RED MANTA

OneDrive for Business Mistakes

Registered Address | One Elmfield Park, Bromley, BR1 1LU
Company Registered Number: 5929395, Company VAT Number: 939 4938 63

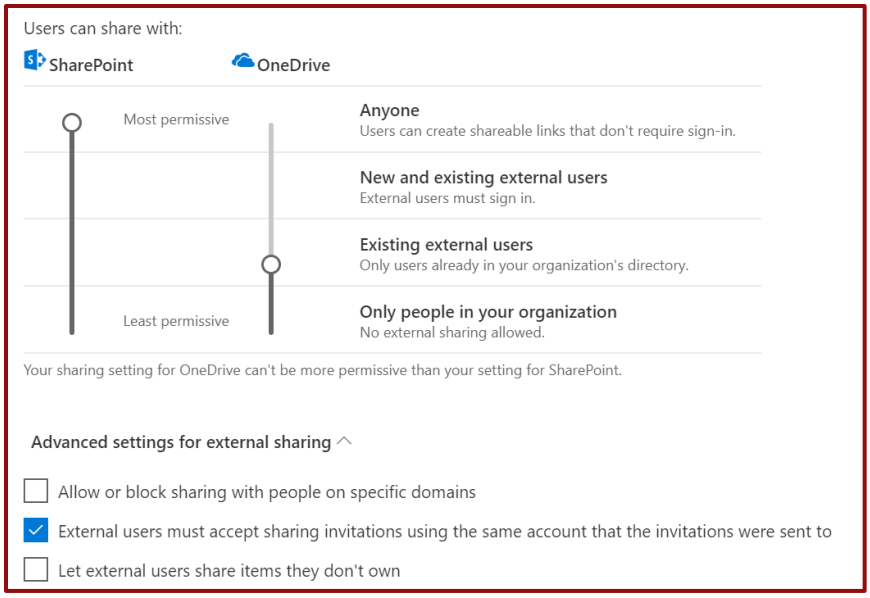
Background

Since its launch back in 2007, OneDrive has seen many changes and not just in name. Previously known as SkyDrive Pro until a lawsuit with the media broadcaster BSkyB resulted in Microsoft renaming the product to OneDrive for Business in 2013. Confusingly, the name OneDrive for Business is often interchanged with the term “My Sites” when dealing with SharePoint on-premises products and SharePoint Online. In addition to the business product, there is also a consumer product simply called OneDrive.

To utilise OneDrive for Business successfully, there are two pieces to the puzzle, the OneDrive for Business Site Collection for storing content in SharePoint Online and the OneDrive for Business client for synchronising files between Office 365 services and the user’s local machine. A OneDrive for Business Site Collection can be automatically provisioned for each user as part of licencing SharePoint Online or the creation can be controlled by administrators. When enabling users for OneDrive for Business, the default configuration may not always be the best. Here we set out some common mistakes we have seen when companies configure OneDrive for Business for end-users.

External sharing

This is the most common headache we’ve seen with companies who have already deployed OneDrive for Business. By default, external sharing is enabled from OneDrive for Business sites and depending on the configured method of sharing, items shared with external users may no longer be traceable.



By limiting what can be shared and by whom from OneDrive for Business, companies can help mitigate data leaks.

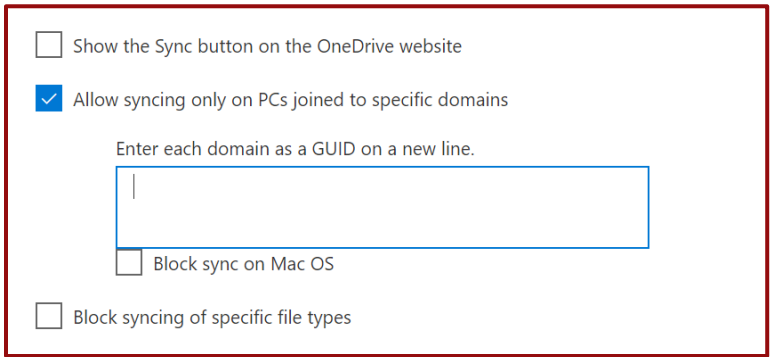
Clean-up

When a user leaves a company and the account is marked for deletion, the OneDrive for Business Site Collection is deleted after 30 days. As part of the Clean-up process a user's line manager, if known can automatically be granted permission to the Site or alternatively a SharePoint administrator can be nominated.

