

MFG219615

Autodesk Vault – Configuration Part 1

Christopher Benner
Powell Fabrication & Manufacturing, LLC

Mark Lancaster
Synergis Engineering Design Solutions

Learning Objectives

- Learn how to create users and groups within Vault
- Learn how to establish the correct user and folder permissions to protect your data
- Learn how to set up projects and establish working folders
- Learn how to move locally stored CAD data to the Vault

Description

Now that you have purchased one of the Vault products, you need to get the environment set up for you and your users. This class will look at what to do once the Vault Server has been installed. We will discuss topics such as creating users and groups, setting up permissions and security, establishing projects and working folders, and getting your CAD content into the Vault itself.

Speaker(s)

Christopher Benner

CAD Department Supervisor at Powell Fabrication & Manufacturing, LLC in St. Louis, Michigan. I have been working as a mechanical designer and drafter for more than 20 years, using Autodesk products for most of that time. I was inducted into the first class of Autodesk Expert Elites for my activity on the Autodesk discussion forums and social media, and for my CAD Tips, Tricks & Workarounds blog. I've spoken at Autodesk University 5 years in a row, including a trip to Moscow in 2014 to speak at AU Russia. My specialties are Inventor Tube & Pipe and Frame Generator, Content Center and Vault Professional.

Mark Lancaster

As a Product Support Specialist for Synergis Engineering Design, a top tier Autodesk Partner reseller, I'm passionate about helping customers get ahead and stay ahead with their Autodesk solutions. I'm an Autodesk Certified Inventor Professional with expertise in frame generator, routed system, content center, and iLogic, and am proud to have Autodesk's Expert Elite status as a Helpdesk technician. I currently and continually support users around the globe through the Autodesk Installation/Licensing and Inventor forums. I'm no stranger to the CAD world. I bring 20+ years of experience and industry knowledge in the manufacturing world and 15+ years in 3D modeling to the table, which allows me to better understand the unique challenges our clients face. Plus, I'm a self-taught AutoCAD user since Release 9. Everyday I'm proud to live out my motto, "I'm here to assist you in getting your job done" and help you find better ways of accomplishing your own work.

Other Specialties: Autodesk Vault, Fusion 360, Autodesk Licensing/Subscription, Pro/E, Smarteam, and Lean Manufacturing

Getting Started

Congratulations! You've made the decision to dive into the world of Autodesk Vault. So, as you already know from having done your homework (but included here for those who haven't gotten that far yet), here is a breakdown of the Vault products for review.

Vault Basic

Vault Basic can be used to organize, manage and track your data and documents in a central location. Basic has Check in and Check out capabilities to protect data, and basic version controls. Users can easily share and reuse data and even work with "AnyCAD" data. Vault Basic can be integrated with Microsoft Office as well, to manage documents, spreadsheets and presentations.

Vault Workgroup

Vault Workgroup aims to help teams share design and engineering information more easily. Incorporating all of the functions of Vault basic, Workgroup also adds easy administration functions to control access and permissions across workgroups in an organization. Workgroup also adds lifecycle and revision controls directly in the application interface.

Vault Professional

Vault Professional continues to build on the functionality of the above products by adding multi-site tools such as replication to further connect design teams around the world. In addition to tracking lifecycles and revisions, Professional also offers tools for Engineering Change Orders and Bills of Materials. Integration with ERP systems makes it easier to share this data with the entire enterprise.

Vault Office

Vault Office is a separate product available for purchase, which provides basic vaulting capabilities for non-CAD users. Autodesk Vault Office delivers single document check-in and check out via the Vault web client and the add-in, allowing you to manage all of your office data, including Word documents, spreadsheets, and presentations.

Now that you are a subscriber to one of these fine products, you will want to know how to set up all of your options before you start adding files and using the system. This class will start with the assumption that you have done your homework well and have already installed the Vault Server and Client software, so we will not be dealing with installation and licensing. This class picks up at the next stage and will look at setup items such as adding users, giving them the proper permissions to do their jobs, and configuring the environment based on how you have chosen to use Vault.

Since Vault Professional has the most features available, we will be focusing our discussion here. So, getting right into it, let's look at how to add Users and Groups.

Users, Groups & Roles

Although there are no set guidelines or rules stating you must configure your Vault in a certain order, Mark and I believe that to properly start your configuration, you'll need to first understand roles within Vault. Roles can simply be interpreted as giving a user or a group of users the ability to do certain functions within Vault, like edit a document, rename files, delete folders or change Vault administrative settings. Yes, roles could also be considered a form of permission and they're actually called "Role Based Permissions". When working with Vault Basic, roles tend to be more important than using roles under Vault Workgroup or Professional. Later on we will be discussing additional permissions (⚠ *Vault Workgroup or Professional Only Feature*) options within vault. However, roles and permissions (⚠ *Vault Workgroup or Professional Only Feature*) do work together to control what the user can and cannot do with Vault. The important thing for you to consider is:

Not putting too much thought into your roles and/or permissions could end up providing access to information that certain users should not be permitted to access

Over thinking it, could also back users into a corner where they do not have the proper access to files requiring modifications

In the end you'll need to find that balancing point between roles and/or permission within your Vault infrastructure.



Roles

Roles are like the foundation of your entire Vault security and actually they are the lowest form of security you can apply to your Vault users or designated groups. Vault provides numerous pre-defined roles such as ADMINISTRATOR, DOCUMENT EDITOR 1 & 2, DOCUMENT CONSUMER, ITEM EDITOR 1 & 2 and many more that set the tone of your Vault security. But when permissions (⚠ *Vault Workgroup or Professional Only Feature*) are applied, permissions may end up blocking certain functions that the user is entitled to under their roles. For example a user could be assigned the "Admin" Vault role which entitles the user access to all of the Vault role functions, however an access control list (ACL) permission could be in place blocking them from viewing, deleting, and/or modifying certain documentation within your vault.

Each “Role” has a designated set of functions that controls what the user can and cannot do in Vault. For example, a “Document Editor Level 1” has the ability to do this:

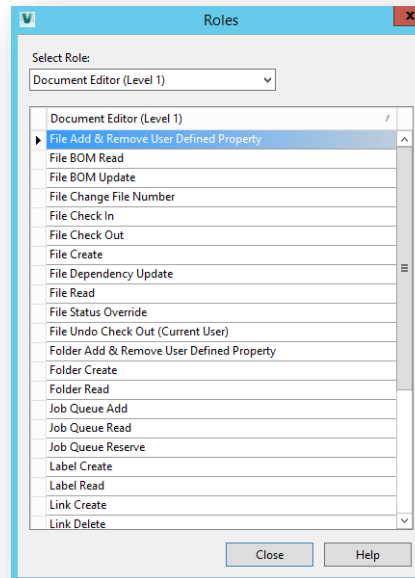
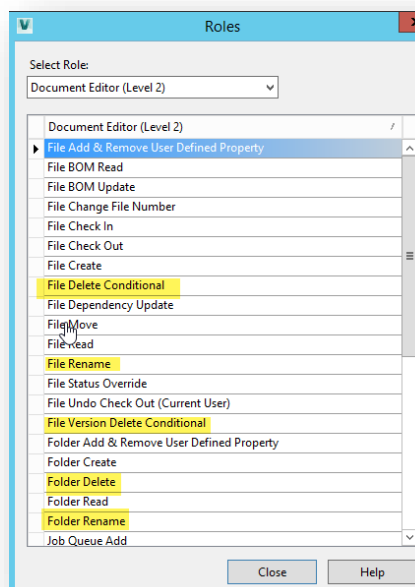


IMAGE DOES NOT FULLY REPRESENT ALL OF THE FUNCTIONS A DOCUMENT EDITOR LEVEL 1 IS ENTITLED TO.

Where as a “Document Editor Level 2” has the ability to perform level 1 functionalities plus additional functions as highlighted below:



DIFFERENCES BETWEEN LVL 1 AND 2 ARE NOT FULLY DOCUMENTED WITHIN THIS IMAGE

Roles often time have overlapping abilities as shown in the images above. When dealing with roles, the lowest role capability is always the winner. Let's say a given user was assigned the role of "Document Editor Level 1" as well as "Level 2". Level 2 gives the user the ability to delete files, rename folders, etc. However, since they're also assigned the "Level 1" role, those additional "Level 2" capabilities are no longer permitted because the lowest role assignment of "Document Editor Level 1" will always trump "Level 2" if they are assigned to the same user or group. Outside of permissions, many times when users are not permitted to do such functions, but have the capability assigned to them under a given role, most likely the cause is associated to the user having a lower role assigned to them somewhere else.

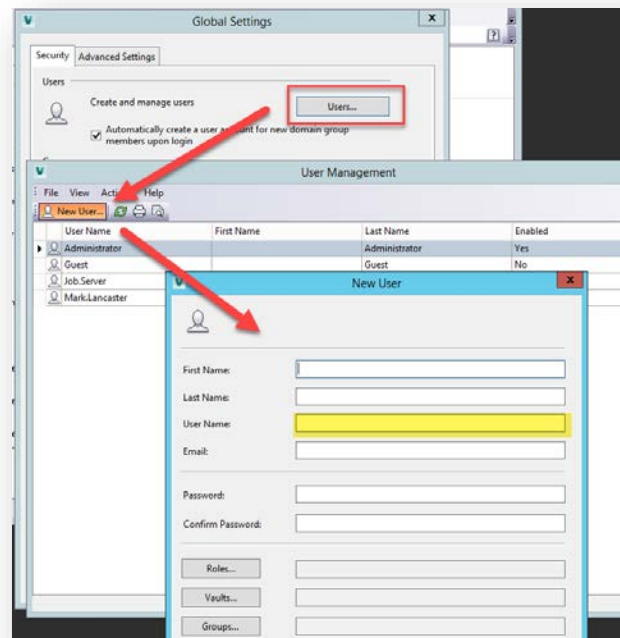
Additional information about Vault Roles

- Roles are based on a global vault settings. For example, a company may have different vault databases they are accessing through a given vault server or via a replicated environment. Meaning if a person is assigned a given role under this condition that role is still the same no matter what vault database or replicated server is being accessed.
⚠ There is an exception to this and we will discuss this later under the Vault Group section.
- Although there are numerous [roles](#) within Vault, not all roles are available due to the level of Vault you have.
- **⚠ Vault Professional Only Feature:** With the release of Vault 2018 (Professional level only), three (3) new Vault Administrator roles (security, project, and configuration) were added to provide certain administrated functions without the need to assign full vault admin rights to a given user or group.
- **⚠ Vault Professional Only Feature:** In Vault 2019, there's now an ability to [create custom roles](#) making it easier to define a specific role configuration for your users/groups.
- As a recommendation, take the time and create a spreadsheet to define what roles are assigned to your users. This approach could end up be beneficial and making it easier to create and manage your users going forward.

	A	B	C	D	E	F	G
1							
2		Administrator	Full privileges within to all folders all the time and administrative privileges on the	11	Change Order Editor Level 2	Configuration Administrator	Content Center Administrator
3	Vault User						
4	John Depp						
5	Tony Tiger						
6							
7							

Vault Users (Accounts)/User Management

Without having a user account for Vault or a properly defined one, there's no way for an individual to log in and/or access the vault or the data within it. For all flavors of Vault, a user account can be created based on what's called a static vault account. However, this type of account must be created by an individual who has been assigned the Vault Administrator role or by accessing the vault using the Administrator (static vault account) credentials.



USER MANAGEMENT INTERFACE PER THE ADMS CONSOLE.

By default, Vault is provided with two (2) static accounts. One is associated to the main Vault Administrator account and the other is a disabled “Guest” account.




The static vault administrator account is provided with a blank password. We highly recommend that you immediately define a password meeting your company’s policies and guidelines and not leaving this important vault account wide open (without a password).

In certain cases, due to your company’s security guidelines, you may have to disable the static Administrator account. Before doing this make sure you have already defined another account as the Vault Admin. Mark and I also recommend the following

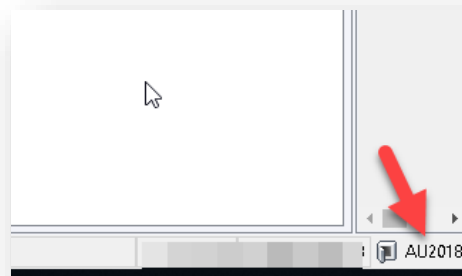
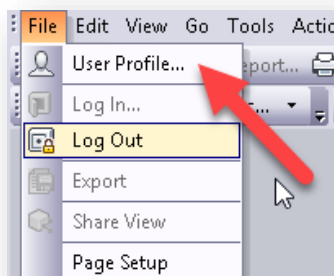
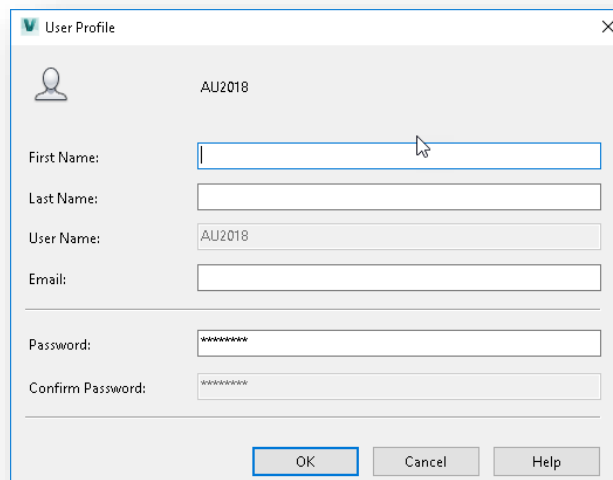
- Designate up to at least two (2) individuals that will have Vault Admin access and/or credentials to be a Vault Administrator.
- Create two (2) separate accounts if a given individual will be assigned the Vault Administrator capability and also act as a normal Vault user. Force them to switch accounts to make administrated changes, not allowing them to always have the ability to making changes on the fly.
- In certain companies and organizations, your IT support group or rules/policies may not permit normal users to be assigned Vault Administrator roles or have that capability. Under this condition your IT group needs to be fully trained on Vault Administrated functions.
- ⚠ When working with accounts associated to Vault Administration, it’s important that you pay attention and never lock the administrator out of your Vault. Under certain conditions you may end up having to reach out to your reseller and/or Autodesk (support case) to have the main Vault Administrator account restored.

- *Per Mark Lancaster this has happened to a couple of customers he supports and so it is possible to do this.*

 Before jumping in and creating any additional static vault accounts, make sure you have a plan in how this will be accomplished. We recommend that you define a standard and stick with it. Once a static vault account is created, it is unable to be removed. Modifying, disabling or promoting to a domain account is only permitted once the account is created.

When creating a user account, the only mandatory field is the user name. However, without defining at least a single role, enabling the user and indicating the database they will access, the user is still unable to access your vault infrastructure. A user account may end up being related to numerous roles, different vault databases and groups. Other special user accounts may be created to perform certain tasks or functions within Vault. For example, you may want to create a static vault (user) account to log in and run the job processor.

If a user is assigned a static vault account, they have the ability to manage their own account (for example change their account password) through the Vault client file pull down menu or through their vault name located in the lower right-hand corner of the Vault client.

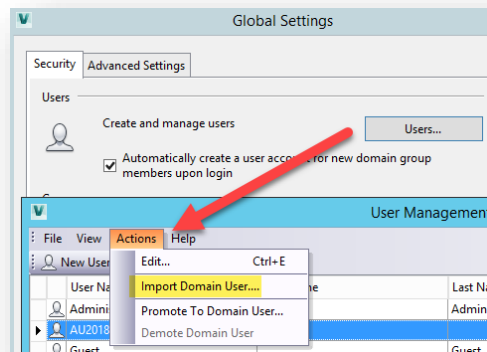



The 'User Profile' dialog box for the 'AU2018' vault account contains the following fields and controls:

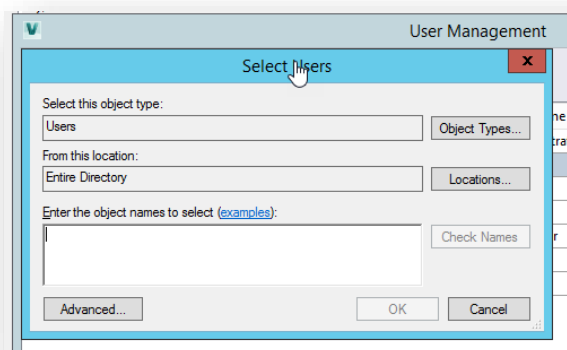
- First Name:** An empty text input field.
- Last Name:** An empty text input field.
- User Name:** A text input field containing the value 'AU2018'.
- Email:** An empty text input field.
- Password:** A text input field with masked characters (*****).
- Confirm Password:** A text input field with masked characters (*****).
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom.

Active Directory Domain Account: *Vault Professional Only Feature*

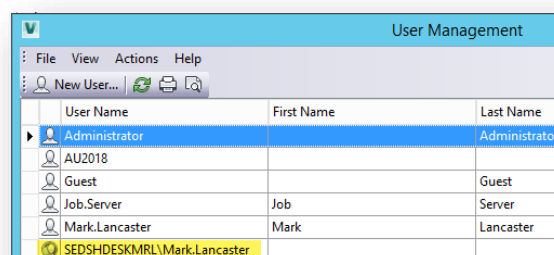
This type of account is based on your active directory account for your network infrastructure or in simple terms it imports your credentials/information that you use to log into Windows (or via Windows Authentication). In this case, the designated Vault administrator imports your domain account into Vault and the information (first, last, email address, and Windows user name/password) is populated into the user management interface. If an existing static vault account (user name) matches the domain user account, a prompt will appear asking if you want to link or not link the existing static vault account with this domain account.



Alternate method: Right mouse click on an existing user and select Import Domain User.

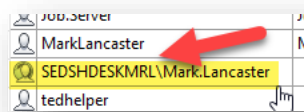


At this point you may want to involve your IT support group if you don't have a grasp on domain accounts.



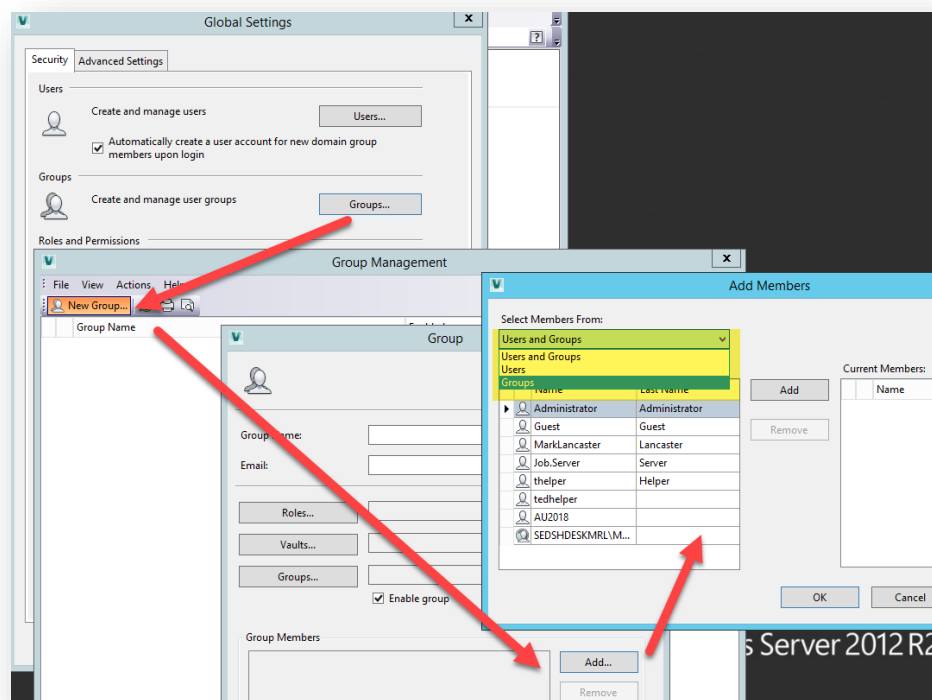
Once imported, the vault administrator will still have to define the vault database, roles and groups this domain account will require. Just like a vault static account, once it is created, it too is unable to be removed. Disabling or demoting it to a static vault account is only permitted at that time. Updating the account is performed through the domain account. For example, if the user changes his/her (Windows users) password through Windows, the next time they access vault, the domain account will update the password automatically within Vault.

Just like Vault roles, vault accounts are global vault settings and carry over no matter what vault database (on a given server) or replicated server is being accessed. Also notice the difference in the naming of the user's account and icon in the highlighted information of the image below. The icon represents this account as being associated to a domain account. While the server name prior to the actual user's name is the actual domain the user account is associated to.




Vault Groups/Group Management

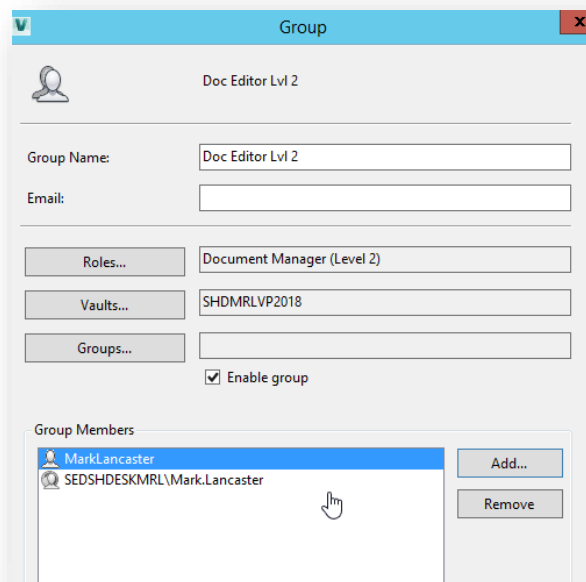
Groups in Vault are basically an extension of defining a user's access, thus making it easier to assign roles and database access to a group of users that require the same configuration. Although defining groups is optional, in most cases vault admins take advantage of this capability.




GROUP MANAGEMENT INTERFACE PER THE ADMS CONSOLE.

 Just like with vault accounts, before jumping in and creating any groups, make sure you have a plan for how this will be accomplished. Once a group is created, it too is unable to be removed. Modify, disabling or promoting to a domain group is only permitted.

With groups, you simply define the group name, its roles, vault (database) access and its members. The members themselves will be defined by existing user accounts and/or groups. Which means a group could contain members of a sub-group. Just like with vault accounts, a group could have many roles, different vault access and also be affiliated with other groups.



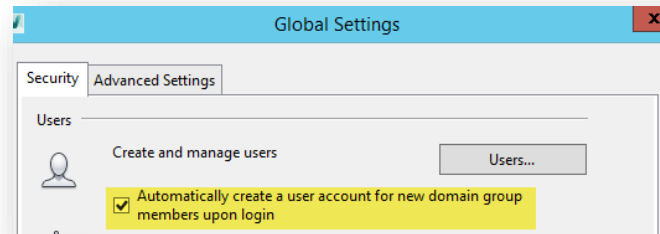
 When you start mixing user's accounts and groups within your configuration you'll need to take precautions in order to make sure you're not creating a circular reference or an overlapping configuration between user's accounts and group definitions. Remember the lowest role definition always wins. *If it becomes too complex for you to understand or figure out, you over thought the process.* 😊

Active Directory Domain Group: *Vault Professional Only Feature*

This type of group is based on an active directory group that your IT support team has already created to control permissions and/or security within your network. Additional information:

- Just like the active directory domain (user) account, the designated Vault admin must import the domain group into Vault. Under Groups, select Actions/Import Domain group or right mouse click on an existing group and select Import Domain Group.
- If an existing group matches the imported domain group name, a prompt will appear asking if you want to link or not link the existing group with this imported domain group.

