SmartVault Sharing and Managing Access

Table of Contents

Introduction 2

SmartVault User Types and Invitations 2

- User Type Descriptions 2
- Inviting Users 2
- Sharing and Access to Your Account 3

Sharing Via Group Memberships 3

- Group Descriptions 3

Sharing Via User Access Grants on Folders 4

- Sharing & Manage Access Dialog 5
- Editing Access Dialog 5
- Editing Access Dialog & Access Descriptions 5

Sharing via QuickBooks Company Access 6

Quick Review 6

- Account Level 6
- Vault Level 7
- Folder Level 7
- QuickBooks Company Level 7

Introduction

This document provides an overview of how to Share and Manage Access in your SmartVault account. It introduces many SmartVault concepts, including user ids, folders, groups, and access control. Some of the topics below are applicable to specific account types/plans, so please read the descriptions carefully.

SmartVault User Types and Invitations

Every SmartVault user has a user id, which is an email address. To share your documents, a user is first invited to an account and then given access. Every user that is invited to an account consumes a user license, so before inviting a user to your account you should determine what type of user license they will have. Brief descriptions of user types are provided below to help determine which license type is most appropriate:

User Type Descriptions

Administrator – Available on all account types. Administrators have full access to the account, vaults, folders, and documents. This includes the ability to add and remove users, upgrade the account, close the account, and modify the billing information. For Accountant Edition accounts, these users do not count towards licenses.

Users – Available on all account types except an Accountant Edition (AE) account. Users can be granted specific access to any vault or folder within the account. They can upload and view files in the SmartVault web portal, create and delete folders, and grant other users and guests access to folders under their control. Users have access to the SmartVault web portal, desktop, and drive.

Guests – Available only on v3 accounts types (Lite, Individual, Team, and Professional). Guests can be granted access to view, upload and delete files in the SmartVault web portal but cannot create folders or invite other users or guests. Guests do not have access to the SmartVault desktop or drive.

Clients – Available only on v3 account types (Lite, Individual, Team, and Professional) and an Accountant Edition (AE) account. Clients can upload and view files in the SmartVault web portal, but they cannot create or delete folders. They have access to the SmartVault desktop, including the toolbar, inbox and ability to map a drive to SmartVault. For v3 accounts, inviting client user types requires upgrading the account and adding a Client Users.

Bookkeepers – Available only on an Accountant Edition (AE) account. Bookkeepers can be granted access to specific client vaults within your account and do not count towards the vault user count when given this access.

Accountants – Available only on a Business Edition (BE) account. Accountants can be granted access to your account and do not count towards your user count when given this access. They have full access to the account, including backups.

Inviting Users

Before a user can be granted access to anything in your account, they must be invited. Inviting a user adds the user id to your account and determines what type of user they will be. An invited user does not gain any access, unless invited as an administrator.

For first time SmartVault users, inviting sends an email to their user id, which they can accept or decline. Until they accept or decline, they are listed as “pending activation” in your user account. If the invitee declines the invitation, the pending user is removed from your account, including any access granted. For users that already have an activated SmartVault user id, an invitation simply adds them to your account and the invitee does not need to take any action.

User initiations are managed by signing into the SmartVault web portal and using the “Invite/Remove Users” task on the account. From the “Invite/Remove Users” dialog you can view invited users by their user type. A brief description of each user type is available on the respective tab by hovering your cursor over the green disk with the ‘?’ on it. You can also invite additional users and select what type of user you want them to be in your account. User invitations (and any access granted) can also be eliminated by removing the user.

Sharing and Access to Your Account

Once a user is invited to an account, you will want to start sharing your folders and documents with them. To share you give them access to the vaults, folders and documents as needed (unless the user was invited as an Administrator, which provides full access to everything).

SmartVault provides two methods of granting access: groups and user grants. Groups allow you to quickly grant vault-wide access by simply adding the user pre-defined groups with pre-established access. Whereas user grants allow very granular control of access on a per user/per folder basis. Direct access grants and group membership can coexist, but with the resulting access being the aggregate of combined access. These are described in more detail in the sections below.

