SD226750

# Managing CAD and BIM Standards Using Vault

Bobby Henry
Toll Brothers Inc.

Carl Smith
IMAGINiT Technologies

## Learning Objectives

- Learn how to create custom user groups, file categories, and file lifecycles to support standards management
  - Vault Configuration
- Learn how to configure products such as AutoCAD, Revit, and Inventor to look at Vault for the latest standards
  - Product Configurations
- Discover workflows for modifying, testing, and deploying standards
  - Workflows for Updating Content
- Learn how to set up workflows to automate rapid deployments of standards
  - Deployment Configuration

## Description

This course is designed to assist in utilizing Vault for managing company standards within your organization. It will cover how to set up custom file categories, file lifecycles, user groups to support an innovative way of managing company standards within Vault, along with tracking any changes. We will discuss how configure the primary products within the Autodesk collections to look at the new working folders for updates to standard content. Finally, we will learn how to automate deploying these changes to all users, so they will always have the latest and greatest content and standards as soon as they become available.

## Speakers

## Bobby Henry

Bobby Henry is an AutoCAD Certified professional with 18 years' experience in the residential home building industry. His field experience has help him develop a thorough knowledge base of construction materials, applications, and building methodology. He now currently works for Toll Brothers, Inc. as the Asst. CAD Manager helping support their architectural department to resolve user issues and create solutions to problems from changes in workflows or product changes. He also leads various projects ranging from implementing new software releases, proof of concepts, and new Autodesk software.

bhenry@tollbrothers.com

## Carl Smith

Carl Smith is an Autodesk certified instructor, sought after speaker, and blogger. His analytical abilities and problem-solving expertise have made him a key member of many successful teams, particularly in the manufacturing and electro-mechanical engineering industries. Working as lead consultant, project manager and head trainer, Carl has in-depth knowledge of Autodesk products and their application in manufacturing plants across the U.S.

csmith@rand.com

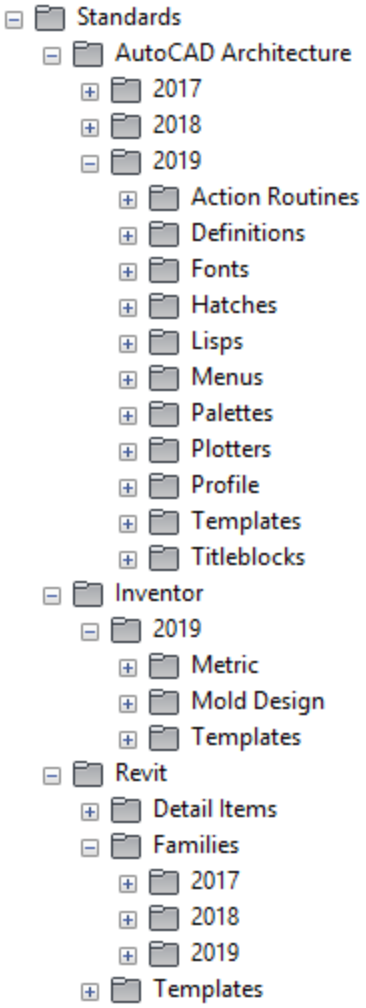

# Contents

## Vault Configuration

The Vault Data Management software helps designers and engineers organize design data, manage documentation, and track revisions along with other development processes. But it can also be configured to manage a companies' standard content allowing updates on users' machines to be controlled with precision and a level of automation that even network locations cannot accommodate. Let's go over some of the foundational aspects to achieving this.

### Folder Structure

With the dynamic needs and requirements from company to company based on the products that they use; an ideal folder structure can only be determined by you. But, I will list some basics below to help get you mind thinking of how you might be able to better manage any existing and future content that you would like to manage in Vault.




### Product Types and Versions

If you manage multiple versions of the same product, then you might want to segregate content based on the product versions. A prime example of this would be if you work with outside consultants or vendors and maintain 2 product versions for backwards compatibility, like AutoCAD 2017 and AutoCAD 2018. This would allow you to have support any product specific content without any conflictions with newer content that has been modified or upgraded due to a drawing format change like there was in 2018. This same concept applies for things like Revit families where you may want to keep a subset of folders for each year so that any existing projects that was developed, and needs to stay within, in a certain product version will have version specific content available.

### Content Types

There may be scenarios when you may want to group some content by the product/year/type and then other times by product/type/year. That is dependent on the what works best for the company and the software that must be managed. Think ahead on how the content will be used and how user friendly the structure is as well.

### User Groups

Groups have roles and permissions assigned to them that define which actions they can take, and which vaults they can access. You can create groups of users, assign roles and permissions to the group, and even add other groups as a sub-group. As a member of a group, a user has all the permissions and roles assigned to the group. When you add sub-groups to a primary group, it allows the users to have the same roles and permissions as multiple groups simultaneously. It is best practice to assign users to a group as much as possible rather than giving them permissions to a specific folder location.

Although groups can be disabled, Vault will not allow them to be deleted or removed. So, it is important to plan out what groups you will need to create and the usage of each one. By assigning users to groups and then granting folder membership to those groups, you can easily manage users and their access to vault folders. This is the best practice for creating a Vault security model. Below, we will review some base groups that will aid in managing and testing changes to standard content. Treat this list as an example or guide because your groups will vary depending on the requirement or workflows specific to the company.

### Support Team

User(s) that will be making modifications to the standards or content will need to be assigned to this group. It will give them full control to make changes, approve, and even delete files that may no longer be needed.

### Pilot Team

When there is a need to perform any testing to the standards or content, users can be assigned to this group to allow them to have the Read permission on files that are in alpha or beta stage. They will be allowed to get the files and verify that they work as intended.

### Standards Editor

Sometimes you want to get a subject material expert (SME) to make modifications to standards or content without the ability to finalize the content and creating this group will help you to do just that. It will also allow you to isolate who is making changes to company standards while having the ability to delegate the task of updating content to selected members.

### Template Editor

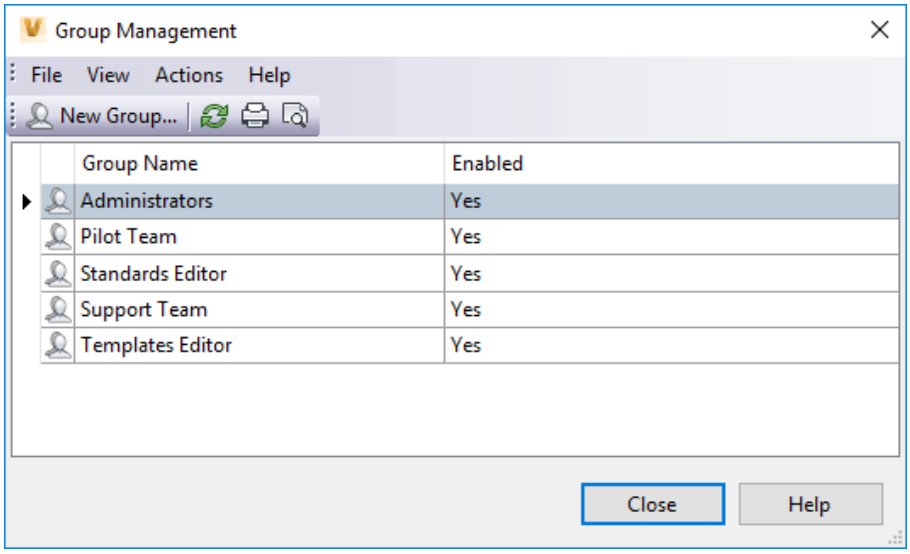
If you only allow specific user(s) to make changes to template files, then you may want to create this group. As with the Standards Editor above, it will also allow you to isolate who is making changes to company standards while having the ability to delegate the task of updating templates to selected members.

Before we get started on creating the groups, we should think about what actions they will be performing inside Vault and what are the proper roles to assign to them. This is majorly dependent on how your company operates, so what I list below are just logical suggestions based from what works well for me. Also, if you find that assigning the Support Team with administrative privileges is not best, then skip down to the Roles section prior to setting up that user group to save time while configuring these. If you are ok with them being administrators, then proceed the following steps to create each group that you have decided would be best to accommodate your company's workflow.