- If the (active directory) member of the imported domain group does not already exist in Vault, their vault (domain user) account will automatically be created upon log in, if this option is checked

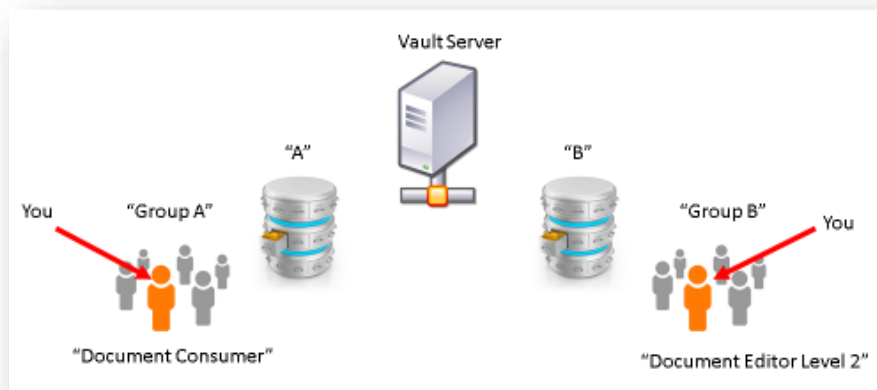


- ⚠️ Allowing this option could permit a user or a group of users to access Vault when they shouldn't have the ability to do so
- Once imported, the vault administrator will still have to define the vault database, roles and groups this domain group will require
- Members within this domain group can only be modified through the domain group that your IT configured. If members are added or removed, the domain group within vault **must be manually updated** by right mouse clicking on the domain group and select "Update Domain Group"
- Just like a normal vault group, once it is created, it too is unable to be removed. Disabling or demoting it to a normal group is only permitted.

As a reminder again, vault user's accounts are a global setting. When it comes to groups, they could be a global setting or not depending on how they are configured.

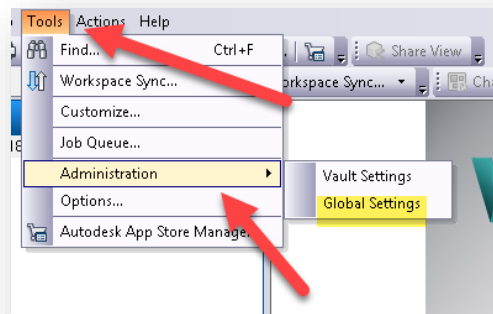
For example:

When a user (or users) is assigned to a specific group that only has access to a certain vault database (on a given Vault server) their role is per that database they're accessing. Since the Vault account is a global setting they could also participate in another group (with other roles) that only has access to another vault database (on a given Vault server).



In this case the Vault user (or group of users) would have a given role in one database but another role in the other vault database.

Individuals assigned the Vault Administration capabilities can create, modify, and promote/demote users/groups through the Vault ADMS console or via the Vault (thick) client (Tools/Administration/Global Settings).



Vault Folder Structure

Before we get into permissions, Chris and I want to take a little shortcut and briefly point out a couple of items regarding your Vault folder structure. However, since that structure can be configured in numerous ways and everybody wants it their way, it is impossible for us to cover this subject matter without impacting other Vault topics. In the end, the points we want to make are:

- Keep the vault folder structure simple or per the KISS approach.
- Do not bury and bury folders on top of sub-folders. Exceptions to this may include folders that are system generated such as those created when using Inventor's Frame Generator.
- Keep folder names simple and use abbreviations.
- Perhaps create folder structures for departments, template models, and year of the project.

Vault Permissions

Understanding and deploying permissions is a crucial step in securing your Vault infrastructure. Defining a role (or roles) for a given user is one of those mandatory actions for the user to at least access vault. As indicated earlier, roles play an important part under Vault Basic and not as much under Vault Workgroup or Professional. In the end roles are just basically allowing a given user access to use those functions across the board.

In most cases this is not what you want to occur when you get into Vault Workgroup or Professional. Just because a user can modify a document (based on role definitions), there may be certain documents within your vault (⚠ *Vault Workgroup or Professional Only Feature*)

that you don't want this user or users to modify, delete, or even view. This is where the actual vault permissions come into play.

Before we get into applying permissions in our Vault, let's go over the basics. There are three (3) types of permissions, Roles, ACL (Access Control List), and Lifecycle state permissions.

ACL Permissions ⚠️ *Vault Workgroup or Professional Only Feature*

As indicated earlier, roles are the lowest form of permissions. The next level would be ACL (Access Control List) followed by lifecycle state which would be the highest permission control. It may sound a little confusing at this point but let's try to take a real life example and talk about how these three (3) levels of permissions work in Vault Workgroup/Professional. For example, you and your friend are going to a popular night club here in Vegas and there is a line to get in. That's like you waiting for access to your vault.



Next, you're at the front of the line and paying the cover charge to get in.



Your cover charge is similar to the Vault role or roles that you were assigned. Meaning it gives you access to the night club (and you dance, socialize, and drink the night way because you're allowed to).



Your friend, however, connects with other friends at this nightclub and they find out there's a special party in the back. But to gain access to this party, you need a unique stamp on your hand. This stamp is like the ACL permissions (⚠️ *Vault Workgroup or Professional Only Feature*) within Vault. Meaning you're in vault (or our nightclub) but without this given stamp (ACL permission). You're unable to access this special party (like a file, folder, or etc. in Vault). After consulting your vault admin, (paying off the door man) you end up getting the stamp (corrected permission) and access to this great party.



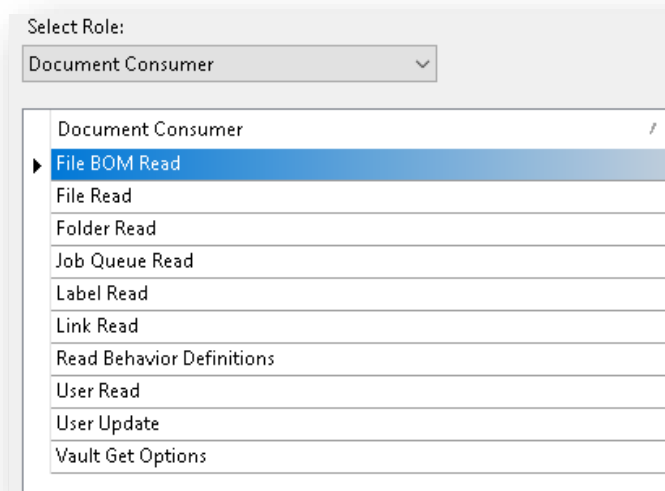
Now, this party is also offering certain drinks at no cost or like an open bar. You have decided you want a different type of drink, but you must pay full price for it. This is like a Lifecycle State permission (⚠️ *Vault Workgroup or Professional Only Feature*) in vault. Meaning the state of a document (or a drink) can be accessed by all, but another state of the same document (special drink) cannot be accessed by certain individuals (unless you pay for the drink, in our example).

Access Control List (ACL) Permissions: ⚠️ *Vault Workgroup or Professional Only Feature*

In simple terms, the ACL permissions grants users and/or groups the right to access (or not to access) certain files, folders, items and custom objects within your Vault. Overall this type of permissions is called “OBJECT BASED PERMISSIONS”. But there are two (2) types of ACL permissions, one is called “SYSTEM ACL” and the other as “OVERRIDE ACL”.

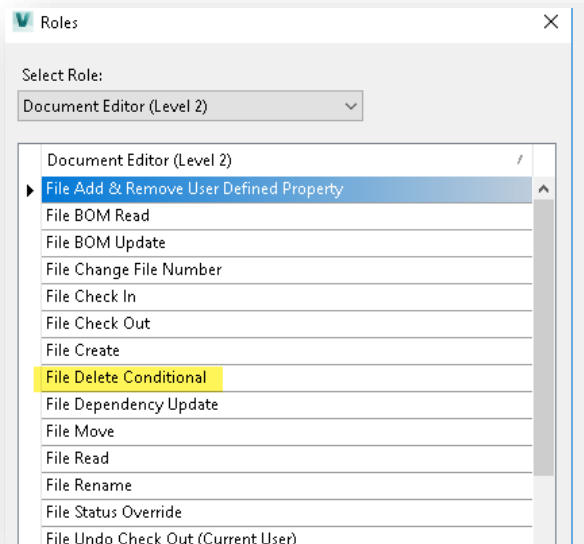
System based ACL permission is a normal (ACL) permissions that would be applied to files, folders, etc. However, an “override” ACL permission can also be applied to “override” the system based ACL permissions that may have been applied to files, folders, items, and custom objects within your Vault. We will discuss these two (2) types shortly.

As indicated earlier, ACL permission is the 2nd level of permissions that you can apply to control access within your vault. However, depending on your assigned role, ACL permissions may or may not trump the role based permissions that the user or group has been entitled to. For example, if a Vault user is assigned the role of a “Document Consumer”



Giving that same user the ability to modify a certain file through ACL permissions will not allow the user to have that ability to modify file(s) that their Vault role doesn’t permit. Lowest permission wins which in this case is the role based permission.

But if the user was actually given a role of “Document Editor Level 2” (ability to delete files within Vault)



and an ACL permission of deny for deletion was assigned to a given file, the ACL permission would win in this case. Or trump the “Document Editor Level 2” ability to delete this given file.



Is your head spinning yet regarding permissions?

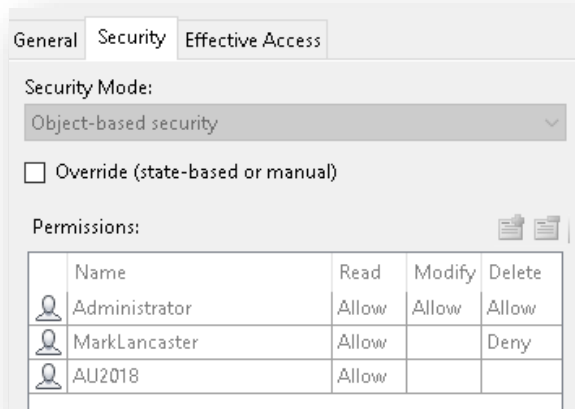
Remember what I said? You need to find the balance between your roles and permissions.

Let's move on...

The following section is only for Vault Workgroup or Professional infrastructures

ACL permission is broken into 3 sections, “READ”, “MODIFY”, and “DELETE”. Where-as roles are just like a light switch, an on/off ability to the given role functions within Vault. Under each

ACL section (read, modify, delete), a user (or group) could have an ACL permission of “ALLOW”, “DENY”, or “NONE” (blank).



ALLOW: You’re permitting the user (or group) to read, modify, or delete.

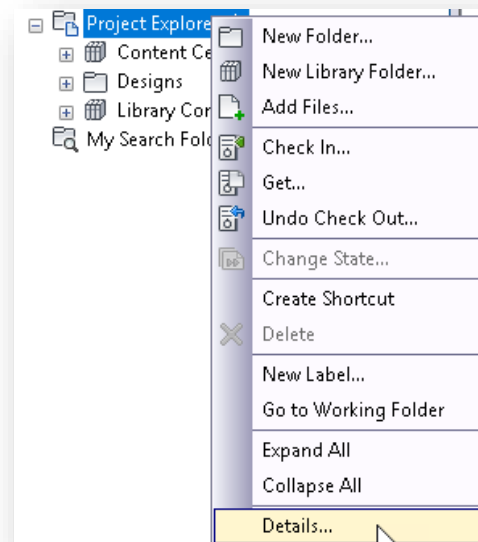
DENY: You’re not permitting the user (or group) to read, modify, or delete.

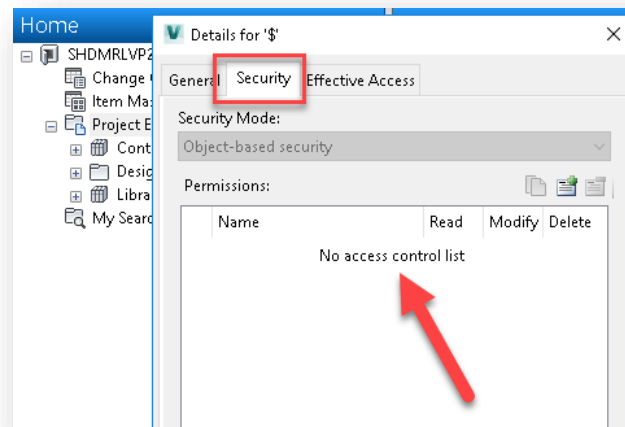
NONE (blank): Basically, you’re not indicating they have either allowed or denied rights at this point. Their other permissions (roles, override ACL, lifecycle state) would take control at this point.

Let’s walk through how we would assign ACL permissions to files/folders within your Vault.

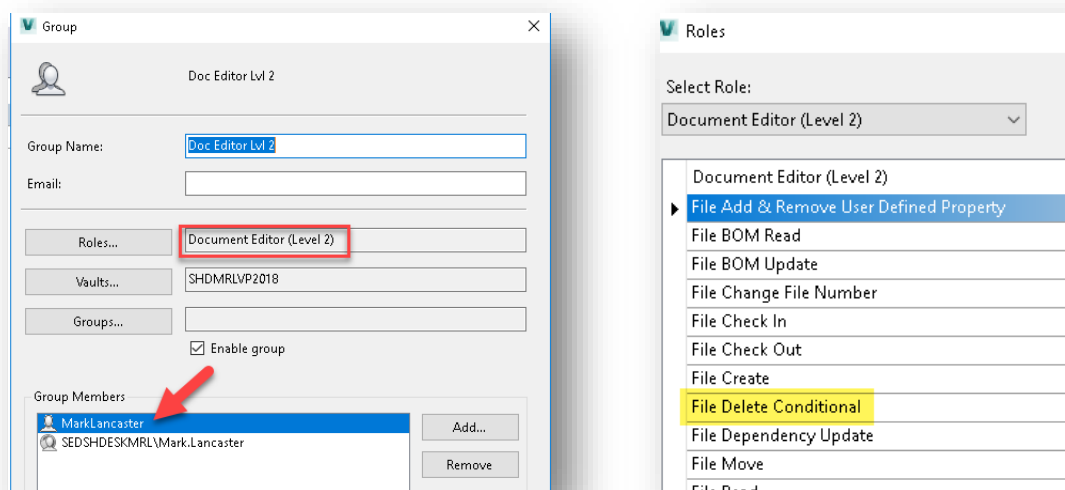
First, I’m accessing Vault Workgroup or Professional through the related Vault client. In addition, I’m logging into the client using the vault administrator credentials and right mouse clicking on the Vault Project Explorer and selecting “Details” to access the security aspect of this location.

As you can see at the root of my vault, there’s no ACL permissions defined (under the “Security” tab).



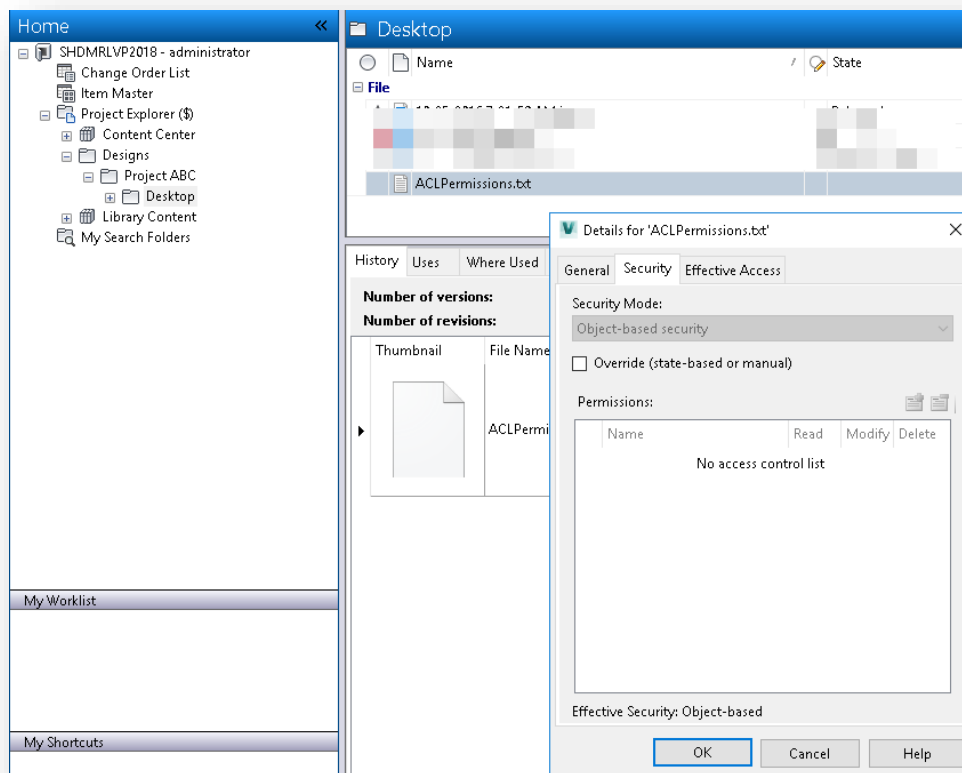


Now let's go a little deeper in the vault folder structure and define a restrictive ACL on a given file. Meaning we don't want a certain vault user (Mark.Lancaster for example) to have the ability to delete this file even though their vault roles allows them to do this. First the vault user Mark.Lancaster is part of a group assigned the "Document Editor Level 2" rights, giving him access to delete files or conditional delete access.

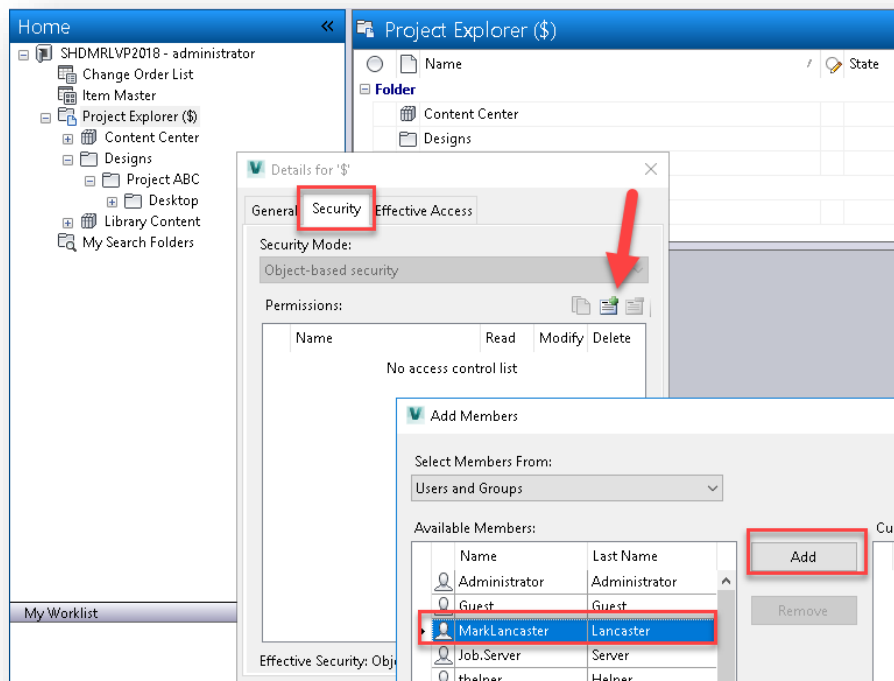


Yes, I just threw another vault term at you. Conditional delete means the file can be deleted if there's no relationship created within Vault for that given file. Once a relationship is built (i.e. vault versions, lifecycle process, linked to other models/drawings, etc.), the file can no longer be conditionally deleted.

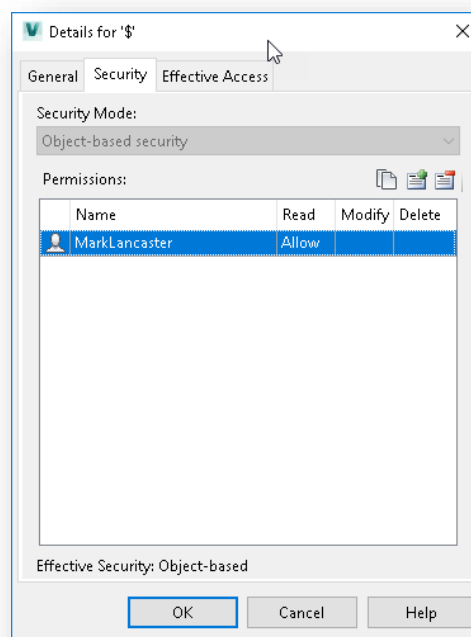
On this simple ASCII text file there's no vault relationship or ACL permissions in place, thus allowing user Mark.Lancaster to delete this file.



But, as indicated earlier we don't want this to occur. So, let's defined the ACL that prohibits this user from doing so. You can see in the image above, on the security tab, the only thing we're allowed to do at this point is to create an Override ACL permission. We could do that, but it's not a recommended workflow. In fact, we really need to start the ACL permission at the root of our vault and work down from there. Although this next section will be a quick/simple overview of (and example for) applying ACL permissions, make sure to properly define the permissions you require. Once again, I right mouse click on the Project Explorer or the root of your vault, select Details and the Security tab.

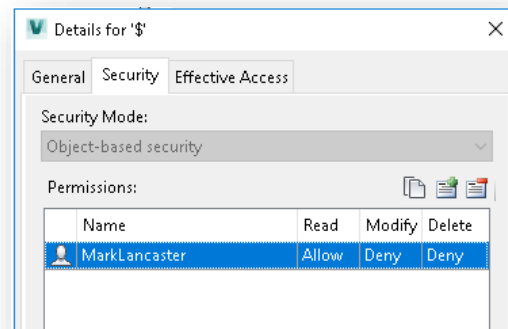
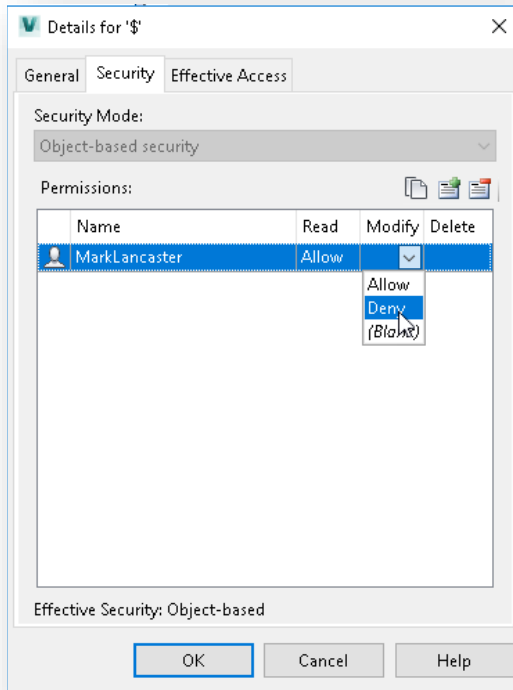


From there I select the add button (meaning “ADD” to the ACL permission), select the user (users or groups) followed by the “ADD” button. Now the user is added to the “current member” list and the okay button is selected to continue.

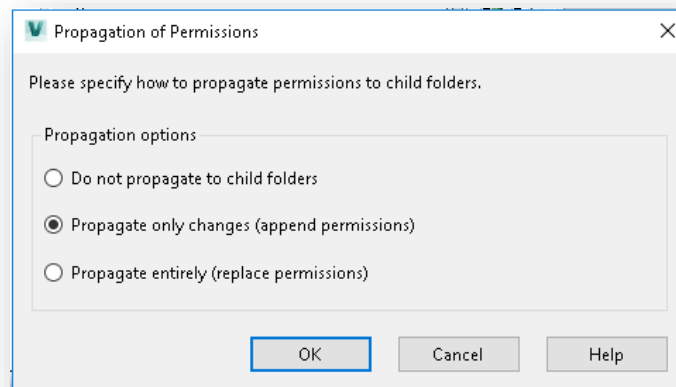


At this point, the role assigned to Mark.Lancaster is brought into the ACL permissions. But you may be asking yourself, the Document Editor Level 2 role does permit the user to modify and delete folders and files. Why is there no “ALLOWED” for those sections where-as the read section is defined as “ALLOWED”. When it comes to viewing or reading folder and files, if a user has the proper access to vault, they are always guaranteed to at least view folders/files. For modifying and/or deleting at this point you’re not saying 100% they are permitted to do so or saying 100% they are not entitled to do so. As indicated earlier, the blank section means other permissions defined at this point will take precedent. Meaning the “Document Editor Level 2” roles give Mark.Lancaster the right to modify and delete this folder. But is this something that you want to happen at the root of your Vault, a Vault user allowed to modify and/or delete things at the root of your vault. *As a former Vault Administrator, **I would never allow a common vault user to have this right.***

Let’s apply the correct ACL permissions to user Mark.Lancaster. Select in the “Modify” cell and select “Deny”. Repeat for deleting and select the OK button to create the ACL permissions.