Sharing Via Group Memberships

SmartVault provides groups on each vault making it easy for you to share on a per vault basis. When a user is added to the group, they become a group member. A group member automatically gains all the access assigned to that group for all the folders and documents in the vault. Access gained by group memberships cannot be restricted at a folder level, as any access granted to a user to specific folder can only increase a user’s access beyond that assigned to the group.

Sharing via group membership is supported by all SmartVault account types.

Group membership is managed by signing into the SmartVault web portal and using the “Managing Groups” task on a vault. From the “Manage Group Members” dialog you can manage group membership by adding and removing users. A brief description of each group is available on the respective tab by hovering your cursor over the green disk with the ‘?’ on it.

Group Descriptions

Before leveraging SmartVault groups to share, you’ll want to understand what access each group grants. Below are descriptions for each vault-level group:

Managers – Vault Managers have full access to the vault, folders and documents, including the ability to add/remove users from vault groups. This is a point of delegation where a user operates in an administrative capacity within the vault. It is designed for users that need to be able manage the vault and all its content. Guest and v3 client user types cannot be members of this group.

Full Access – Full Access users can see all documents and notes in the vault, as well as create and delete them. They cannot change user access in the vault. Users, guests, and clients can be members. This group is designed for users that need to be able to view, upload, create and delete documents in the vault.

Read Only – Read Only users can see all documents and notes in the vault, but they cannot create, modify, or delete them. Users, guests, and clients can be members. For users that need to see documents, but never modify them or upload additional documents. This group is designed for users that need to see documents, but never modify them or upload additional documents.

Inbox Full Access – Inbox Full Access can only access the Inbox folders specific to the QuickBooks Companies. They can see all documents and notes in the Inbox folders, as well as create and delete them. They cannot change user access in the vault. Users, guest, and clients can be members. This group is designed for users that only need access to scan and upload documents to the inbox for later processing.

Sharing Via User Access Grants on Folders

SmartVault supports granting access on folders, making it easy for you to share on per folder basis. With direct user access grants, access is only gained on folders where explicitly given. This allows you very granular control of what folders and documents a user can and cannot see, and what the user can and cannot do with them.

Each grant is specific to the folder where specified, and only the documents contained directly in that folder. Access granted on a folder does not automatically flow to subfolders, thus the user gains the access only to the immediate folder and files. When a subfolder is created, the subfolder gets a copy of the parent folder's access settings. Also, the access settings of a folder can be manually propagated down the entire sub-hierarchy to sub-folders and documents by replacing access.

Direct user access can supplement the access gained granted through group. However, access cannot be reduced by providing lower access at the folder level than given to the group. The resulting access of both group and direct access to a folder is the aggregate of them both.

Sharing via access grants on folders is only supported for v3 accounts types (Lite, Individual, Team, and Professional). Folder sharing does not apply to the "Applications" folder hierarchy for QuickBooks company files since that is managed by Sharing via QuickBooks Company Access (see next section).

Folder sharing is managed by signing into the SmartVault web portal and using the "Share & Manage Access" task on a folder. From the "Share & Manage Access" dialog you can manage user access to the folder adding, editing, and removing users.

Sharing & Manage Access Dialog

This dialog is used to view, add, edit, remove, and replace access setting on folders. It is separated into the tabs, which are used as described below:

Users tab – The Users tab list all users with access to this vault or folder. It allows you to grant access to users and modify existing access. Use the "Grant user access" link to add users to the list. When granted access defaults to 'Read' and the added user appears in the list. Once in the list of users, access can be edited or the user's access removed.

Groups tab – The Groups tab lists all of the groups in the vault and the access each group has on that vault, folder or QuickBooks Company. This access cannot be edited in the tab or changed elsewhere.

Advanced tab - The user access granted on this folder can be propagated to subfolders by replacing access. Just click the Replace button and confirm the operation. Be aware this will overwrite current access settings on all subfolders.

Editing Access Dialog

User access on the vault or folder can be changed by checking the appropriate boxes. Multiple boxes can be checked, and in most cases 'Read' access must be granted so the user can see the folder.

Editing Access Dialog & Access Descriptions

The "Edit Access" dialog is used to specify access setting for a user on a specific folder. User access on the vault or folder is changed by checking the appropriate boxes. Multiple boxes can be checked, and 'Read' access must be granted so the user can see the folder.

