse proxy device and Office 365 Provide the name of the certificate, including the file extension and the location where it’s stored	
Secure Channel SSL Certificate friendly name	(Optional) Friendly name of this certificate, if there is one	
Type of certificate	Wildcard or Subject Alternative Name (SAN) certificate?	
Expiration date	Date the certificate expires	
Secure Channel SSL Certificate password	If this certificate contains a private key, record the password assigned to the certificate	

Web application SSL Certificate information

Information needed	Description	Value
Web application SSL Certificate location and filename	Provides a secure communication channel between the reverse proxy device and Office 365 Provide the name and location of the certificate, including file extension	
Web application SSL Certificate friendly name	Friendly name of this certificate	
Type of certificate	Wildcard or SAN certificate?	
Expiration date	Date the certificate expires	
Web application SSL Certificate password	If this certificate contains a private key, record the password assigned to the certificate	

Primary web application (host-named site collection) information

Information needed	Description	Value
Primary web application URL	The URL, including the port number, of the web application you want to use for SharePoint hybrid (such as, https://sharepoint)	
Port number of the web application	Port number configured for the extended web application (such as, 443)	
Protocol of the web application	Protocol used for the extended web application (such as, http or https)	
Host-named site collection URL	Date the certificate expires	
Web application SSL Certificate password	URL of the top-level site collection of the web application you are using for SharePoint hybrid (such as, https://spexternal.adventureworks.com)	

Primary web application (path-based web application without alternate access mappings/AAM)

Information needed	Description	Value
Primary web application URL	The URL, including the port number, of the web application you want to use for SharePoint hybrid	
Port number of the web application	Port number configured for the extended web application (such as, 443)	
Protocol of the web application	Protocol used for the extended web application (such as, http or https)	

Primary web application (path-based web application with alternate access mappings/AAM)

Information needed	Description	Value
Primary web application URL	The internal URL of the primary web application, including the port number	
Port number of the extended web application	The port number assigned to the extended web application; this is needed when configuring the reverse proxy device	
AAM zone of the extended web application	The AAM zone you chose when extending the primary web application	
Bridging URL	URL you use when you add an AAM (internal URL) to the zone of the extended web application URL is comprised of the protocol of the extended web application and the host name you want to use as the bridging URL	

SharePoint Online Secure Store target application

Information needed	Description	Value
Target application ID	Target application ID that you assigned to the target application	
Target application display name	Friendly name of the target application	
Target application admins Target application members	Federated users you want to enable to use hybrid functionality or the security group in Office 365 that contains the federated users	

Bidirectional topology

A two-way topology enables bidirectional hybrid service integration between SharePoint Server 2013/2016 on-premises and Office 365. For example, a search can be configured to allow federated users to see both local and remote search results in either SharePoint Server 2013/2016 on-premises or SharePoint Online search portals. Bidirectional topologies, like inbound topologies, require a reverse proxy device, in addition to a virtual private network (VPN) and/or Microsoft DirectAccess.

Configure federated search

To configure search results once the desired topology has been implemented, refer to the steps that follow in this section.

Create a result source that defines how to get results from SharePoint Online

In this procedure, you create a result source in the SharePoint Server 2013/2016 deployment. This result source is a definition that specifies SharePoint Online as a provider of search results. This definition specifies each of the following:

- The SharePoint Online URL from which to get search results
- The protocol for getting those results
- The method for authenticating against SharePoint Online

Result sources can be created at the Search service application level, the site collection level, or the site level. In this procedure, you create the result source at the Search service application level. This will make the result source available to any query rule that is created at the same level, and also any query rule that is created for a site collection or site that is in a web application that consumes the Search service application.

For more information about result sources, go to the following resources:

- Understanding result sources for search in SharePoint Server 2013
- Configure result sources for search in SharePoint Server 2013

Use the following steps to create the result source:

1. Verify that the user account you use to perform this procedure is an administrator for the Search service application.
2. In Central Administration, in the **Application Management** section, click **Manage service applications**.
3. Click the desired Search service application.
4. On the **Search Administration** page, in the **Quick Launch**, click **Result Sources**.
5. On the **Manage Result Sources** page, click **New Result Source**.
6. On the **Add Result Source** page, in the **General Information** section, type a name for the new result source in the **Name** text box—for example, **Get results from SharePoint Online**. Optionally, type a description in the **Description** box—this will appear as a tooltip when the pointer rests on the result source on certain configuration pages.
7. In the **Protocol** section, select **Remote SharePoint**.
8. In the **Remote Service URL** section, type the address of the root site collection in SharePoint Online from which you want to get search results, such as **https://adventure-works.sharepoint.com**.
9. In the **Type** section, select **SharePoint Search Results**.
10. In the **Query Transform** section, do one of the following:
    - Keep the default query transform **{searchTerms}**, which is a query variable that stands for the query that the user typed, as it was changed by the most recent query transform.
    - Type a different query transform in the text box, or click **Launch Query Builder** if you want to use Query Builder to help you configure a query transform.

    Note: You can use the query transform to narrow the search results to a specified subset—for example, a subset that is from a particular SharePoint site collection or site. However, if you are not familiar with query transforms, we recommend that you keep the default here. For more information, go to the following resources:

   - [Plan to transform queries and order results in SharePoint 2013]
   - [Query variables in SharePoint Server 2013]

11. In the **Credentials Information** section, select **Default Authentication**.

12. Click **Save** to save the new result source.

Create a query rule to turn on hybrid search results in SharePoint Server 2013/2016

In this procedure, you create a query rule in the SharePoint Server 2013/2016 deployment. This query rule uses the result source that you created in the previous procedure. When the query rule fires, it causes search results from the SharePoint Online search index to be displayed in a result block on a search results page in the SharePoint Server 2013/2016 deployment. The results from the SharePoint Online search index are displayed along with results from the SharePoint Server 2013/2016 search index.

Query rules can be created at the Search service application level, the site collection level, or the site level. In this procedure, you create the query rule at the Search service application level. Because you create the rule at this level, the rule can apply to queries that users submit in sites or site collections that consume the Search service application.

Use the following steps to create the query rule:

1. Verify that the user account you use to perform this procedure is an administrator for the Search service application.

2. In Central Administration, in the **Application Management** section, click **Manage service applications**.

3. Click the Search service application in which you created a result source in the previous procedure.

4. In the **Search Administration** page in the **Quick Launch**, click **Query rules**.

5. On the **Manage Query Rules** page, do the following:

   5.1 Under **For what context do you want to configure rules?**, in the **Select a Result Source** drop-down list, select a result source for which you want this query rule to be applicable. For testing, we recommend you select **Local SharePoint Results** here. If you do so, then by default the query rule will be applicable when a user performs a query in the **Everything** search vertical in the enterprise Search Center. On the **Add Query Rule** page, in the **Context** section, you can add or remove result sources.

   5.2 Optionally, under **For what context do you want to configure rules?**, in the **User Segments** drop-down list, select a user segment for which you want this query rule to be applicable. User segments are based on terms that describe users in the term store of a managed metadata service application. On the **Add Query Rule** page, in the **Context** section, you can add or remove user segments.

   5.3 Optionally, under **For what context do you want to configure rules?**, in the **Topic Categories** drop-down list, select a topic category for which you want this query rule to be applicable. Topic categories are based on terms for categories in the term store of a managed metadata service application. On the **Add Query Rule** page, in the **Context** section, you can add or remove categories.

   5.4 Click **New Query Rule**.

6. On the **Add Query Rule** page, do the following:

   6.1 In the **General Information** section, in the **Rule Name** text box, type a name for the new query rule.

6.2 In the **Context** section, under **Query is performed on these sources**, select either **All sources** if you want this query rule to be applicable for queries that users submit against any result source, or select **One of these sources**, and then optionally click **Add Source** to add other result sources. (When you select **One of these sources**, this query rule will be applicable only when a user submits a query against one of the result sources in this list. Therefore, make sure that the result source appears for which you want this query rule to be applicable—for example, **Local SharePoint Results**. Optionally, under **Query is performed from these categories**, specify the topic categories from which to perform the query. And then, under **Query is performed by these user segments**, specify user segments to which you want the query rule to apply.

6.3 In the **Query Conditions** section, specify conditions to control when the rule will fire, or click **Remove Condition** if you want the rule to fire for any query text. For testing, it's a good idea to click **Remove Condition**.

6.4 In the **Actions** section, under **Result Blocks**, click **Add Result Block**.

6.5 In the **Add Result Block** dialog box, do the following:

6.5.1 Optionally, in the **Block Title** section, in the **Title** text box, change the title to the text that you want to display above the result block on the search results page, such as **Results for "{subjectTerms}" from SharePoint Online.**

6.5.2 In the **Query** section, in the **Configure Query** text box, either keep the keep the default query, which is **{subjectTerms}**, or use Query Builder to help you configure a query, type a different query in the text box, or click **Launch Query Builder**. If you are not familiar with transforming queries, we recommend that you keep the default query here. For more information, go to:

- Plan to transform queries and order results in SharePoint 2013
- Query variables in SharePoint Server 2013

6.5.3 In the **Query** section, in the **Search this Source** drop-down list, select the name of the result source that you created in the previous procedure in this guide.

6.5.4 In the **Query** section, in the **Items** drop-down list, select the number of search results from SharePoint Online that you want to show in this result block on the search results page.

6.5.5 In the **Settings** section, select **More link goes to the following URL**, and type the URL for the link to a page that displays more results from the SharePoint Online search index. For example, to specify the main search results page as the page that displays more results, you can usually type a URL of the following form (followed by "**?k={subjectTerms}**" to signify the user's search query): http://*domain_name*.com/sites/*Search_Center_name*/pages/results.aspx?k={subjectTerms}. When end users click **Show More**, they will see more results for the result block.

6.5.6 For the placement of the block of results from SharePoint Online relative to the results from SharePoint Server 2013/2016, either select **This block is always shown above core results** to display the result block at or near the top of the first page of search results (useful for testing or when most of the relevant content is located in the remote search index) or select **This block is ranked within core results (may not show)** to display the result block ranked by relevance compared to the core results (default setting that is typically the best choice in a production environment).

6.5.7 Optionally, in the **Group Display Template URL** text box, specify a different URL for the group display template.