Upon selecting the OK button, a message like this will appear since we’re applying ACL permissions to a vault folder.



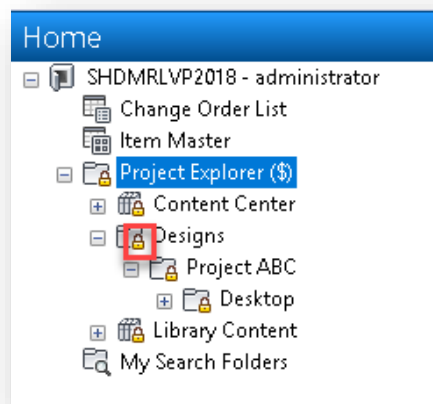
Before we move on and complete our transaction for ACL permissions on user Mark.Lancaster, let's discuss these options.

“Do not propagate to child folders”: Simply means do not pass this given ACL definition to any other folders below this one.

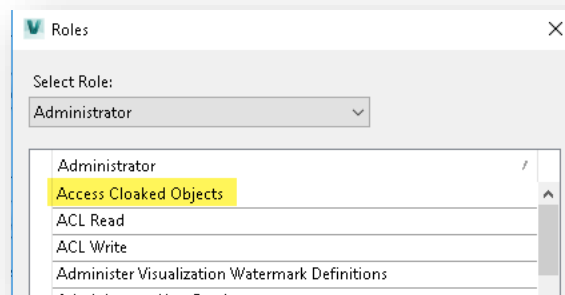
“Propagate only changes (append permissions)”: Means take the changes, propagate them at this level and any folder below. But do not over-write existing ACL permissions and just append the changes.

“Propagate entirely (replace permissions)”: Means take the changes, propagate them at this level and any folder below. Also over-write existing ACL permissions that may be in place. Because we're defining the initial ACL, I will leave the default propagate options as is. However, based on what you're doing, make sure to select the correct propagate option (and yes there's no undo functions for this).

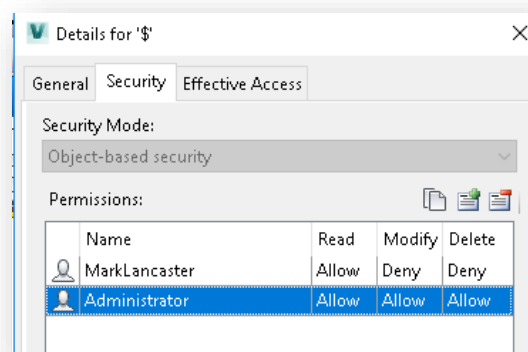
After Vault refreshes with the new ACL permissions, something doesn't look right in the navigation pane.



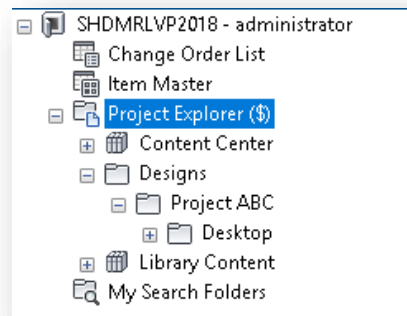
There are locks on the folders below the root of the vault. How is this even possible when I'm logged in as the vault administrator? I did this to make an important point regarding ACL permissions. When you start developing ACL permissions, you must always consider the Vault Administrator accounts and admin groups in the ACL to ensure Vault Administrators are not being blocked when they shouldn't be. Vault admins do have the "Star Trek" cloaking device capability (the ability to change ACL permissions even when blocked).



It is still important that you don't rely on this cloaking capability all the time. Now let's go back and fix that ACL permissions properly.

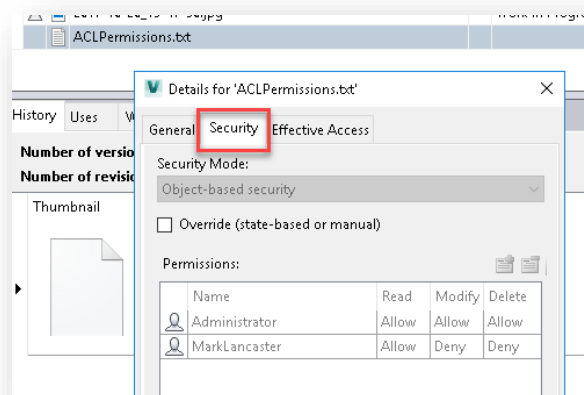


When I go to propagate at this point I want to select the option "Propagate entirely (replace permissions)" because I want to ensure the vault admin has the right permissions in the folder structure below. But again, I'm only selecting this option because I'm initially setting up ACL permissions within my vault. If there were other restricted Vault Admin permissions already in play (folder structure below), the other propagate options would be used instead. As you can see the refreshed vault now shows the admin to have the proper folder access.

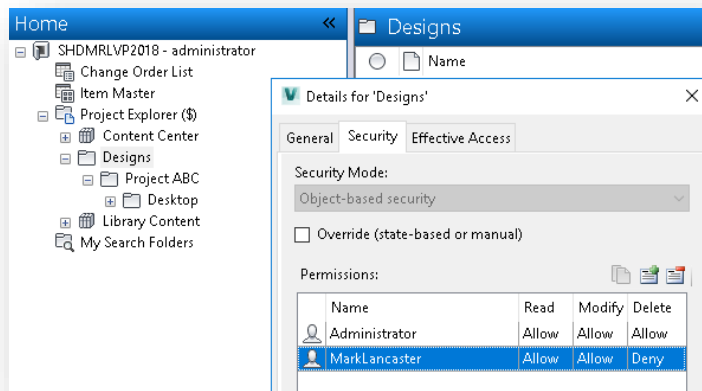


Yes, we have properly started the ACL folder permissions for our vault, but it's not completed because we have now locked out the other Vault users. In our example we are going to move on and define the ACL permissions for the original file we don't want user Mark.Lancaster to delete. However, it's important before going too far, that you develop a somewhat properly configured overall ACL (vault) folder permission within vault. In the beginning it's not going to be possible to catch everyone, but at least have a great starting point and develop as you go.

Now when we look at that file that we don't want user Mark.Lancaster to delete, our ACL permissions are setup properly (and denying the user from deleting).



But what's wrong at this point? Because the file took on the folder ACL permission we have now blocked this user from modifying the file when they need too. A few hundred words ago I spoke of two types of "ACL permissions". There's normal and override ACL permissions. Up to this point we have been doing normal ACL permissions. So should we be using override ACL permission on this file to change the modify aspect to "Allow". Again, this is a possibility. But at this point we would create additional administrative work that's not really needed. So, ask yourself, where does this individual need modify rights within the folder structure? In the end why give a user the "Document Editor Level 2" role for working with folders and files, but take it all away and then give it back on a given file. Too much administrative work in my opinion. Let's head back up our folder structure and give user Mark.Lancaster the proper ACL folder permissions.

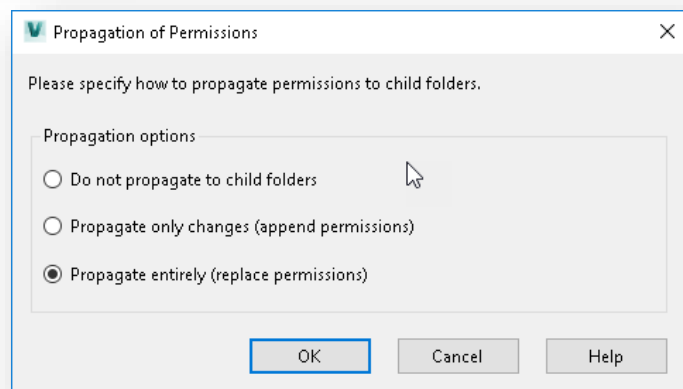


At the “Designs” folder level, one folder below the root of Vault, I’m changing user Mark.Lancaster to now have the ability to modify files and folders below it.

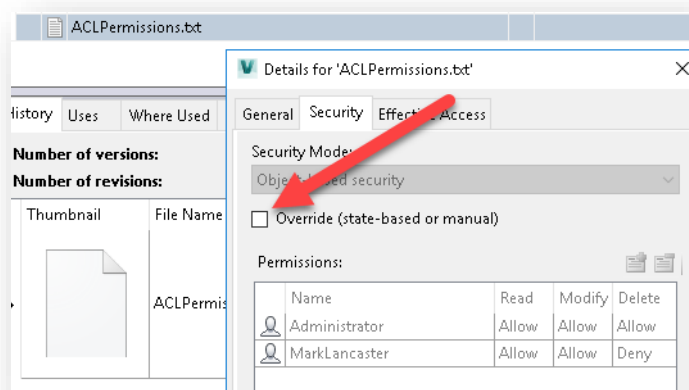
Perhaps I still want to restrict user Mark.Lancaster from deleting files and folders below that location or perhaps I want to “ALLOW” it to occur or not imply (set to none/blank) it at all. The choice is yours.

Once the ACL folder permission is created, the propagate message appears and defaults to “Propagate entirely (replace permissions).”

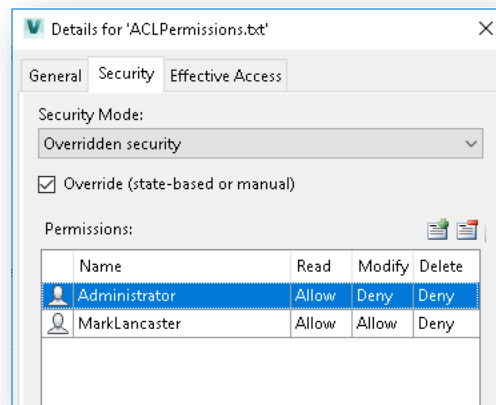
Yes, we want to replace the permissions below it. Appending them could result in a lower permission trumping the permission you want. Select the option you’ll need based on the folder and file structure permission you’ll require.



Okay let’s change our goal. Right now, we’re allowing the Vault Administrator the ability to read, modify and delete files. Perhaps in this scenario, we want to make sure the vault admin doesn’t have the ability to modify and delete this important document. This is where “OVERRIDE ACL” permissions come into play. Right mouse click on the given file, select “Details” and the security tab.



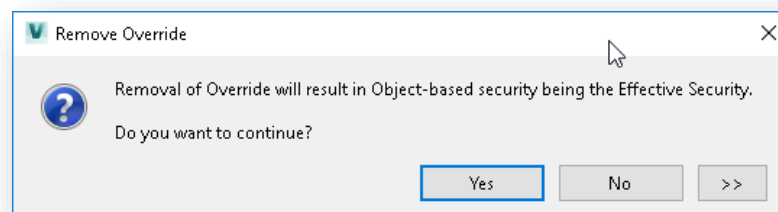
As stated earlier our options are limited at this point because the file is taking on the folder ACL permissions. We must do an ACL permission override by selecting the override option. From here we change the defined user(s) or group(s) access, add more users/groups, or remove existing members from the ACL. The override is a powerful option to ACL permission, but only use this option when needed. In our example I'm overriding the ACL file permission on the administrator account.



Once the ACL permission is applied, no propagate message appears because the override is being applied to a given file. But next to the vaulted file a lock now appears, representing the vault admin is now locked from modifying and deleting it.



The entire folder structure where this file is located, would not be impacted by the override file permission settings. Down the road if you elect to remove the override ACL permission, unchecking the option will cause a message like this to appear (confirming if you want to remove or not).

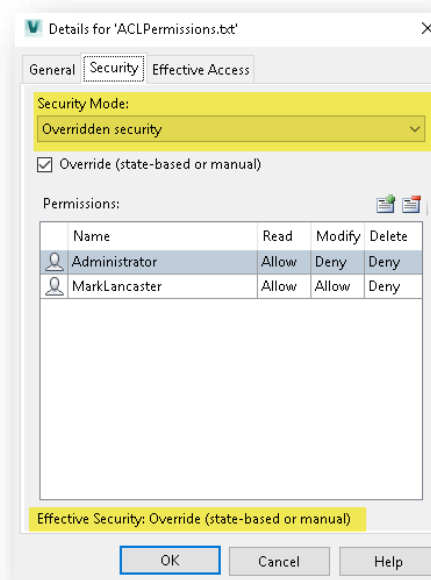


Removal of the override will reset the permissions back to the normal ACL permissions or the current object base security (for the given Vault location). As you can see there are two (2) ways of applying ACL permissions to folder and files. But choose wisely in developing your required permissions.

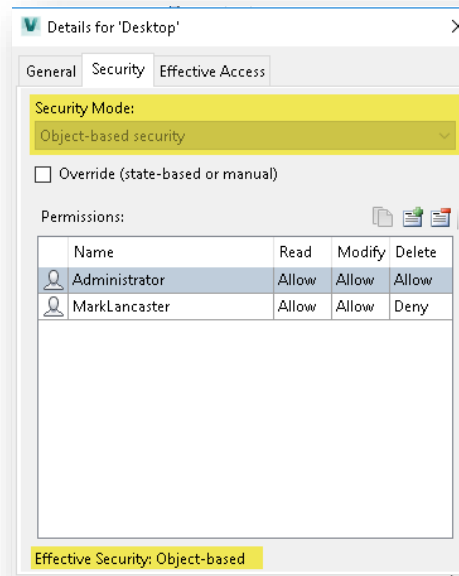


Prior to Vault Workgroup or Professional 2016, in order to check one's permission regarding folders and/or files, you either had to log in as that user or create a dummy static vault account with the same permissions. With 2016 and re-interfaced in 2017, you can now check any user ACL permissions a couple of ways.

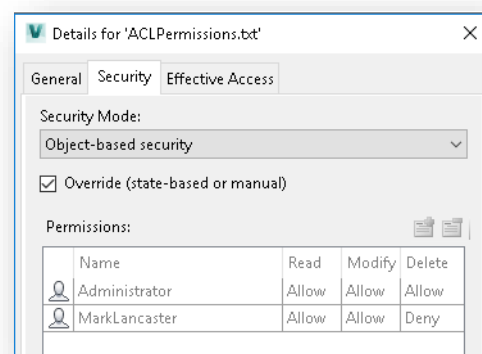
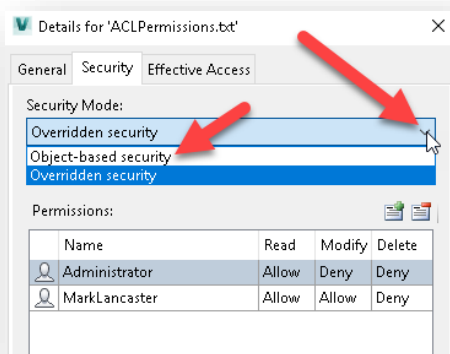
In our above example where we restricted the vault admin from modifying and deleting the given file, we may want to know what the actual ACL permission was instead. To do this, we can simply change the "Effective Security" aspect of the file. Right now, our file "Effective Security" is set to override.



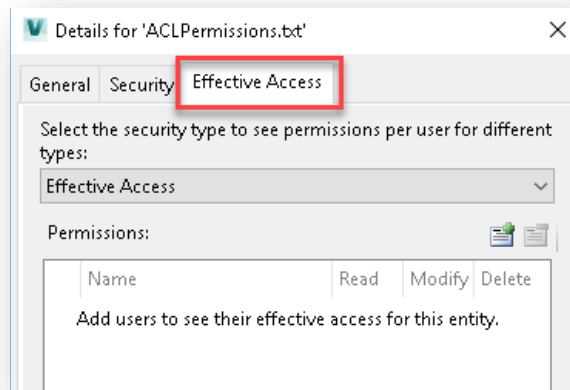
If we look at the “Effective Security” of the folder where this file resides, we see something different.



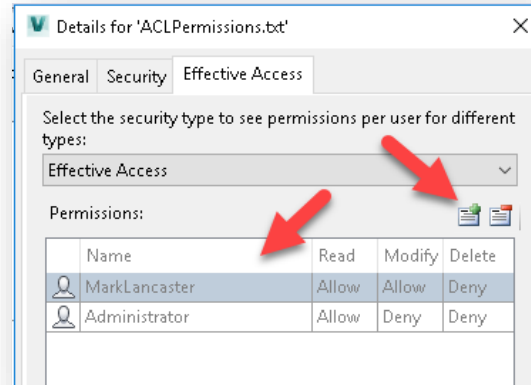
At the folder level, it's normal ACL permissions (or object-based security), while at the file level it's override ACL. But we really don't need to back up at look at the folder level to check this. In the override permission at the file level, we can toggle to see what the normal ACL permissions was coming in as.



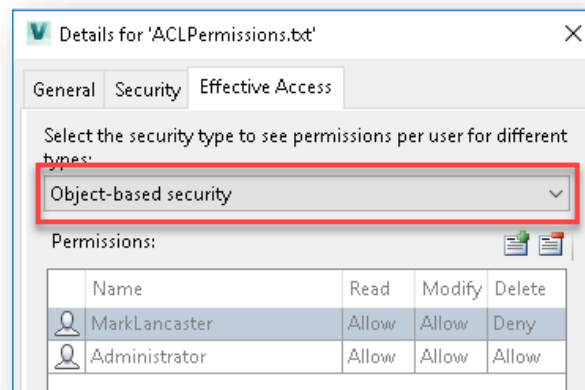
Although this is one way of knowing what permissions were set prior to this, most times we really want to check individual users' permissions at a given folder level or file using the “Effective Access” tab.



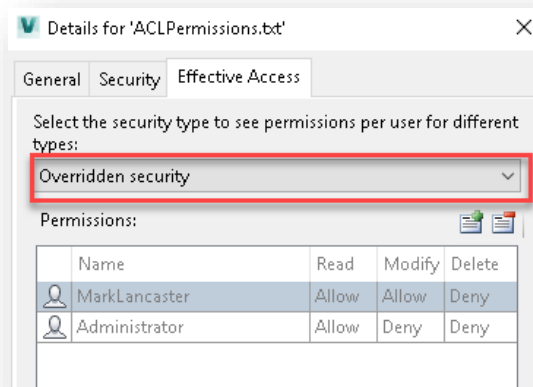
Effective access indicates what the controlling permissions are in play for the selected members. This effective access could be based on lifecycle state permissions, override ACL permissions or normal ACL permission (object based security). Role based permissions are not part of this scope. In addition, we can still take a peek at the object based or override security for those who are listed. Although we just set up the permissions for our vault admin and user Mark.Lancaster, let's still take a peek using the "Effective Access" tab after we add the members.



In our case we haven't applied any lifecycle state permission, so our effective access is solely based on the override ACL permission that we applied to this given file.

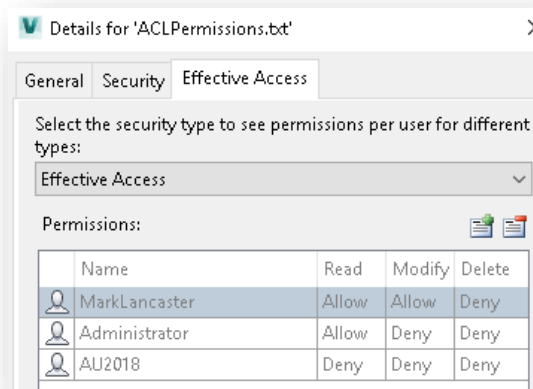


When we switch over to object based security (or normal ACL permissions), you can now see the Administrator account now states “ALLOW” across the board because we’re now viewing ACL permission leading up to the file.



Now when switched to overridden, you can see the administrator access is the same as “Effective Access”, because they are the same.

In this next example, let’s check a user who’s not even part of the ACL listing. Let’s add user AU2018 to it.



Yes, we would know at this given point, user AU2018 would be denied across the board. Remember we just set up our ACL permissions and user AU2018 didn't participate in that ACL listing. But think a month or more down the road. Are you going to remember everybody's permissions? Perhaps user AU2018 belongs to a group and that group participates in the ACL permissions (normal or override). The "Effective Access" is a good way of checking individual permissions. One final thought on checking permissions through the "Effective Access" tab. When a user or users are added (or even removed), the list is only present for that given session check. If you leave the tab and come back, the list of members is blank, and you would have to create it again.

Lifecycle State Permission

Let's review again.

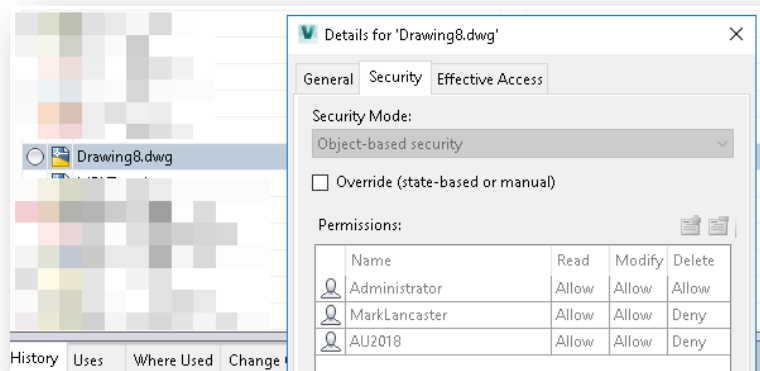
Role permission: On/Off switch giving users the ability to perform certain functions within Vault.

ACL permission: The ability (or not the ability) to read, view or delete folders, files, items and etc within Vault.

Lifecycle State permission: Works in the same manner as ACL permission but its security is solely based on the (lifecycle) state of the file.

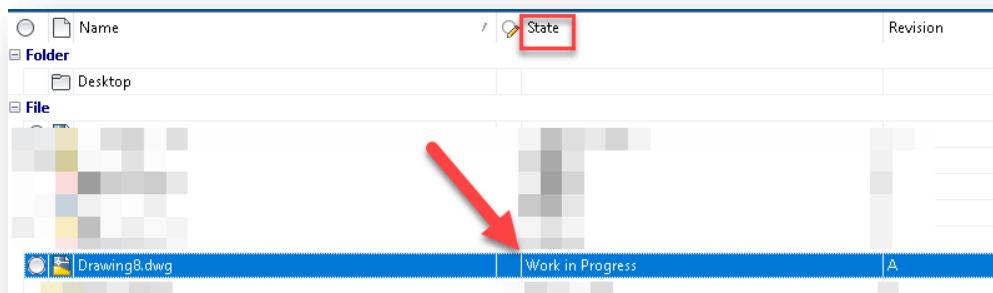
Let's look at another example...

Again, we are jumping ahead and the assumption at this point is that everything required for Lifecycle State management is in place. Later, we will cover what "Lifecycle States" are. We have this drawing (Drawing8.dwg) in our Vault that has the following ACL permissions

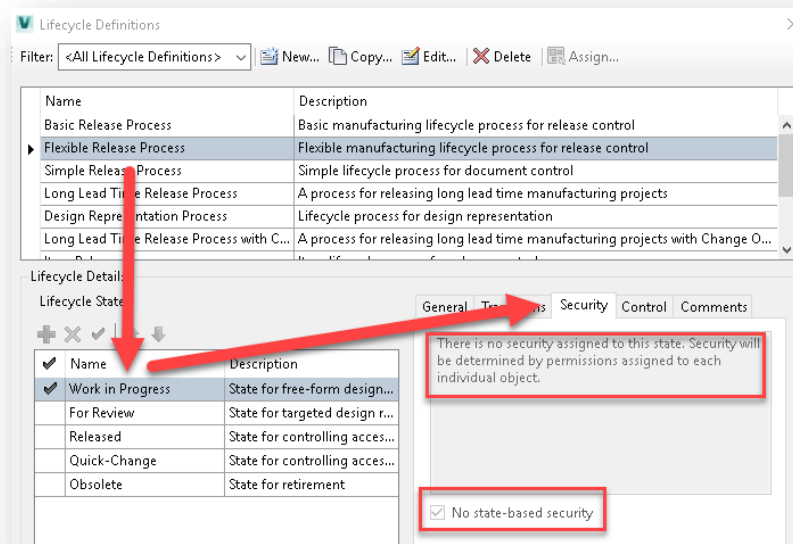


Vault users Mark.Lancaster and AU2018 also have a role of “Document Editor Level 2”. Whereas the Administrator has Vault Administrator role.