Before using direct access grants to share, you'll want to understand each type of access. Multiple access options can be selected. Below are descriptions for each access type as shown on the "Edit Access" dialog.

Full Access – For all user types, grants Read, Write, Create, and Delete for folder and documents as defined below. This is just an easy way to grant everything without checking them one by one.

Read – For all user types, grants access to see the folder and only read the documents contain within it. Cannot add, modify, or delete documents or folders.

Write – For all user types, grants access to edit documents and document properties (name, description) as well as folder properties, including the folder name. Cannot add or delete documents.

Create – For all user types, grants access to create documents, meaning they can upload to the folder. For users of type user, give the ability to create subfolders. They cannot edit or delete existing documents or folders.

Delete – For all user types, grants access to delete documents. For users of type user, they can also delete this folder. Note that guests and clients cannot delete folders regardless of access settings.

Sharing via QuickBooks Company Access

SmartVault supports granting access on QuickBooks company integrations, making it easy for you to share on per company basis. With direct user access grants, access is only gained on QuickBooks companies and folders where explicitly given. This allows you very granular control of what company folders and documents a user can and cannot see, and what the user can and cannot do with them.

Each grant is specific to the company file where specified, and only the documents and folders contained directly in that company folder. Access can be granted via three different options:

No Access - Grants "no access" to any documents or notes in the company folder. This is the default when a user is initial granted access to the company.

Full Access – Grants "full access" to all documents, backups, and Inbox for the company file.

Selective Access – Allows granting selective access on a per company folder basis. Access grants can include uploading, modifying or deleting documents for the selected company folders. Company Inbox access can be enable/disabled separately from other folders. Select this option only if you need advanced access for limited access users.

Company file user access can supplement the access gained granted through group. However, access cannot be reduced by providing lower access at the company level than given to the group. The resulting access of both group and company folder access settings is the aggregate of them both.

Sharing via group membership only supported for v3 accounts types (Lite, Individual, Team, and Professional).

Company folder sharing is managed by signing into the SmartVault web portal and using the "Share & Manage Access" task on a company folder. From the "Share & Manage Access" dialog you can manage user access to the folder adding, editing, and removing users.

Quick Review

Here's a review of what you can do at each level of the hierarchy in the SmartVault web portal.

Account Level

Invite Users and Remove Users based on user types. Remember, all users who need access to an account, vault, folder or company file must be invited to the account. The steps are:

1. Right click on the account name
2. Select *Invite/Remove users….*
3. Select the appropriate tab for the desired user type
4. Click on *Invite* _____*…*
5. Enter the desired email address for the user
6. Send the invitation

Vault Level

Manage Group Members – you can add or remove users from the vault groups to grant access to the vault. The steps are:

1. Right click on the vault name
2. Select *Manage Group Members…*.
3. Select the appropriate tab and click on *Add member…*
4. Place a check mark next to each user and click the *Add* button

Grant direct user vault folder access – you can directly grant or remove user access to the vault folder. The steps are:

1. Right click on the vault name
2. Select *Sharing & Manage Access…*
3. Click on *Add users…*
4. Place a check mark next to each user and click the *Add* button
5. Click the *Edit* link to change access from read only
6. Choose the desire access options
7. Click the *Save access* button

Folder Level

Grant direct user folder access – you can directly grant or remove user access to a folder. The steps are:

1. Right click on the folder name
2. Select *Sharing & Manage Access…*
3. Click on *Add users…*
4. Place a check mark next to each user and click the *Add* button
5. Click the *Edit* link to change access from default "read only" access setting
6. Choose the desire access options
7. Click the *Save access* button

QuickBooks Company Level

Grant direct QuickBooks company folder access – you can give a user access to a specific company only, rather than every company folder in the entire vault. The steps are:

1. Right click on the QuickBooks company folder name
2. Select *Sharing & Manage Access…*
3. Click on *Add users…*
4. Place a check mark next to each user and click the *Add* button
5. Click the *Edit* link to change access from default of "no access" setting
6. Choose one of the three options and if applicable check desired checkboxes
7. Click the *Save access* button