1. Select **Tools** ➤ **Administration** ➤ **Global Settings**
2. In the Global Settings dialog, select the **Security** tab
3. Click **Manage Groups…**
4. In the Group Management dialog box, click **New Group**
5. In the Group dialog box, specify the following settings for each group, then click **OK**
    a. Support Team:

   i. Group Name: *Support Team*
   ii. Role: *Administrator*
   iii. Vault: *(Your current production server)*
   iv. Group Members: *(Your Selected Members)*
b. Pilot Team:
   i. Group Name: *Support Team*
   ii. Role: *(Blank so user inherits pre-existing permissions)*
   iii. Vault: *(Your current production server)*
   iv. Group Members: *(Your Selected Members)*
c. Standards Editor:
   i. Group Name: *Support Team*
   ii. Role: *Document Editor (Level 2)*
   iii. Vault: *(Your current production server)*
   iv. Group Members: *(Your Selected Members)*
d. Template Editor:
   i. Group Name: *Support Team*
   ii. Role: *Document Editor (Level 2)*
   iii. Vault: *(Your current production server)*
   iv. Group Members: *(Your Selected Members)*

6. Click **Close**

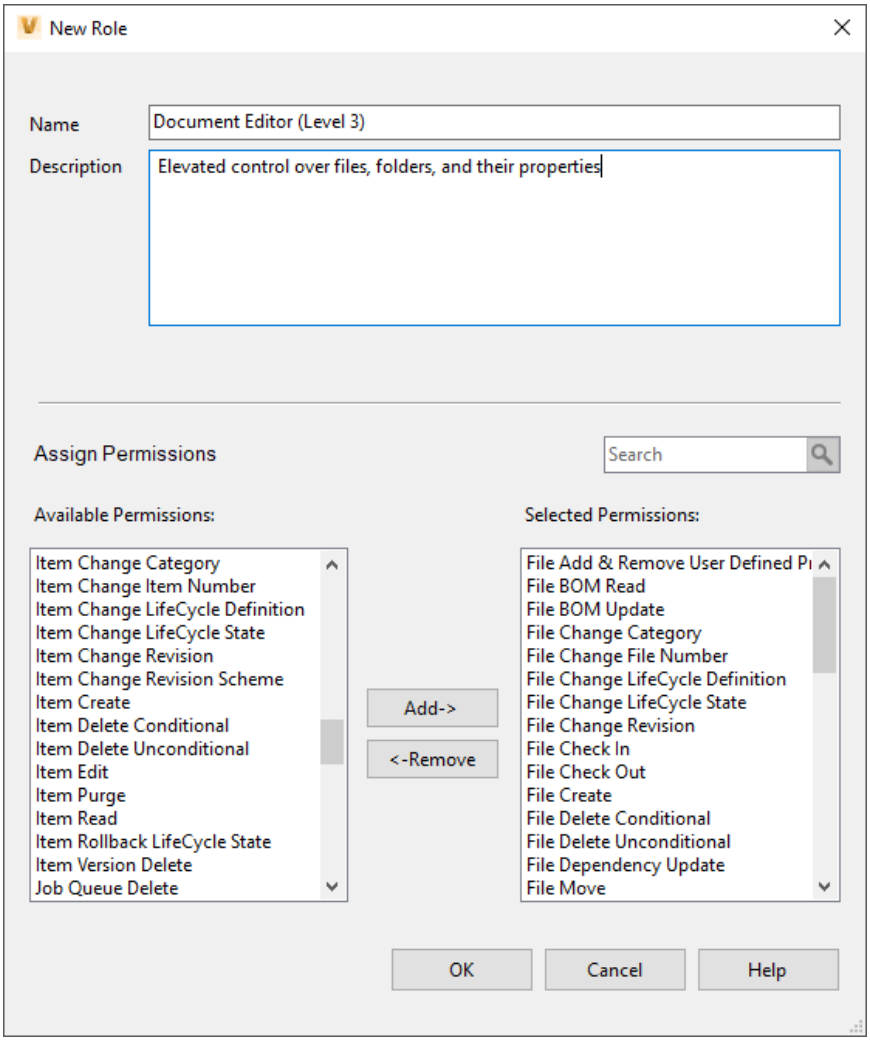



## Roles

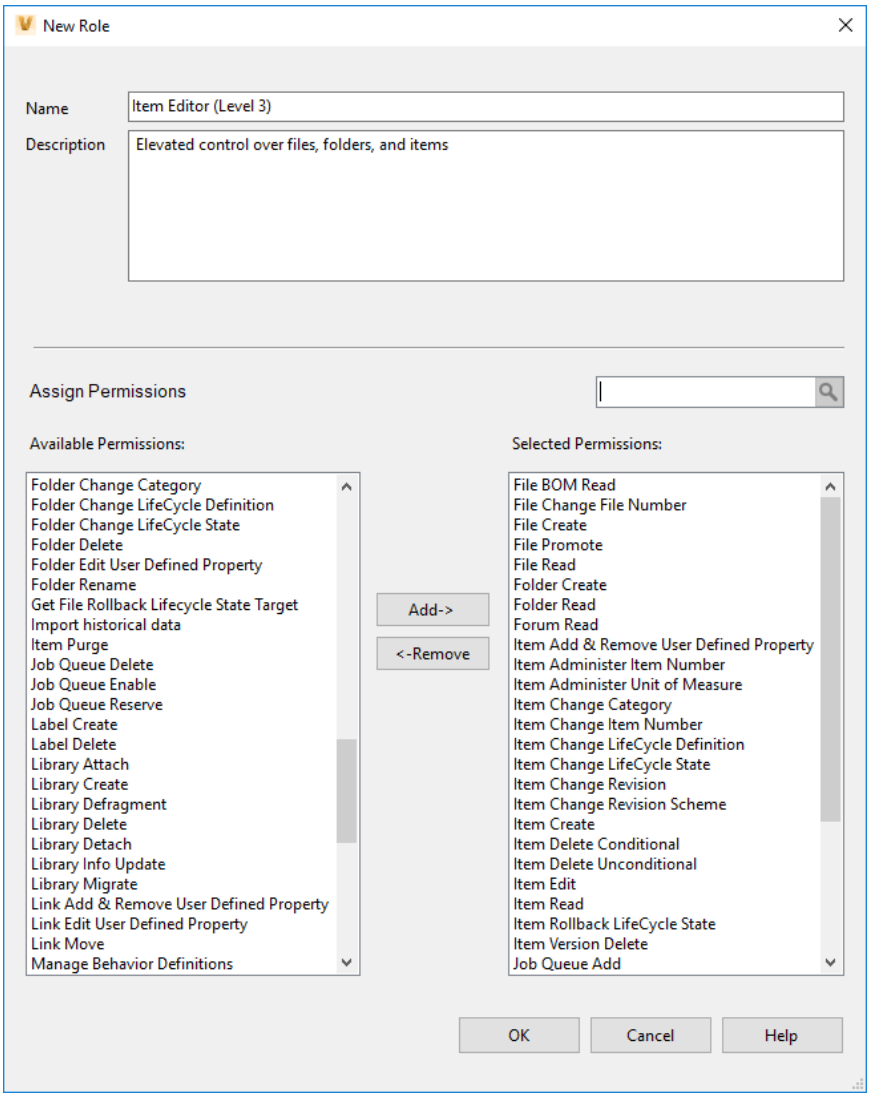
Vault 2019 has a new feature that has been highly requested for years now, which is the ability for administrators to create custom roles with a unique set of permissions that leverages elevated object permissions above the default roles.

One specific permission that I find very useful with managing company standards is the loving "File Delete Unconditional". A role with this permission allows support members to manage content at a lower risk than being members Administrators group and having full privileges. So, we will start by creating this new role now and adding that permission, along with some other useful permissions, that way the Support Group can efficiently manage the companies standard content throughout its' lifecycle.

1. Select **Tools** ➤ **Administration** ➤ **Global Settings**
2. In the Global Settings dialog, select the **Security** tab
3. Click **Manage Roles…**
4. In the Role Management dialog box, select the *"Document Editor (Level 2)"* role
5. Click **Copy**
6. For the Name, enter *"Document Editor (Level 3)"*
7. For the description, enter "*Elevated control over files, folders, and their properties*"
8. Under Available Permissions, select the following and click **Add**
   a. File Change Category
   b. File Change LifeCycle State
   c. File Change Revision
   d. File Delete Unconditional
   e. File Rollback LifeCycle State
   f. File Version Delete Unconditional
   g. Folder Change Category
   h. Folder Change LifeCycle State
9. Click **Add**, followed by **OK**



10. If you use Inventor and work with Items, then select the "*Item Editor (Level 2)*"
11. For the description, enter "*Elevated control over files, folders, and their properties*"
12. Under Available Permissions, select the following and click **Add**
    a. Item Administer Item Number
    b. Item Administer Unit of Measure
    c. Item Delete Unconditional
13. Click **Add**, followed by **OK**
14. Click **Close**