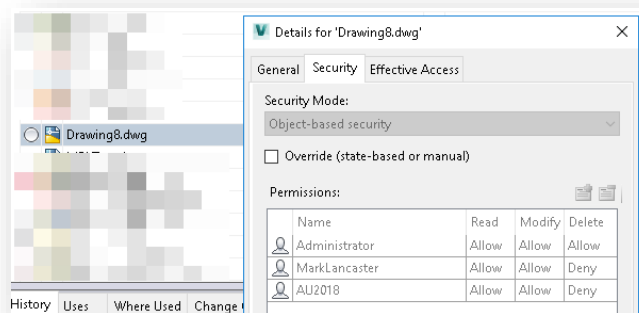
In addition, the drawing has a (Lifecycle) state of Work-In-Progress.



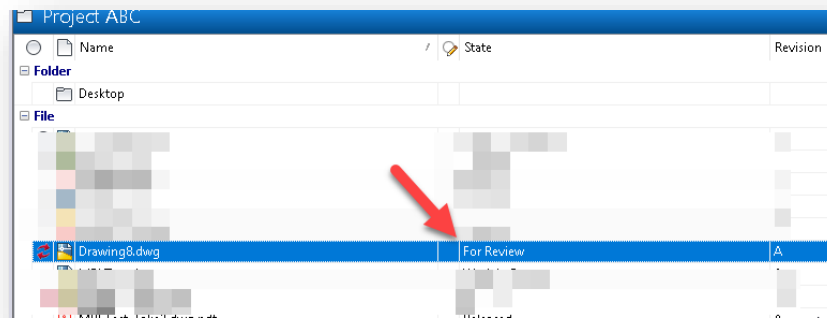
For this given lifecycle mechanism, our “Flexible Release Process” indicates for the state of “Work in Progress” there’s no “state” defined permissions.



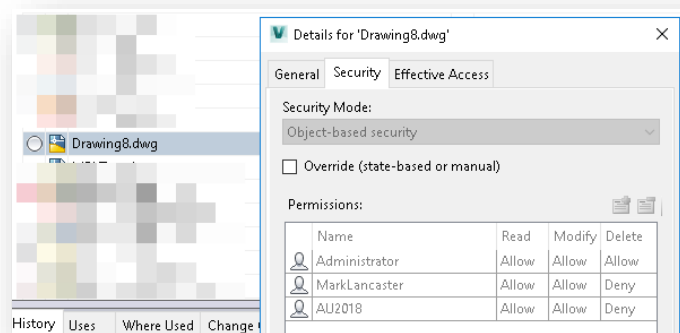
As a reminder the user's ACL permission is still taking control at this point since our lifecycle settings indicates the state of "Work in Progress" has "No state-based security".



Although we're not going to cover the workflow in how to change states of our drawing within vault, let us still change the state from "Work in Progress" to "For Review" in order to demonstrate this. In addition, the following image is based on the Vault Administrator currently being logged into Vault Professional.

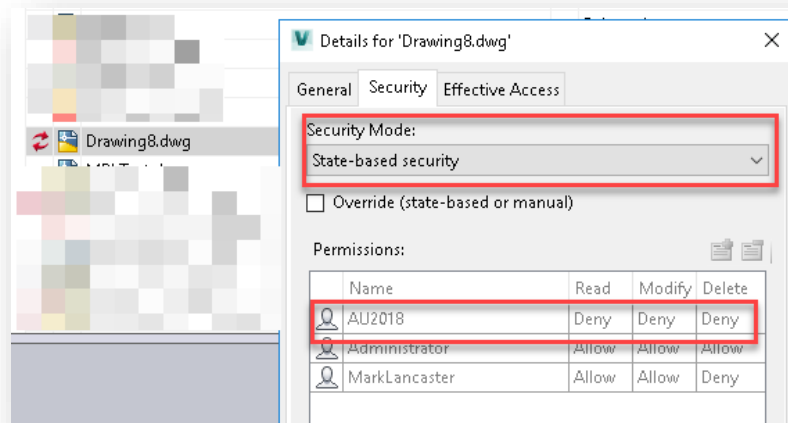


Now when vault user “AU2018” logs in, they are unable to see this file. Remember they did have an ACL permission of “ALLOW” for read.

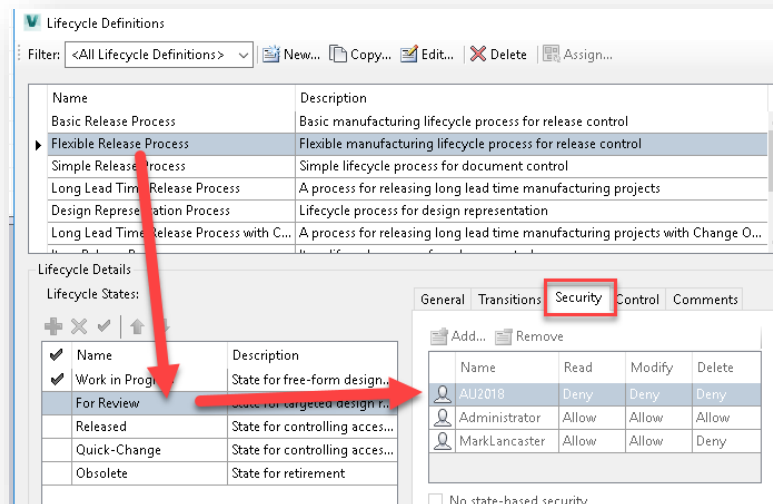


Why are they unable to see this drawing now?

Let’s take a step back and look our security again. In the image above, permissions are solely based on object-based security (or ACL permissions). When the image was taken, we were looking at security of the given drawing at the state of “work in progress”. Remember at that state, there was no state based security being applied, so ACL permission or object based security was still controlling it. Now let’s look again at the drawing security to see if anything has changed when the state was changed from “Work in Progress” to “For Review”.



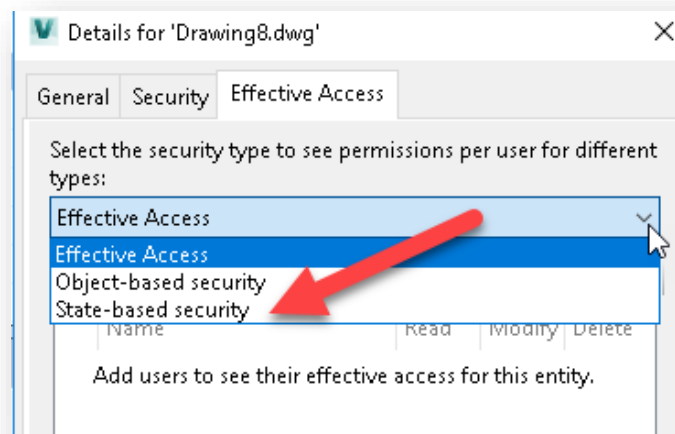
What does the “Security Mode” pull-down now state for our drawing? It’s now based on “Lifecycle State” permissions and those permissions end up denying vault user “AU2018” the ability to read, modify and delete this drawing under the state “For Review. In the end, you may be asking yourself where this permission came from. Let’s take a peak back at our lifecycle settings within Vault.



Let’s recap our example

- User “AU2018” was assigned the “Document Editor Level 2” role giving permissions to read, modify and conditional delete files within Vault. **1st level permissions – ROLES taking control**
- For “Drawing8.dwg”, user “AU2018” permissions were changed to ACL or object based permissions thus denying the user from deleting this given file. **2nd level permissions – ACL or object based security taking control.**

- Initially the drawing had a state of “Work In Progress” and the ACL permissions for this user still controlled it. **2nd level permissions – ACL or object based security taking control.**
- The state of “Drawing8.dwg” was changed from “Work in Progress” to “For Review”
- Due to our lifecycle state mechanizing, user “AU2018” was denied read, modify, and delete rights since “Lifecycle State” permissions now took over. **3rd level permissions – Lifecycle State permission taking control.**
- Now that “state” security is in control at this given state, when we look at “effective security” on this drawing we can now see “state” security is an option for reviewing user’s permissions.

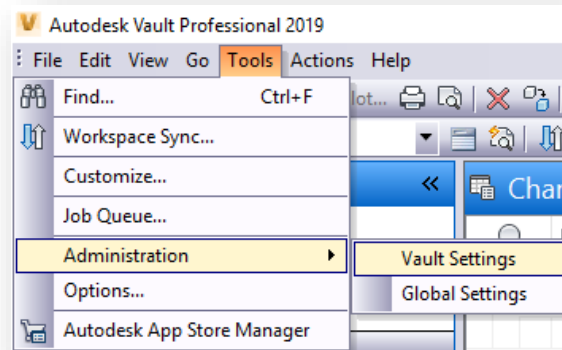


As you can see, the different levels of permission play an important role in defining access for your Vault users. Another question we often hear... We want certain vault users of our Engineering or perhaps another department to only view documentation that has been released. When those same documents are being modified or under review, we want to block these users from viewing those types of files or having the ability to view changes that are being made. This is where “Lifecycle State” permissions plays an important role in accomplishing that requirement. When we transition from “Released” to “Work in Progress” or transition between other lifecycle states, we want to apply the “state” security to control the access since ROLES and ACL permissions do not permit that type of control.

Do you now have a grip on permissions? Let’s move on to other settings within Vault.

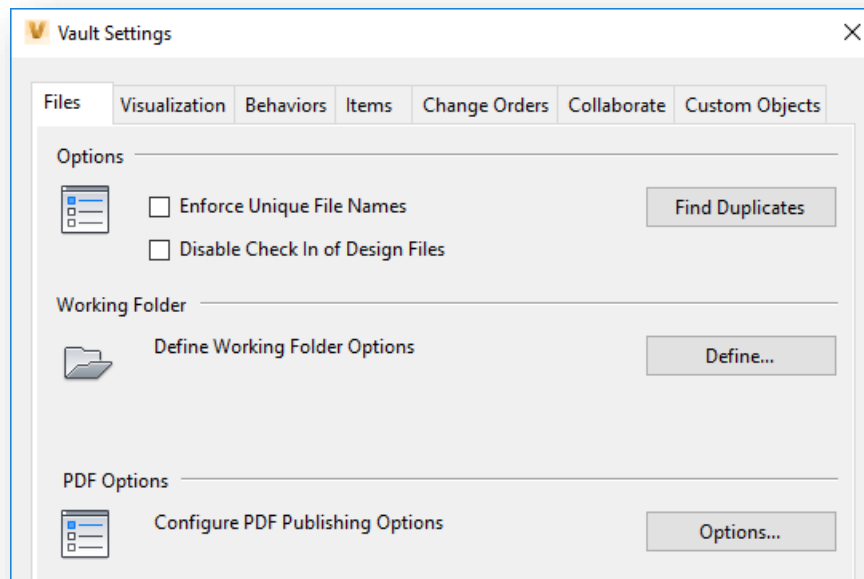
Basic Vault Settings

A user with Administrative permissions can add or modify basic Vault settings, such as setting or creating Categories, Revisions Schemes and controlling Lifecycle Transitions. These settings and more can be found in a location that you, as Admin, are sure to memorize quickly. From the main Vault Toolbar, select Tools\Administration\Vault Settings



Let's take a look at what we can do with this set of tools. Unless otherwise noted, these screenshots are all taken from within Vault Professional 2019.

Files Tab



Options

Enforce Unique File Names

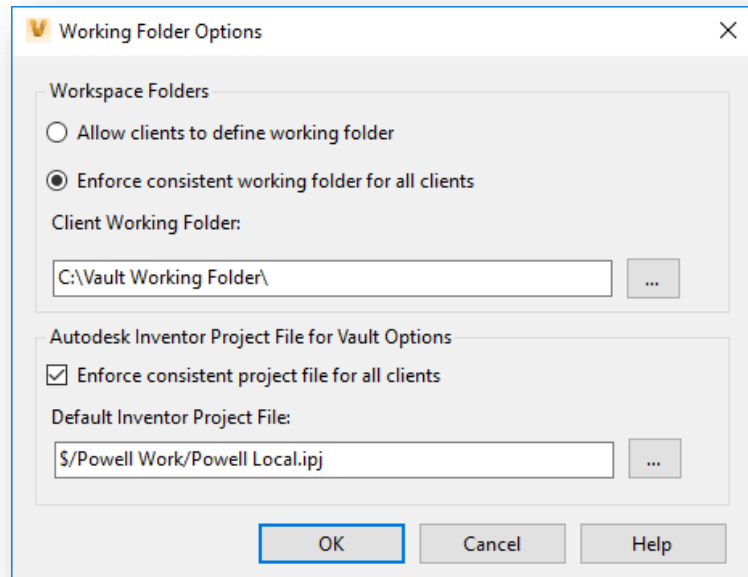
This tool, when checked, will not allow files to be checked into the Vault if the file name is the same as a file already existing in the database. Use the Find Duplicates button to find and deal with any existing duplicates, before checking the box to enforce this rule.

Disable Check In of Design Files

Use this to ensure that files can only be added to the Vault by using the Add In Clients found in applications that you are using. Examples include AutoCAD, Inventor and Revit, among others. With this checked, files may not be dragged and dropped into the Vault or added from the Vault Client. This will ensure that file relationships are not lost during the check in process.

Working Folder Options

This lets you decide whether to enforce a default working folder location for all users, as well as specifying a default Inventor Project. In the example shown, we have set the client working folder to C:\Vault Working Folder. This essentially maps this local working folder to the root folder in Vault, seen as **Project Explorer(\$)**.



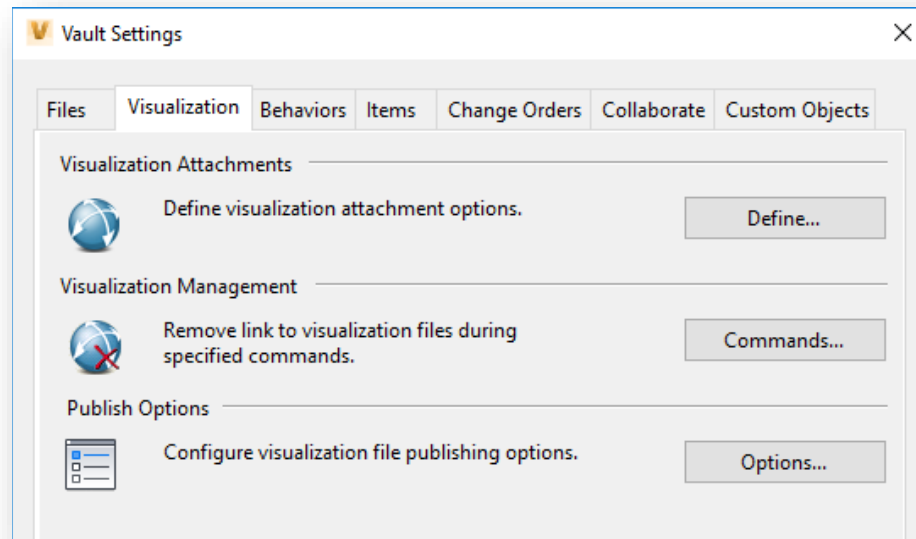
Properties **Vault Basic Only Feature**

In Vault Basic this is where you would manage User Defined Properties. A File Properties button (not shown) opens the Property Definitions dialog.

Configure PDF Publishing Options

Found on the Files tab in Vault Professional 2019, this will be discussed in the section below on Visualizations.

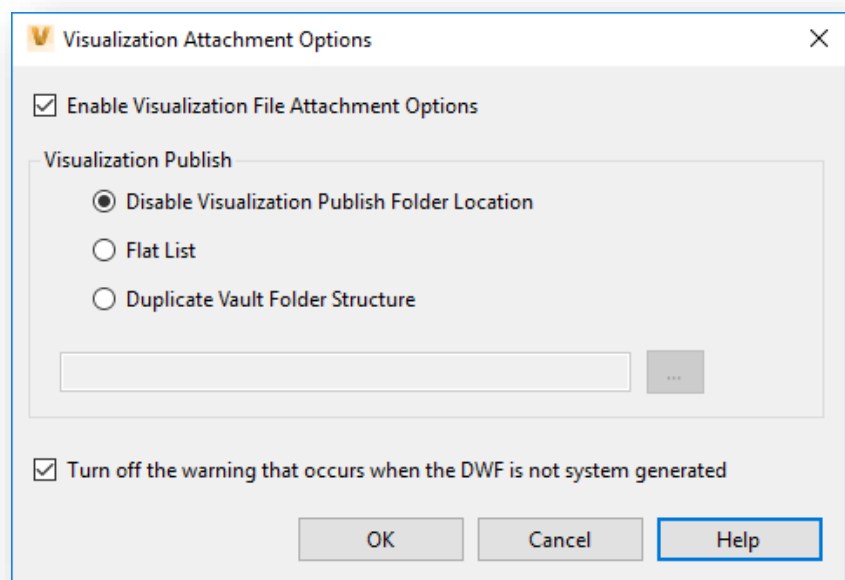
Visualization Tab



Visualization Attachment Options

Select the Define Button to the right of Define Visualization Attachment Options.

Enable Visualization File Attachment Options is checked by default. This creates visualizations for files that have changed, or do not already have a visualization. This can be disabled if you need to keep the size of the Vault down, and visualizations can be created on demand for just those files that you want.



Visualization Publish

This section deals with keeping local copies of visualization files, such as in a shared network location or on individual workstations. To prevent local storage of visualization files, select the Disable button at the top. Other options are to store the files locally in a single folder location in a Flat List, or to store them in a folder structure mimicking the Vault structure. If either of these options is selected, click on the browse button below to select a folder location for publishing.

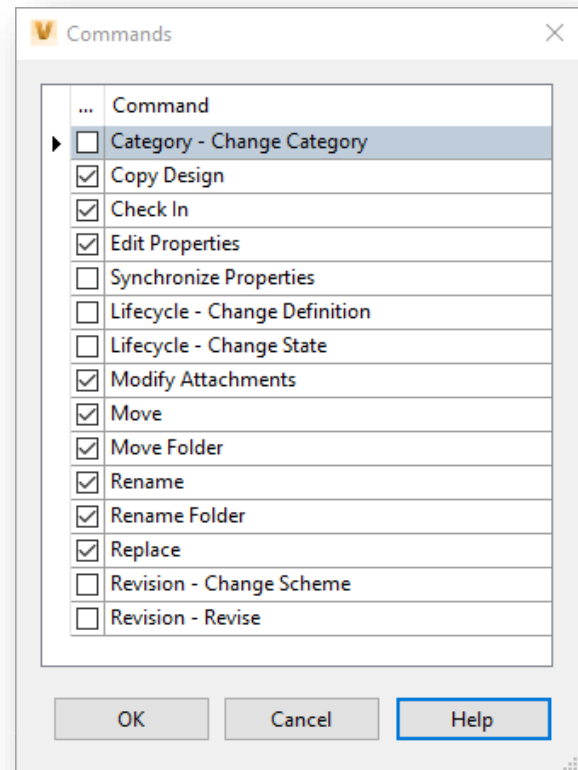
The last check box is used to disable the Vault warning when a DWF is not generated by the system. Note that by default, visualization files that are system generated are hidden in your file list. If you want to show them, go to Tools\Options and select Show Hidden Files.

Visualization Management

In this section, you can manage which tasks break the link between a file and its visualization attachment. Any task that can cause a version change of a file automatically breaks this link so that an outdated DWF cannot be attached to a file. The following commands are set to do this by default:

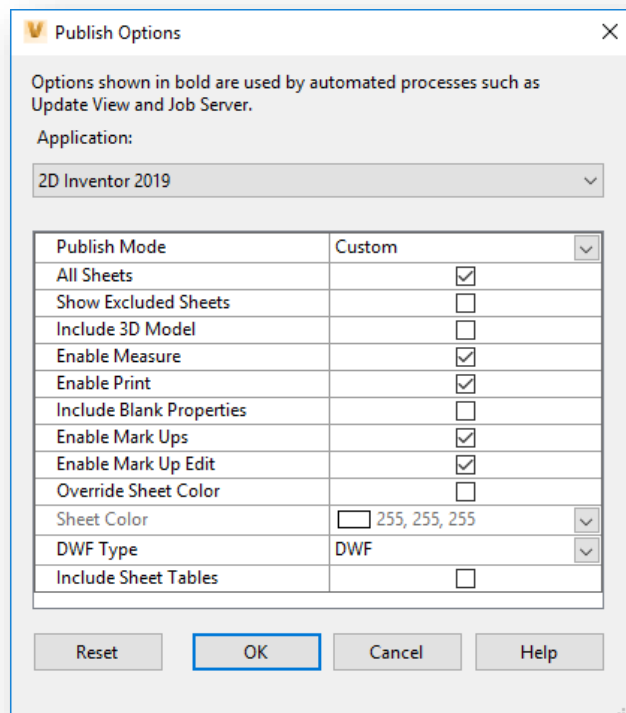
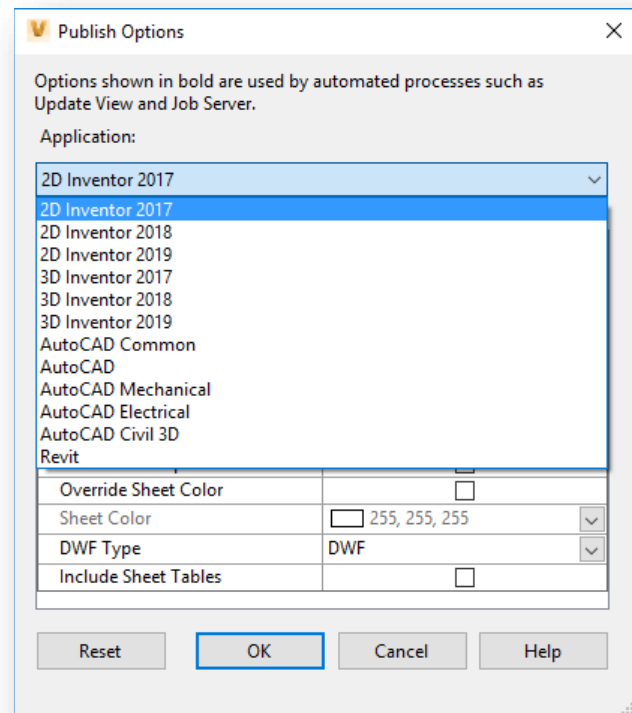
- Copy Design
- Check In
- Edit Properties
- Modify Attachments
- Move
- Move Folder
- Rename
- Rename Folder
- Replace

In this image, you can see that there are other options to choose from but be aware that these settings may affect the reliability of your visualizations.