6.5.8 Optionally, in the **Item Display Template** text box, specify an item display template.

6.5.9 Click **OK** to add the result block. On the **Add Query Rule** page, in the **Publishing** section, select **Is Active**. When a query rule is active, it fires whenever the query conditions are met. Optionally, specify a **Start Date**, an **End Date**, a **Review Date**, and a **Contact**. The start date and end date specify when the query rule will be active. If you specify a start date without an end date, the rule will always be active after the start date. If you specify an end date without a start date, the rule will always be active until the end date. If you do not specify a start date or an end date, the rule will always be active.

6.5.10 Click **Save**. After a few moments, when federated users submit queries from the SharePoint Server 2013/2016 Search Center against a result source that you specified, they will see results from both search indexes.

Note: *A federated user* is a user whose on-premises AD DS domain account is synchronized between SharePoint Server 2013/2016 and SharePoint Online, and who accesses resources in both environments by authenticating with the federation identity provider, such as AD FS 2.0.

Try a search from the SharePoint Server 2013/2016 Search Center

To validate your configuration for displaying search results, you can log on to SharePoint Server 2013/2016 as a federated user and try some searches from the Search Center.

> **Note:** If you are using SSO, it is important to test hybrid Search functionality by using federated user accounts. Native Office 365 user accounts and AD DS accounts that are not federated are not recognized by both directory services. Therefore, they cannot authenticate using SSO and cannot be granted permissions in both deployments. For more information, go to Accounts needed for hybrid configuration and testing.

To try a search from the SharePoint Server 2013/2016 Search Center:

1. Log on to the SharePoint Server 2013/2016 deployment as a federated user who has been activated in SharePoint Online and who has permission to view the root site collection in SharePoint Online.
2. Go to the enterprise Search Center.
3. Click a search vertical that uses a result source that you specified in the second procedure in this guide.
4. In the **search** box, type a test query, such as the name of your company. Make sure that the test query yields search results from the SharePoint Server 2013/2016 search index and the SharePoint Online search index.
5. Click the search icon, or press **Enter.** On the search results page, you should see results from the SharePoint Server 2013/2016 search index and a result block from the SharePoint Online search index. If you do not see results from both search indexes, do the following:

   5.1 Verify that the search system in SharePoint Server 2013/2016 has crawled the local content. For information about how to view the crawl log, see View search diagnostics in SharePoint Server 2013.

   5.2 Verify that you have configured the hybrid SharePoint environment as described in the following articles, and in the following order:

   - SharePoint Server 2013 hybrid configuration roadmaps

Search

- Configure server-to-server authentication from SharePoint Server 2013 to SharePoint Online

5.3 Verify that you have configured Search features and functionality as described in this article.

5.4 Correct any errors or omissions and try another search. If you still do not see search results from both search indexes, check the SharePoint Unified Logging Service (ULS) logs, also called the SharePoint trace logs. For more information, go to the overview of Unified Logging System (ULS) Logging.

Cloud hybrid search

Cloud hybrid search is the next generation in hybrid search solutions available in SharePoint Server 2013/2016. Cloud hybrid search is provisioned as a Cloud Search Service Application in SharePoint. The Cloud Search Service Application, unlike classic federated hybrid search, unifies crawled content into a single index stored in Office 365.

Cloud hybrid search architecture

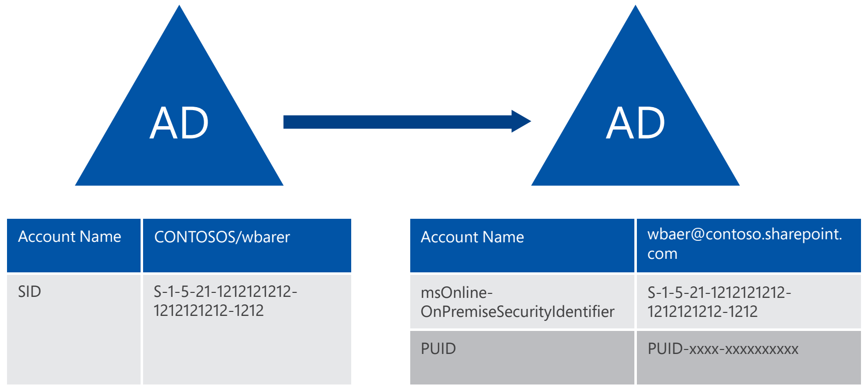
The Cloud Search Service Application operates similarly to the native Search Service Application used to index and discover on-premises content. However, when using the Cloud Search Service Application, content processing, index storage, and analytics processing occur in Office 365. Unlike the native Search Service Application, the Cloud Search Service Application does not use discrete content processing, analytics, and/or links database because these components are managed in Office 365. However, their respective databases are provisioned with the Cloud Search Service Application, although they remain idle.

The Cloud Search Service Application uses a unique managed property as part of the SharePoint Online search schema to identify on-premises content by setting the property to “True.” With this managed property in SharePoint Online search, you can validate the search service by using *isexternalcontent:1* in a search query.

Property name	Type	Multi	Query	Search	Retrieve	Refine	Sort	Safe	Mapped Crawled Properties
IsExternal Content	Yes/No	-	Query	-	Retrieve	Refine	Sort	Safe	IsExternalContent

Identity and security with cloud hybrid search

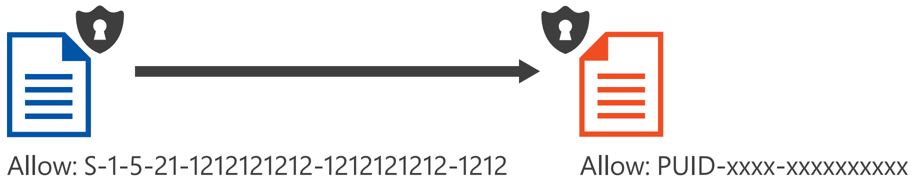
The Cloud Search Service Application uses security principals managed on-premises that are synchronized with Azure AD through DirSync.



Account Name	CONTOSOS/wbarer
SID	S-1-5-21-1212121212-1212121212-1212

Account Name	wbaer@contoso.sharepoint.com
msOnline-OnPremiseSecurityIdentifier	S-1-5-21-1212121212-1212121212-1212
PUID	PUID-xxxx-xxxxxxxxxx

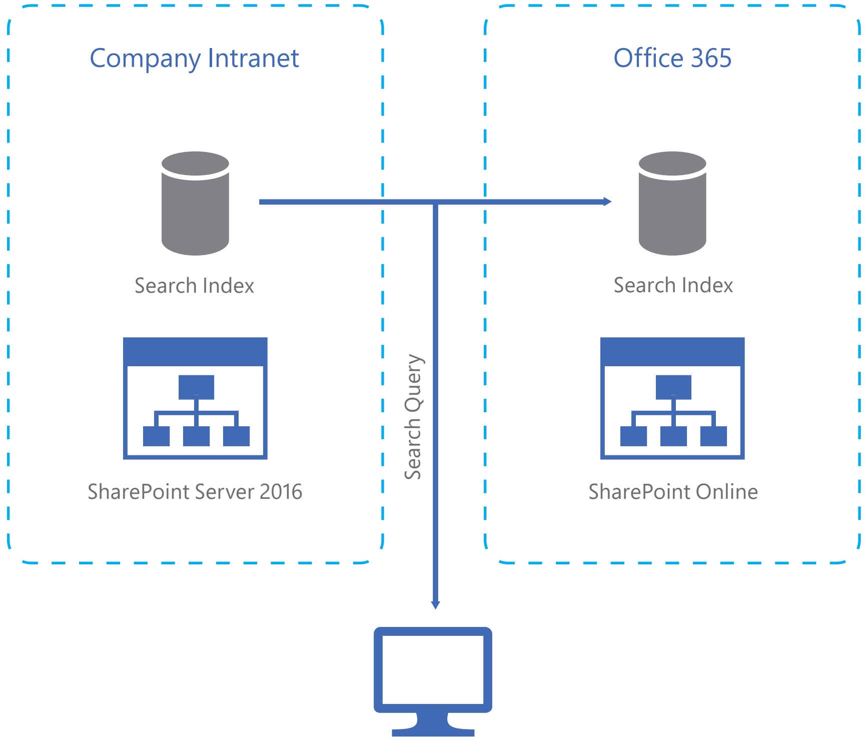
As items are indexed in Office 365, the access control entities are looked up in the cloud directory service. User SIDs are mapped to PUIDs; Group SIDs are mapped to Object IDs; and <Everyone> and <Authenticated Users> are mapped to <Everyone except external users>.


Allow: S-1-5-21-1212121212-1212121212-1212
Allow: PUID-xxxx-xxxxxxxxxx

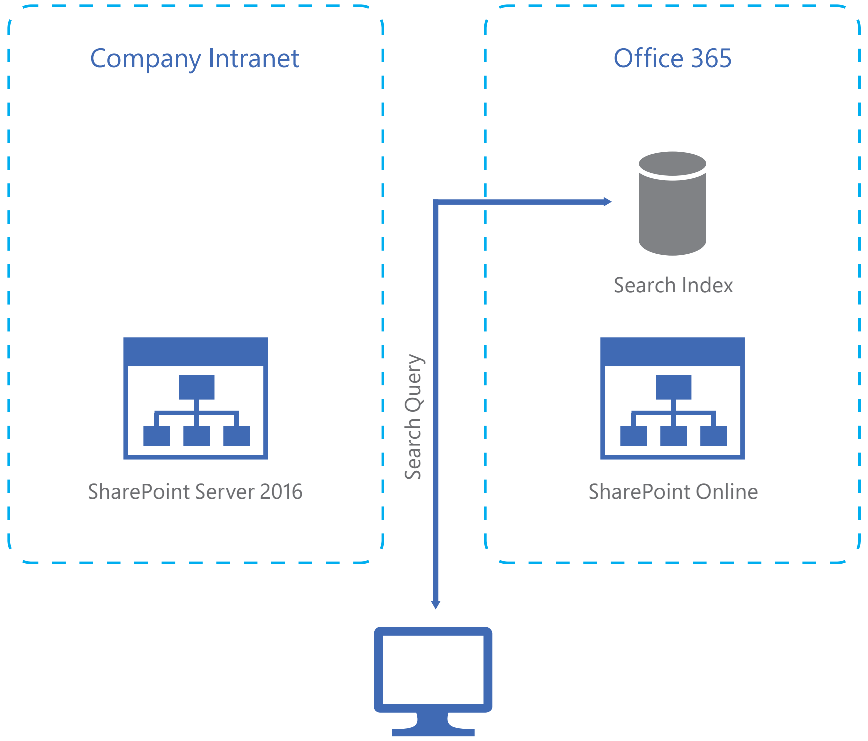
Cloud hybrid search versus federated hybrid search

The primary difference in cloud hybrid search is how the search index is stored and managed. In a cloud hybrid search scenario, the search index for both on-premises and Office 365 crawled content is stored in Office 365. However, a federated hybrid search maintains a discrete index for on-premises content (stored on-premises) and Office 365 content (stored in Office 365). Search results are obtained from each location where an index is stored. Additionally, in a federated hybrid search scenario, each search implementation is managed separately. With cloud hybrid search, all search configuration is performed in Office 365. Cloud hybrid search benefits from the cloud-hosted index by providing access to additional Office 365 search and discovery innovation, including Office Graph and Delve and search-driven experiences like eDiscovery in SharePoint Online.

