Vault Collaborative Authoring with Microsoft Office FAQ

General

Is Collaborative Authoring available in all Vault applications?

Collaborative Authoring is a feature of the Vault Platform and is available in any Vault application that has document management capabilities.

Does Collaborative Authoring work with Excel as well?

Users can use Collaborative Authoring with Microsoft Word, PowerPoint, and Excel files.

Will the process work with ISI toolbox and Writer?

Collaborative Authoring does not support PDF. ISI toolbox is primarily used for PDF.

Is there a limit on the size of the documents for this feature?

The technical limits of Word can be found at https://docs.microsoft.com/en-us/office/troubleshoot/word/operating-parameter-limitation.

In our experience, co-authoring in Word performs better with smaller files (less than 100 pages) and small teams (5-10 authors). If you are authoring very large files, you should consider disabling the auto-save feature. If you are experiencing issues authoring large files in Word, please contact Microsoft for support.

How is Collaborative Authoring different from third party solutions like PleaseReview?

PleaseReview is a specialized tool for complex document review, redaction and structured co- authoring which helps the document owner maintain total control over all aspects of the document and the review process itself. PleaseReview is recommended for collaborating with large groups of reviewers who are looking to maintain a very high level of control over the document and the review process. More information on PleaseReview can be found here: https://www.ideagen.com/products/pleasereview.

I am not clear on the Microsoft product naming - what is Office 365, OneDrive, SharePoint, Office, etc.?

Office 365 is the umbrella name for the cloud-based Office product. Microsoft recently announced that Office 365 SMB offerings have been renamed to Microsoft 365. It has two distinct offerings:

1. Microsoft 365 (Home) is a consumer cloud product and offers subscription-based client applications and OneDrive personal storage. There is no company or tenant for the consumer product. The Collaborative Authoring feature does not work with this product.
2. Microsoft 365 Business is the Business cloud product and offers subscription-based client applications, Exchange, OneDrive for Business, SharePoint and other services. Microsoft 365 Business includes a tenant (Directory) for the company. Collaborative Authoring works with Microsoft 365 Apps, Business Standard & Business Premium.

"OneDrive for Business" and "SharePoint" run on the same Microsoft 365 platform, just 2 different UIs. Similar to RIM and Clinical are both on Vault Platform. OneDrive for Business is intended for personal file storage and SharePoint is intended for team files. Collaborative Authoring integrates with the Microsoft 365 platform. The consumer "OneDrive" and the business "OneDrive for Business" are built on different platforms and are totally different products.

Are there typically performance differences between using SharePoint and OneDrive?

There is no performance difference. We require that the document is setup using a SharePoint Shared Document Library, since these are not tied to a specific user. You do not want the checked out documents to be tied to a single user account because it gets deleted when a user is removed. OneDrive is not designed to be used for group document sharing.

For a technical issue (i.e. a locked file or if the author is not around to recheck it in) do we contact Veeva or Microsoft?

If a document is locked in Vault, a Vault Admin can unlock the workflow. If you have issues getting set up or checking out/in, Veeva Support can help. If you are seeing issues while users are in Word and collaborating, you will want to work with Microsoft.

Vault Functionality

How does Collaborative Authoring compare to Vault File Manager? Do you anticipate any issues when utilizing File Manager?

Files checked out with Vault File Manager can only be edited by the user who checked them out, whereas Collaborative Authoring allows multiple users to edit the same document at the same time. Additionally, Vault File Manager is only available on Windows, and Collaborative Authoring is currently limited to Microsoft Office files. There are no issues with using Vault File Manager.

Is the standard 'Check-Out' option still functioning when the document is checked out for Collaborative Authoring? And if so, what happens if someone accidentally checks it out using that option?

The standard Check-Out function is not available when a Collaborative Authoring check-out is initiated. Similarly, if the standard Check-Out is initiated, the Edit button for Collaborative Authoring will not be available until the document is checked back in or canceled.

What happens to other users editing the document if a document is checked in? or the check-out is canceled?

Users working together should communicate about their progress and use workflows to coordinate. When a document is checked in, Vault removes all user permissions to the Office edit version and checks in the current edit version with all users' changes. If users try to open or save additional changes to the edit-version after check-in, they will see a permission error or be asked to log in with a different account.

An alternative to checking in a document is the Save to Vault function. When this function is used, the latest version of the document is saved to Vault, but the Collaborative Authoring session is not ended, allowing users to continue with their edits.

What happens to other users editing the document if the check-out is canceled?

When a check-out is canceled, Vault removes all user permissions to the Office edit version and discards any changes made since the last version was saved to Vault. If users have the file open, they will be notified within the Office application that they have a permission error with the file.

Have you heard of more challenges with Collaborative Authoring in certain applications (e.g. Excel more challenging than Word?)