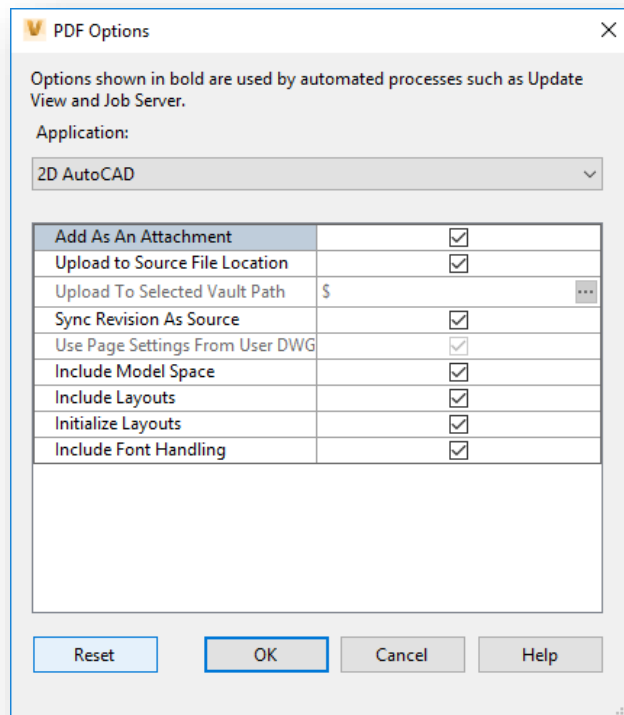
Publish Options

Vault Client publishes a DWF file whenever a file is checked in, or the users selects the Update button in the file preview window to manually generate a new visualization. Visualizations are created based on these Publish Options, which can be set for the applications shown in this graphic:



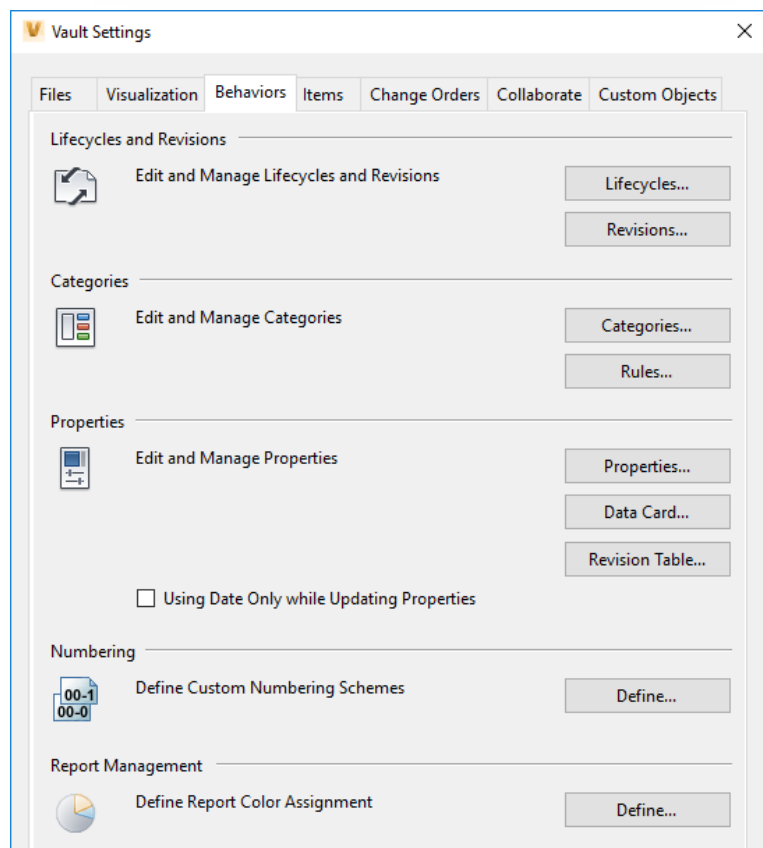
This image shows an example of one of the settings pages, and what settings you can change. These vary from one application or release, to the next. This happens to be Inventor 2D for 2019.

As promised, here is a screen capture of the PDF publishing options from the Files Tab. These options apply to 2D AutoCAD and 2D Inventor PDF Publishing. The options shown checked are the default or “out of the box” options.



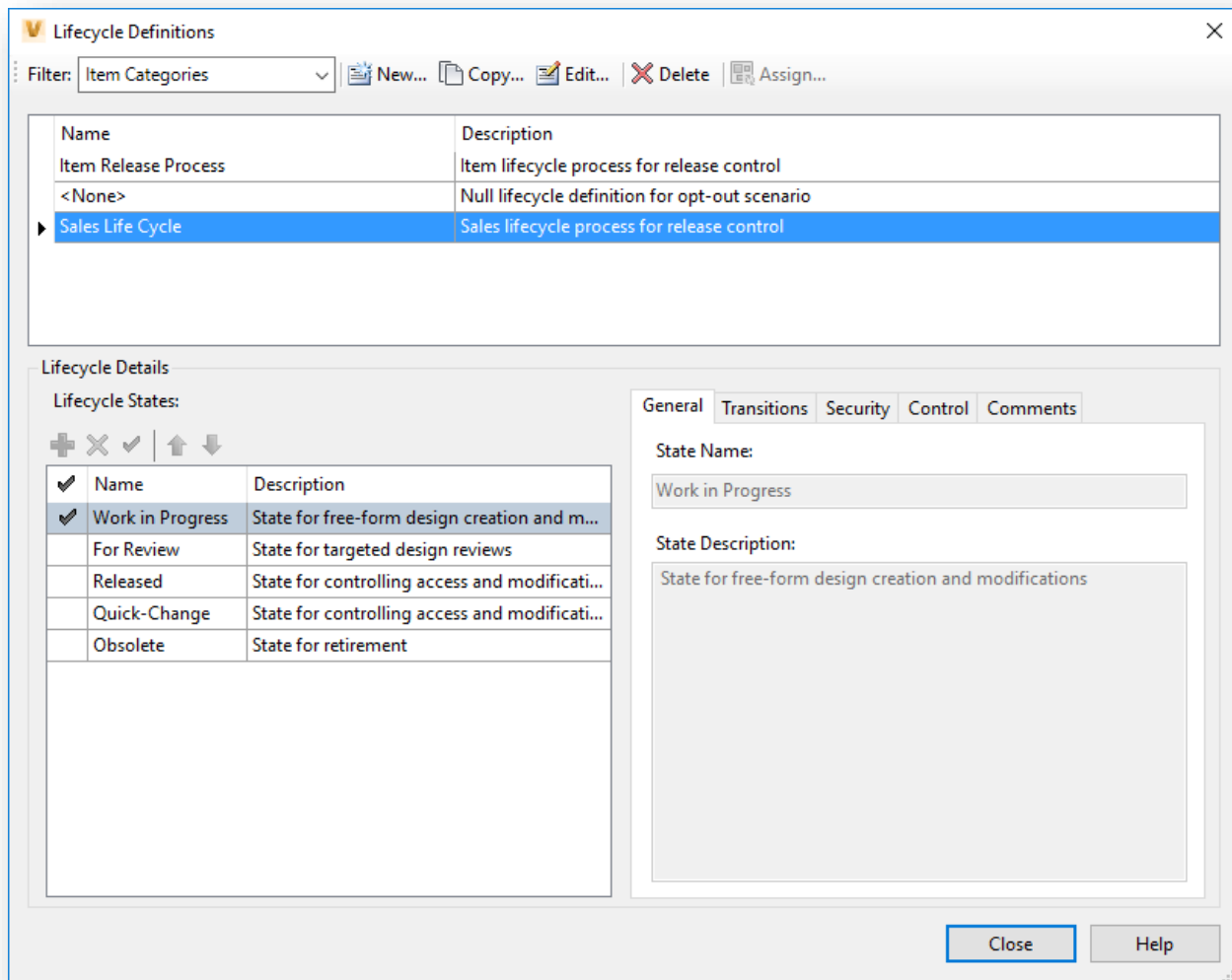
Behaviors Tab

This tab is where you, as a Vault Admin, might spend a lot of your time. Here is where you will create and manage things like Lifecycle Definitions, Revision Schemes, Categories and Properties among others. This tab is only available in Vault Workgroup and Professional.



Lifecycles

Used with files, projects, folders, items and custom objects; lifecycles are used to set permissions, behavior and properties to objects in the Vault. These are based on various states that follow the natural flow of your design process. Some examples of lifecycle states are Work in Progress, Review or Released.

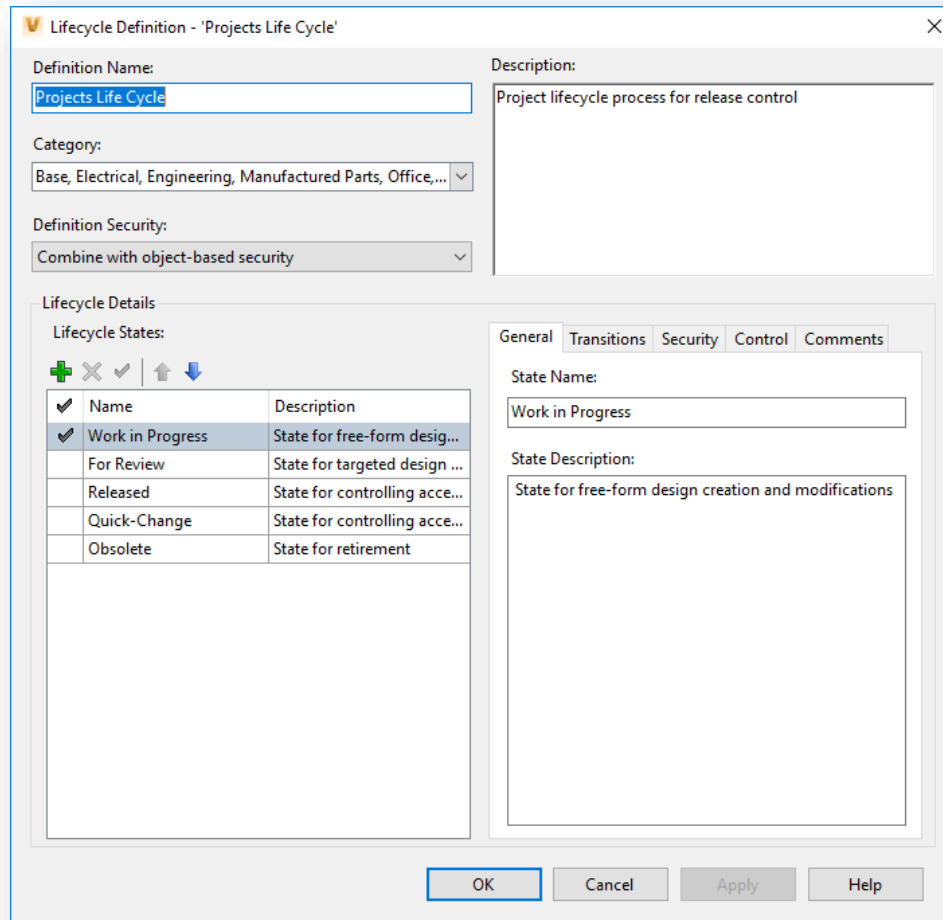


Objects move through the states either automatically, based on transition rules, or manually with user actions. As they move from state to state, transition rules can also set automatic behaviors to take place. One example of this would be a file being moved from Released to Work in Progress, this action may be set to automatically trigger a revision change on the object.

Mark has already discussed lifecycle state security, but here we can see how it fits with transitions. Following the same example above, the file in Released state may have Deny permissions on Modify, making the file read only to all except Administrators. Moving the file to Work in Progress might then change the permissions to Allow so that the file can be modified by authorized users.

Looking in more detail at the Lifecycle Definition, there are several areas to be familiar with.

On the main page, you can create a new lifecycle from scratch, copy or edit existing lifecycles, or delete them. Filter the list of lifecycle definitions by selecting a filter from the window in the upper left.



Lifecycle Definition - 'Projects Life Cycle'

Definition Name:

Category:

Definition Security:

Description:

Lifecycle Details

Lifecycle States:

Name	Description
<input checked="" type="checkbox"/> Work in Progress	State for free-form design...
<input type="checkbox"/> For Review	State for targeted design ...
<input type="checkbox"/> Released	State for controlling acce...
<input type="checkbox"/> Quick-Change	State for controlling acce...
<input type="checkbox"/> Obsolete	State for retirement

General | Transitions | Security | Control | Comments

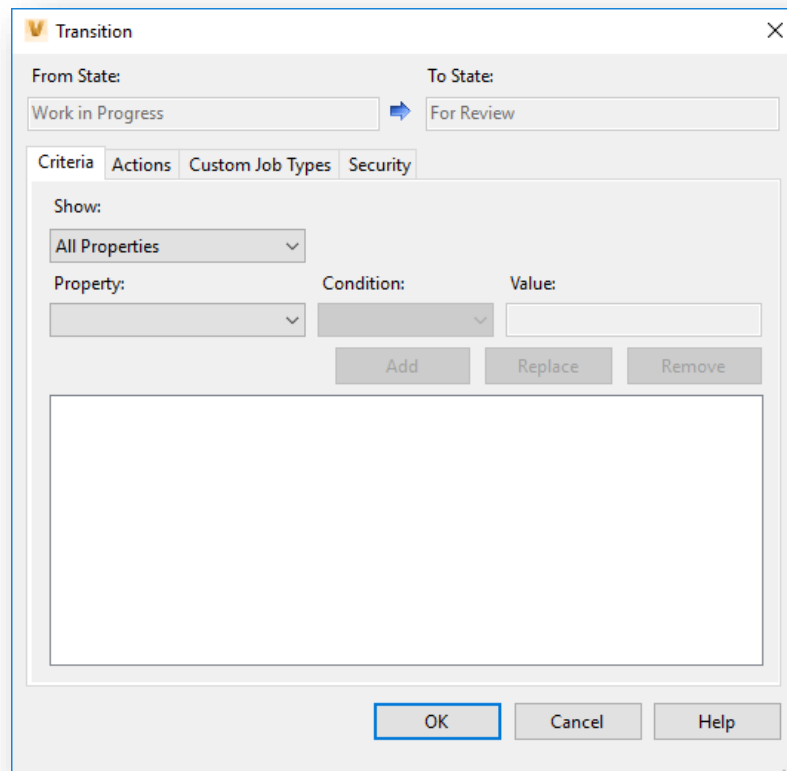
State Name:

State Description:

OK Cancel Apply Help

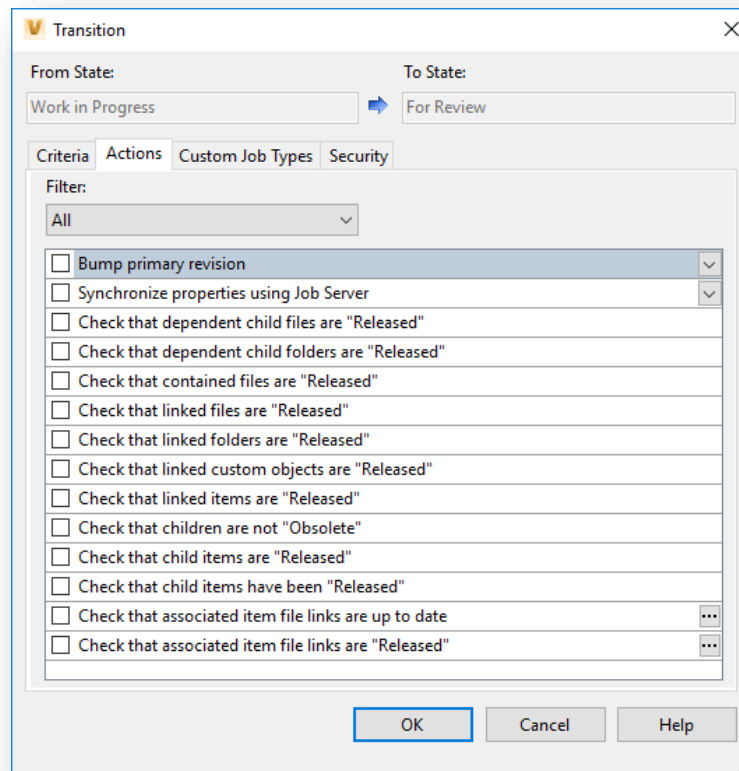
Selecting New will open this same screen with none of the fields populated, allowing you to name the definition and enter a description, assign it to categories and choose a security scheme. Below you can add Lifecycle states which fit your design process, select a default, and re-order the list. On the right, the **General** tab shows the state name, and lets you enter a description.

Transitions will show you all of the available state transitions based on the lifecycle states you have created. Selecting Edit on any row will allow you to apply some settings to each transition if you wish.



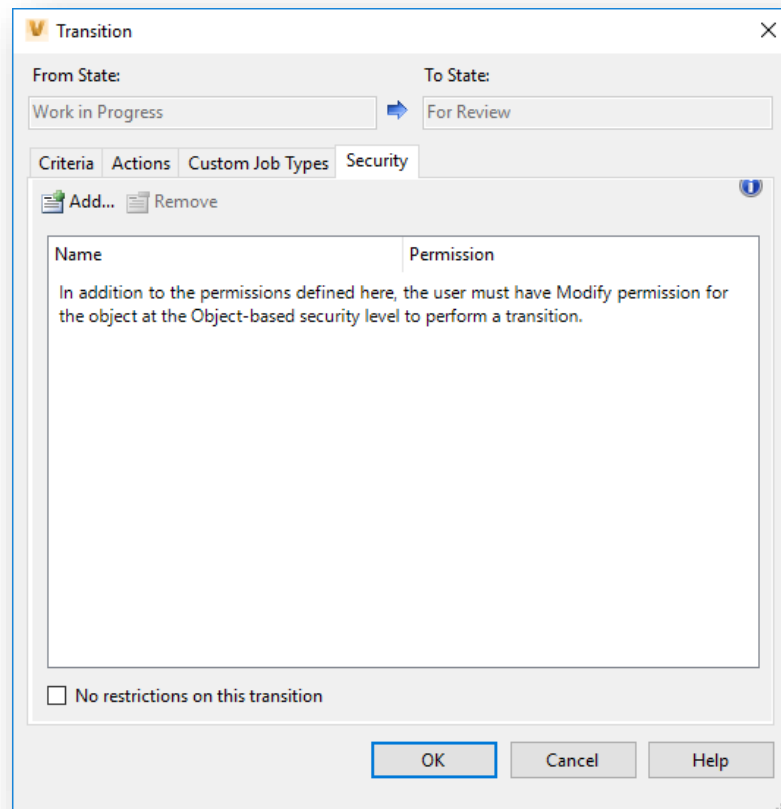
The image shows a 'Transition' dialog box with a close button (X) in the top right corner. It features two text input fields: 'From State:' containing 'Work in Progress' and 'To State:' containing 'For Review', separated by a blue arrow icon. Below these is a tabbed interface with four tabs: 'Criteria' (selected), 'Actions', 'Custom Job Types', and 'Security'. Under the 'Criteria' tab, there is a 'Show:' section with a dropdown menu set to 'All Properties'. Below this are three columns: 'Property:' with a dropdown menu, 'Condition:' with a dropdown menu, and 'Value:' with a text input field. Underneath these columns are three buttons: 'Add', 'Replace', and 'Remove'. A large, empty rectangular box occupies the lower half of the dialog. At the bottom right, there are three buttons: 'OK' (highlighted with a blue border), 'Cancel', and 'Help'.

Under **Criteria**, you can set property conditions that must be met before the transition will be allowed. One example might be “Part Number is not empty”.



Actions is where you can set up additional actions that will take place along with the state change, such as a revision bump.

Custom Job Types allows you to assign a custom job that has been written by a programmer, which will run when the state transition takes place.



The options under the *Security* tab are based on the Definition Security you selected when creating the definition. If you chose to combine with Object Based security, then these settings, along with Object Based permissions set on the object itself, will combine to set the users effective permissions for this state transition. If you selected Override Object Based security, these settings will become the effective permissions for the transition. There is also a check box for No Restrictions, which keeps any object-based security as the effective permissions.

Lifecycle Definition - 'Projects Life Cycle'

Definition Name: Projects Life Cycle

Category: Base, Electrical, Engineering, Manufactured Parts, Office,...

Definition Security: Combine with object-based security

Description: Project lifecycle process for release control

Lifecycle Details

Lifecycle States:

Name	Description
Work in Progress	State for free-form design...
For Review	State for targeted design ...
Released	State for controlling acce...
Quick-Change	State for controlling acce...
Obsolete	State for retirement

General Transitions Security Control Comments

Add... Remove

Name	Read	Modify	Delete
Engineering	Allow	Allow	Deny
CAD	Allow	Allow	Allow

☐ No state-based security

Options

☐ Security for associated files of items Configure...

☐ Security for files inside folders Configure...

OK Cancel Apply Help

Security is where you indicate permissions for the individual state. Add or remove users or groups and set what permissions they will have for Read, Modify & Delete for any object controlled by this lifecycle definition, in this state. For example, certain users may be allowed to delete files in this state, while others are not. This security will also depend on the Definition Security option as talked about in the previous section. You can also set No state-based security, and select security options associated files of Items, and files inside folders.

Lifecycle Definition - 'Projects Life Cycle'

Definition Name: Projects Life Cycle

Category: Base, Electrical, Engineering, Manufactured Parts, Office,...

Definition Security: Combine with object-based security

Description: Project lifecycle process for release control

Lifecycle Details

Lifecycle States:

Name	Description
Work in Progress	State for free-form design...
For Review	State for targeted design ...
Released	State for controlling acce...
Quick-Change	State for controlling acce...
Obsolete	State for retirement

General Transitions Security **Control** Comments

☐ This is a "Released" state

☐ This is an "Obsolete" state

Controlled versions (do not purge)

☐ All

☒ First and last

☐ Last

☐ None

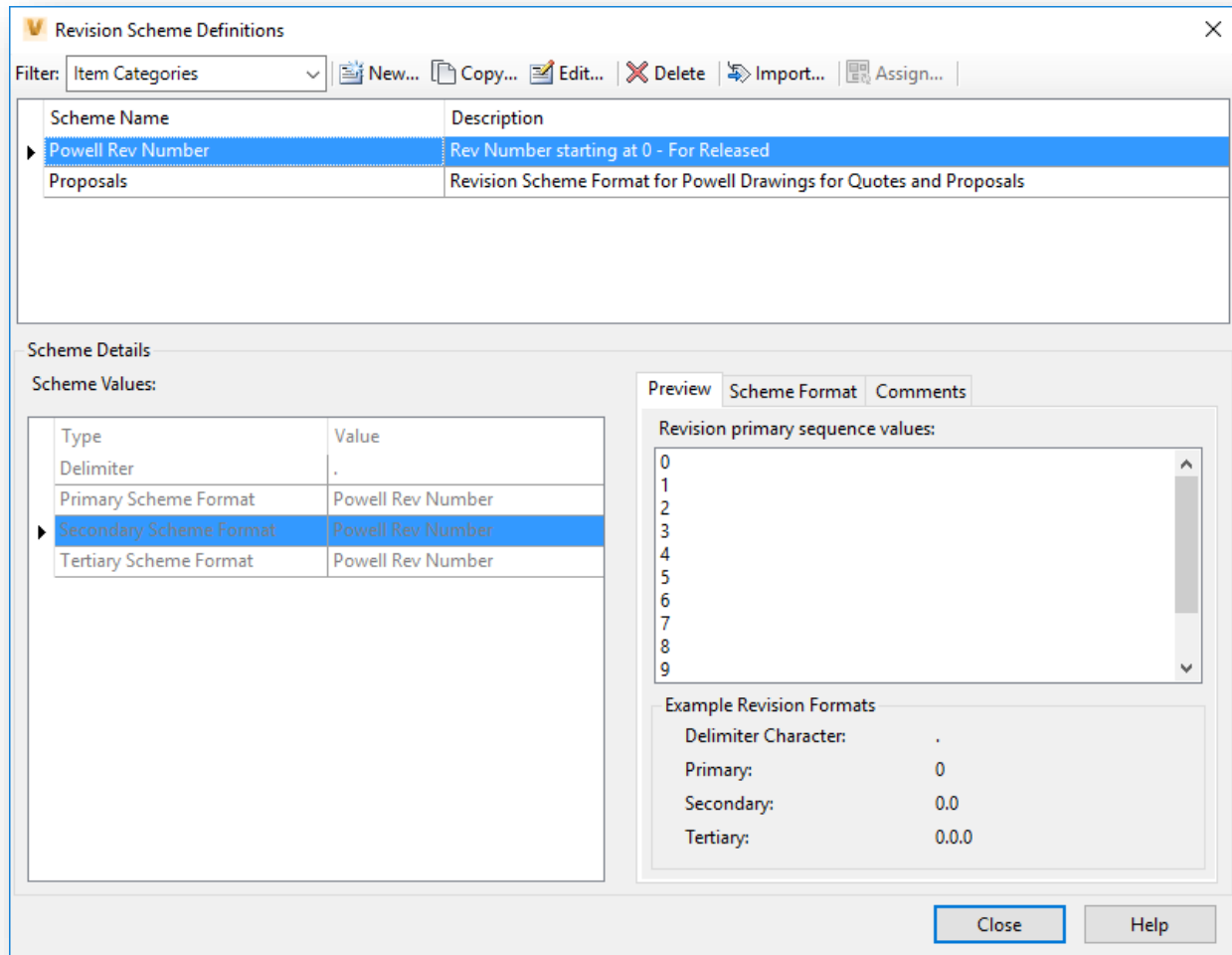
All versions in this state will be removed during a purge, except the first and last version in each series.