Federated Search



Cloud Hybrid Search



For customers in heavily regulated industries and/or customers who have significant investment in search customization, federated hybrid search may be a good option because it does not require change to the existing search environment and indexed content remains isolated and stored on-premises.

Provision a Cloud Search Service Application

Use the following steps to provision a Cloud Search Service Application:

1. Verify that the user account performing this procedure is a member of the Farm Administrators group associated with the farm for which you want to create the service application.
2. In Central Administration, in the **Application Management** section, click **Manage service applications**.
3. On the **Manage Service Applications** page, click **New** and then click **Search Service Application**.
4. On the **Create New Search Service Application** page, accept the default value for **Service Application name** or type a new name.

5. Select **Cloud Search Service Application** from the list of available options.

6. In the **Search Service Account** list, select the managed account that you registered previously to run the search service.

7. In the **Application Pool for Search Admin Web Service** section, do the following:

   7.1 Select the **Create new application pool** option, and then specify a name for the application pool in the **Application pool name** text box.

   7.2 In the **Select a security account for this application pool** section, select the **Configurable** option. Then, from the list, select the account that you registered to run the application pool for the Search Admin Web Service.

8. In the **Application Pool for Search Query and Site Settings Web Service** section, do the following:

   8.1 Choose the **Create new application pool** option and specify a name for the application pool in the **Application pool name** text box.

   8.2 In the **Select a security account for this application pool** section, select the **Configurable** option. Then, from the list, select the account that you registered to run the application pool for the Search Query and Site Settings Web Service.

9. Click **OK**.

Configure the Cloud Search Service Application

Prerequisites

Configuring the Cloud Search Service Application requires installing one or more applications on the SharePoint Server that hosts the SharePoint Central Administration website.

Microsoft Online Services Sign-In Assistant for IT Professionals

- Download and install the Microsoft Online Services Sign-In Assistant for IT Professionals RTW.

The Microsoft Online Services Sign-In Assistant (MOS SIA) provides end-user sign-in capabilities to Microsoft Online Services, such as Office 365. The MOS SIA installs client components that allow common applications, such as Microsoft Outlook and Lync, to authenticate to Microsoft Online Services. The MOS SIA can also provide an improved sign-in experience, so end users can access Microsoft Online Services without having to re-enter their credentials. This download is intended for IT professionals for distribution to managed client systems as part of an Office 365 client deployment, via Microsoft System Center Configuration Manager (SCCM) or similar software distribution systems. This download is unnecessary for users who are installing Office 365 by means of the Office 365 Desktop Setup application because the MOS SIA is installed as part of the desktop setup process.

Azure Active Directory Module for Windows PowerShell

- Download, install, and run the Azure Active Directory Module for Windows PowerShell (64-bit version). You can use this module for Azure AD administrative tasks, such as user management, domain management, and SSO configuration.

Onboard-HybridSearch.ps1

Download Onboard-HybridSearch.ps1. This sets up server-to-server authentication and configures trust between SharePoint Server 2013/2016 and your Office 365 tenant. Server-to-server authentication allows servers that are capable of server-to-server authentication to access and request resources from one another on behalf of users.

Use the following steps to set up server-to-server authentication:

1. Verify that you are a member of the Administrators group affiliated with the server on which you are running Windows PowerShell cmdlets.
   - **Securityadmin** fixed server role on the SQL Server instance.
   - **db_owner** fixed database role on all databases that are to be updated.

If you do not have permissions, contact your setup administrator or SQL Server administrator. An administrator can use the **Add-SPShellAdmin** cmdlet to grant permissions to use SharePoint 2013 cmdlets. For additional information about PowerShell permissions, go to Add-SPShellAdmin.

2. In the SharePoint 2013 environment on the farm receiving server-to-server requests, start the SharePoint 2013 Management Shell.
   - For Windows Server 2008 R2:
     - In the SharePoint 2013 environment, on the **Start** menu, click **All Programs**, click **Microsoft SharePoint 2013 Products**, and then click **SharePoint 2013 Management Shell**.
   - For Windows Server 2012:
     - In the SharePoint 2013 environment, on the **Start** screen, click **SharePoint 2013 Management Shell**. If SharePoint 2013 Management Shell is not on the Start screen, right-click **Computer**, click **All apps**, and then click **SharePoint 2013 Management Shell**. Learn more about interacting with Windows Server 2012.
3. At the Windows PowerShell command prompt, type the following command:

```
./Onboard-HybridSearch.ps1
```

The onboarding script prompts the Office 365 Tenant to be configured as a URL, for example *https://<customer>.sharepoint.com*, in addition to the credentials of the administrator associated with the Office 365 tenant to be configured.

> Note: When configuring a Cloud Search Service Application in an environment where one or more Search Service Applications are provisioned, the PortalUrl and HybridSsaId parameters need to be passed to ./Onboard-HybridSearch.ps1 at runtime. For example:
>
> ```
> ./Onboard-HybridSearch.ps1 -PortalUrl <customer.
> contoso.com> -HybridSsaId <Cloud Search Service
> Application Guide>
> ```

Create a content source

For users to get search results, the Cloud Search Service Application must first crawl the corresponding content. Crawling requires at least one *content source*. A content source is a set of options that you use to specify the type of content to crawl, the starting URLs to crawl, and when and how deeply to crawl. Similar to a native Search Service Application, when the Cloud Search Service Application is created, a content source named "Local SharePoint sites" is automatically created and configured for crawling all SharePoint sites in the local server farm and for crawling user profiles.

You can create content sources to specify other content to crawl and how the system will crawl that content; however, you do not have to create other content sources if you do not want to crawl content other than the SharePoint sites in the local farm.

Limit content in the Office 365 index

Those who wish to store only a portion of their content in the Office 365 index with cloud hybrid search can limit what content is crawled and processed by the Cloud Search Service Application. This is done by creating discrete content sources to crawl, thereby restricting content not included in those content sources.

Configure the SharePoint Server 2016 Beta 2 Search Center

Because the Cloud Search Service Application index is managed in Office 365, results are returned via Office 365. To simplify search and discovery for users, use the following steps to configure the on-premises Global Search Center URL with the URL of the SharePoint Online search center:

1. Verify that the user account performing this procedure is a member of the Farm Administrators group for the farm for which you want to create the service application.
2. In Central Administration, in the **Application Management** section, click **Manage service applications**.
3. On the **Manage Service Applications** page, select the **Cloud Search Service Application** from the list of available Service Applications.
4. On the **Search Administration** page, locate the **Global Search Center URL** field and specify the location of the SharePoint Online

search center (for example, https://<customer>.sharepoint.com/Search/Pages).

Optionally, a native Search Service Application can be provisioned in SharePoint Server 2016 Beta 2 that returns on-premises results, or a cloud hybrid search can be combined with a federated search.

Customizing the search experience

The Cloud Search Service Application shares a similar architecture as the native SharePoint Search Service Application; however, customization is limited because the search experience is derived from Office 365.

Learn more about cloud hybrid search.

	SharePoint Server	SharePoint Online
Custom iFilters	x	
BCS Connectors	x	
Partner Connectors	x	
Custom Security Trimming	x	
Tenant Level Schema Mapping		x
Site Collection Schema Mapping	x	
Custom Entity Extraction	x	
Content Enrichment Web Service	x	
Query Rules	x	x
Result Sources	x	x

Choosing between federated and cloud hybrid search

The choice between implementing federated versus cloud hybrid search solutions depends on your business needs, desired user experience, and constraints, including corporate and/or regulatory compliance. For example, your organization may keep sensitive content that cannot be stored in cloud services.

Hybrid Team Sites

Hybrid Team Sites provides a solution to help hybrid users reconcile and rationalize site membership and discovery across SharePoint on-premises and Office 365. For example, if you're a member of several Team Sites in your organization, you may want to start following them for easy access. A followed Team Site gets listed on your Sites page, and when you follow sites, you can navigate quickly to site libraries from OneDrive for Business or from the Sites tile on-premises or in Office 365.

When you follow a site, a link to it is added to your Followed Sites list. Users using both SharePoint Server 2016 Beta 2 and SharePoint Online will have different followed lists for sites in each location. The Hybrid Team Sites feature consolidates the information from both locations into the SharePoint Online list in Office 365.

Learn more about Team Sites.

Profile redirection

Profile redirection is a component of the Hybrid Team Sites feature introduced in SharePoint Server 2013 Service Pack 1. Profile redirection, in a Hybrid Team Sites configuration, redirects cloud users to their profile in Office 365 powered by Delve. This ensures that hybrid users have a single place for their profile information.

Learn more about profile redirection.

Extensible app launcher

The app launcher is a familiar feature in Office, and it has been extended to SharePoint Server 2016. The app launcher provides a common location to discover new apps and navigate SharePoint on-premises and Office 365.

The extensible hybrid app launcher is designed to help you get to your Office 365 apps and services from SharePoint Server 2016 Beta 2. The extensible app launcher is enabled when enacting Hybrid Team Sites and/or OneDrive for Business. After you enable this feature, you'll see the Office 365 Delve and Video apps, along with your custom Office 365 tiles, appear in your SharePoint Server 2016 Beta 2 app launcher.

Learn more about the extensible app launcher.

Office 365 Video

Office 365 Video is an intranet website portal where people in your organization can post and view videos. It's a streaming video service that's available with SharePoint Online in Office 365. Office 365 Video is a great place to share videos of executive communications or recordings of classes, meetings, presentations, training sessions, and so forth. It can be integrated with SharePoint Server 2013/2016 via embedding and the app launcher.

Embed

This option applies to SharePoint Server 2013/2016.

You can display a video that is managed in the Office 365 Video portal on a SharePoint Online site or a SharePoint site with a hybrid SSO setup by inserting the embed code for the video on your site.