PowerPoint files can sometimes be very large in file size (lots of images and videos) or have a lot of slides, so it's important to check that your changes have been saved successfully to SharePoint. To do this, check the "Save" status at the top of the desktop Office application before using the "Check In" action in Vault. Additionally, users may see an additional browser prompt when checking out PowerPoint files, asking if they want to open PowerPoint. This isn't something that Vault controls.

Who can check-in a document from Office 365?

The user who checked out the document or the document owner can check it in from Office 365. If an administrative override is needed, the Vault Owner can also check in the document.

When a document is checked back in, is there a way to see previously tracked changes?

A Vault Rendition setting can be enabled to view track changes as part of the Viewable Rendition. Even if the setting is disabled, markup will remain in the source document.

Can I add people while the document is open for authoring?

You can add more participants to an ongoing session by adding them to the workflow and granting them edit permissions in Vault through the Sharing Settings.

Does the Service Account require a Vault Account? What level of access does the Service Account have in Azure?

The Service Account does not require an account in Vault. The Service Account’s permissions in Azure should follow the principle of least privilege and should therefore be provided with limited access to the SharePoint site that is used for Collaborative Authoring.

How will Collaborative Authoring impact sponsors that leverage e-signature software such as DocuSign? And have you tested this as part of the release?

This feature does not affect e-signature functionality in Vault, as signature pages are added to Vault documents when finalized. We have not yet tested this with third-party integrations.

Can you configure the review workflow / review document state to prevent annotations and just use Collaborative Authoring for review?

Yes, you can set up a workflow as you choose and then you can decide what the users are supposed to do as a part of the task that that workflow contains.

Does Collaborative Authoring only work in conjunction with workflows and if so, which?

Collaborative Authoring does not require a Vault workflow. Users with the right permissions can edit documents without a workflow, but it is best to use one to manage who can edit and when. This increases control and communication during the co-authoring process. To protect your SharePoint from having unnecessary active documents at once, it is recommended that your workflows have Entry Criteria to validate that documents are not checked out before they can reach a specified lifecycle state.

Can Collaborative Authoring be used in a Multi-Document Workflow?

Yes, Collaborative Authoring is available within multi-document workflows as the functionality is based on document lifecycle state permissions.

Is there an Audit Trail as long as the document is checked out, or do you only see an Audit Trail for new versions (i.e. from 0.1 to 0.2)?

The Audit Trail will display: (1) the initial checkout action, (2) all collaboration users document views (when a collaboration user opens in MS Office) (3) when all collaborators complete their workflow task (4) the check-in action.

When using co-authoring with SharePoint, users can see the document's version history within the Word application (i.e. outside of Vault). Does the same functionality exist in Vault with Collaborative Authoring?

When you end the Collaborative Authoring session from a Vault perspective and you check in the document after all the contributors have completed their edits, we will remove that version from the Microsoft side. That temporary version where it's being saved as people are collaborating will then be removed from that server. The purpose is to remove access to multiple different versions and avoid end-user confusion. You view the version history when you are looking at a document in Word.

SharePoint allows for the version history to be accessed and restored to a previous version within the collaborative environment. Does the Veeva collaborative environment allow for that?

You can view the Version History of a document from the Word Desktop client and restore it to a previous version. These versions are only the changes that occurred since the document was checked out from Vault.

Are you able to export all changes?

You can extract changes from the version history or run a comparison report between versions to see the changes at a glance.

Can you export a binder to a CSV file/excel file to show the status of each document (i.e. Authoring, In Review, etc.) and who it's currently assigned to?

You can run a report to see the status of various documents and various workflows, whether it be an authoring workflow, review workflow, etc. You can then export the results of that report to a CSV/Excel file.

Office 365 Functionality

How many users can work on a document at the same time?

Microsoft indicates that co-authoring is designed to work for small teams of about 5-10 users. Our testing has shown that the performance of co-authoring varies with the number of users and the size of the document. Customers should consider these expectations when determining if Office 365 will satisfy their use cases.

In the track changes information, is it obvious who made what changes?

Track changes is a functionality of MS Word and you can hover over the tracked changes to see which user made the change.

Can Track Changes be turned on by default for all the collaboration from Vault if preferred?

Yes. You can create the template file with Word Track Changes on, and then it would be enabled for all users.

Do all users need to have Track Changes enabled for these to appear correctly, or will only one user need to turn this on for the authoring session?

Once it is turned on in the document it is turned on for all until someone turns it off.

Can all authors see other authors work in progress?

Yes, all authors can see other changes, and this happens periodically if auto-save is on.

How do you manage saving the document and keeping the changes made by other people?

The document is stored in a central location that all users sync their changes to via their local machines. It is one copy in a certain central location set up in your SharePoint environment.