Use in states such as 'Work in Progress' where the delta may be useful.

OK Cancel Apply Help

Control tab is where you set "released" or "Obsolete" states and decide which versions of objects may be purged when the purge command is run. **Comments** tab is where you can enter any default comments you would like to use for each state. You can set multiple comments to choose from and set one as the default. Administrators may create as many new lifecycle definitions as they feel are necessary to the project workflow.

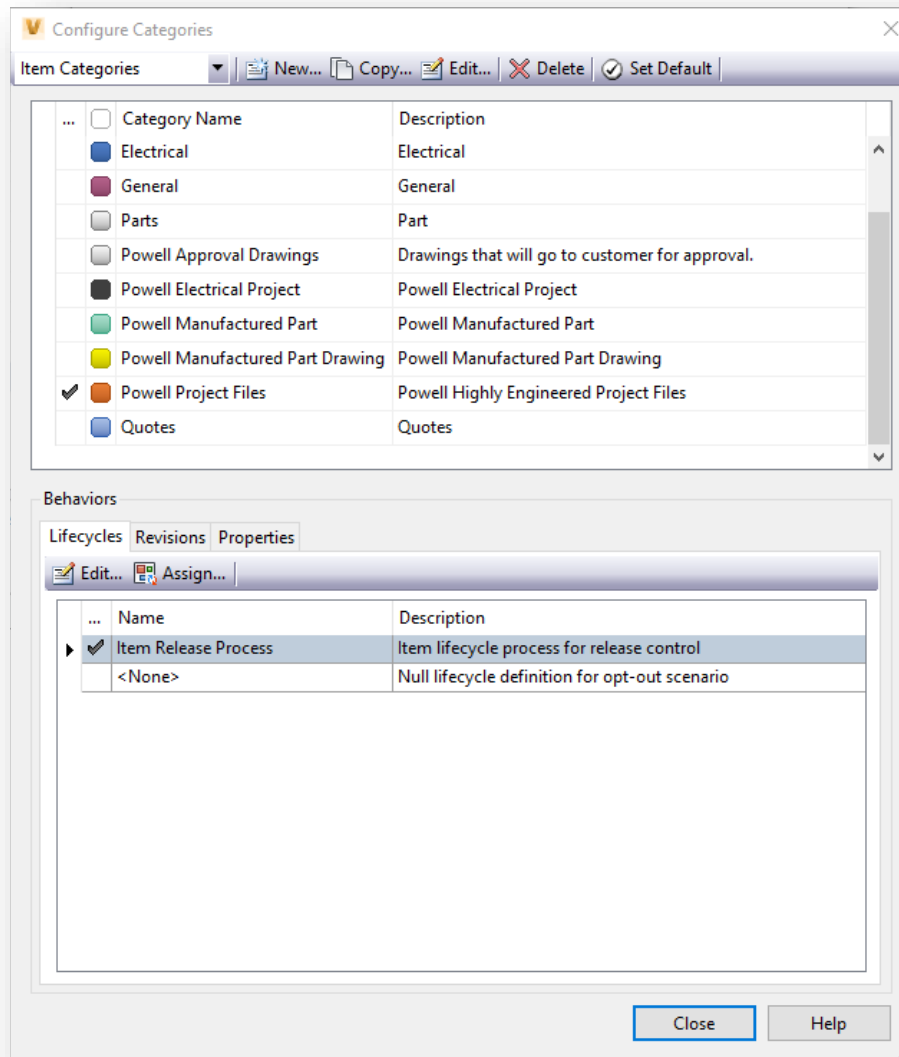
Revisions



Here is where you can define and manage any number of revision schemes for your Vault objects. Revisions can be applied to all category types, such as Files, Folders or Items. You can create different schemes for different object types, such as is shown above. One scheme is used for production drawings, and the other for sales and quoting documents.

You have control over how the revisions look, including deciding whether to use numeric or alpha revisions, what character is your primary revision (for example 1 or 0). Select categories from the drop-down list and use Assign to add or remove revision schemes from that category. Use lifecycle transitions to determine how and when the revision is automatically advanced on a Vault object. Revisions may also, if allowed by user permissions, be manually changed by selecting an object and using Actions\Change Revision.

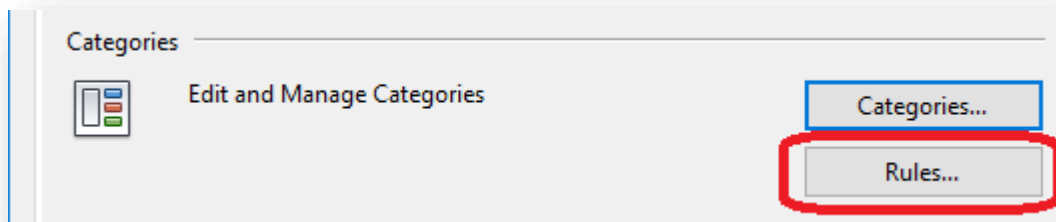
Categories



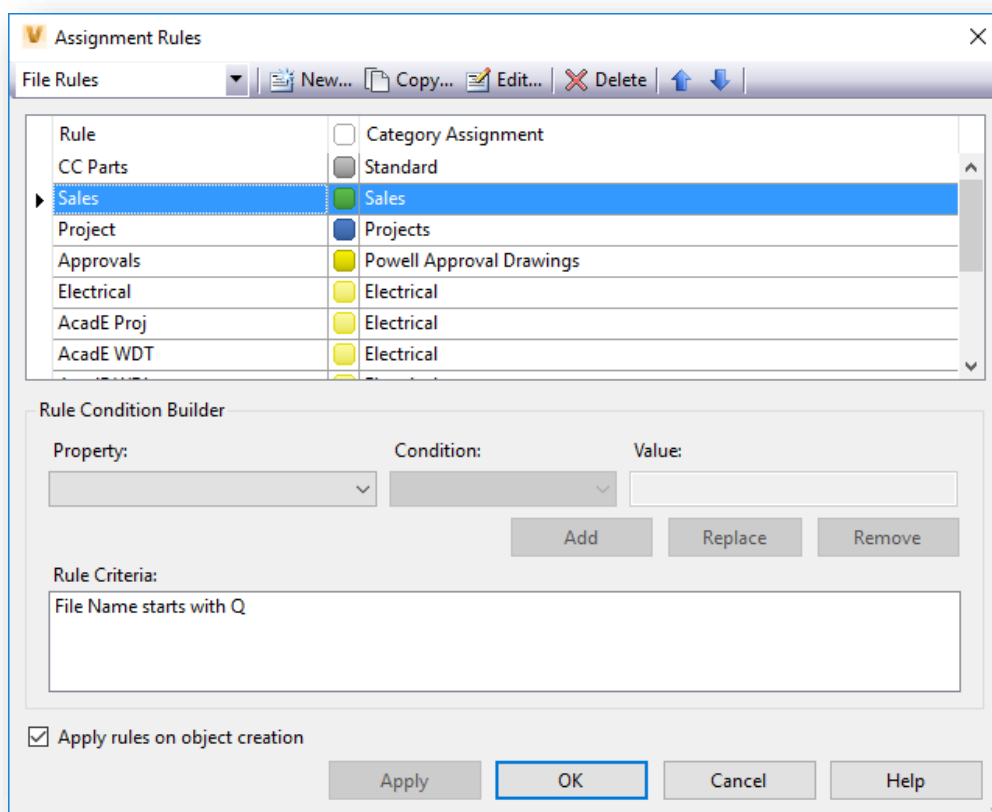
Create and customize categories and rules to organize your project data. Categories can be created for Files, Items, Folders and Custom Objects. Under the Behaviors section on the bottom of the Configure Categories dialog, assign or edit Lifecycles, Revisions and Properties that apply to a specific category. The Edit button here will take you directly to the configuration screen for that item. For example, on the Lifecycles tab, selecting Edit will open the Lifecycles Definition dialog that we discussed above.

For each category grouping, eg. Files or Items, you can select a Default Category. Any new objects added to the Vault that do not meet the criteria of any category Rules (see next section), will be added to the Default Category for that object type.

Category Rules

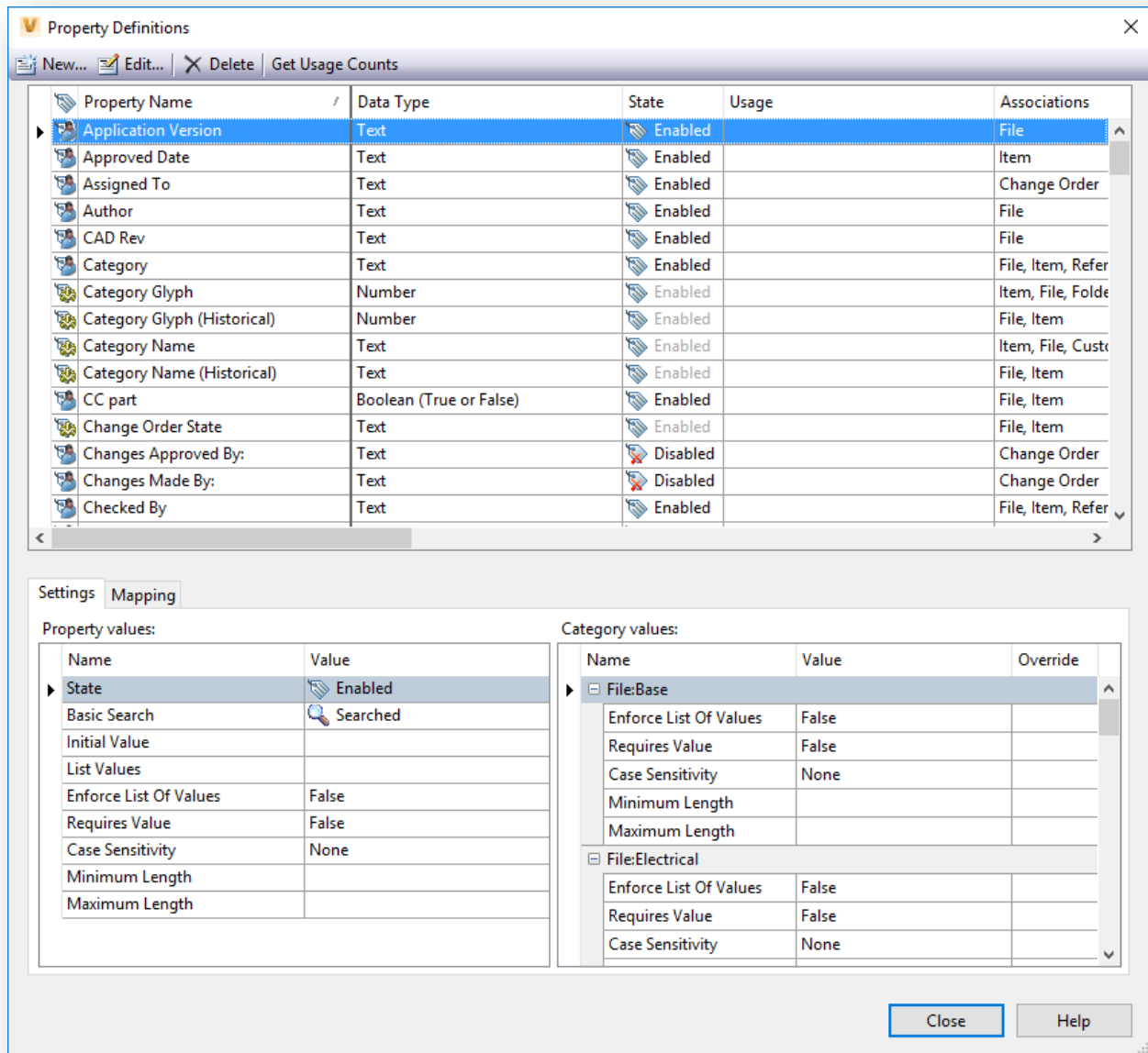


Using rules, you can automate which category an object is assigned to in the Vault. Rules may be as complex or simple as needed. For example, in this image:



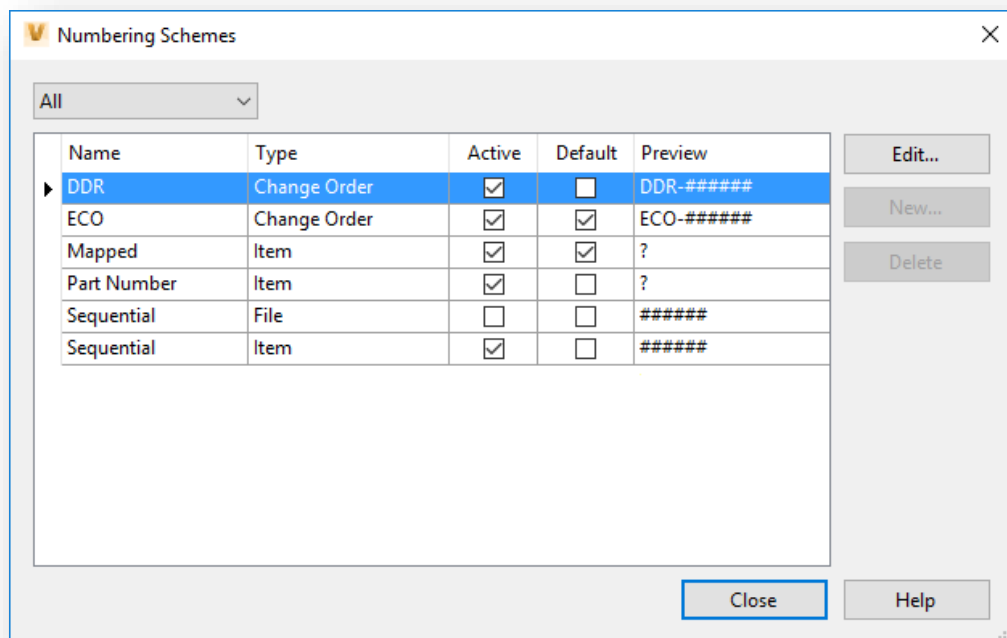
The rule is very simple. All Quote drawing names begin with a Q and are followed by the quote number. The rule then assigns any new file checked in starting with a "Q", to category Sales. To follow this, there is also an Item Category called Quotes. The rule for this category uses another simple condition: Category is Sales. Use the Condition Builder to add conditions based on property values to build your rules.

Properties



Properties are attributes associated with files in Vault. These can be either System Properties or User Define Properties (UDP). The Property Definitions is used to manage these attributes. We are not going to spend a lot of time here, simply because there is an entire session devoted to Properties, from AU2017. While not my most shining moment speaking at AU, the handout for [this class](#) still contains a much more in depth look at managing Vault Properties.

Data contained in properties can be mapped to and/or from a file to capture or populate similar properties on your CAD files themselves. For example, Revision properties such as the Date, Description and Approver can be filled out in the Vault on a change order, and then pushed to the revision table on a drawing in Inventor.

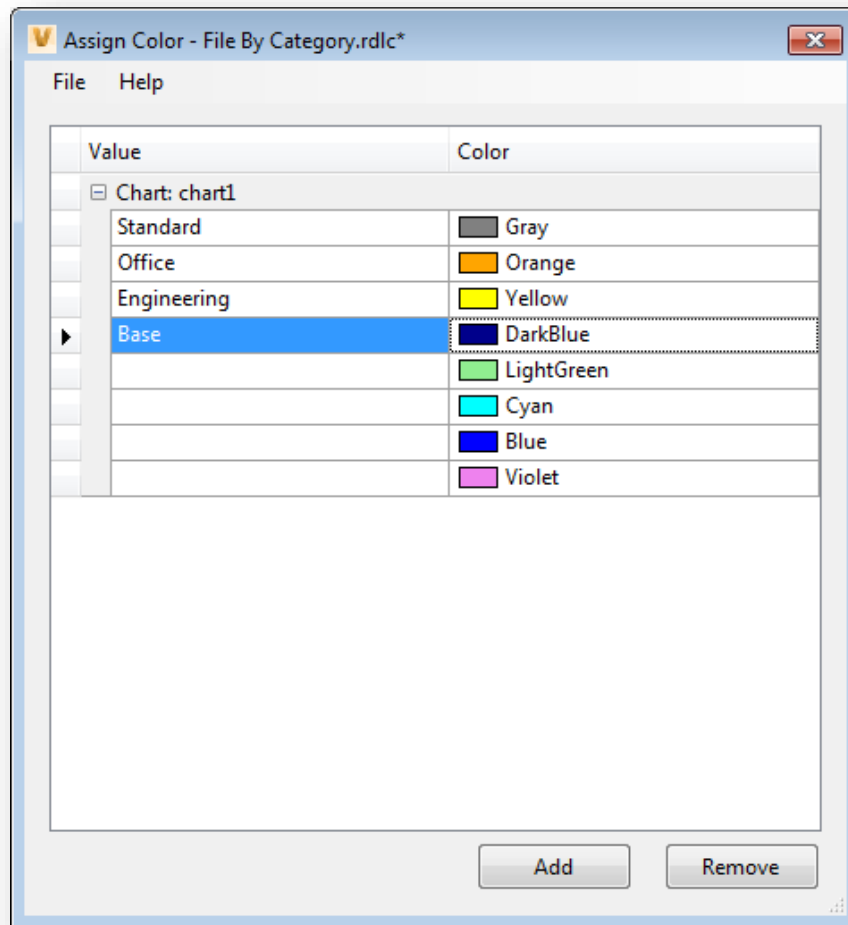


Numbering Schemes

Numbering schemes are used to assign how your Files, Items and Change Orders are named, when they are added to the Vault. There are three existing schemes you can choose from, or you can create custom schemes of your own based on one or more parameters. If no numbering scheme is desired for an object type, simply uncheck the Active & Default boxes.

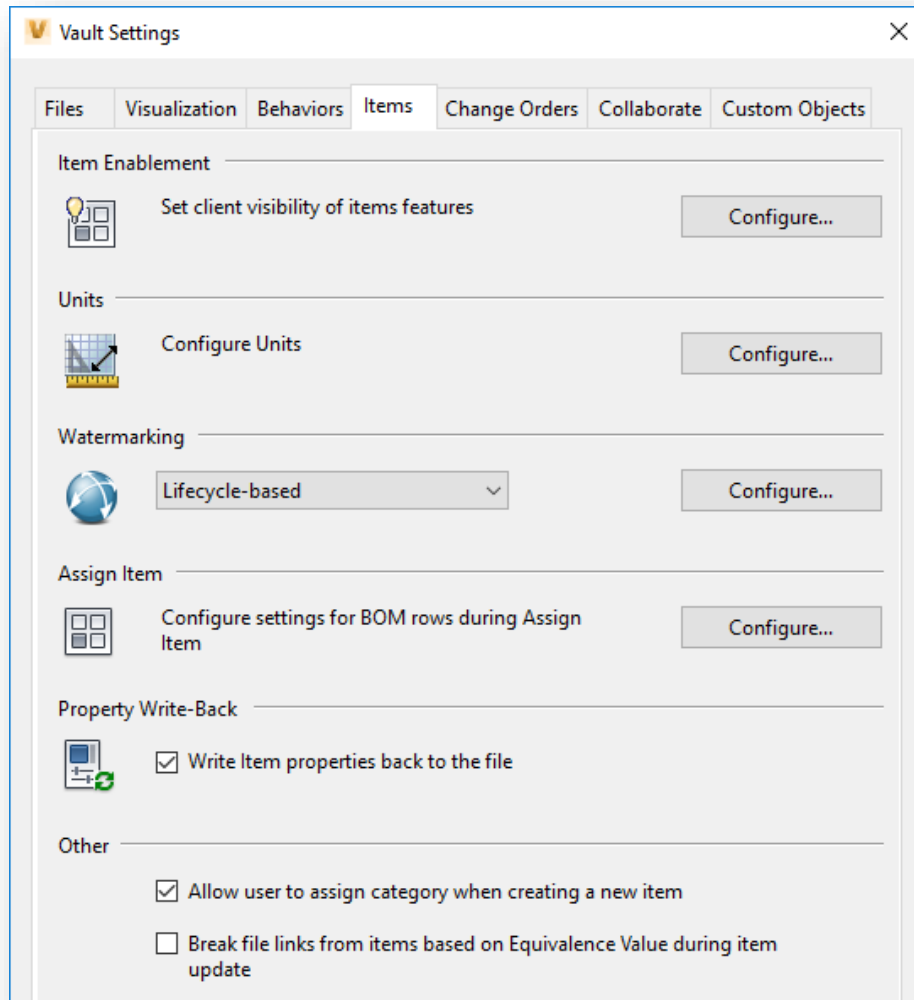
Mapped	Item names are generated based on the user-defined properties mapped to the item in the Map Properties dialog.
Sequential	File or Item names are generated sequentially. This is the default number scheme and cannot be edited or deleted.
ECO	Change Order names are generated based on a defined fixed text, a delimiter, and an auto-generated number.
Custom	Object names are generated based on a custom design. This feature provides the flexibility to create a numbering scheme where the name carries information about the object.

Define Report Color Assignment



This tool allows admins to assign colors to a Data Mapping report template. A report must be generated before the value columns will be populated in this editor, but once populated, these can be customized. The Data Mapping report is a feature of the Inventor Vault Add in, and is only used with Vault Professional and Workgroup.

Items Tab

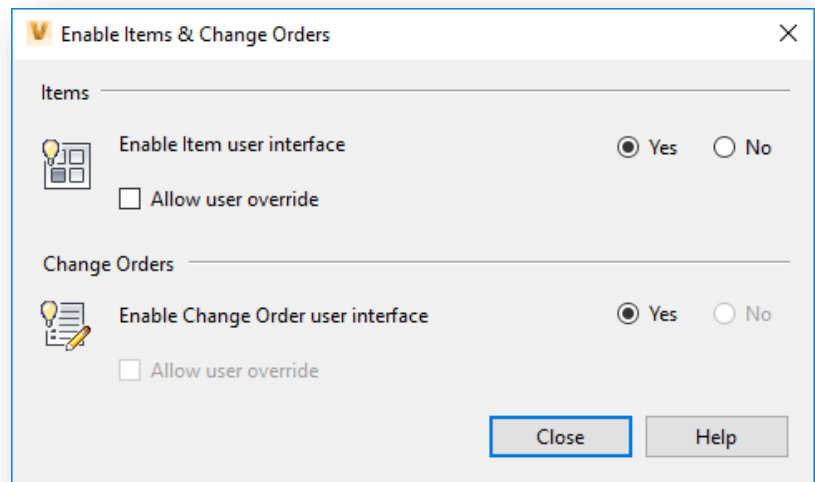


An Item is essentially what your company makes, builds, sells or manages. Items may be parts, assemblies, BOM's or documents. An Item is identified by a unique Item number. Items are managed in Vault Professional in the Item Master, a complete list of all Items in the Vault. Files needed to produce the Item are linked to the Item for easy retrieval.

This tab offers options for configuring Item behavior.

Item Enablement

Select Configure to show the Enable Items and Change Orders dialog. Use these to enable or disable these features to control access to them. Also choose whether to allow user override if disable is checked.