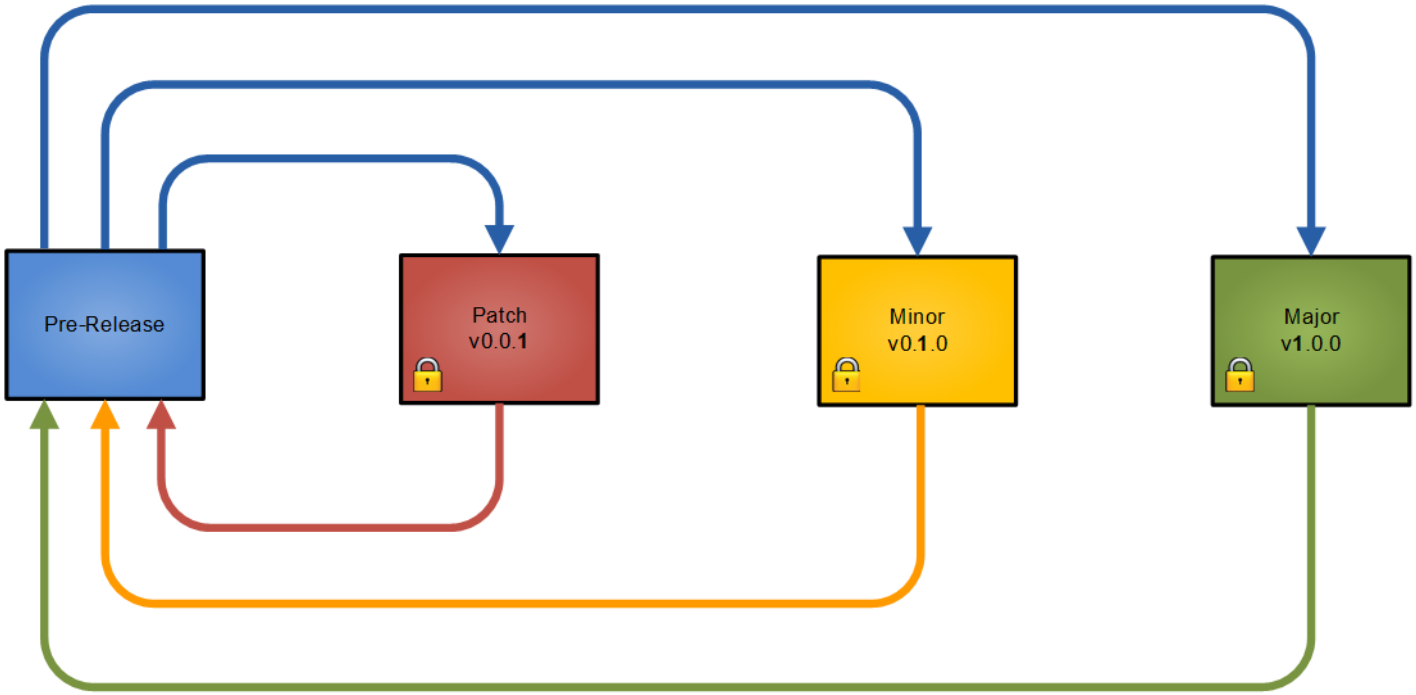

## Lifecycles and States

A lifecycle definition is an engine that can be configured to automatically assign security, behaviors, and properties to Vault objects based on where the object is in the life of the design process. It uses states to identify the object's status in the lifecycle. Examples of states are Work in Progress, For Review, or Released. An object moves from one state to another based on the lifecycle definition's transition rules. These transition rules determine when the state change happens, if it can occur manually or automatically (or both), based on criteria determined by the administrator. The lifecycle definition also determines if any other automatic behaviors occur based on a state change. The Change State dialog does not support more than one entity type at a time. For example, the user cannot change state on a file and folder at the same time.

### Standards Lifecycle

The file lifecycle that we will be creating to apply to all files and items is based on the Semantic Versioning system [1], also known as SemVer. This has become a very popular due to its simplistic yet effective method and

will allow us to efficiently track changes made to file and item standards. This is due to SemVer being a 3-component system in the format of x.y.z where x stands for a major version, y stands for a minor version, and z stands for a patch. So, the result is Major.Minor.Patch. I have added a "Pre-Release" state that allows for members of the Pilot Team to be able to test the software and validate there is no bugs present prior to releasing it to whole company.



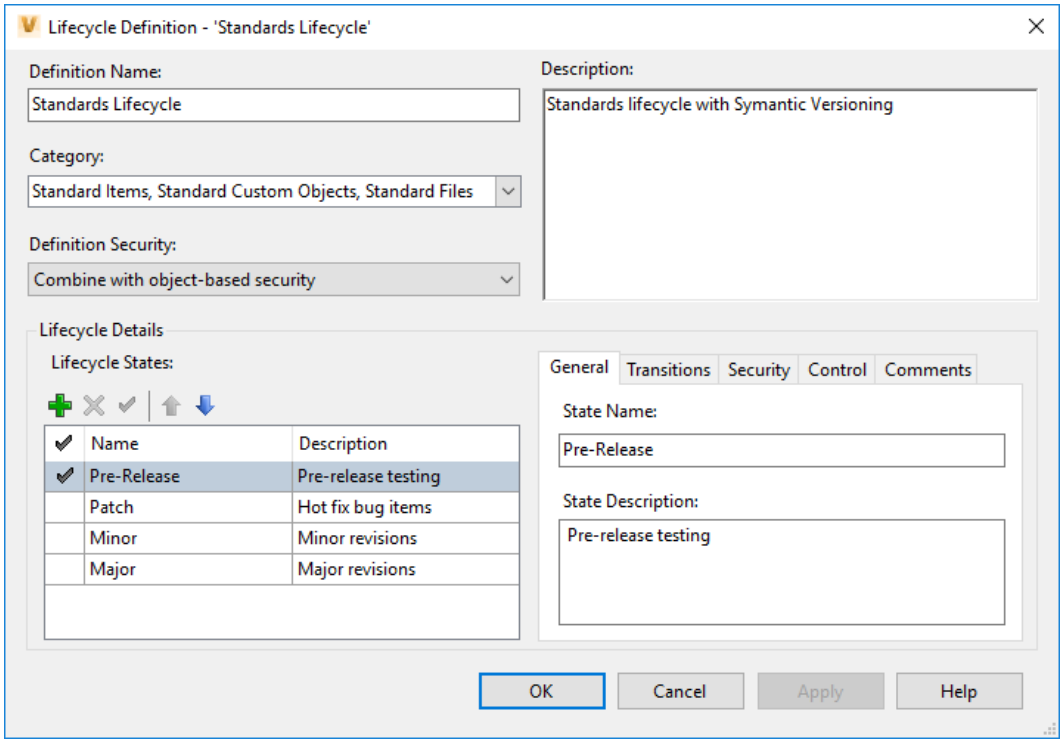

1. Click **Tools** ➤ **Administration** ➤ **Vault Settings**
2. On the Vault Settings dialog box, select the **Behaviors** tab ➤ **Lifecycles**
3. Click **New** to launch the Lifecycle Definition - New Definition dialog box
4. In the Definition Name field, enter "*Standards Lifecycle*"
5. Do not select any categories at this time because those will be applied as we create the categories
6. In the Description field, enter "*Standards lifecycle with Symantic Versioning*"
7. We will keep the Definition Security as the default "*Combine with object-based security*". This will create a dual-gate system that will allow us to control individuals access to our standards effectively without having to worry about a state-based security overriding the permissions we have on a standards folder.
8. Under Lifecycle Details, click the **Plus (+)** button to create the following lifecycle states in order:
    a. Pre-Release:
        i. State Name: *Pre-Release*
        ii. State Description: *Pre-Release testing*
    b. Patch:
        i. State Name: *Patch*
        ii. State Description: *Hot fix bug items*
    c. Minor:

   i. State Name: *Minor*
   ii. State Description: *Minor revisions*
d. Major:
   i. State Name: *Major*
   ii. State Description: *Major revisions*

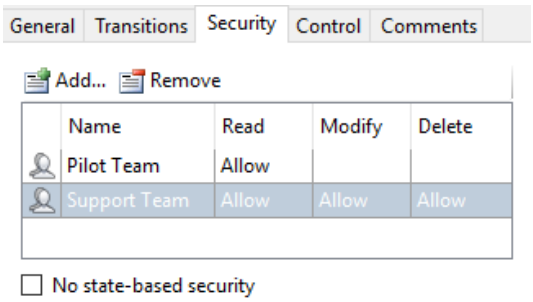
9. Once you have created these lifecycle states, select the "*Pre-Release*" lifecycle state in the Lifecycle Details list and click the **Checkmark** to set it as the default state for this lifecycle definition.

   NOTE: The order of the lifecycle states determines the order in which they are displayed in the Change State dialog. So, if you created them out of order, then you can reorder the states by selecting a state in the Lifecycle Details view and clicking the **Up** or **Down** arrow.

10. Click the **Apply** button to set the states

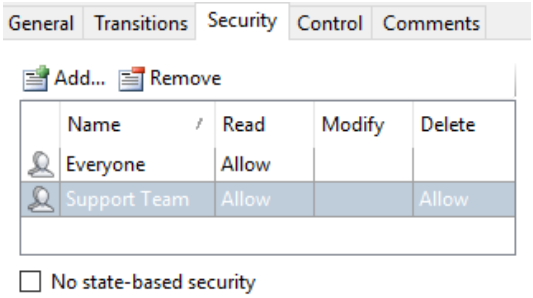



11. Select the "*Pre-Release*" lifecycle state, then:
    a. Click the **Security** tab
    b. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
    c. Under the Select Members From section, click the drop-down and choose **Groups**
    d. Select the "*Pilot Team*" and "*Support Team*", followed by clicking **Add…** then **OK**
    e. Set "*Pilot Team*" to have Allow permission for only "*Read*"
    f. Then set "*Support Team*" to have Allow permission for "*Read*", "*Modify*", and "*Delete*"




g. Click the **Control** tab
h. Check the "*This is a Released state*" toggle
i. Under Controlled versions (do not purge), click the "*All*" toggle
j. Click the **Comments** tab, followed by **Add…**
k. In the Enter Comments field, enter "*Issued for pre-release testing*"
l. Click **Ok**

12. Select the "*Patch*" lifecycle state, then:
    a. Click the **Security** tab
    b. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
    c. Under the Select Members From section, click the drop-down and choose **Groups**
    d. Select the "*Everyone*" and "*Support Team*", followed by clicking **Add…** then **OK**
    e. Set "*Everyone*" to have Allow permission for only "*Read*"
    f. Then set "*Support Team*" to have Allow permission for "*Read*" and "*Delete*"




g. Click the **Control** tab
h. Check the "*This is a Released state*" toggle
i. Under Controlled versions (do not purge), click the "*All*" toggle
j. Click the **Comments** tab, followed by **Add…**
k. In the Enter Comments field, enter "*Hotfix Revision*"
l. Click **Ok**