Embedding videos in SharePoint Server

To embed a video from Office 365 Video on your site, you first need to get the embed code for the video you want to display. Use the following steps to get the embed code:

1. Sign in to Office 365 as a user who has admin permission for the SharePoint Online site where you want to embed the video.
2. Select the **Office 365 app launcher** icon and then select the **Video** tile. This takes you to Office 365 Video.
3. Go to the full playback page for the video that you want to display on your site.
4. On the Office 365 Video top navigation bar, choose **Embed**. A box will appear with the embed code for the video.
5. Copy the full embed code. Be sure to include the beginning **<** and the ending **>**.

Once you have the embed code, use the following steps to add it to your SharePoint site:

1. Navigate to the page on your site where you want to display the video.
2. On the Office 365 top navigation bar, choose **Edit**. Alternately, you can click the **Page** tab and then choose **Edit**.
3. Click the area of the page where you want to embed the video.
4. On the ribbon, click the **Insert** tab and then choose **Embed Code**.
5. Paste the embed code you copied into the **Embed** box. Then click **Insert**.
6. On the Office 365 top navigation bar, choose **Save**.

App launcher

This option applies to SharePoint Server 2016.

When configuring Hybrid Team Sites in SharePoint Server 2016, the Office 365 app launcher tiles are pushed to the SharePoint Server 2016 app launcher. The extensible hybrid app launcher helps users have a more seamless experience when navigating between SharePoint Server 2016 and Office 365. This feature is enabled as part of hybrid sites features in SharePoint Server 2016.

OneDrive for Business redirection

OneDrive for Business is a personal library for storing and organizing your work documents. As an integral part of Office 365 or SharePoint Server 2013/2016, OneDrive for Business lets you work within the context of your organization with features such as direct access to your organization's address book.

If you're using Office 365, you get unlimited space in the cloud for OneDrive for Business. If your OneDrive for Business library is hosted on a SharePoint server in your organization, your organization's administrators determine how much storage space is available.

All files that you store in OneDrive for Business are private initially, unless you decide to share them. You can easily share a file with everyone in your organization by placing it in the "Shared with Everyone" folder. You can also share files with specified co-workers so you can collaborate on projects. If you're signed in to Office 365, you may even be able to share with partners outside of your organization, depending on what your company allows.

OneDrive for Business coexistence

A common migration approach adopted in many organizations is to begin project planning with the broad goal of a one-time, wholesale migration of content from a source to a destination. However, such an approach is often prone to failure because:

- There is more source content than can be migrated in the time originally specified.
- All users cannot be migrated at the same time due to internal considerations, such as the migration of applications that use the source content store to an updated set of applications that use the target content store.
- More time is needed to train each user department on the best use of their SharePoint environment.

This wholesale migration approach creates the need for the content migration project to include a coexistence strategy: the simultaneous use of the source and target content stores (and associated applications and business processes) until all content, applications, and users have been successfully migrated to the new environment.

During the coexistence period, based on business requirements, there are additional technical process requirements for keeping the content synchronized between the original source content store and target environment. This may involve ongoing one-way synchronization (incremental migrations) from the source content store to the target store. In addition, there may be a requirement to support bi-directional content synchronization and change conflict resolution to support simultaneous use of both environments while they coexist.

Following successful coexistence, the original source content store and applications can be backed up and then decommissioned. It is very important to plan for this event; otherwise, there will be a few users who continue to use the old environment. A coexistence period that runs longer than necessary means increased operations and support costs.

OneDrive for Business coexistence gives SharePoint Server 2013/2016 the ability to extend your existing SharePoint Server 2013/2016 on-premises deployment to Office 365 and take advantage of the scale and innovation provided through the cloud. In SharePoint Server 2013 Service Pack 1, functionality is included that enables IT administrators to selectively redirect their users to OneDrive for Business in Office 365 from SharePoint Server 2013. This same capability is native to SharePoint Server 2016.

Planning

Before deciding on a migration strategy, it is vital that you perform an analysis of your current environment. This analysis should focus on the SharePoint workloads and content that you plan to move to OneDrive for Business. The analysis should give you a clear understanding of the content and customizations you have in your on-premises environment. You should then create a content and customization roadmap that covers what content and customizations will be moved to OneDrive for Business and how they will be moved.

Bandwidth planning

The preferred methodology to measure impact of bandwidth requirements when deploying OneDrive for Business is to measure the results of a pilot group. However, if a measurement is required prior to any deployment within your organization, you can use the OneDrive for Business Client Network Bandwidth Calculator to provide an estimate of bandwidth requirements.

Learn more about the OneDrive for Business Client Network Bandwidth Calculator.

OneDrive for Business sync client deployment planning

Organizations can deploy the OneDrive for Business sync client by allowing their users to download the rich client and/or app. Optionally, it can be deployed to users using Click-To-Run technology for a managed, IT-led approach.

Scenario	Steps	Example Configuration.xml

IT-managed internal OneDrive for Business deployment	**1.** Customize a Click-To-Run for Office 365 installation.
	2. Create a custom Configuration.xml configuration file. See example and refer to the linked article above for additional guidance.
	3. Download the OneDrive for Business Click-To-Run deployment source and copy to a network location accessible to the target users.
	4. Note specific configuration options and product ID details.
	Sample:
	`\\server\share\setup.exe /`
	`download \\server\share\`
	`CustomConfiguration.xml`
		`<Add SourcePath="\\`
		`server\share\C2R _ deploy"`
		`OfficeClientEdition="32" >`
		`    <Product`
		`ID="GrooveRetail">`
		`      <Language ID="en-us" />`
		`    </Product>`
		`</Add>`

IT-managed OneDrive for Business silent desktop deployment
(SxS w/ Office 2010)
	Refer to Steps **1-3 above** and configure the custom Configuration.xml to specify the configuration options for deployment. (See example for additional guidance.)
	Sample:
	`\\server\share\setup.exe /`
	`configure \\server\share\`
	`CustomC2RConfig.xml`
		`<Add SourcePath="\\`
		`server\share\C2R _ deploy"`
		`OfficeClientEdition="32" >`
		`    <Product`
		`ID="GrooveRetail">`
		`      <Language ID="en-us" />`
		`    </Product>`
		`  </Add>`
		`<Display Level="None"`
		`AcceptEULA="TRUE" />`

OneDrive for Business Next Generation Sync Client deployment planning

The OneDrive for Business Next Generation Sync Client lets you connect and sync files from your OneDrive for Business. You can add a work or school account to the new OneDrive for Business sync client and sync all your files to your computer.

Important

This release of the OneDrive for Business Next Generation Sync Client has a number of valuable features for you and your organization. Before deploying, there are some known issues that you should review before determining whether this new client is currently appropriate for your organization.

The following content will help IT administrators understand how to configure and deploy the new OneDrive for Business sync client in an enterprise environment, including:

- Steps for using OneDriveSetup.exe to install OneDrive.exe on users' computers
- Using appropriate registry key values to control what type of OneDrive account your users will configure
- Deciding what's best for you and your enterprise
- The OneDrive deployment package
- Links to additional resources about the new OneDrive for Business sync client

It is helpful to be familiar with enterprise deployment tools, such as System Center Configuration Manager 2012 (SCCM) or Group Policy, to deploy .exe files and modify local system registries. Learn more about using SCCM.

Note: The new OneDrive for Business sync client is only supported in Windows 10, Windows 8, and Windows 7. Windows 8.1 is currently not supported. Also, the new OneDrive for Business sync client doesn't yet support syncing site libraries or on-premises instances of OneDrive for Business (when your organization doesn't subscribe to Office 365).

Overview of the deployment process

The goal of the IT administrator in deploying the new OneDrive for Business sync client is to install OneDrive.exe to each user's machine and then to have them configure file synchronization to their machines using their Office 365 business accounts. This will enable them to use the new OneDrive for Business sync client.

There are three steps in this process:

1. Add the configuration registry keys to each computer.
2. Deploy OneDrive.exe by running the installer (OneDriveSetup.exe) with the /silent command line parameter.
3. Run OneDrive.exe with desired command line parameters to launch the process.

Important

If your users are currently using the OneDrive for Business sync client (groove.exe) for their work and business files, and you want to move them to the new OneDrive for Business sync client, see Transition from the previous OneDrive for Business sync client before proceeding. You will need to make some additional considerations to ensure that the transition is successful.

Add configuration settings registry keys to each computer

Prior to installing OneDrive.exe, you need to deploy the OneDrive configuration settings to each computer. This is done by adding the settings as registry key entries to the computer local registry. An administrator can use these settings to control how and when users set up their OneDrive business accounts on their computers.

The configuration settings are set on each computer by adding them as regkey entries to the computer local registry in the following hive:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\OneDrive

There are two registry keys that IT administrators can use to control the new OneDrive for Business sync client's configuration settings:

- Default to Business
- Add an Account

Note: Registry key files (*.reg) for each configuration setting are included in the OneDrive deployment package and can be deployed on a user's machine using SCCM or Group Policy. Additional OneDrive.exe administrative controls can be added after deployment. See Administrative settings for the new OneDrive Sync Client to add additional administrative controls to help manage your OneDrive.exe users through Group Policy settings after it is deployed.

Default to Business

The Default to Business registry key entry (**DefaultToBusinessFRE**) can be added to your users' machines so that the Welcome to OneDrive wizard for configuring a work or school account is shown by default when a user launches the new OneDrive for Business sync client. The wizard walks users through configuring the new OneDrive for Business sync client for synchronization with their business files, essentially adding them as a business user.

To view what your users will see when walking through the wizard, go to Get started with the new OneDrive Sync Client in Windows.

IT administrators can use the Default to Business registry key setting effectively to prompt a large number of users to configure the new OneDrive for Business sync client after it is installed.

DefaultToBusinessFRE setting	User see this when OneDrive.exe is first started.
Regkey is present on system and enabled (set to value of "1")	User is presented with the OneDrive business configuration experience if OneDrive.exe is launched by the user and no accounts have already been configured in OneDrive.exe.
Regkey is not present on system or disabled (set to a value of "0")	User is presented with the OneDrive personal experience.

You can set the Default to Business key by deploying the DefaultToBusinessFRE.reg file included in the OneDrive Deployment Package onto your users' machines. This adds the following key:

```
[HKEY _ CURRENT _ USER\SOFTWARE\Microsoft\OneDrive]

“DefaultToBusinessFRE “=dword:00000001
```

Add an account

What if one of your enterprise users cancelled out of the Welcome to OneDrive wizard to configure their work or business account when it was first run? Or, what if you simply want to provide your users the convenience of adding their Office 365 business account to use with the new OneDrive for Business sync client whenever they want? Fortunately, there is a way for them to configure OneDrive.exe for their Office 365 business account at a later time.