Enable Items & Change Orders

Items

Enable Item user interface ☒ Yes ☐ No

☐ Allow user override

Change Orders

Enable Change Order user interface ☒ Yes ☐ No

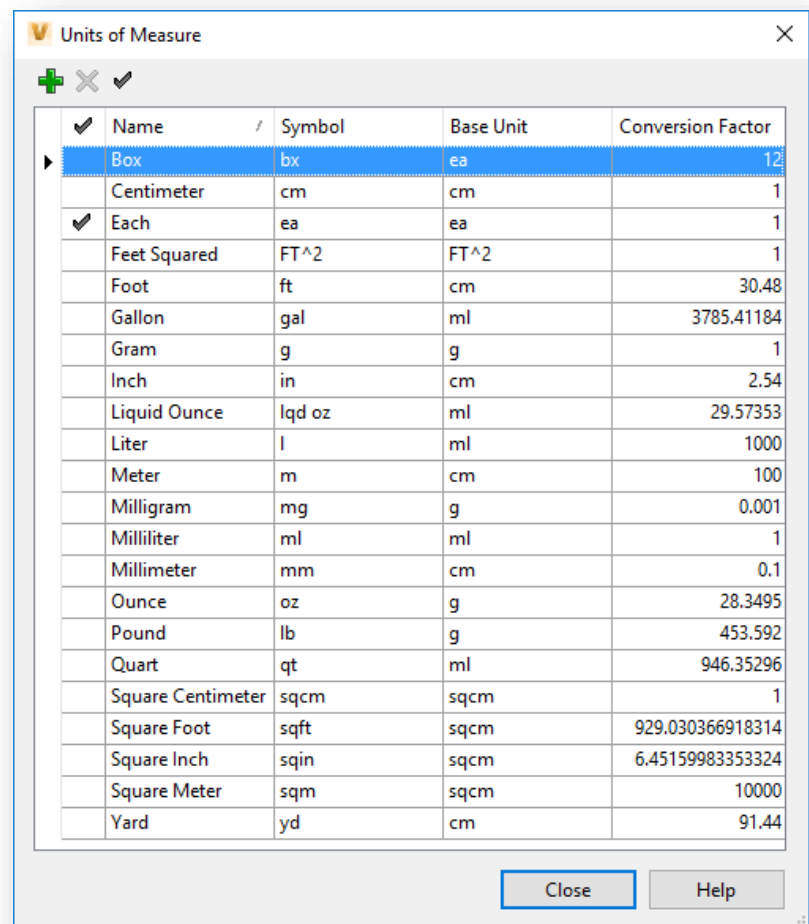
☐ Allow user override

Close Help

Units of Measurement

Items contain a Bill of Materials of any components associated with the Item. For example, an Inventor assembly Item will contain a full BOM of the assembly components.

Use this tool to set the units for this BOM. Accept the defaults, modify them, or add any that you need that are not there already.




Units of Measure

✓	Name	Symbol	Base Unit	Conversion Factor
▶	Box	bx	ea	12
	Centimeter	cm	cm	1
✓	Each	ea	ea	1
	Feet Squared	FT^2	FT^2	1
	Foot	ft	cm	30.48
	Gallon	gal	ml	3785.41184
	Gram	g	g	1
	Inch	in	cm	2.54
	Liquid Ounce	lqd oz	ml	29.57353
	Liter	l	ml	1000
	Meter	m	cm	100
	Milligram	mg	g	0.001
	Milliliter	ml	ml	1
	Millimeter	mm	cm	0.1
	Ounce	oz	g	28.3495
	Pound	lb	g	453.592
	Quart	qt	ml	946.35296
	Square Centimeter	sqcm	sqcm	1
	Square Foot	sqft	sqcm	929.030366918314
	Square Inch	sqin	sqcm	6.45159983353324
	Square Meter	sqm	sqcm	10000
	Yard	yd	cm	91.44

Close Help






Watermarking

Items may be watermarked based on lifecycle state, specific properties, or custom text. The position, text style and color can also be customized. Select the type of watermark you would like to configure from the pull down menu on the left, and then select configure to set the options you want. If no watermark is desired, select the None option. An example of a lifecycle based watermark configuration is shown below. Note that these are tied to categories and lifecycle definitions that were discussed above. The lifecycle states you have already configured are used, and you decide the text that is displayed for each state, along with the location, font, color and size.

 Lifecycle Watermarks

Filter: Item Categories

Name	Description
Item Release Process	Item lifecycle process for release control
<None>	Null lifecycle definition for opt-out scenario
Sales Life Cycle	Sales lifecycle process for release control

Lifecycle State	Watermark Text	Location	Font	Color	Size
Reference Only! - Work In Progress	Reference Only! - Not Approved for Construction	Border	Arial		Small
Reference Only! - In Review	Review Copy - Not Approved For Construction	Border	Arial		Small
Quick-Change	QUICK-CHANGE	Diagonal	Tahoma		Medium
Obsolete - Do Not Use	OBSOLETE	Diagonal	Arial		Medium
Approved For Construction	Approved For Construction	Border	Arial		Small

OK

Cancel

Help

Assign Item

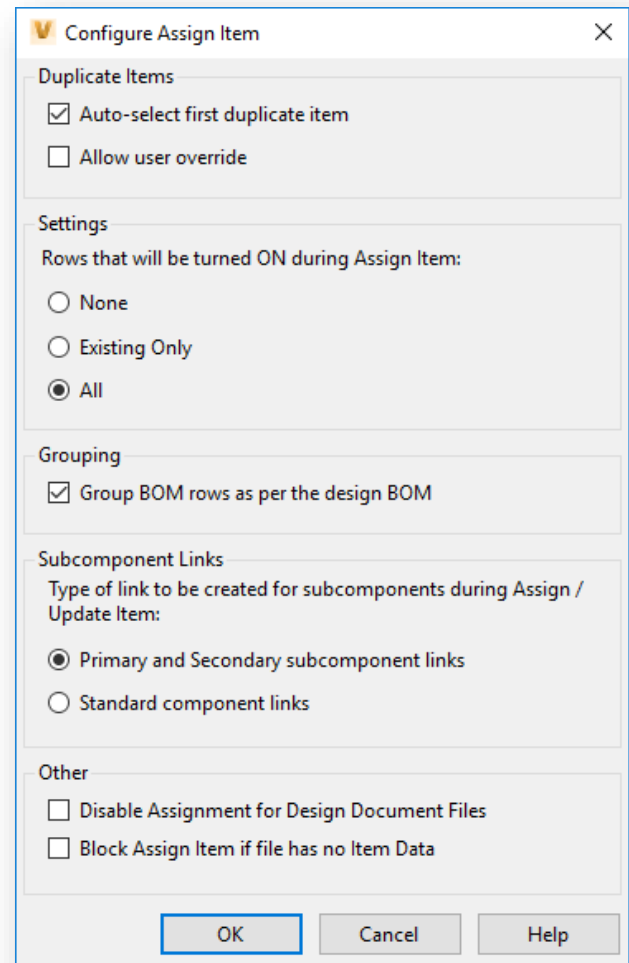
This section allows you to configure whether BOM rows of an Item are turned on automatically or not. It also contains settings for handling duplicates as well as grouping and how to deal with subcomponents.

If BOM rows that will be turned on is set to None, they can still be turned on manually from the Item editor.

In Grouping, checking this option will merge rows of your BOM the way that they are merged (or not) in your design BOM. For example, if your Inventor BOM is merged based on Part Number, your Item BOM will also follow that.

Under Subcomponent links, select your option for the type of link to be used for subcomponents, when items are Assigned or Updated.

In Other, you can block design documents such as Inventor .idw files from being assigned Items. They will instead be linked to the Items that they represent.



The image shows a 'Configure Assign Item' dialog box with the following settings:

- Duplicate Items:**
 - ☒ Auto-select first duplicate item
 - ☐ Allow user override
- Settings:**

Rows that will be turned ON during Assign Item:

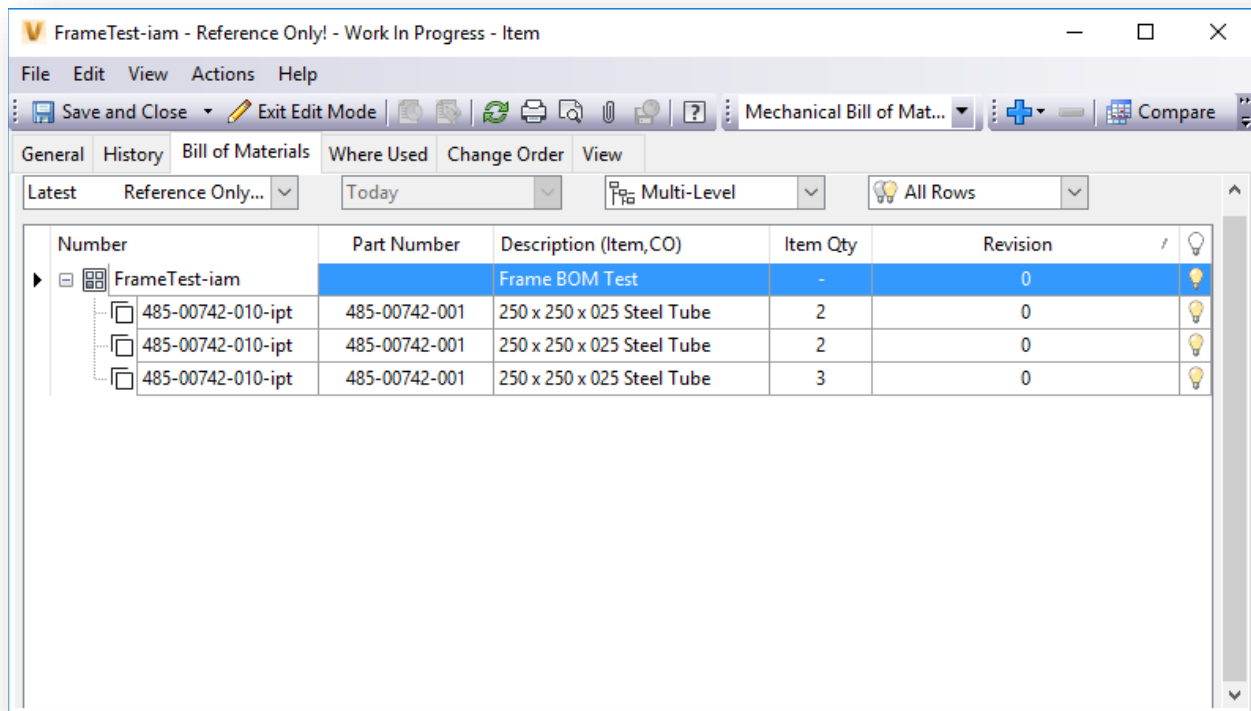
 - ☐ None
 - ☐ Existing Only
 - ☒ All
- Grouping:**
 - ☒ Group BOM rows as per the design BOM
- Subcomponent Links:**

Type of link to be created for subcomponents during Assign / Update Item:

 - ☒ Primary and Secondary subcomponent links
 - ☐ Standard component links
- Other:**
 - ☐ Disable Assignment for Design Document Files
 - ☐ Block Assign Item if file has no Item Data

Buttons at the bottom: OK, Cancel, Help.

An example of a simple Item BOM is shown below. Based on the settings shown above, all rows were turned on automatically. Any components that did not already have an Item assigned were assigned on automatically, and since this small frame assembly was made from one stock size of steel, the elements were all assigned (1) item. They are shown as separate line items based on the length. You can set your BOM's up to appear in many different ways, to best suit your needs.



Number	Part Number	Description (Item, CO)	Item Qty	Revision
FrameTest-iam		Frame BOM Test	-	0
485-00742-010-ipt	485-00742-001	250 x 250 x 025 Steel Tube	2	0
485-00742-010-ipt	485-00742-001	250 x 250 x 025 Steel Tube	2	0
485-00742-010-ipt	485-00742-001	250 x 250 x 025 Steel Tube	3	0

Property Write Back

Properties set on an Item will be written back to the files, using the Vault Add Ins, Vault Explorer or the Job Processor. Uncheck this box to disable this feature.

Other

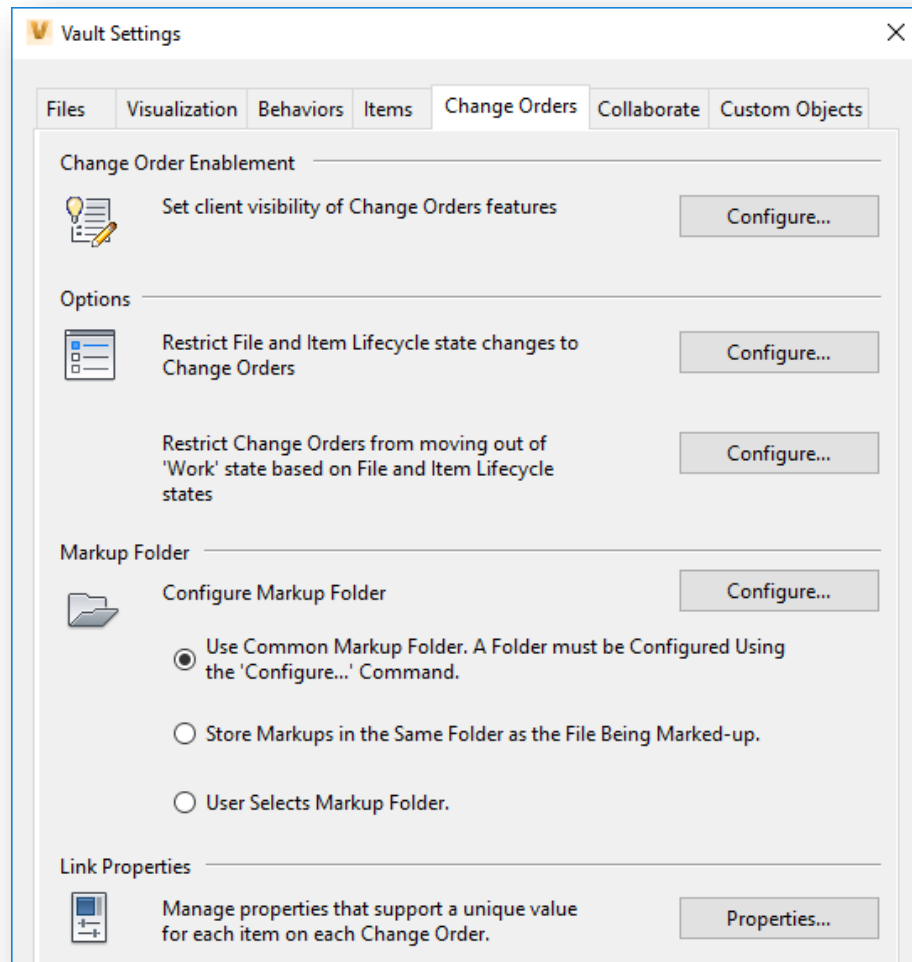
Allow User to assign category when creating a new item.

This is checked by default to allow users to select an Item category when a new Item is created. This is not true if a file is assigned to an Item, and there are category rules in place for the Item creation.

Break file links from items based on Equivalence Value during item update.

If checked, Vault will break the link between an Item and a file if equivalence values do not match when the Item is updated.

Change Orders Tab



Configure settings for Change Orders in Vault Professional.

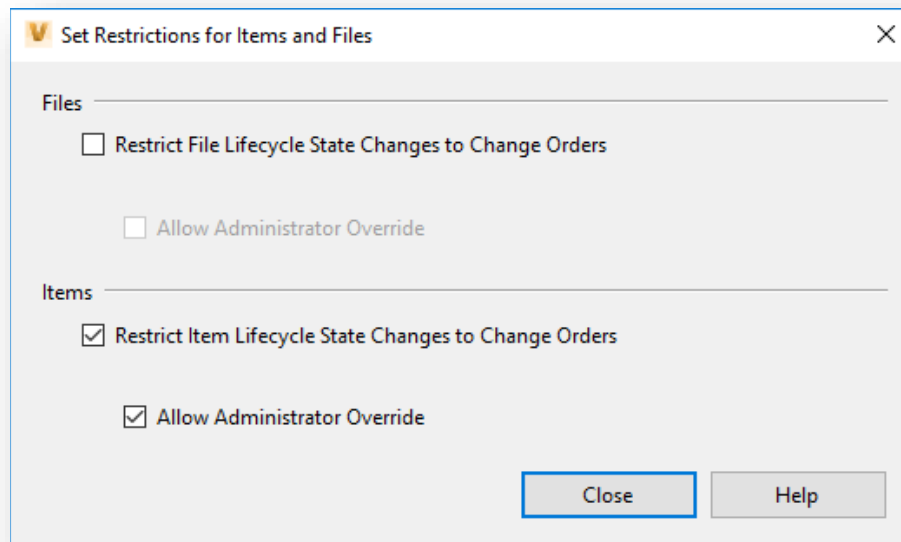
Change Order Enablement

Essentially the same tool as the Item Enablement on the previous tab.

Options

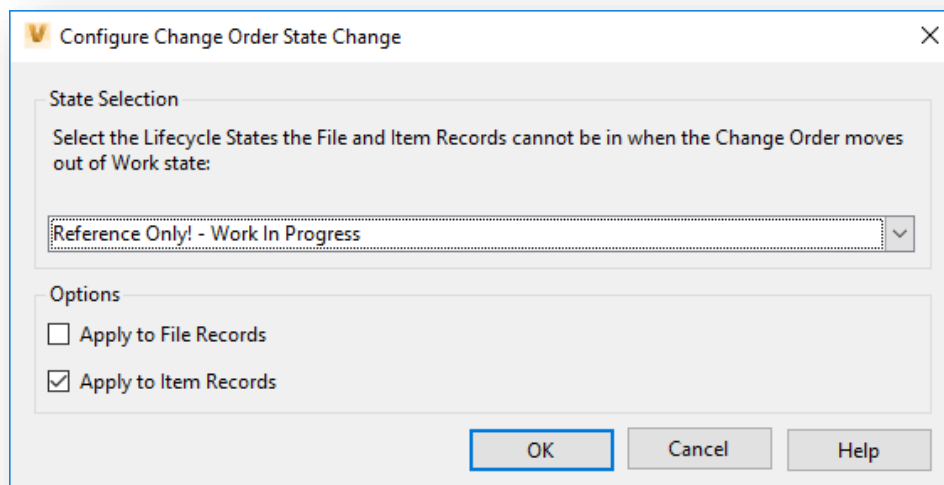
Restrict File and Item Lifecycle changes to Change Orders

Check the boxes to restrict files or Items from being moved from one lifecycle state to another, except inside of a change order. Also contains an option to allow Admin override.



Restrict Change Orders from moving out of “Work” state based on File and Item Lifecycle States.

This allows you to set a specific State the File or Item cannot be in when a Change Order moves out of the Work state.

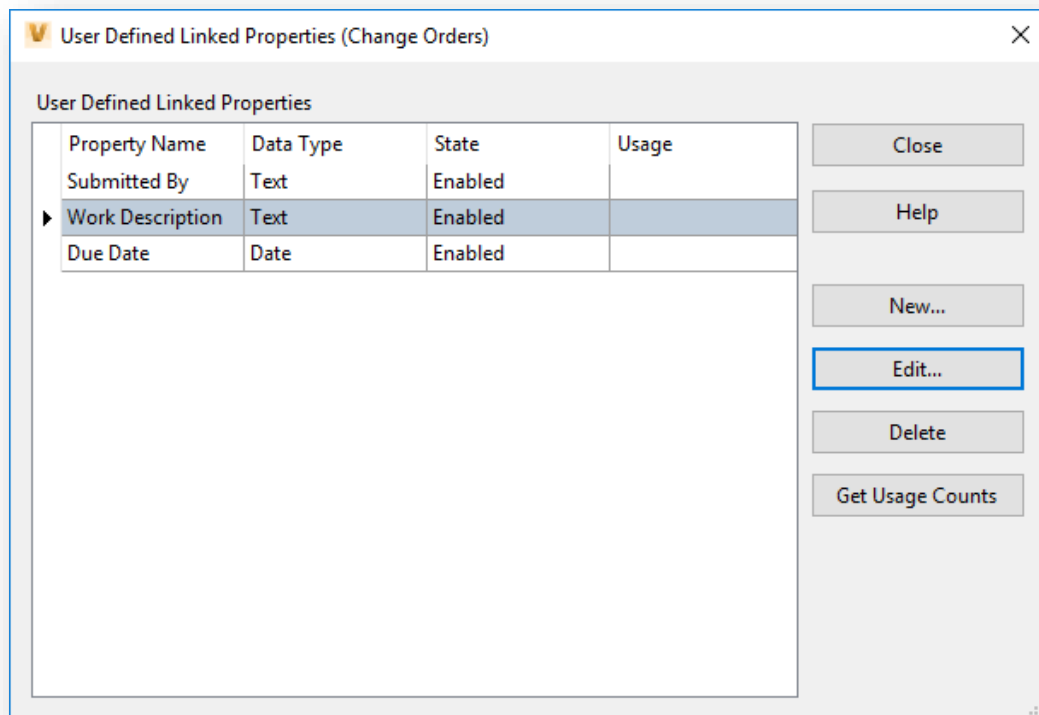


Markup Folder

Configure Markup Folder lets the admin decide if ECO markups will reside in a common folder, the same folder as the file being marked up, or in a user defined folder. Selecting configure, along with the first option, opens a Vault explorer window and the admin selects a folder location for the markup files.

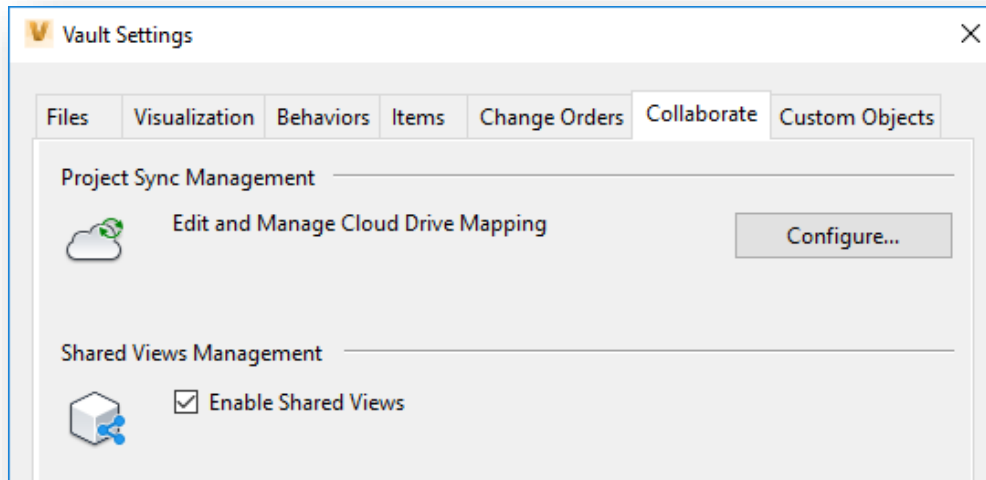
Link Properties

Create user defined properties which can be linked to individual records on a change order and support a unique value for each item. Example:



Collaborate Tab

Enable, disable and configure Project Sync and Shared Views.



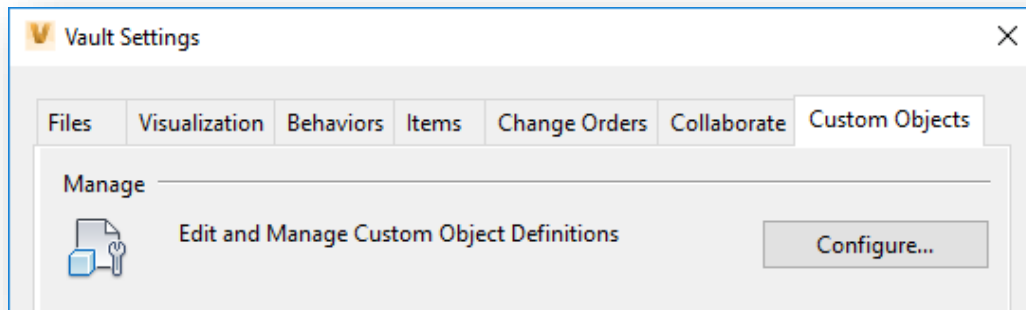
Project Sync Management

This feature is only available in Vault Professional and requires a subscription to Fusion Team. It allows you to upload content to, and download from, a cloud drive. It also allows for syncing files between the Vault and the cloud drive.