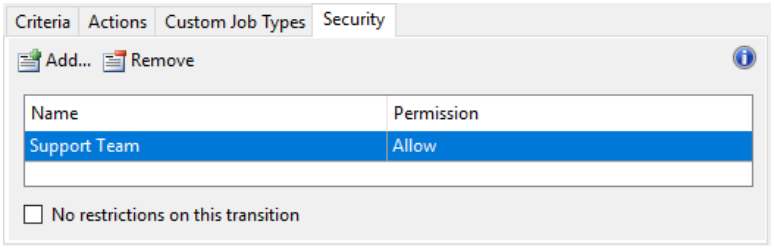
13. Select the "*Minor*" lifecycle state, then:
    a. Repeat steps 12.a through 12.i
    b. Click the **Comments** tab, followed by **Add…**
    c. In the Enter Comments field, enter "*Minor Revision*"
    d. Click **Ok**

14. Select the "*Major*" lifecycle state, then:
    a. Repeat steps 12.a through 12.i
    b. Click the **Comments** tab, followed by **Add…**
    c. In the Enter Comments field, enter "*Major Revision*"
    d. Click **Ok**
15. When finished, click **Apply**

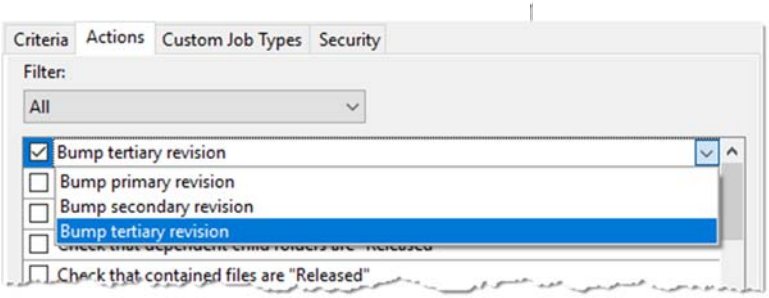
Now comes a very monotonous part, which is setting the Actions and Security for Lifecycle State as well as each available transition per. The primary goal is to only allow members of the "*Support Team*" to be able to change states, only members of the "*Pilot Team*" see the files in the "*Pre-Release*" state, and then allow "*Everyone*" to see the files in any approved state. We will also want to set the appropriate "*Bump Revision*" action for transitions that are leaving the "*Pre-Release*" state.

NOTE: Although you do not have to duplicate work on states you had previously done, it is best practice to work from top to bottom and verify that everything was setup properly. For example, if you are configuring the "*Pre-Release*" lifecycle state and change the "*Pre-Release to Patch*" transition, this will also change the "*Pre-Release to Patch*" transition under the "*Patch*" lifecycle state. So, let's get started.

16. Click the "*Pre-Release*" lifecycle state, then:
    a. Click the **Transitions** tab
    b. Do the following for the "*Pre-Release from Patch*", "*Pre-Release from Minor*", and "*Pre-Release from Major*" transitions:
        i. Select the transition, then click **Edit…** to open the Transition dialog box
        ii. Click the **Security** tab
        iii. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
        iv. Under the Select Members From section, click the drop-down and choose **Groups**
        v. Select the "*Support Team*", followed by clicking **Add…** then **OK**
        vi. The "*Support Team*" will be given the Allow permission by default
        vii. Click **OK**

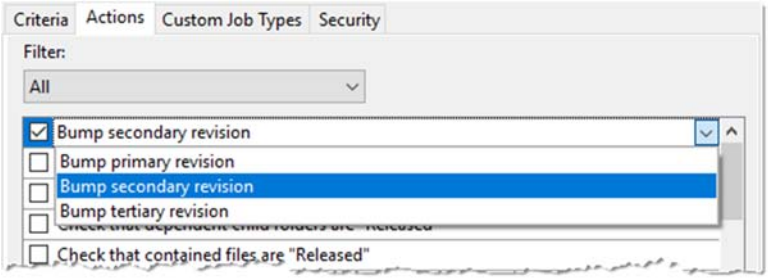



    c. Back under the Transitions tab, select the "*Pre-Release to Patch*" transition, then:
        i. Click **Edit…** to open the Transition dialog box
        ii. Click the **Actions** tab
        iii. Check the "*Bump primary revision*"
        iv. Click the drop-down button and select "*Bump tertiary revision*"



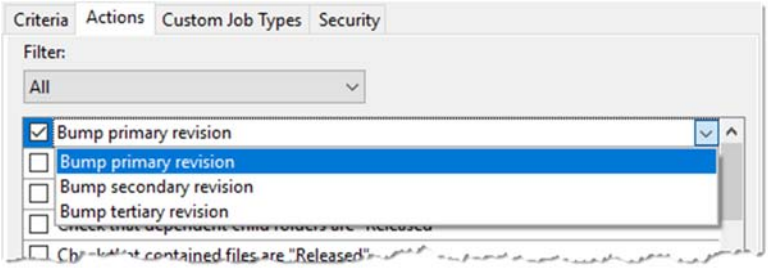

v. Click the **Security** tab and repeat steps 16.b.iii through 16.b.vii

d. Back under the Transitions tab, select the "*Pre-Release to Minor*" transition, then:
   i. Click **Edit…** to open the Transition dialog box
   ii. Click the **Actions** tab
   iii. Check the "*Bump primary revision*"
   iv. Click the drop-down button and select "*Bump secondary revision*"




   v. Click the **Security** tab and repeat steps 16.b.iii through 16.b.vii

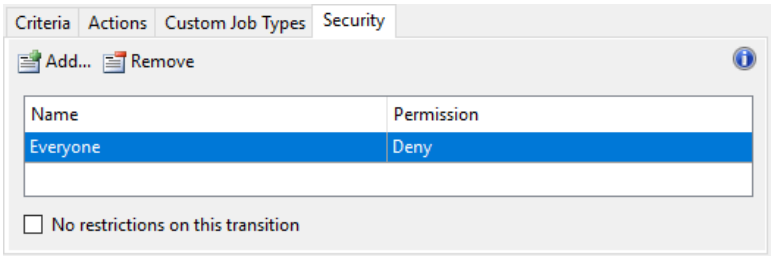
e. Back under the Transitions tab, select the "*Pre-Release to Major*" transition, then:
   i. Click **Edit…** to open the Transition dialog box
   ii. Click the **Actions** tab
   iii. Check the "*Bump primary revision*"
   iv. Click the drop-down button and select "*Bump primary revision*"




   v. Click the **Security** tab and repeat steps 16.b.iii through 16.b.vii

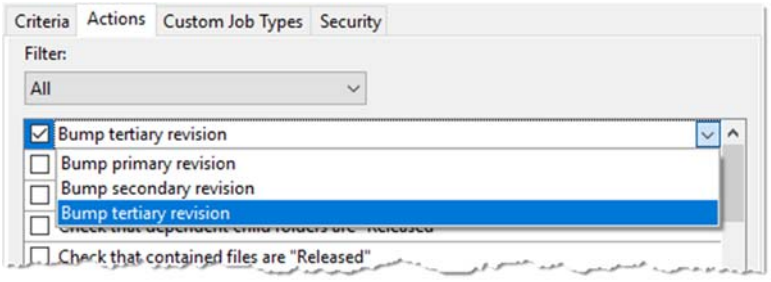
17. Click the "*Patch*" lifecycle state, then:
    a. Click the **Transitions** tab
    b. Do the following for the "*Patch to Minor*", "*Patch to Major*", "*Patch from Minor*", and "*Patch from Major*" transitions:
       i. Select the transition, then click **Edit…** to open the Transition dialog box
       ii. Click the **Security** tab

iii. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
iv. Under the Select Members From section, click the drop-down and choose **Groups**
v. Select the "*Everyone*", followed by clicking **Add…** then **OK**
vi. Change the "*Everyone*" groups permission to "*Deny*"
vii. Click **OK**



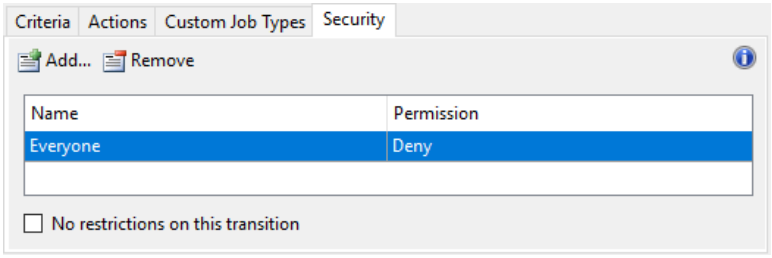

NOTE: The reason why we want to do this is to prevent from jumping between released states. There should never be a reason why you want to bypass testing the files in the "*Pre-Released*" states. But if you find that you would like to allow this, then just follow the steps listed in 16.b and allow for the "*Support Team*" to make the transitions only.

c. Back under the Transitions tab, verify the following is the same for both the "*Patch to Pre-Release*" and "*Patch from Pre-Release*" transitions:
   i. Click **Edit…** to open the Transition dialog box
   ii. Click the **Actions** tab
   iii. Check the "*Bump primary revision*"
   iv. Click the drop-down button and select "*Bump tertiary revision*"