What we highly recommend for all users is to have auto save on for those types of documents that are in Word, so as everyone is typing it saves automatically to that central location. We would also recommend that the last user in the document or the document owner clicks Word's save button before closing that document as a best practice. To ensure that the changes are saved back to Vault, users can initiate the Save to Vault function.

Can anyone alter other users' contributions to a document?

Yes, this is a feature functionality within the Microsoft co-authoring. Co-authoring is restricted on a paragraph basis in scenarios where multiple users are authoring a particular document. Meaning, a user could not go into the same paragraph or section that the other user is editing in real-time until they are out of that paragraph.

For situations where not all users are editing while online, additional coordination is needed to minimize any edit conflicts.

Does this feature support all templates (i.e. custom or out of the box)?

Generally, yes. The Collaborative Authoring feature doesn't require specific templates, whether customer-created or provided by Microsoft or another supplier. The integration edits the document in a local version of Word, so if the template works in the local version of Word it works with the Collaborative Authoring feature as well.

Can users share documents using the Office "Share" button?

No. Office 365 is used only for authoring. Workflow and Sharing should be done using Vault so that permissions are correctly managed, and audit is captured. Turning off sharing in Office 365 is one of the security hardening steps that are recommended in our Technical Configuration Checklist.

How can I support custom macros?

Vault does not support editing or collaborating on documents with macros (e.g. files with .docm extensions). To use macros, customers will need to distribute them via local template files (dot) installed on end-user machines.

What Office 365 attributes will Veeva have access to?

The Collaborative Authoring integration runs using delegated permissions for the Vault Collaboration User, which requires specific permissions. The permissions are included in the product documentation, but the key one is File - Rewrite - All, so we have access to all files checked into that **site** where the Vault Collaboration User is an owner. Our application will not have access to any other data in your Office 365/SharePoint system other than that site. This is in line with the principle of least privilege.

Will Collaborative Authoring work with conditional access on Office 365?

Yes. It is just a SharePoint site and document library, so if you did set up a conditional access, you could apply that. You would want to work with us via a Support ticket so that you can ensure that your policies don't block the integration.

Does Veeva have any recommendations on site storage sizing?

The default setting in SharePoint for site collection storage is "Automatic" which is the recommended setting as it allows SharePoint to allocate more storage as needed.

If a hard storage limit is set, you should specify this based on the expected usage, factoring in the recycle bin. Not setting an adequate limit may result in receiving the following error ‘Server capacity has been exceeded’.

What happens to the temporary files on the SharePoint site?

Vault cleans up checked-in or cancelled files by deleting them from the site, this sends them to the recycle bin in SharePoint. These files are permanently deleted automatically by SharePoint after 93 days.

Following this policy allows customers to recover documents that may have been modified and then canceled or recover an intermediate ending version for a document that was checked into Vault, which was a requirement of the feature.

Are there any other limitations that SharePoint imposes?

The supported limit of unique permissions for items in a SharePoint library is 50,000. To prevent this limit from being reached, users should check in their documents once the editing is complete. To facilitate this behavior, Admins should consider using Entry Criteria to validate that documents are not checked out before reaching Steady State.

Configuration & Setup

What are the Office 365 license requirements to use the CA feature?

Customers must have an Office 365 tenant with SharePoint. End-users, including guest users, must have Microsoft 365 Business or Office 365 enterprise licenses that include Office client applications. We recommend using one of the following licenses:

- Microsoft 365 Business Standard/Premium
- Microsoft 365 Apps
- Office 365 E3 or Office 365 E5.

The Vault user email address must match the email used in Azure AD for correct assignment of permissions.

Do we need a federated Azure active directory to use this with SharePoint?

You need Azure Active Directory and Office 365 to make this feature work.

If I have multiple Vaults, how many Apps Registrations, Service Users, and Document Libraries do I need?

Customers should have separate Apps, Users, and Sites for Sandbox and Production. This is to ensure that sandbox accounts do not have access to Production data. Within an environment level (e.g. all Production) you can re-use a single App, Document Library, and service user. The benefit of using a single document library and Service Account user for each Vault is that it is easier to set up and maintain each additional Vault (without the need to request changes from the Azure IT team). The only caveat is if a specific Vault has unique security, operational, or compliance requirements. If the customer operates each Vault quite differently with unique security, operational or validation requirements we would recommend using separate document libraries. This would allow you to put in place different validation testing or operational procedures (e.g. SharePoint security tools) for each Vault. The integration settings are specified at the Vault level, so you can use separate Document Libraries for each Vault.

Can you use Collaborative Authoring across users in different Vaults, or do all authors have to have accounts within the Vault that the document is authored?

All authors need access to each Vault in which the source document resides.