The **EnableAddAccounts** registry key setting allows your users to do exactly that. After OneDrive.exe is added to their system, users will be able to configure the OneDrive.exe sync client for a business account through their OneDrive.exe settings. In order for users to access their OneDrive.exe settings, they must either:

- Have OneDrive.exe installed and already have a personal account configured
- Have OneDrive.exe installed and be using Windows 10

If either of the above conditions are true, your users will be able to access OneDrive.exe settings by going to the **Windows System Tray** on their computers, right-clicking the **OneDrive - Personal** icon, then clicking **Settings.**

The presence of the EnableAddAccounts regkey on your users' systems will add an **Add an Account** section to the **Account** tab in the OneDrive settings. Click the **Add a Business Account** button to launch the Welcome to OneDrive wizard to configure a business account.

You can set the Add an Account key by deploying the EnableAddAccount.reg file included in the OneDrive Deployment Package onto your users' machines. This adds the following key:

```
[HKEY _ CURRENT _ USER\SOFTWARE\Microsoft\OneDrive]

"EnableAddAccounts"=dword:00000001
```

Deploy OneDrive.exe using the OneDriveSetup.exe installer

After setting the desired registry values, the next step is to run the OneDriveSetup.exe installer on each machine. This will install the OneDrive executable file under the directory **%localappdata%\Microsoft\OneDrive**. The OneDriveSetup.exe installer for Windows can be saved to a local network share for deployment through SCCM. Download the OneDriveSetup.exe installer for Windows.

There are two options for deploying the OneDriveSetup.exe installer:

- OneDriveSetup.exe (no command line parameter)
- OneDriveSetup.exe /silent

Deploying without a command line parameter

Deploying **OneDriveSetup.exe** with no command line parameter will install OneDrive.exe with the installation status visible to the user.

Additionally, after installation, OneDriveSetup.exe automatically executes OneDrive.exe, which automatically starts the Welcome to OneDrive wizard for the user (either to configure a personal or business account, depending on the presence of the DefaultToBusinessFRE registry key).

Deploying with the /silent command line parameter

Deploying **OneDriveSetup.exe /silent** will install OneDrive.exe transparently to the user. Additionally, OneDriveSetup.exe will not launch OneDrive.exe automatically after installation completes. The IT administrator will need to launch OneDrive.exe through an additional command. Deploying OneDriveSetup.exe /silent allows you to control when to launch OneDrive.exe and pass any additional command line parameters to OneDrive.exe.

Launching OneDrive.exe

After OneDrive.exe has been installed through the OneDriveSetup.exe installer, the OneDrive process can be launched by running OneDrive.exe along with one of the following configurations:

- `%localappdata%\Microsoft\OneDrive\OneDrive.exe (no command line parameter)`
- `%localappdata%\Microsoft\OneDrive\OneDrive.exe /configure _ business:<tenantId>`

Note: When using SCCM, make sure OneDrive.exe is run with user rights permissions, not as an administrator. An error will display if it is run with elevated permissions.

Launching OneDrive.exe without a command line parameter

Launching OneDrive.exe with no command line parameter starts the OneDrive process. Your users' experience will depend on whether a OneDrive account has been configured previously on the device.

Scenario	Result
No accounts have yet been configured for OneDrive.exe on the device	OneDrive.exe will reference the DefaultToBusinessFRE registry key and display the appropriate Welcome to OneDrive wizard (for business or personal).
One or more accounts have already been configured for OneDrive.exe on the device	OneDrive.exe will start all OneDrive processes and no Welcome to OneDrive wizard will be shown to the user.

Launching OneDrive.exe /configure_business:<tenantID>

Launching OneDrive.exe with the command line parameter `/configure _ business:<tenantId>` will check to see if an account associated with a specific tenant has already been configured on the machine. The Welcome to OneDrive wizard be displayed to the user only if an account of that tenant has not yet been configured.

When OneDrive.exe is launched, it will check for the presence of **ConfiguredTenantId** in the system registry under **HKEY_CURRENT_USER\SOFTWARE\Microsoft\OneDrive\Accounts\Business1** (or **Business2**, **Business3**, and so on) for a value matching the one provided in the `/configure _ business:<tenantId>` parameter. If the user has not yet signed in to OneDrive.exe with the specified tenant, the wizard will open for the user.

For example, running `OneDrive.exe /configure _ business:12345678-1234-1234-1234-123456789012` will have the following effects:

1. The system registry will be checked for the presence of **ConfiguredTenantID under HKey_Current_User\Software\Microsoft\OneDrive\Accounts\Business1** (or **Business2**, **Business3**, and so on).
2. If this key exists, it will check to see if it has a value of **12345678-1234-1234-1234-123456789012.**
3. If the value matches, nothing will happen.
4. If the value does not match, the Welcome to OneDrive wizard will launch to configure a business or work account.

Running `OneDrive.exe /configure _ business:<TenantId>` is a great way to target only users who have not yet signed in with a desired account without bothering users who have already set up OneDrive.

> Note: If you need help about finding your TenantID for your organization in Office 365, go to Find your Office 365 tenant ID.

What’s the right deployment method for you?

When planning to deploy the OneDrive.exe client to their enterprise users, there are three deployment scenarios IT administrators need to consider:

- Install the OneDrive.exe client on users’ machines
- Install the OneDrive.exe client on users’ machines, and then have them configure their business accounts
- Display the Welcome to OneDrive wizard only to users who still need to set up their business accounts

Install the OneDrive.exe client on users’ machines

Maybe all you’re interested in is getting the new OneDrive for Business sync client onto your users’ machines. If all you want to do is install OneDrive.exe on a machine, you can use either SCCM or a Group Policy script to execute the following:

<pathToSomeAccessibleNetworkShare>\OneDriveSetup.exe /silent

Result: OneDrive.exe is installed transparently on your users’ machines, but it is not automatically launched. Users can launch OneDrive.exe by opening their OneDrive folder in File Explorer or by launching OneDrive from the Start menu. Or, IT administrators at any later time can run **%localappdata%\Microsoft\OneDrive\OneDrive.exe** through SCCM or a Group Policy script to automatically open OneDrive.exe on a user’s machine.

Install the OneDrive.exe client on users’ machines and have them configure their business accounts

In what is likely the most common scenario, you want to install OneDrive.exe on your users’ machines and have them sign in with their business accounts as soon as possible. Use either SCCM or a Group Policy script to do the following:

1. Add **DefaultToBusinessFRE.reg** and **EnableAddAccounts.reg** to the user’s machine.
2. Execute `<pathToSomeAccessibleNetworkShare>\OneDriveSetup.exe /silent`.
3. Execute `%localappdata%\Microsoft\OneDrive\OneDrive.exe /configure _ business:<tenantId>`.

Result: OneDrive.exe is installed transparently on your users’ machines, and those who have not yet signed in to OneDrive with the desired tenant are shown the Welcome to OneDrive wizard.

Display the Welcome to OneDrive wizard only to users who still need to set up their business accounts

In this scenario, some time has passed since you installed the OneDrive.exe client on your users' machines, and you're not sure whether all your users have connected their business accounts. To be certain, you want to relaunch the Welcome to OneDrive wizard, but only for those users who haven't yet set up a business account. You can use either SCCM or a Group Policy script to do the following:

Execute `%localappdata%\Microsoft\OneDrive\OneDrive.exe /configure _ business:<tenantId>`

Result: The `/configure _ business:<tenantId>` parameter allows IT administrators to display the wizard only to users who still have not yet set up a business account with the desired tenant.

The OneDrive Deployment Package

The OneDrive Deployment Package contains the registry key files (.reg) that are used to control how and when your users set up OneDrive for their business accounts on their computers. It also contains links to resources to help IT administrators deploy OneDrive.exe and the registry keys to users in their enterprise environment through deployment tools, such as SCCM or Group Policy.

The OneDrive Deployment Package contains:

- DefaultToBusinessFRE.reg file
- EnableAddAccounts.reg file
- ADMX templates
- URL files pointing to deployment and administration documentation

Download the OneDrive Deployment Package for Windows. Be sure to get the file titled "OneDrive for Business Next Generation Sync Client" and the documentation and administrative template files (ADMX/ADML/REG) for Windows.

Plan for performance issues

IT administrators need to plan for performance issues that might happen when deploying the new OneDrive for Business sync client. After receiving the new OneDrive for Business sync client and configuring their business accounts for file sync, a large number of users all syncing files across your networks might adversely impact network performance.

One of the most effective ways to address performance issues when deploying to a large number of users is a phased rollout. Limiting the number of users who sync their files over the same time period will limit the amount of traffic on your network.

Some additional things you might want to consider:

- **Identify potential bottlenecks early:** Consider making special considerations for groups of users who have a lot of large files. For example, video department users may have large video files they will need to sync to OneDrive. You might ask them to sync their files during a time when network traffic is low.
- **Monitor performance:** If you are doing a phased rollout, monitor network performance levels with your first rollout and use that information to adjust the next set of rollouts accordingly.
- **Communication is key:** Make sure your users clearly understand what is expected of them to keep your deployment plan on schedule. Before the rollout begins, you should communicate what is required when they see the Welcome to OneDrive wizard and who can help if they encounter a problem.

Learn about the OneDrive for Business Next Generation Sync Client.

Content migration

To ensure a frictionless transition for users, a successful OneDrive for Business deployment requires a successful content migration plan. The most common definition of content migration is the moving or copying of documents from a source content store to a target content store. The process of migrating content from one content store to another requires an appropriate level of planning. Small content migration projects of a few hundred documents may not require sophisticated planning, processes, or tools. On the other hand, projects involving thousands or millions of documents require careful planning and a process framework. Effective content migration frameworks are composed of:

- Models for the source and target content stores
- Processes used to plan, execute, and track the migration process
- Tools to support the chosen processes
- Best practices

Analyze existing content and distribution

The most important aspect of migration is determining where the source content resides, which can include files shares, existing file share and sync solutions, or SharePoint sites. There may be differing content structures and capabilities associated with each source content location. For example, a SharePoint site source content repository may have event-based workflow and/or fine-grained permissions associated with individual documents.