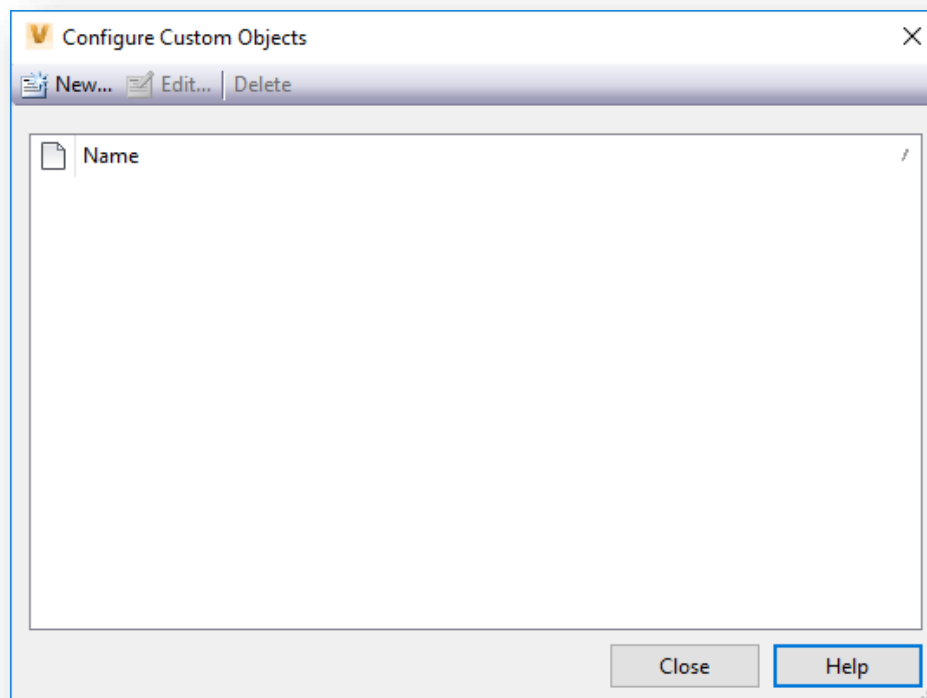
Shared Views Management

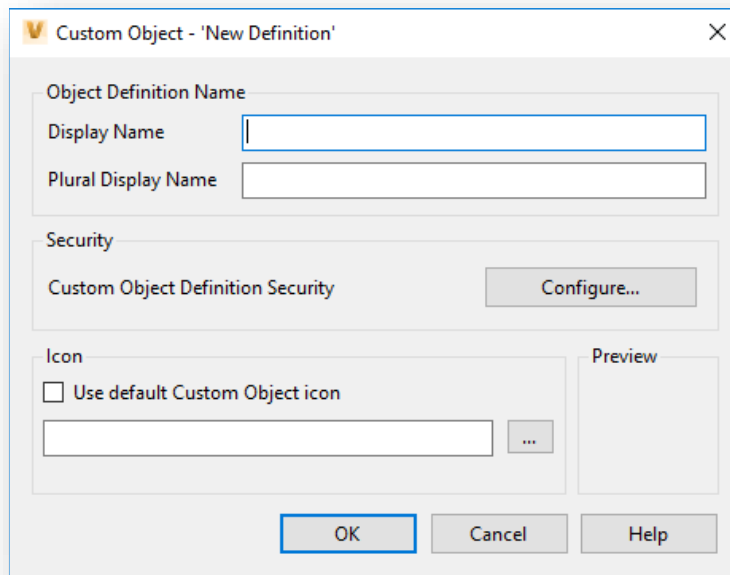
Available for Vault Workgroup and Professional, Shared Views let you create a visual representation of your design and place it in the cloud to share with others. You get a link that you can share with others, and all that is required to see the shared view is a browser. Users can view, comment and even mark up the shared view without affecting the original Vault data. The link is good for 30 days.

Custom Objects Tab



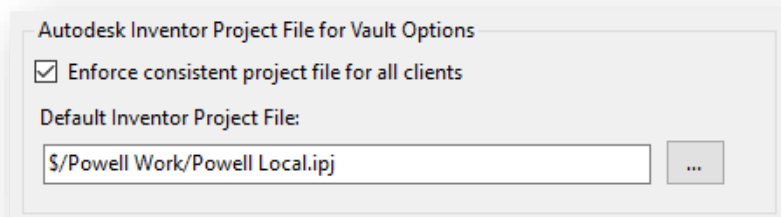
Custom Objects are new Vault entities created by the Vault admin to meet a very specific need for which a Vault tool does not already exist. A Custom Object definition refers to the type of entity being created, while Custom Object instances refer to individual items created using that definition. An example may be a Custom Object called Contacts, in which users may enter contact information for people involved in a specific project. Select Configure to create a new Custom Object definition, and assign it lifecycles, categories and properties.





Projects

When I talk about Projects in Vault, I am referring to two different things. The first would be setting up a default Inventor project, for those of you setting up Vault in an Inventor environment. As admin, you can choose to enforce a consistent project file for all users and specify the location of that project in the Vault. Users must download a copy of this project file onto their workstations and place it into the same path as specified by this setup. This is found under the Files Tab of Vault Settings, as seen in the above section.

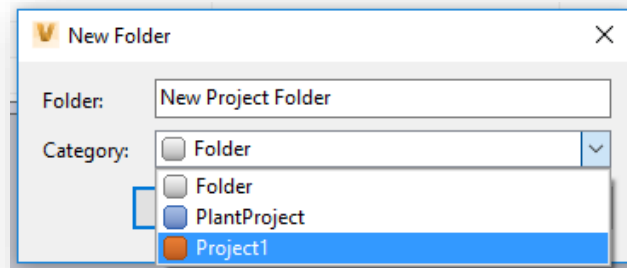


If the project file needs to be modified, it must first be checked out from the Vault. Using security setting, you can control who has permission to do this. If changes are made, the local copies of the project file would need to be refreshed, but this assures that all users will be using the same project settings. This may not make sense for every work environment, so you would have to determine if it works for you.

The second Project type in Vault, is a project folder. Vault lets you set up folders as projects to organize related data for easy access. Steps for doing this are:

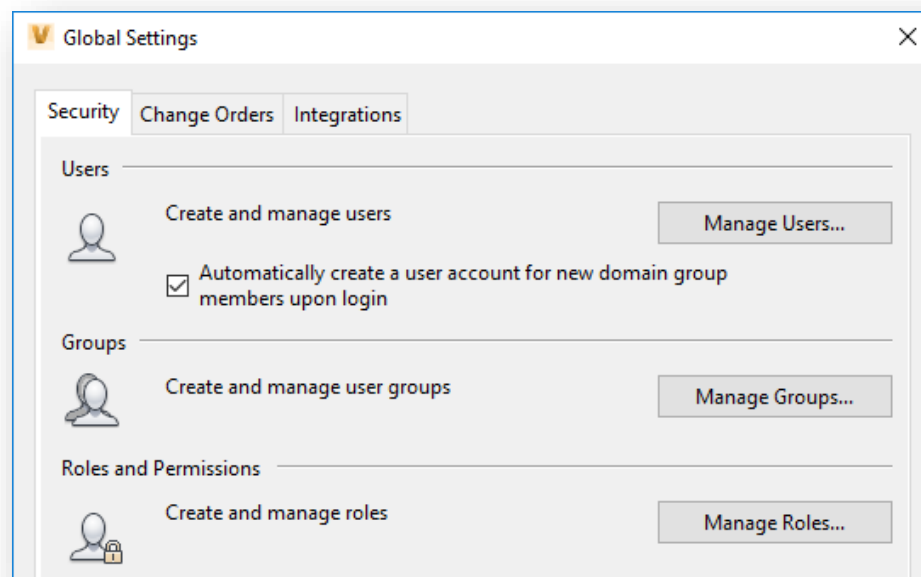
- Create a new Folder Category under Vault Settings. Give it a name and description that relates to your project intent and select a color for the folder.
- Find a location in your Vault Explorer that would make sense for the project.

- Create a new folder in this location and assign it to the folder category you created for the project. Name it so that it will be easily recognized.



- Add new data to the folder for your project or use links to existing data in other locations. Where links have been used, a shortcut to the data will be created in the project folder. In this way you can organize data from several locations into one project folder so it is easier to get to in the future.

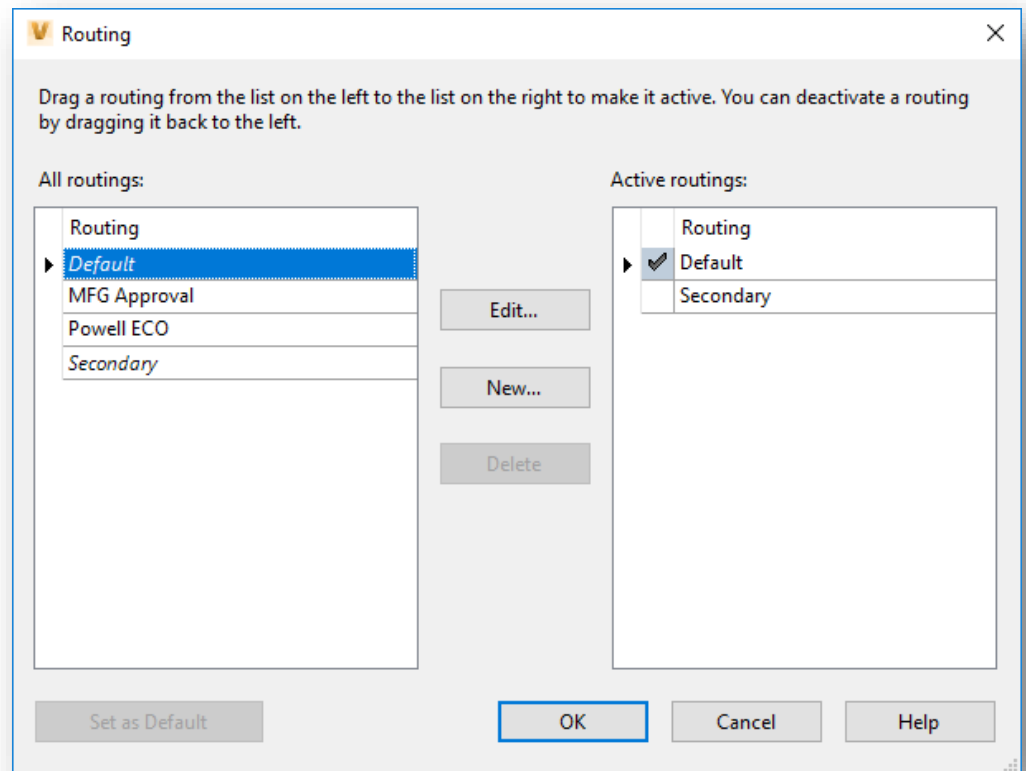
Global Settings



As Mark has already discussed the Security tab in his segment on Users, Groups & Roles way up top.... I will not repeat what he said so well.

Change Orders

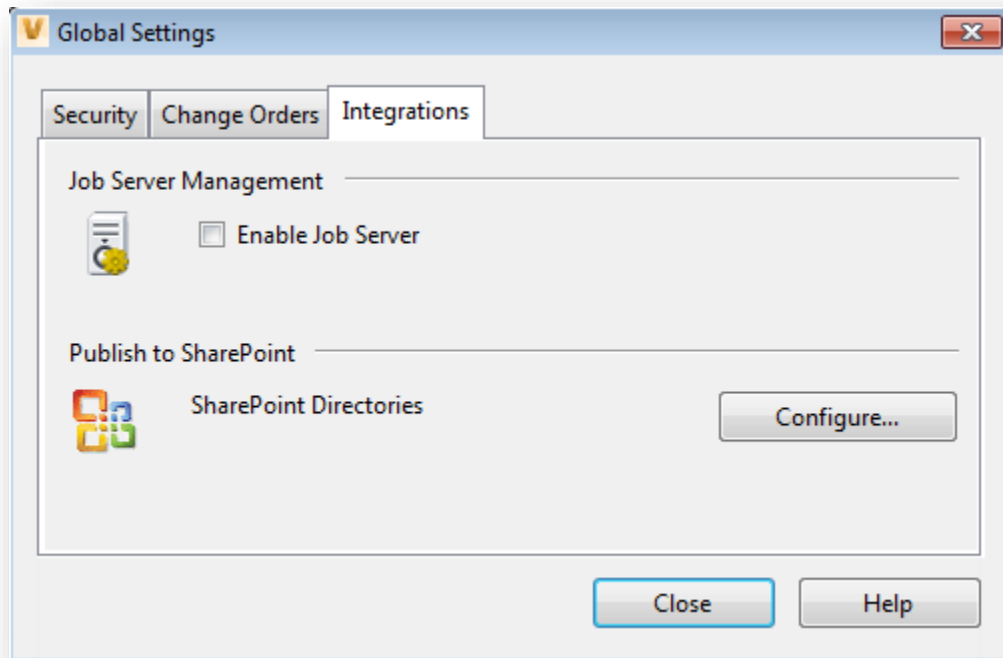
On this tab in Global Settings, the Admin can define and activate routing lists for change orders in Vault Professional.



In creating or editing a routing, the Admin adds users names to the list and assigns to them the roles they will need to carry out their part in the change order process. By dragging a routing definition to the right column, it becomes active and is available for use on a change order. This can be helpful for having change orders being performed by different teams in the organization, or for when someone is on vacation. The default routing will be assigned to a change order when it is created, and can be changed at that time, or at any point in the ECO life cycle, by editing the routing.

Select from one of two workflow definitions, either standard or with a check state required.

Integrations



Job Server Management

Administrator must check this to enable the job server so that it can be used to process jobs.

Publish to SharePoint

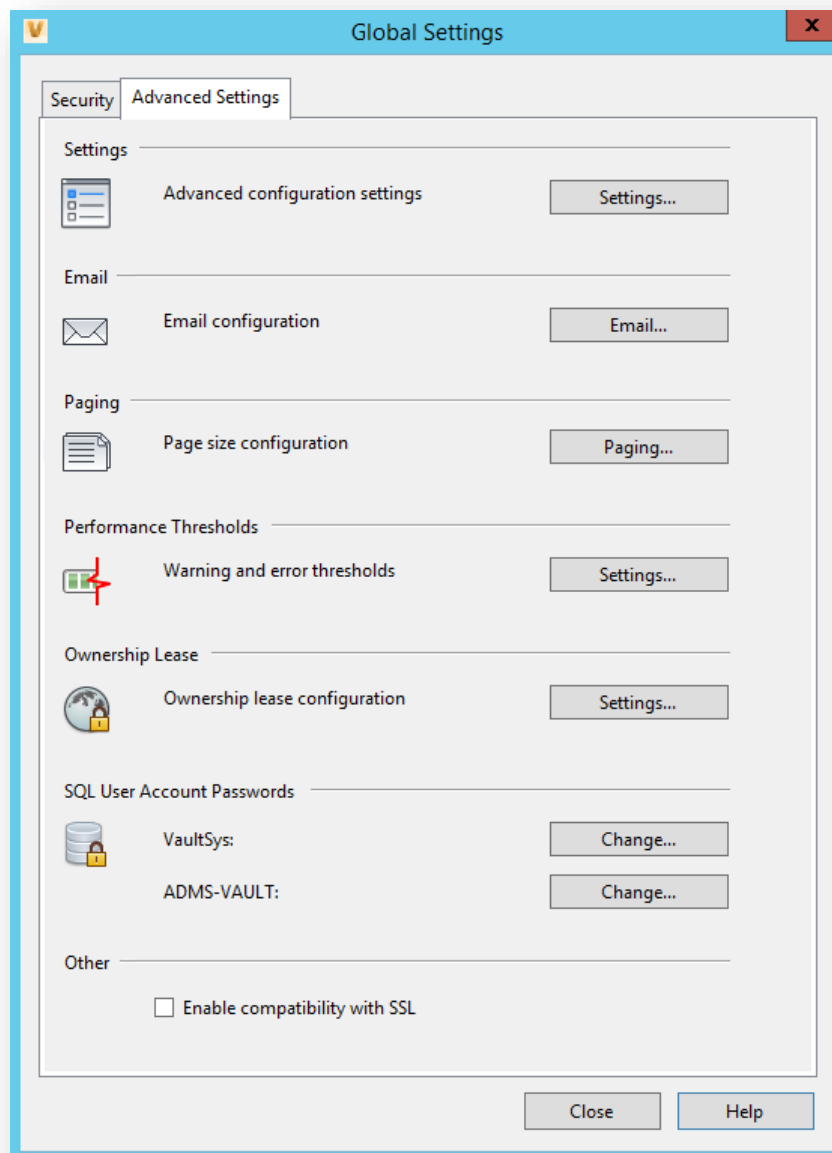
Use configure to setup publishing options to SharePoint directories. For more information on the integration of Vault & SharePoint, here are some helpful links. The first is a tale of my own integration back in 2014. It's a little dated, but still valid.

[My Journey Into Darkness](#)

[From Autodesk Knowledge Network](#)

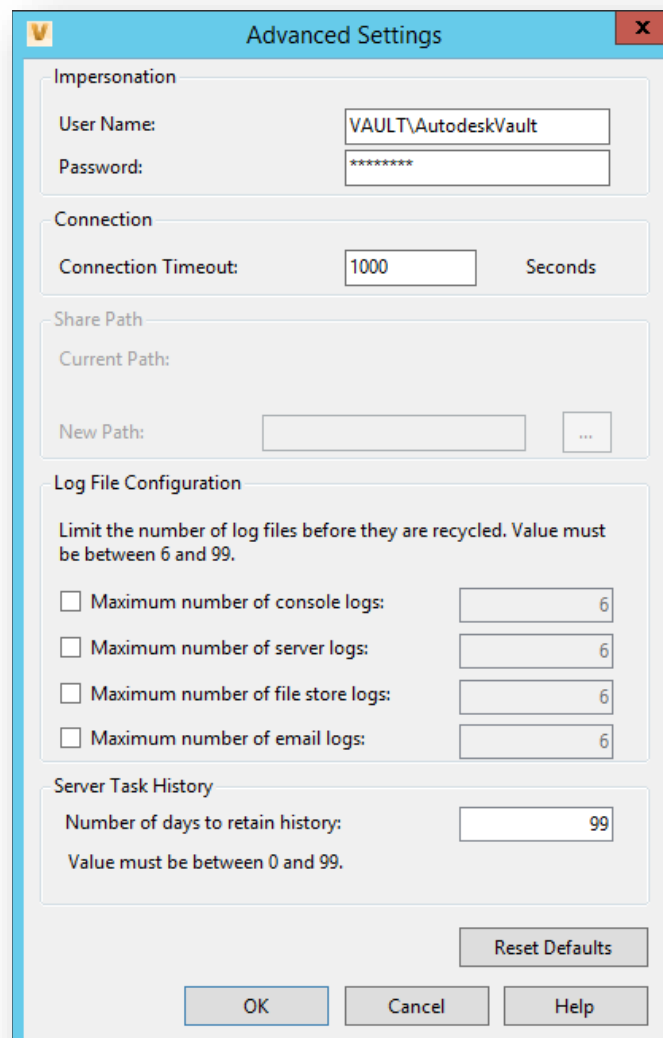
Global Settings – ADMS

On your Vault server, in the Autodesk Data Management Server (ADMS), there is another Global Settings menu that we wanted to bring to your attention. In the ADMS console, select Tools\Administration. The first tab – Security, is exactly the same as this tab on the Global Settings menu found in Vault Client. It used to create and manage Users, Groups & Roles.



On the Advanced Settings tab, there are some tools that are not found in Vault Client. Let's walk through them.

Advanced Configuration Settings



Advanced Settings

Impersonation

User Name: VAULT\AutodeskVault

Password: *****

Connection

Connection Timeout: 1000 Seconds

Share Path

Current Path:

New Path: ...

Log File Configuration

Limit the number of log files before they are recycled. Value must be between 6 and 99.

☐ Maximum number of console logs: 6

☐ Maximum number of server logs: 6

☐ Maximum number of file store logs: 6

☐ Maximum number of email logs: 6

Server Task History

Number of days to retain history: 99

Value must be between 0 and 99.

Reset Defaults

OK Cancel Help

Impersonation

This is the account that Vault uses for the web services, to communicate to and from the file store, and to and from the local Vault configuration files. The default user name is AutodeskVault, but can be set to a Domain account, and the password can also be set or changed.

Connection Timeout

To increase the amount of time before the connection between server and client times out. This is helpful if the connection is timing out before large files can finish being transferred.

Share Path

This is used when Vault has been configured during installation to use a remote SQL instance. This type of configuration requires a shared network folder as a transition area, and can be set or changed here.

Log File Configuration

Set the number of log files to retain on the server. The minimum is 6, and the maximum is 99.

Email Configuration

Vault can send emails to users identified on an ECO routing, during state changes. Use this tab to set up the email SMTP Server and to send test emails.

Page Size Configuration

Use this to set the number of rows of data displayed on each page in the Vault. A lower number can be used to increase performance. This number must be between 25 & 1000.

Performance Thresholds

Set the number of files to be processed at which a user will get a warning or error.

Ownership Lease

Determines the default length of an ownership lease. This is the length of time, when a user in a connected workgroup takes ownership of an object, before any other user can take or request ownership.

SQL User Account Passwords

Used to modify the passwords to the SQL accounts from the defaults used during installation.

Note: With any Password changes in Vault settings, make a copy of the new password and place it in a safe location.

Other

Use the checkbox to enable SSL compatibility if your IIS server is configured to use SSL (Secure Sockets Layer) security.

Adding Data to the Vault

Now that you have configured your Vault settings the way you want them, and have added your users, groups and set permissions, it is time to get your data into the Vault. There are several ways to do that. The preferred method is to check in your files from the CAD application, using the **Vault Add Ins**. Doing this will assure that all file references, data links and associated files are kept together. While it is possible to add files from within the Vault client, or even drag and drop files or folders to the Vault, these methods will not retain any file references or links. Opening an Inventor assembly, for example, after using one of these methods, will likely lead to missing component references.

If you are at this stage of the game, however, you are probably looking at adding a large quantity of files to your new Vault. Using the Add Ins for this could take weeks or months. The temptation to drag and drop will be strong. As the voice of experience.... Don't do it.

For large quantities of files, you will probably want to look at using **Autoloader**. This is a tool specifically designed for bulk adding files to the Vault. As the files are being loaded, they are copied to a temporary location first. Any file resolution errors are addressed, the files are organized... and then uploaded to the Vault.

There are some important System Requirements for this, and recommendations for using this system. It's important to get this right since you are dealing with large amounts of data. I would strongly recommend that you make a good backup of the files you will be moving before attempting this. [This Document](#) from the Autodesk Knowledge Network does a great job of explaining the use of Autoloader, and I suggest reading it through and following it carefully if you use this tool.

In Conclusion....

Well, Mark and I have crammed a lot of knowledge into you. How you put this all together for your Vault setup depends on how you want to use Vault in your organization. I strongly recommend (always), have a testing environment set up that includes a copy of your Vault Server and a Client machine. This way you can set things up and test them, tweak them or dump them altogether before going into a live environment with your users.

Make use of the [Autodesk Community](#), the [Knowledge Network](#), [Forums](#) and look for Autodesk Vault all over social media. Mark, myself, Irvin Hayes Jr. and many others are out there watching for your questions and ready to help in any way that we can.

Thank you for attending this class!