To be able to use Collaborative Authoring with an external organization, i.e. CRO, do we have to provide Veeva Vault licenses to them?

External users must be registered in Azure AD as guests, have an active Microsoft 365 / Office 365 license and a Vault license. Alternatively, you can grant these external users access to your tenant by providing them contractor accounts with a corresponding Microsoft 365 license.

Can Collaborative Authoring be disabled once I have enabled it in a Vault?

Yes. In order to disable this feature, you must check in or cancel the checkouts of all documents. You can use the 'Check out Type' filter to find all the documents that are currently checked out using Collaborative Authoring. Once you have completed that, you will then have an option to remove the Collaborative Authoring settings with the Vault Admin UI.

You can see more information in Vault Help.

Is SharePoint required or can I use OneDrive for Business?

OneDrive is not supported. Collaborative Authoring integrates with the Office 365 platform, and we **require** using a SharePoint Shared Document Library for file storage, as they are intended for shared document collaboration. In our documentation, we provide instructions on configuring the security settings of the Shared Document Library in SharePoint to prevent access to checked out files via the SharePoint UI. Therefore, OneDrive for Business is not compatible with Collaborative Authoring

Why do you require a Service Account?

We use a Service Account so customers are able to restrict access to the Vault integration to the specific Document Library where Vault files are stored. Vault never stores the credentials for the Service Account and customers are able to apply controls, such as multi-factor authentication, to control the use of the Service Account.

Where is the appropriate place within your SharePoint environment to locate this team site?

Some customers choose to create a new site collection specifically for this, and others will create a new site under an existing collection. That decision will be driven based on your security requirements, as well as the ownership model that you have in place. What's critical here is that the Vault Collaboration User be the owner of that site. Because we're creating a team site, a team site has a default document and live-shared document library, and that's where we would put the checked out documents.

Are there any special considerations for pre-release environments?

Every time a Vault is refreshed the Collaborative Authoring integration is deauthorized. In order to re-authorize, you will need to re-enter the credentials established during the initial setup process. The App Registration, Team Site & Collaboration User do not need to be re-established.

Considering pre-release environments are refreshed on a frequent basis, we recommend that you store the credentials established during the setup process in a safe & accessible location. This will help minimize the level of effort needed to re-authorize the connection and the potential need to contact your Azure IT department.

Security & Compliance

Is this feature Validated?

The integration between Vault and Office 365 is Validated as part of the Vault Platform Validation. You can find the requirements and test protocols in the Files and Renditions section of the Vault Validation Documents, requirements FILE-12, in the Veeva Compliance Docs Vault. Veeva does not validate Microsoft Office 365 itself. Our position is that Microsoft Office 365 is part of the "source editing toolset" and does not require additional validation since review and approval still occur within Vault. Customers should consider their specific application of this feature to determine if additional Validation is required.

Does the Service Account need to have a non-expiring password?

The Service Account does not need to have a non-expiring password. In fact, we do not store that password at any time in Vault. The password is only entered by your SharePoint Admin at the time that they're authorizing the connection.

If we have configured an SSO integration with Azure AD to access Vault and Office 365 uses the same identity, should we anticipate any access issues?

There are no anticipated issues if you're using single sign-on for both Vault and Office 365.

Why does the Registered Application require the documented permissions?

The permissions required for the Vault Application are based on the least-permissions principle. All permissions are delegated permissions for the Vault Collaboration Service Account user.

With this delegated permission model, we do not have access to any files beyond those checked out of Vault. Also, since we use a Service Account, we cannot perform any actions on behalf of an actual user. All operations we perform are tied to our Service Account user.

Below are details for how each required permission is used:

- File.Read.Write.All - Allows the integration to create files, manage security, read, and delete files checked out of Vault.
- User.read, email, and profile - Used to show user names and set permissions based on their email addresses. These are read-only permissions.
- Offline access and open id - Used to get security tokens for our integration. If you don't have these permissions, the integration will not be able to connect to the Office 365 environment.

Note that the permissions below are optional for the Registered Application, as they are specifically used for granting Vault the ability to automate the process of adding external users with Vault accounts to your Azure AD:

- User.Invite.All
- User.ReadWrite.All
- Directory.ReadWrite.All

When you're editing a document, is there the possibility to introduce malware? Does Microsoft or Veeva scan incoming files?

There are many security add-ons to Office 365 that can detect malware. For Vault, we require that customers do the malware detection prior to upload.

How do you map the Vault user to the Azure user?

The user email in Vault is used to identify the Office 365 user.

Are the checked out files stored in OneDrive or in SharePoint?

The checked out files are stored in a SharePoint shared document library. We do not store the files in OneDrive (a personal document library) as OneDrive is not intended for group collaboration.

Need help navigating these questions and answers?

Reach out to the Veeva Team: rd_csm@veeva.com