Identify the working set of content

SharePoint Server 2013/2016 does not provide an out-of-the-box solution to facilitate content analysis related to migration. However, you can use the audit feature of SharePoint Server 2013/2016 to track which users have taken what actions on the sites, content types, lists, libraries, list items, and library files of site collections. Knowing who has done what with which information is critical for many business requirements, such as regulatory compliance and records management, and it can support identifying how frequently specific files are used. On a site-collection by site-collection basis, a site collection administrator can retrieve the history of actions taken by a particular user and the history of actions taken during a particular date range.

When auditing content usage, you should identify two sets of data based on policies: working set and non-working set. For example, the working set can be considered content modified or used within the previous six-month period, whereas the non-working set can be content that has not been modified or viewed within that period. Using this information, you can decide which content should be considered for migration to OneDrive for Business.

Learn more about configuring audit settings for a site collection.

After content has been properly classified into working and non-working sets, you need to elect how content should be archived.

SharePoint Server 2013 includes features that can help organizations implement integrated records management systems and processes. In SharePoint Server 2013, you can manage records in an archive, or you can manage records in the same document repository as active documents.

By using the SharePoint Server 2013 in-place approach, when you declare that a document has become a record, the document remains in place but SharePoint Server 2013 manages it as a record. For example, a document might get a different retention policy when it is declared to be a record, or users might be unable to edit it.

Learn more about records management in SharePoint 2013.

Depending on the source content repository, source content may have additional descriptive information associated with the file, including:

- **Metadata:** Additional descriptive information stored in a document, a companion file, or a record in a database or line-of-business application
- **Structure:** Information implied by the folders and containers used to store or group the content files
- **Access controls:** The security mechanisms (usually associated with the folder structures) that control the rights granted to a particular user for reading, writing, creating, and deleting content

- **Event-based workflow:** Application logic that may be associated with a content store or folder that is executed when a new document is created or a change to an existing document is made
- **File and folder restrictions:** Limitations based on the length of file and folder names or the set of valid characters that can be used to name them

Metadata

In SharePoint 2013/2016, the Managed Metadata Service Application makes it possible to use managed metadata and share content types across site collections and web applications. A managed metadata service publishes a term store and, optionally, content types; a managed metadata connection consumes these.

Prior to migrating the working set to OneDrive for Business, you should evaluate what metadata is associated with the source content and the approaches required for retention, if desired.

If the source content has assigned terms based on a Managed Metadata Term Store, differences in the metadata property values will exist. This scenario occurs when the values of a property in the target SharePoint environment are different from those used for the corresponding property in the source content store. A frequent example of this is when a source property uses a numerically coded value, such as a term in the Managed Metadata Term Store where the term itself is assigned a unique identifier used throughout the server farm environment; such a term cannot simply be recreated in the destination environment, as the unique identifier will differ.

Structure

How content is structured is a product of information architecture. Structure enables simplified navigation and discoverability. Depending on the source location and migration methodology, a simple drag-and-drop approach may be used to maintain the structure of user content across the source and destination. In addition, a number of third-party tools are designed to support the preservation of the content structure during migration.

Access controls

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 OneDrive for Business, your organization will use either a manual approach or a third-party migration tool.

One way to manually move content to OneDrive for Business is by connecting the OneDrive for Business sync client to OneDrive for Business. You can then upload content to the OneDrive for Business sync client, and it will automatically synchronize to OneDrive for Business. Another manual approach is to use the capability of SharePoint to upload multiple files. This will enable you to upload batches of files all at once.

> Note: If you use manual migration methods, the uploaded files will appear as having been 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 a migration tool to migrate your SharePoint content, be sure to verify that the tool meets your requirements and supports all the SharePoint artifacts you want to migrate. Refer to the third-party tool's documentation and evaluate what preparation steps your organization will need for implementation.

Microsoft partners are also available to assist with migrating SharePoint content to OneDrive for Business using third-party tools. The Office 365 Marketplace provides names of recommended deployment partners that can assist with SharePoint content migrations.

Workflow and other considerations

Although workflow or application migration appears as the last step in the process, this step usually begins immediately after planning is complete and runs in parallel with the core migration processes. This is because this migration step usually requires some level of custom software development to implement the event-handling logic or the deployment and configuration of a third-party workflow solution. The amount of effort required for this step can vary considerably depending on the original workflow requirements of the source content and any new workflow requirements for the migrated content.

File and folder considerations with OneDrive for Business

For documents stored outside of SharePoint and considered for migration, the underlying file system determines the limitations on the length of file and folder names and the set of valid characters that can be used to name them. These can differ from those allowed or disallowed by OneDrive for Business.

When considering a migration to OneDrive for Business, you should be aware of the specific file and folder considerations. While some considerations exist that are explicit to OneDrive for Business and SharePoint, others are derivative of the underlying client and/or server file system. For example, on Microsoft Windows the following characters cannot be used in files or paths:

<,>,|,☺,☻,♥,♦,♣,♠,♫,☼,►,◄,↕,‼,¶,§,▬,↨,↑,↓,→,←,∟,↔,▲,▼,:,*,?,\,/

Paths

<,>,|,☺,☻,♥,♦,♣,♠,♫,☼,►,◄,↕,‼,¶,§,▬,↨,↑,↓,→,←,∟,↔,▲,▼,:,*,?,\,/

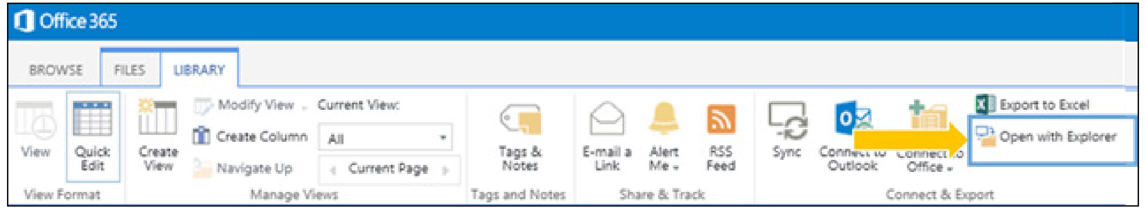
> Note: The above represents an array returned by the **Path.GetInvalidFileNameChars** and **Path.GetInvalidPathChars** methods respectively. These methods, however, do not return a complete set of characters invalid in file and path names because they can differ depending on the underlying file system. On Windows-based desktop platforms, invalid path characters might include ASCII/Unicode characters 1 through 31, as well as quote ("), less than (<), greater than (>), pipe (|), backspace (\b), null (\0) and tab (\t), in addition to those in the example above.

File and folders preceded by underscore (_)

Files and folders with names preceded by the underscore character (_) are considered "hidden." This limitation is derived from the Win32FileAttributes in the WebDAV protocol. In scenarios where (_) precedes a file and/or folder, such as _Documents or _document.docx, the file and/or folder will be visible in the OneDrive for Business sync client and the Web UI. However, when using Explorer View in the Web UI, files and folders preceded by (_) will not be visible. Explorer View in OneDrive for Business uses the WebDAV protocol, which is an extension of the HTTP protocol used to enable management of documents stored on World Wide Web servers. The scenario herein is based on limitations implied in Microsoft FrontPage 2000.

[Learn more about folders.](#)

In OneDrive for Business, Explorer View can be instantiated by selecting **Open with Explorer** on the ribbon (as shown below).



When you use Open with Explorer, it opens Windows Explorer on your computer and displays the folder structure on the server computer that underlies the site. You can manipulate the files in the folder, such as copying, renaming, deleting, and so forth.

Customers who have deployed OneDrive for Business on-premises can nullify the Win32FileAttributes using PowerShell or C# as illustrated in the following samples:

PowerShell

IT professionals can use PowerShell to remove the vti_winfileattribs folder metadata, as shown in the following:

```
$Folder = (Get-SPWeb http://contoso.sharepoint.com).
Folders["<DocLib _ Name>"].SubFolders["< _ Folder _
Name>"]

$Folder.Properties["vti _ winfileattribs"]=""
```

C#

Developers can use the SPFolder.Properties property to enumerate the hash table that contains the metadata for folders, and they can implement the DeleteProperty method to delete the element with the vti_winfileattribs key from the metadata for the folder.

[Learn more about the SPFolder.DeleteProperty method.](#)

WebDAV Resources

WebDAV API functions

[MS-WDV]: Web Distributed Authoring and Versioning (WebDAV) Protocol: Client Extensions

[MS-WDVSE]: Web Distributed Authoring and Versioning (WebDAV) Protocol: Server Extensions

Files and folders preceded or followed by period (.)

A number of restrictions with file and folder naming conventions are derivative of the file system. Developers who use Windows APIs for file and device I/O in many cases understand the various rules, conventions, and limitations of names for files and directories.

Files and folders with names preceded or followed by the period (.) character cannot be stored or synchronized with OneDrive for Business. All file systems follow the same general naming conventions for an individual file: a base file name and an optional extension, separated by a period. The assumption in this case is that the period separates the base file name from the extension in the name of a directory or file.

Restricted characters in file and folder names

Beyond the limitations documented previously, users can create files and folders using any character, including Unicode characters and characters in the extended character set (128–255). Exceptions include the following reserved characters:

- **<** (less than)
- **>** (greater than)
- **:** (colon)
- **“** (double quote)
- **/** (forward slash)
- \ (backslash)
- **|** (vertical bar or pipe)
- **?** (question mark)
- ***** (asterisk)

These limitations are applicable to Windows.

In addition, you cannot use:

- **~** (Tilde)
- **#** (Number sign)
- **%** (Percent)
- **[ ]** (Braces)
- **{ }** (Angle brackets)
- **?** (Question mark)

> Note: You cannot use the period character consecutively in the middle of a folder name. In the Windows File System, two consecutive periods (..) are used as a directory component in a path to represent the parent of the current directory, for example “**..\temp.txt**”.

These limitations are applicable to OneDrive for Business and SharePoint 2013.

Learn more about character limitations.

Other considerations

SharePoint 2013 and OneDrive for Business do not provide support for POSIX semantics; that is, a folder "Foo" and "foo" are considered the same, as opposed to differing paths.

Configuring OneDrive for Business redirection in SharePoint Server 2013/2016

Create a pilot group

Large scale, immediate migration should be avoided because it limits the granularity of data collection and problem resolution. A small, targeted pilot enables an organization to selectively migrate a portion of users while collecting feedback and addressing any issues prior to extending migration to the broader organization. A pilot group should consist of key stakeholders who possess a technical acumen and are capable of influencing users within their departments as evangelists for new technologies.