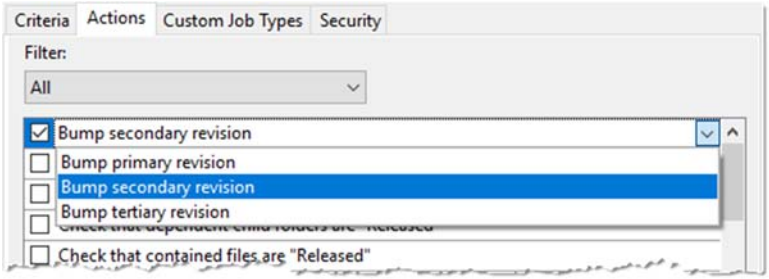

18. Click the "*Minor*" lifecycle state, then:
    a. Click the **Transitions** tab
    b. Do the following for the "*Minor to Major*", "*Minor to Patch*", "*Minor from Major*", and "*Minor from Patch*" transitions:
       i. Select the transition, then click **Edit…** to open the Transition dialog box
       ii. Click the **Security** tab
       iii. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
       iv. Under the Select Members From section, click the drop-down and choose **Groups**
       v. Select the "*Everyone*", followed by clicking **Add…** then **OK**

vi. Change the "*Everyone*" groups permission to "*Deny*"
vii. Click **OK**

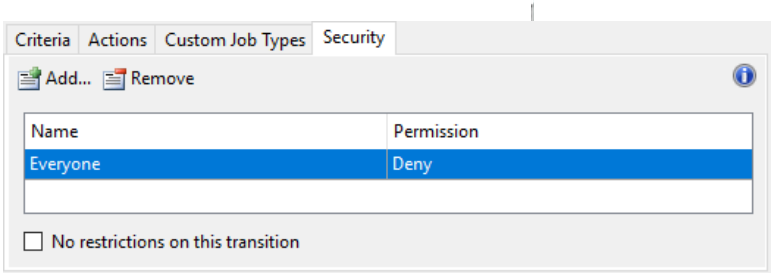



NOTE: The reason why we want to do this is to prevent from jumping between released states. There should never be a reason why you want to bypass testing the files in the "*Pre-Released*" states. But if you find that you would like to allow this, then just follow the steps listed in 16.b and allow for the "*Support Team*" to make the transitions only.

c. Back under the Transitions tab, verify the following is the same for both the "*Minor to Pre-Release*" and "*Minor from Pre-Release*" transitions:
   i. Click **Edit…** to open the Transition dialog box
   ii. Click the **Actions** tab
   iii. Check the "*Bump primary revision*"
   iv. Click the drop-down button and select "*Bump secondary revision*"

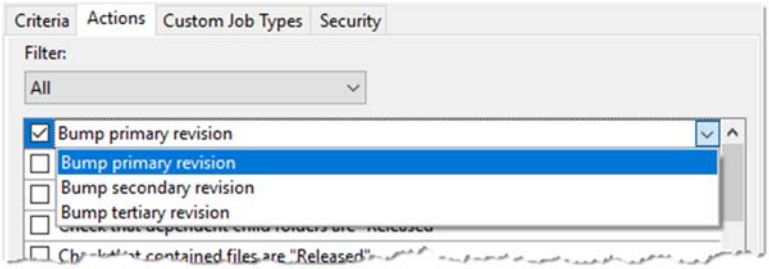



19. Click the "*Major*" lifecycle state, then:
    a. Click the **Transitions** tab
    b. Do the following for the "*Major to Minor*", "*Major to Patch*", "*Major from Minor*", and "*Major from Patch*" transitions:
       i. Select the transition, then click **Edit…** to open the Transition dialog box
       ii. Click the **Security** tab
       iii. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
       iv. Under the Select Members From section, click the drop-down and choose **Groups**
       v. Select the "*Everyone*", followed by clicking **Add…** then **OK**
       vi. Change the "*Everyone*" groups permission to "*Deny*"
       vii. Click **OK**




NOTE: The reason why we want to do this is to prevent from jumping between released states. There should never be a reason why you want to bypass testing the files in the "*Pre-Released*" states. But if you find that you would like to allow this, then just follow the steps listed in 16.b and allow for the "*Support Team*" to make the transitions only.

c. Back under the Transitions tab, verify the following is the same for both the "*Major to Pre-Release*" and "*Major from Pre-Release*" transitions:
   i. Click **Edit…** to open the Transition dialog box
   ii. Click the **Actions** tab
   iii. Check the "*Bump primary revision*"
   iv. Click the drop-down button and select "*Bump primary revision*"



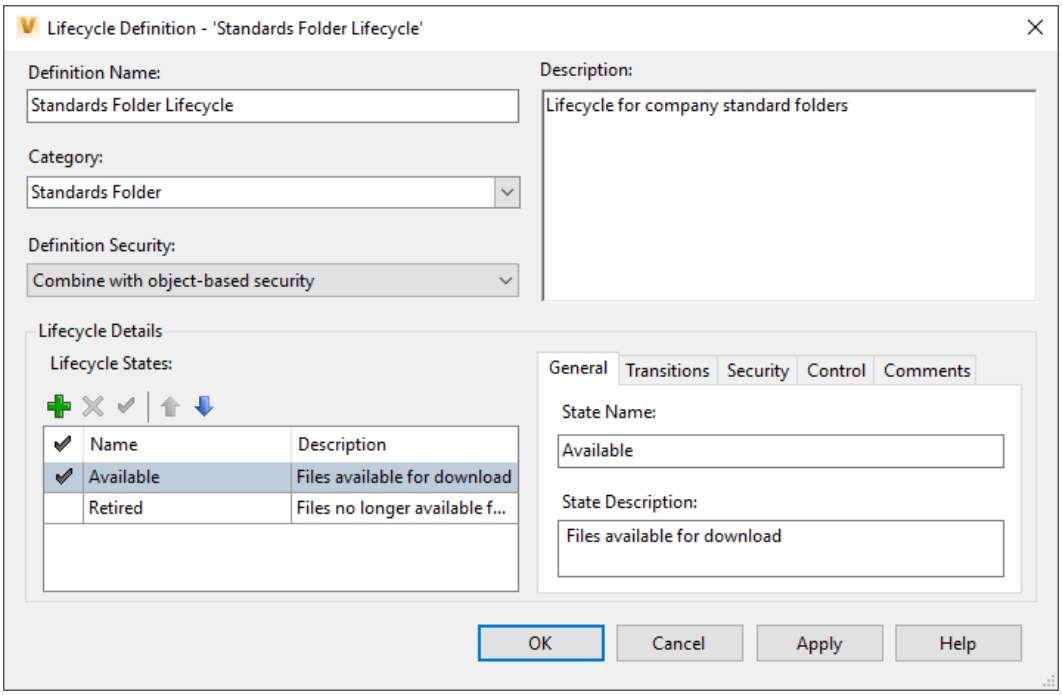

20. When finished, click **Apply**

## Standards Folder Lifecycle

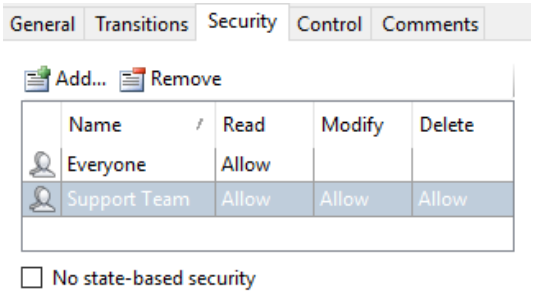
The folder lifecycle that we will be creating to apply to all standards folders will allow for the folder to be visible when the files are in production and invisible when they no longer are. This is achieved by creating two states; Available and Retired. When in the Available states, everyone will be able to see the parent folder, all sub-folders, and any files within this location. Once you switch the folder to the Retired state, the parent folder, all sub-folders, and any files within this location will be hidden.

1. Click **Tools** ➤ **Administration** ➤ **Vault Settings**
2. On the Vault Settings dialog box, select the **Behaviors** tab → **Lifecycles**
3. Click **New** to launch the Lifecycle Definition - New Definition dialog box
4. In the Definition Name field, enter "*Standards Folder Lifecycle*"
5. Do not select any categories at this time because those will be applied as we create the categories
6. In the Description field, enter "*Lifecycle for company standard folders*"
7. We will keep the Definition Security as the default "*Combine with object-based security*". This will create a dual-gate system that will allow us to control individuals access to our standards effectively without having to worry about a state-based security overriding the permissions we have on a standards folder.
8. Under Lifecycle Details, click the **Plus (+)** button to create the following lifecycle states in order:
    a. Available:
        i. State Name: *Available*
        ii. State Description: *Files available for download*
    b. Retired:
        i. State Name: *Retired*
        ii. State Description: *Files no longer available for download*
9. Once you have created these lifecycle states, select the "*Available*" lifecycle state in the Lifecycle Details list and click the **Checkmark** to set it as the default state for this lifecycle definition.