By configuring delegation, files can be copied to a more suitable location before the data is erased preventing valuable files from being lost.

Sync

One of the main advantages of the OneDrive for Business client is the ability to synchronise content from a user's OneDrive for Business Site Collection and SharePoint Online libraries. To fully protect company information, additional services such as Conditional Access and Intune can be deployed to prevent data being accessed from unmanaged locations and/or devices.



Even without utilising these services, administrators can ensure that their users can only synchronise files to domain joined machines by adding domains as GUIDs to the allow list.

Migrating content

When considering enabling OneDrive for Business for users, one of the main purposes is to remove the reliance on on-premises file shares by migrating users' personal drives to the OneDrive for Business service.

Companies can ensure that not only is the data relevant and still required but that it is migrated to the correct location.

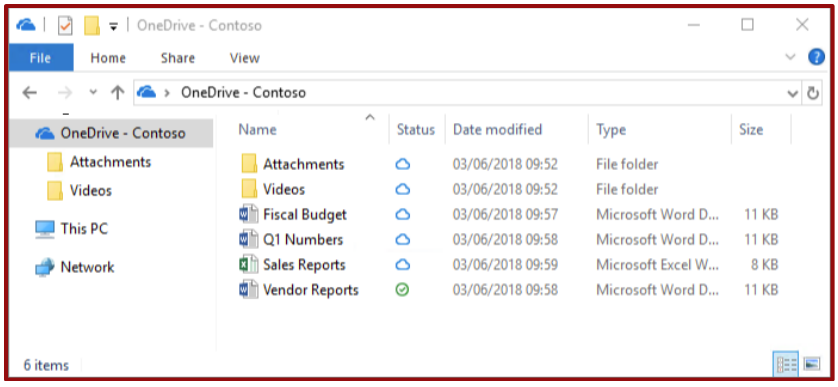
Group Policies

When deciding whether to install the OneDrive for Business client for end-users, attention to the configuration options available via Group Policies are often overlooked. There are several group policies that administrators can apply to help stop users making configuration changes to the client, limit the bandwidth being used when on metered networks and prevent users synchronising with personal OneDrive accounts.

Administrators should study the configuration possibilities for OneDrive for Business policies.

Files On-demand

Introduced for Windows 10 with the Fall Creators Update (16299.15), Files On-demand allow users to see the all files and folders within their OneDrive for Business Site Collection from Windows Explorer. If a user wants to open a file which hasn't already been synchronised, the OneDrive for Business client downloads the document on the fly. With some Office 365 licencing providing upwards of 1 TB of storage per user, local disk storage can eventually become a limitation.



By not enabling this feature, administrators run the risk of clients filling up the local storage by downloading every file during the sync process.

Education

Lastly, educating users on the best way to use OneDrive for Business and what type of data should and shouldn't be stored in the Site Collection should not be underestimated. Microsoft have made great advances in providing tutorials on how the service works, but companies should still take precautions to ensure that users are fully aware of the implications when it comes to storing and sharing content. This may include internal guidelines such as prevent the storage of Personal Identifiable Information (PII).

Companies should not rely on Microsoft materials alone and should publish guidelines and training material for OneDrive for Business users.

Conclusion

Allowing users to store and synchronise content using OneDrive for Business is a fantastic way of driving collaboration and remote working. However, unless taken seriously, it can be a headache for administrators and compliance officers responsible for keeping company and client data secure. While settings in the OneDrive for Business Admin Centre, SharePoint Online Admin Centre and Group Policies can be configured to reduce data loss and tightly control functionality, administrators should also explore the options available to them with other Microsoft services such as Azure AD Conditional Access and Device Management with Intune.
For further information on anything discussed in this document or to engage Red Manta to assist with your OneDrive for Business engagement, please contact us.