The pilot group should support defining the general policies surrounding structure and use of OneDrive for Business, as well as documentation efforts that will be useful as more users are added. Communicate with these users regarding early adoption, participation, testing, and acceptance.

Download the SharePoint adoption guide to learn more.

Create Active Directory security or universal group, such as OneDrive Cloud Users

Use the following steps to create a new membership in Active Directory:

1. On a computer that has Active Directory management tools installed, click the **Start** charm and then click the **Active Directory Users and Computers** tile.
2. In the navigation pane, select the container in which you want to store your group. This is typically the **Users** container under the domain.
3. Click **Action**, click **New**, and then click **Group**.
4. In the **Group name** text box, type the name for your new group.
5. In the **Description** text box, enter a description for this group.
6. In the **Group scope** section, select either **Global** or **Universal**, depending on your Active Directory forest structure. If your group must include computers from multiple domains, select **Universal**. If all members are from the same domain, select **Global**.
7. In the **Group type** section, click **Security**.
8. Click **OK** to save your group.

Create and compile audiences in SharePoint Server 2013/2016

Audiences in SharePoint Server 2013/2016 are groupings of users that can be used to target content on a SharePoint Server site. SharePoint Server 2013/2016 allows targeting to the list item level or to the list level. Groupings are determined by membership in Microsoft Exchange Server distribution lists, membership in SharePoint groups, or rules that are configured by an administrator. Each audience must be compiled before content can be targeted to that audience. Compilation identifies membership in an audience by crawling the data most recently reported from the identity management system.

You can add, edit, or delete an audience by using the Central Administration tool in SharePoint Server 2013/2016. When you add a new audience, you also add a rule that determines the membership for the audience. Audiences must always have at least one audience rule.

When you add a new audience, you also select an owner for the audience. The owner should be someone who understands why the audience was created and who can be contacted if there is a problem with the audience. Typically, the owner will be the person who created the audience, but this is not a requirement. Having audience owners is helpful in enterprises that have a large number of audiences created by several different administrators. Use the following steps to add a new audience:

1. Verify that you have at least one of the following administrative credentials:
   - You are a member of the Farm Administrators group.
   - You are an administrator for the User Profile service application that contains the audience you want to edit.
   - You are an administrator for the Audience feature of the User Profile service application that contains the audience you want to edit.
2. In Central Administration, in the **Application Management** section, click **Manage service applications**.
3. On the **Service Applications** page, in the list of service applications, click the row of the User Profile service application you want to configure. This activates options on the ribbon.
4. In the **Operations** group on the ribbon, click **Manage**.
5. On the **Manage Profile Service** page, in the **People** section, click **Manage Audiences**.
6. On the **View Audiences** page, click **New Audience**.
7. On the **Create Audience** page, in the **Properties** section, in the **Name** box, type a name for the new audience.
8. In the **Description** box, type a description of the new audience.
9. In the **Owner** box, type the account name of the user who will own and manage this audience. You can click **Check Names** to verify that you have typed the name correctly, or you can click **Browse** to search for an account name.

10. Select **Satisfy all of the rules** to require that all of the rules need to be satisfied in order for a user to be included in the audience. Or, select **Satisfy any of the rules** to allow membership in the audience as long as any of the rules are satisfied.

11. Click **OK**.

12. On the **Add Audience Rule** page, you can add a rule based on a user—for example, all users who report to a specific manager. To do this, use the following steps:

    12.1 In the **Operand** section, select **User**.

    12.2 In the **Operator** section, select **Reports Under** to create a rule based on organizational hierarchy, or select **Member Of** to target content by group or distribution list.

    12.3 In the **Value** box, type a value or select a user to use when evaluating the property against this rule. For a **Reports Under** rule, select the person who manages the users you want to include. For a **Member Of** rule, select the group or distribution list that the user must belong to in order to be included.

13. You can also create an audience based on a user profile property—for example, all users whose job title is "accountant":

    13.1 In the **Operand** section, select **Property** and then select a user profile property from the list.

    13.2 From the **Operator** list, select an operator for the property. Each user profile property has a slightly different set of operators. For example, the operators for the **Job Title** property are **Contains** and **Not Contains**. To find descriptions of the operators available in the UI, go to Operators (Transact-SQL).

    13.3 In the **Value** section, type a value (for example, **accountant**) to use when evaluating the property against this rule.

14. Click **OK**.

Configure OneDrive for Business redirection in SharePoint Server 2013/2016

Use the following steps to configure OneDrive for Business redirection:

1. Verify that the user account performing this procedure is a member of the Farm Administrators SharePoint group.
2. In Central Administration, choose **Office 365** and then **Configure OneDrive and Sites links**.
3. On the **Configure OneDrive and Sites links** page, in the **My Site URL** box, type the My Site URL that you got from Office 365 portal administration.
4. Specify an audience. Choose **Everyone** if you want all of your users to be redirected, or choose **Use a specific audience** and type the name for the audience that contains your Office 365 users.
5. Optionally, if you also want to redirect the **Sites** page in users' personal sites, select the **Redirect the Sites page** check box.
6. Click **OK**.

It is also recommended that you implement hybrid search to provide unified discovery across SharePoint Server 2013/2016 and OneDrive for Business in Office 365. When choosing SharePoint Server 2013/2016 coexistence with OneDrive for Business, the result is managing content across two separate repositories. While PowerShell exists to manage both infrastructures, users require a unified approach to discovery of content across both infrastructures.

In a SharePoint hybrid environment composed of an on-premises deployment of SharePoint Server 2013/2016 and an instance of Office 365 for professionals and small businesses that includes SharePoint Online, the SharePoint Server search index and the SharePoint Online search index typically contain different content. The SharePoint Server search index contains crawled content from local SharePoint Server sites, file shares, and other sources. The SharePoint Online search index contains crawled content only from SharePoint Online sites. SharePoint hybrid search enables users to get and view search results from both indexes at the same time.

Optional: configure eDiscovery in Office 365

eDiscovery allows records managers and litigators to discover content in electronic format. Typically, eDiscovery requires searching for documents, websites, and email messages spread across laptops, email servers, file servers, and other sources, and collecting and acting on content that meets the criteria for a legal case.

In SharePoint Server 2013, Microsoft added the Hold and eDiscovery feature, which made it possible to place a hold on any site in SharePoint. A records manager could put documents, pages, and list items on hold, which prevented users from deleting or editing them. Microsoft Exchange 2010 introduced ways to place legal holds on mailboxes, conduct searches across multiple mailboxes, and use a PowerShell cmdlet to export mailboxes.

OneDrive for Business redirection

eDiscovery in SharePoint 2013 includes new ways to reduce the cost and complexity of discovery. These include:

- The eDiscovery Center, which is a central SharePoint site used to manage preservation, search, and export of content stored in Exchange and SharePoint across SharePoint farms and Exchange servers
- SharePoint In-Place Hold, which preserves entire SharePoint sites and protects all documents, pages, and list items within the site but allows users to continue to edit and delete preserved content
- Exchange In-Place Hold, which preserves Exchange mailboxes and protects all mailbox content through the same UI and APIs used to preserve SharePoint sites
- Query-based preservation, which allows users to apply query filters to one or more Exchange mailboxes and SharePoint sites and restrict the content that is held

SharePoint Server 2016 introduces new capabilities to identify and search for sensitive content in both SharePoint and OneDrive documents. With this new capability, you can:

- Search for sensitive content across SharePoint Server 2016, SharePoint Online, and OneDrive for Business
- Leverage 51 built-in sensitive information types (credit cards, passport numbers, Social Security numbers, and more)
- Use DLP Queries from the eDiscovery site collection to discover sensitive content relating to common industry regulations from the SharePoint eDiscovery Center, identify offending documents, and export a report
- Turn on DLP Policies from the Compliance Policy Center site collection to notify end users and administrators when documents with sensitive information are stored in SharePoint and to automatically protect the documents from improper sharing

OneDrive for Business redirection

OneDrive for Business redirection

Learn more about searching for sensitive content in SharePoint and OneDrive.

Learn more about using DLP in SharePoint Online to identify sensitive data.

In addition, you can configure eDiscovery in SharePoint Online to complement the on-premises SharePoint environment. You have to be an Office 365 global administrator in your Office 365 organization to configure eDiscovery and set up an eDiscovery Center in SharePoint Online. After you set up eDiscovery, users with the required permissions can create eDiscovery cases, place content on hold, run eDiscovery searches, and export search results.

Learn more about setting up an eDiscovery in SharePoint Online.

Office Graph/Delve

About Office Graph and Delve

Office Graph represents a collection of content and activity and the relationships between them that happen across the entire Office suite. From email, social conversations, and meetings to documents in SharePoint and OneDrive, Office Graph maps the relationships among people and information, and it acts as the foundation for Office experiences that are more personalized for each individual. Office Graph uses sophisticated machine learning techniques to connect people to relevant content, conversations, and people around them. Going forward, Office Graph will continue to evolve and deliver increasingly rich insights in Office 365 and will incorporate support for extensibility to reach beyond Office 365.

Delve surfaces personalized content from across Office 365. Powered by Office Graph, Delve brings you information based on what you're working on, who you're working with, and the permissions you have.

Integrating SharePoint Server 2013/2016 with Delve

SharePoint Server 2013/2016 supports the use of Delve in Office 365 through the Cloud Search Service Application described earlier in this guide.

Yammer

Microsoft Yammer comes in two varieties: Yammer Basic and Yammer Enterprise. Yammer Basic is free and available to all users. It lets employees collaborate with other members of their organization. Yammer Enterprise is a premium version that extends an organization's basic Yammer network. It's offered both as a standalone product and with Office 365 plans. (Compare Office 365 plans.) Yammer Enterprise provides additional tools and resources to help organizations set up the best possible enterprise social network. Learn more about Yammer.

Although SharePoint Server 2013/2016 provides basic enterprise social features, Yammer offers a richer enterprise social experience. You can embed a Yammer feed in a SharePoint site by adding it to the navigation bar. For more information about Yammer features and SharePoint Server 2013/2016, read Work like a network! Enterprise social and the future of work.

Before you integrate Yammer into your SharePoint environment, you should learn about Yammer networks, groups, and users, and understand how they combine to create a foundation for providing you with a rich Yammer experience within SharePoint.