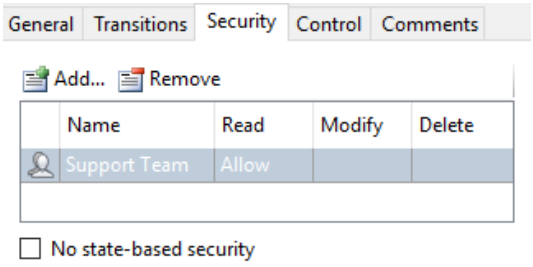
    NOTE: The order of the lifecycle states determines the order in which they are displayed in the Change State dialog. So, if you created them out of order, then you can reorder the states by selecting a state in the Lifecycle Details view and clicking the **Up** or **Down** arrow.
10. Click the **Apply** button to set the states



11. Select the "*Available*" lifecycle state, then:
    a. Click the **Security** tab
    b. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
    c. Under the Select Members From section, click the drop-down and choose **Groups**
    d. Select "*Everyone*" and "*Support Team*", followed by clicking **Add…** then **OK**
    e. Set "*Everyone*" to have Allow permission for only "*Read*"
    f. Then set "*Support Team*" to have Allow permission for "*Read*", "*Modify*", and "*Delete*"



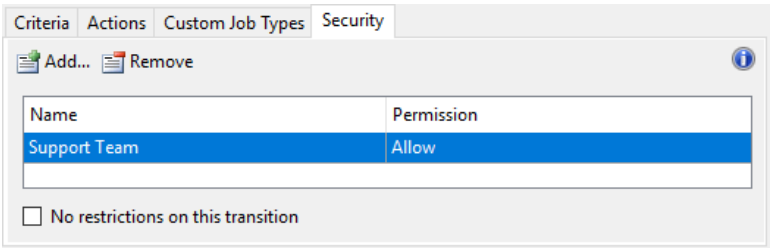

    g. Click the **Control** tab
    h. Check the "*This is a Released state*" toggle
    i. Under Controlled versions (do not purge), click the "*All*" toggle
    j. Click the **Comments** tab, followed by **Add…**
    k. In the Enter Comments field, enter "*Files available for download*"
    l. Click **Ok**
12. Select the "*Retired*" lifecycle state, then:
    a. Click the **Security** tab
    b. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
    c. Under the Select Members From section, click the drop-down and choose **Groups**
    d. Select "*Support Team*", followed by clicking **Add…** then **OK**
    e. Set "*Support Team*" to have Allow permission for only "*Read*"



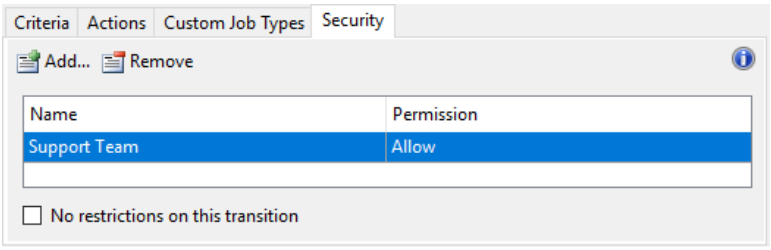

    f. Click the **Control** tab
    g. Under Controlled versions (do not purge), click the "*All*" toggle
    h. Click the **Comments** tab, followed by **Add…**
    i. In the Enter Comments field, enter "*Files no longer available for download*"
    j. Click **Ok**

Now we are back to that monotonous part again, but it won't be as bad this time. Our primary goal is to only allow members of the "*Support Team*" to be able to change states and then allow "*Everyone*" to see the files when they are available.

13. Click the "*Available*" lifecycle state, then:
    a. Click the **Transitions** tab
    b. Do the following for both the "*Available to Retired*" and "*Available from Retired*" transitions:
        i. Select the transition, then click **Edit…** to open the Transition dialog box
        ii. Click the **Security** tab
        iii. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
        iv. Under the Select Members From section, click the drop-down and choose **Groups**
        v. Select the "*Support Team*", followed by clicking **Add…** then **OK**
        vi. The "*Support Team*" will be given the Allow permission by default
        vii. Click **OK**




14. Click the "*Retired*" lifecycle state, then:
    c. Click the **Transitions** tab
    d. Do the following for both the "*Retired to Available*" and "*Retired from Available*" transitions:
        i. Select the transition, then click **Edit…** to open the Transition dialog box
        ii. Click the **Security** tab
        iii. Uncheck the "*No state-based security*" toggle, followed by clicking **Add…**
        iv. Under the Select Members From section, click the drop-down and choose **Groups**
        v. Select the "*Support Team*", followed by clicking **Add…** then **OK**
        vi. The "*Support Team*" will be given the Allow permission by default
        vii. Click **OK**




15. When finished, click **Apply**
16. Take a deep breath and exhale, because we are now done wi

## Revision Schemes

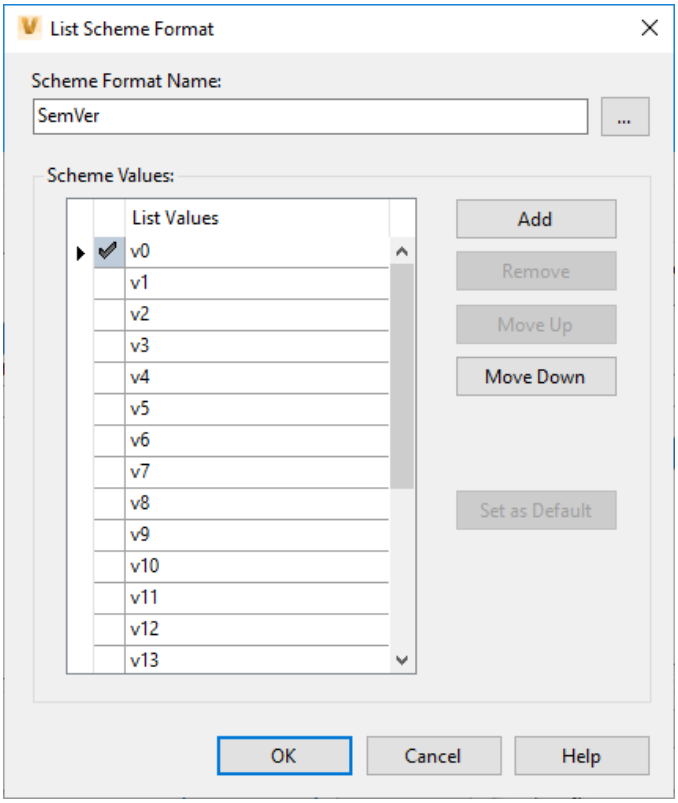
Revision schemes are used to manage versioning during product development. This provides consistency throughout the product lifecycle by applying a common definition and behavior to files and items in a vault. This feature is only available in Autodesk Vault Workgroup and Professional. These versions come with 3 out of the box revision scheme definitions; Standard Alphabetic, Standard Numeric, and ASME Y14.35M.

### Software Versioning

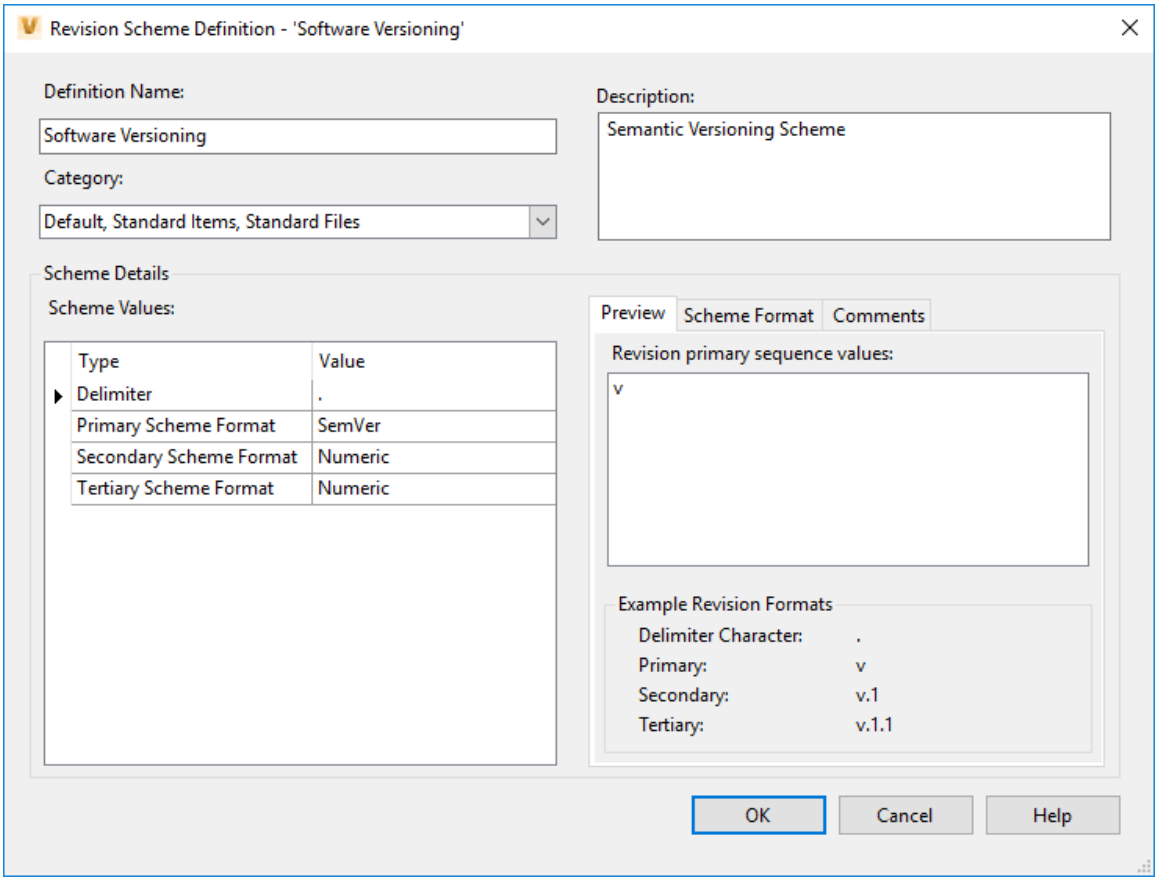
The scheme I suggest using is based on the Semantic Versioning system and will match the File Lifecycle State that we created earlier.

1. Click **Tools** ➤ **Administration** ➤ Vault **Settings**
2. In the Vault Settings dialog box, select the **Behaviors** tab → **Revisions**
3. Click **New**
4. In New Revision Scheme dialog box, change the **Definition Name** to "*Software Versioning*"
5. Set the **Description** to "*Semantic Versioning Scheme*"
6. Click the drop-down menu under **Category** and select "*Standard Items*" and "*Standard Files*"
7. Select the **Scheme Format** tab and then click **New** to open the List Scheme Format dialog box
8. In the Scheme Format Name dialog box, enter "*SemVer*"
9. Click **Add** to create a row for a scheme value, and then enter "*v0*" in the row
10. Repeat this step until you reach at least "v20" to allow for long term growth of the standards version history. If you can foresee maxing this quickly, then go ahead and create values up to "v100".

    NOTE: Once this is scheme is applied, you will not be able to modify it, such as adding additional values.
11. Click **OK** to return to the New Revision Scheme dialog box
12. Under the Scheme Values section, click the drop-down beside each section and set the following:
    a. Primary Scheme Format – SemVer
    b. Secondary Scheme Format – Numeric
    c. Tertiary Scheme Format – Numeric
13. Optionally, you may want to add comments by clicking the **Comments** tab
14. Click **Add**, then add the desired comment in the **Enter Comments** section



15. Click **Ok**




## Categories

Categories are labels that provide a way to group objects logically. Grouping by category also provides a means for assigning a defined set of behaviors and rules to objects. A category can automatically assign user-defined properties to objects in the Vault. They can also be used to automatically assign lifecycle definitions or revision values to files.

Files, folders, custom objects, and items do not necessarily have to be assigned to a category. But if they are not assigned a category, then they use the default behaviors defined for the vault. A category has associated properties and behaviors that are applied to an object when it is assigned to the category. There are three types of behaviors that you can assign:

- Lifecycles (files, folders, and items)
- Revisions (files and items only)
- User Defined Properties (files, folders, and items)

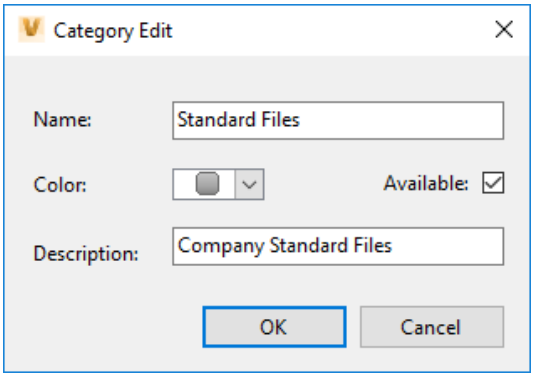
You may find it useful to create some User Defined Properties that will allow you track specific properties on your standards content such as manufacturer, model numbers, product type and/or versions. This will allow you to do things

such as apply filters on any searches in your standards location or restrict what files can be approved and released to users. Think through some scenarios early to help define what may help so you can assign these properties during your initial configuration.

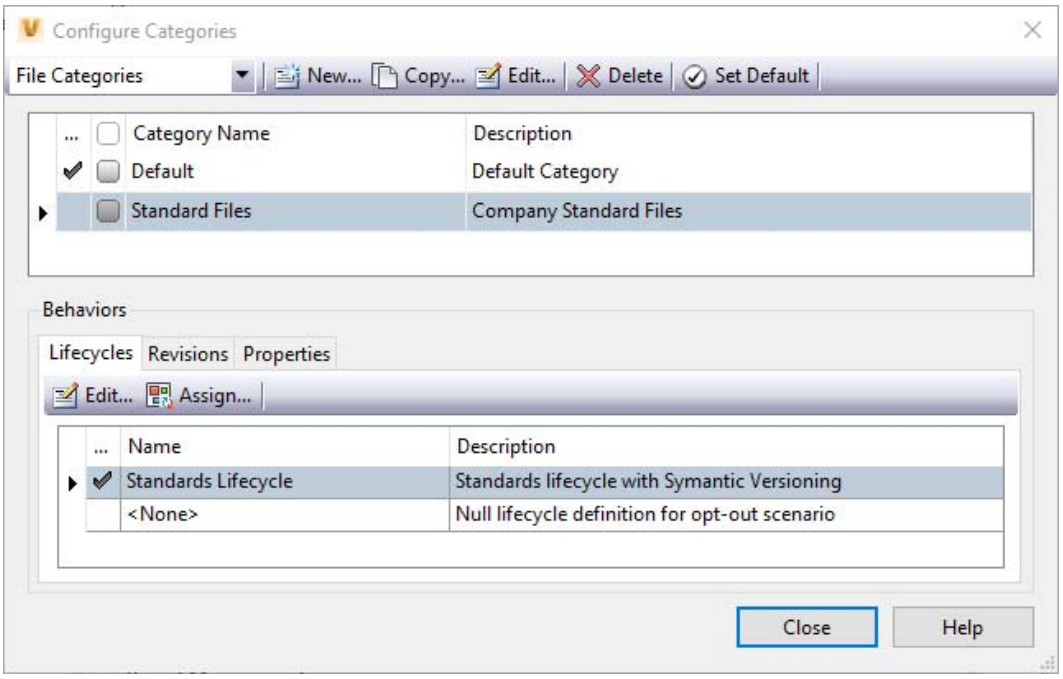
### File Category

Assigning a file category to our standards content will allow us to apply a Lifecyle, Revision Scheme, and any User Defined Properties we wish. To help us track changes and limit any modifications effectively, we will be assigning a Lifecycle and Revision Scheme.

1. Select **Tools** ➤ **Administration** ➤ **Vault Settings**
2. In the Vault Settings dialog box, select the **Behaviors** tab ➤ **Categories…**
3. In the Configure Categories dialog box, select **File Categories** from the top left drop-down list
4. Click **New** to open the Category Edit dialog box
5. In the Name field, enter "*Standard Files*" for the Name
6. From the Color list, select a color glyph to assign to the category
7. Verify the Available check box is checked
8. In the Description box, enter "*Company Standards Files*" as the description for the category
9. Click **OK**. The new category is created with the specified settings and appears in the Category Name list on the Configure Categories dialog box.



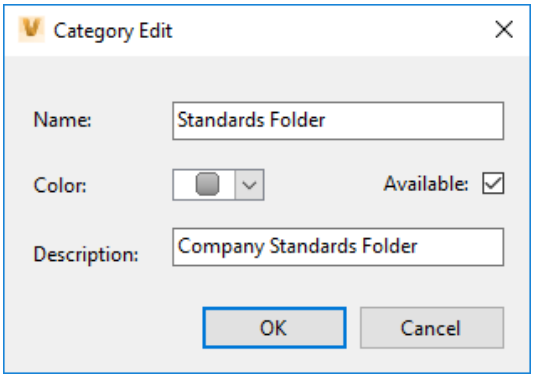

10. Click the **Lifecycles** tab, then click **Assign**
11. On the left side, under All Lifecycle Definitions, select "*Standards Lifecycle*" then click **Add**
12. Now on the right side, under Assigned Lifecycle Definitions, select "*Standards Lifecycle*" then click **Default**
13. Click **OK**. The "*Standards Lifecycle*" is now assigned as the default file category for the "*Standards Files*".
14. Click the **Revisions** tab, then click **Assign**
15. On the left side, under All Revision Schemes, select "*Software Versioning*" then click **Add**
16. Now on the right side, under Assigned Lifecycle Definitions, select "*Software Versioning*" then click **Default**
17. Click **OK**. The "*Software Versioning*" is now assigned as the default revision scheme for the "*Standards Files*".
18. Click the **Properties** tab, then click **Assign**
19. On the left side, under Available Property Definitions, select all the properties that you would like for files
20. Click **Add**, then **OK**. These properties will now be listed Properties pane under the "*User Defined*" section.