You can choose whether to use the social features in SharePoint or Yammer. If you want to take advantage of both by harnessing the power of Yammer with SharePoint, you can use any of the following methods:

Directory synchronization

By using directory synchronization, your organization can use existing on-premises user accounts. Your organization can also significantly reduce operational costs and give its employees safer and easier access to Yammer. Go to Plan for Yammer Directory Sync for more information.

Note that Yammer Directory Sync is being deprecated and will stop working after December 1, 2016. You will not be able to set up new configurations with Yammer Directory Sync after April 1, 2016. We recommend you use Azure AD Connect instead. To learn more, read these two articles: Integrating your on-premises identities with Azure AD and Understanding Office 365 identity and Azure AD.

Learn more about deprecation and transitioning out of Yammer Directory Sync.

Single sign-on (SSO)

SSO lets users seamlessly access Yammer with their existing AD DS corporate credentials through a federated identity provider. We recommend that you use AD FS 2.0 because it provides the easiest identity integration with an existing SharePoint environment.

Learn more about setting up SSO in a Yammer network.

Note that Yammer SSO is being deprecated and will stop working after December 1, 2016. You will not be able to set up new configurations with Yammer SSO and Directory Sync after April 1, 2016. Instead of Yammer SSO, we recommend you use Office 365 sign-in for Yammer.

Learn more about deprecation and transitioning out of Yammer SSO and Directory Sync.

To take advantage of the features that are provided by Yammer, you should integrate the Yammer experience into SharePoint and replace the default SharePoint Server 2013/2016 enterprise social features. You can drive increased collaboration and innovation across your organization by adding Yammer functionality through any of the following methods:

Add Yammer to the navigation bar for SharePoint 2013

You can replace the Newsfeed link with a Yammer link on the top navigation bar for SharePoint. This functionality is included in Service Pack 1 for SharePoint Server.

Use the following steps to add Yammer to SharePoint on-premises navigation:

1. Verify that the user account performing this procedure is a member of the Farm Administrators group.
2. In Central Administration, choose **Office 365** and then **Configure Yammer**.
3. On the **Yammer Configuration** page, select **Activate Yammer**.

Add Yammer to the app launcher for SharePoint Server 2016

You can replace the Newsfeed tile with a Yammer tile on the SharePoint app launcher. This functionality is included in SharePoint Server 2016.

Use the following steps to add Yammer to the SharePoint on-premises app launcher:

1. Verify that the user account performing this procedure is a member of the Farm Administrators group.
2. In Central Administration, choose **Office 365** and then **Configure Yammer**.
3. On the **Yammer Configuration** page, select **Activate Yammer**.

Use Yammer instead of SharePoint Newsfeed features

To take advantage of the features that are provided by Yammer, it's a good idea to replace the default SharePoint Server 2013/2016 enterprise social features with equivalent Yammer features. You can remove the SharePoint Server social web parts from My Sites and Team Sites, and you can hide the user interface controls that provide social functionality.

The new Yammer app for SharePoint lets you embed Yammer feeds into on-premises SharePoint Server 2013/2016 sites to make them more social and engaging. Before you can do that, however, you must do the following:

1. Remove the Newsfeed web parts from My Sites and Team Sites.
2. Hide the user interface controls that provide social features.
3. Install the Yammer app for SharePoint.
4. Add the Yammer feeds to your sites.

Learn more about hiding SharePoint Server 2013 social features.

Use Yammer Embed to add feeds to SharePoint pages

You can use Yammer Embed to embed Yammer feeds in on-premises sites. Yammer Embed is a JavaScript widget that you can add to SharePoint Server 2013/2016 pages to display different kinds of Yammer feeds. Go to Add the Yammer Embed widget to a SharePoint page to learn more.

The following sections describe scenarios common to most customers. For each, the steps required to integrate Yammer with your on-premises SharePoint Server environment are outlined. The steps for each scenario vary based on the state of your existing environment and your current Yammer deployment. Go to Social scenarios with Yammer and SharePoint Server 2013 to learn more.

Business Connectivity Services

The Microsoft Business Connectivity Services (BCS) hybrid deployment scenario allows you to securely publish on-premises data to an external list or app for SharePoint in SharePoint Online. From there, users can view and edit the data, depending on the permissions they have.

Learn more about hybrid Business Connectivity Services solutions.

Duet Enterprise Online for SharePoint and SAP

Duet Enterprise Online for Microsoft SharePoint and SAP is a jointly developed product from SAP and Microsoft that enables interoperability between SAP applications and SharePoint Online. Duet Enterprise Online empowers employees to consume and extend SAP processes and information from SharePoint Online and Outlook 2013. Information stored in SAP applications is not moved into SharePoint. Instead, the information stays in the SAP applications and is surfaced in SharePoint Online. This means, based on an individual user's permissions, the user can view and change information that is stored in an SAP application from within SharePoint sites. Duet Enterprise Online requires a combination of SharePoint Online, an on-premises SharePoint Server 2013/2016 farm, and an SAP system.

Learn more about Duet Enterprise Online.

Plan to deploy Duet Enterprise Online for Microsoft SharePoint and SAP.

Install and configure Duet Enterprise Online for Microsoft SharePoint and SAP.

Extranet sites

An extranet site in SharePoint is a site that organizations create to let external users have access to relevant content and to collaborate with them. Extranet sites allow partners to do business securely with your organization. The content for your partner is kept in one place, and they have only the content and access they need. They don’t need to email the documents back and forth or use tools that are not sanctioned by IT.

Traditionally, deploying a SharePoint on-premises extranet site involved complex configuration to establish security measures and governance, including granting access inside the corporate firewall, plus expensive initial and ongoing costs. But with Office 365/SharePoint hybrid extranets, partners connect directly to a members-only site in Office 365 without access to the corporate on-premises environment or any other Office 365 site. Office 365 extranet sites can be accessed anywhere.

Learn more about hybrid Office 365 extranets.

Document collaboration

A new attachment option—*document collaboration*—is now available in Office 365. In Exchange 2016, this option allows on-premises users to integrate attachments stored on OneDrive for Business directly in their Outlook on web clients.

Learn more about document collaboration.

Hybrid scenario picker

The hybrid scenario picker is a new feature in Office 365 that simplifies the configuration and deployment of hybrid capabilities with SharePoint Server 2013/2016. You can use the scenario picker wizard to redirect OneDrive for Business to SharePoint Online and/or to make a Server-to-Server (S2S)/OAuth connection for your SharePoint hybrid features.

Learn more about the hybrid scenario picker in Office 365.

Conclusion

Hybrid SharePoint is about connecting the best of both worlds—on-premises and cloud—to achieve business value through hybrid pillars. A hybrid solution can help your company get started in the cloud, letting you take a first step to exploring cloud functionality at your own pace. A hybrid environment enables enterprise users to be connected from almost anywhere to the resources and content they need.

Learn more about the benefits of hybrid SharePoint and Office 365.

Resources

SharePoint Hybrid

Appendix A, Migration

When planning your Office 365 deployment, you should evaluate which of the SharePoint capabilities you will implement in your Office 365 environment.

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 you plan to move to SharePoint Online. The analysis should give you a clear understanding of the content and customizations you have in your on-premises environment.

You will then create a content and customization roadmap that covers what content and customizations 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 validate if the customizations can be implemented as sandboxed solutions.

Content migration

Learn more about moving documents and files to your SharePoint Online site.

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 those 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 all at once.

> Note: If you use the manual migration methods described above, the uploaded files will appear as having been created by the user who uploaded them. Also, the timestamp of the file will be the upload time and not the original creation time.

Office 365 provides the following methods for migrating multiple files to SharePoint Online:

Migration method	Description
Office 365 Import service for SPO Migration	Use the Microsoft Office 365 Import service to migrate files from your on-premises file shares or from your on-premises SharePoint Server site.
Links to the SPO Migration API are listed in the SPO Migration Content Roadmap	Use the SPO Migration API to create a migration import job to Office 365 and queue it up for later processing by a separate timer job.
Windows PowerShell cmdlets for SPO Migration Public Preview	Use PowerShell cmdlets for SPO Migration Public Preview to migrate content from an on-premises file share or an on-premises SharePoint Server site to Office 365.

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 it.

Microsoft partners are available to assist with migrating your SharePoint content to SharePoint Online using third-party tools. The Office 365 Marketplace also provides names of recommended deployment partners that can assist with SharePoint content migrations.

Appendix B, Troubleshooting

Because a hybrid environment involves a complex security and authentication topology, it is important to test a given scenario to make sure that users can authenticate from expected locations and that permissions and security trimming produce the expected results. In many cases, the administrator accounts that you use to configure different components in the hybrid environment are not federated with your Office 365 tenant or may not have specific permissions to access resources in SharePoint Server or SharePoint Online.

For example, in a two-way hybrid search environment, an Office 365 global administrator account cannot be used to test search queries from a SharePoint Online Search portal that is expected to return results from the on-premises SharePoint Server farm. These queries are unauthorized because native Office 365 user accounts cannot be authenticated by on-premises Active Directory and have no user profile object in the on-premises SharePoint Server farm. Similarly, an on-premises domain administrator account is unlikely to be federated. Therefore, it cannot be assigned permissions in a SharePoint Online site collection configured for hybrid search. This account cannot successfully use the SharePoint Server Enterprise Search portal to query SharePoint Online.

For these reasons, you should carefully design a test strategy that uses test user accounts that are configured specifically to emulate the authentication and authorization characteristics of a general user in your corporate environment.

The best practice is to design a test plan that follows these general principles:

- Clearly define and document the scope, goal, and procedures for each test. Depending on your architecture and solution, these may include user authentication, authorization, latency between the user interface and data sources, user experience when authenticating from different networks and geographic locations, and component failover or high availability. Don't cut corners by using cryptic notes or combining tests to save time.
- Use test-specific user accounts configured to use group memberships and permissions that are designed to test specific functionality. Don't reuse test accounts between tests; any changes that you make to accounts or permissions between tests may result in conflicts or artifacts that might obscure the test results.
- For each test, decide at the beginning what constitutes success or failure, and establish the specific determining factors.

It is important to test SSO using a non-administrator federated account to make sure that domain users can successfully authenticate. In some scenarios, you may have to test authentication for federated test users from both on-premises computers and the Internet to make sure that the federation identity provider is configured correctly. It is recommended that when you design your test strategy, you plan for test client computers that are appropriately connected to either the on-premises network or the Internet/extranet. In addition, to make sure they are configured correctly, use the security settings and software that you use in production.

Learn more about troubleshooting hybrid SharePoint environments.

Microsoft