## Folder Category

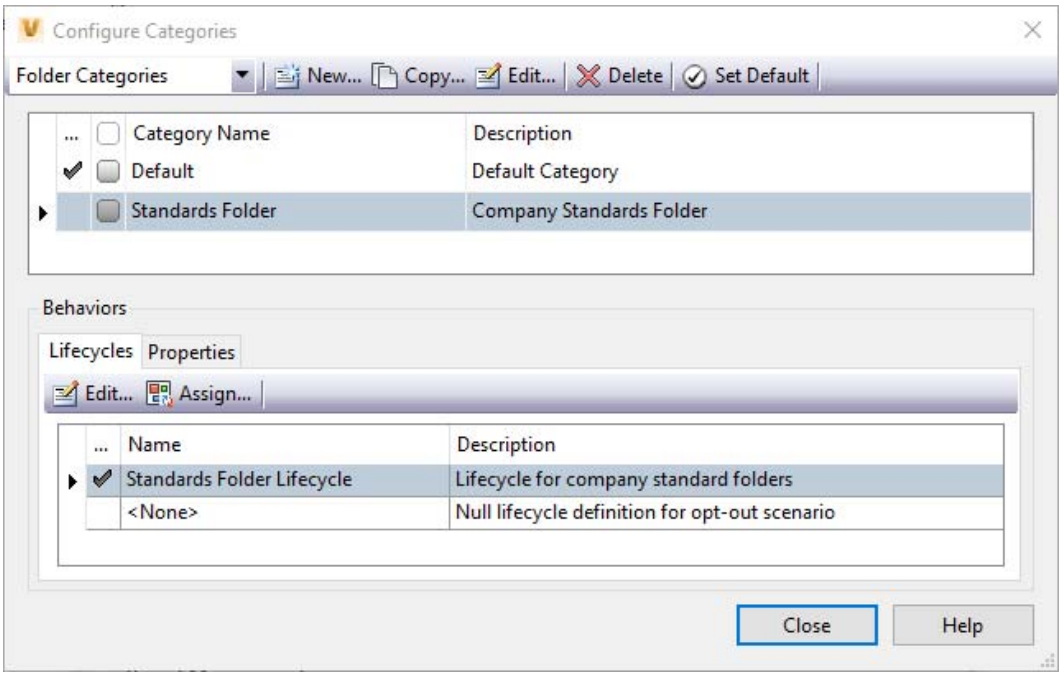
Assigning a folder category to our standards folders will allow us to place a Lifecycle that can help us limit access to content they may no longer offered due to product upgrades or manufacturer changes.

21. In the Configure Categories dialog box, select **Folder Categories** from the top left drop-down list
22. Click **New** to open the Category Edit dialog box
23. In the Name field, enter "*Standards Folder*" for the Name
24. From the Color list, select a color glyph to assign to the category
25. Verify the Available check box is checked.
26. In the Description box, enter "*Company Standards Folder*" as the description for the category
27. Click **OK**. The new category is created with the specified settings and appears in the Category Name list on the Configure Categories dialog box
28. Remain in this dialog box and proceed to the next category




29. Click the **Lifecycles** tab, then click **Assign**
30. On the left side, under All Lifecycle Definitions, select "*Standards Folder Lifecycle*" then click **Add**
31. Now on the right side, under Assigned Lifecycle Definitions, select "*Standards Folder Lifecycle*" then click **Default**
32. Click **OK**. The "*Standards Folder Lifecycle*" is now assigned as the default file category for the "*Standards Folders*".

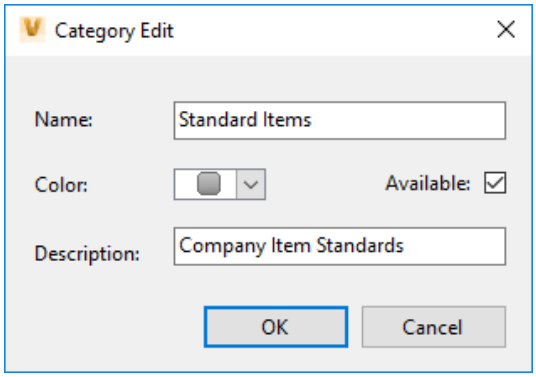
33. Click the **Properties** tab, then click **Assign**
34. On the left side, under Available Property Definitions, select all the properties that you would like for files
35. Click **Add**, then **OK**. These properties will now be listed Properties pane under the "*User Defined*" section.



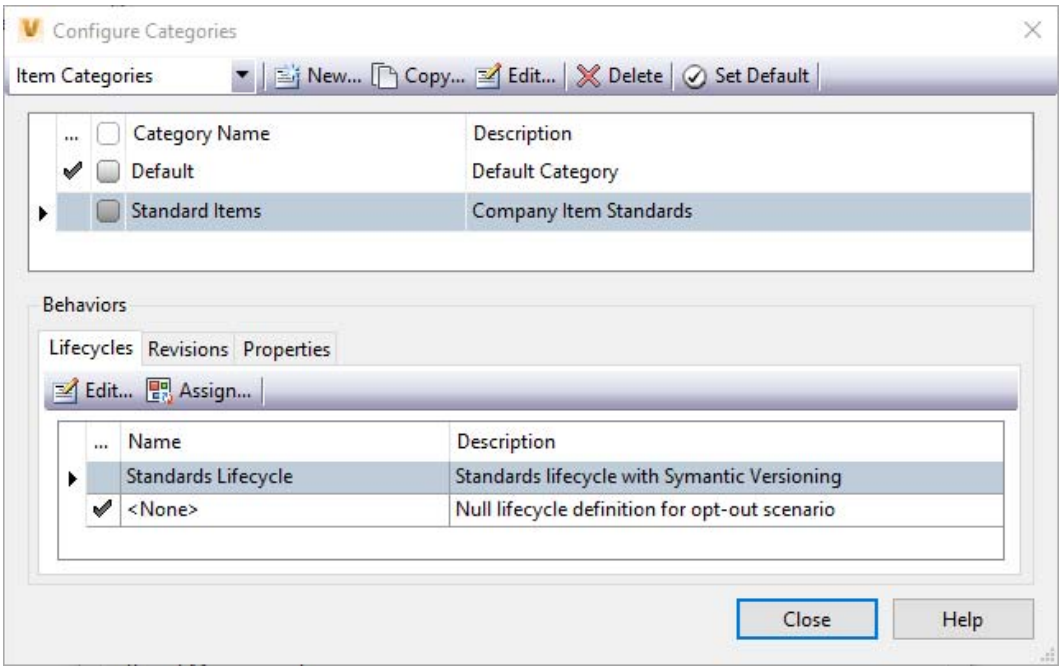

## Item Category

Like individual files, Items can also have their own Lifecyle, Revision Scheme, and any User Defined Properties assigned to them. So rather than trying to manage the release of each individual file, the entire package of relevant documentation can be released from the item level instead. We will be assigning a Lifecycle and Revision Scheme on Items as well to help us track changes and limit any modifications effectively.

36. In the Configure Categories dialog box, select **Item Categories** from the top left drop-down list
37. Click **New** to open the Category Edit dialog box
38. In the Name field, enter "*Standard Items*" for the Name
39. From the Color list, select a color glyph to assign to the category
40. Verify the Available check box is checked.
41. In the Description box, enter "*Company Item Standards*" as the description for the category
42. Click **OK**. The new category is created with the specified settings and appears in the Category Name list on the Configure Categories dialog box
43. Click the **Lifecycles** tab, then click **Assign**



44. On the left side, under All Lifecycle Definitions, select "*Standards Lifecycle*" then click **Add**
45. Now on the right side, under Assigned Lifecycle Definitions, select "*Standards Lifecycle*" then click **Default**
46. Click **OK**. The "*Standards Lifecycle*" is now assigned as the default file category for the "*Standards Items*".
    NOTE: Steps 47-50 are optional. If this conflicts with any standard revision schemes for items, please skip these steps and go to step 51.
47. Click the **Revisions** tab, then click **Assign**
48. On the left side, under All Revision Schemes, select "*Software Versioning*" then click **Add**
49. Now on the right side, under Assigned Lifecycle Definitions, select "*Software Versioning*" then click **Default**
50. Click **OK**. The "*Software Versioning*" is now assigned as the default revision scheme for the "*Standards Items*".
51. Click the **Properties** tab, then click **Assign**
52. On the left side, under Available Property Definitions, select all the properties that you would like for files
53. Click **Add**, then **OK**. These properties will now be listed Properties pane under the "*User Defined*" section.



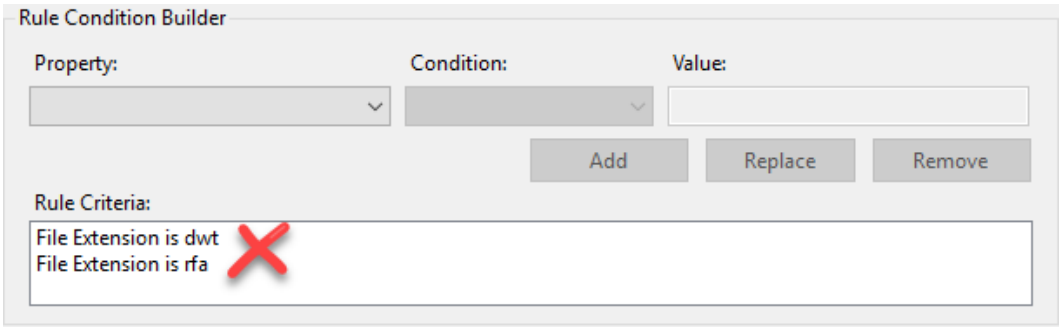

## Rule Sets

Assigning rule sets to a category allows for files, folders, custom objects, and items that meet a set of conditions to be assigned a predetermined category. This could be something like configuring file assignment rules that could look for a set of standard file extensions such as DWT, RTE, RFT, RFA, or RPS and assign them to your standards file category. You can also create a folder assignment rule that will place in new folder that is created in Vault, whether manually or from a check-in folder process, that is within a specified folder path to a predestined category.

Be careful including drawing formats like DWG, RVT, IDW, or MAX because this will create a false positive by assigning the standards category when new files are uploaded into Vault that may just be working files. Also, be aware of the shared file extensions between product developers that you use Vault to manage the standards. For example, the file

extension MAT is both a 3DS Max material file and a Microsoft Access Table, so if you decide to manage both Autodesk and Microsoft products within the same Vault, then you will need to account for this in your configuration to verify that you are not receiving false positives as well.

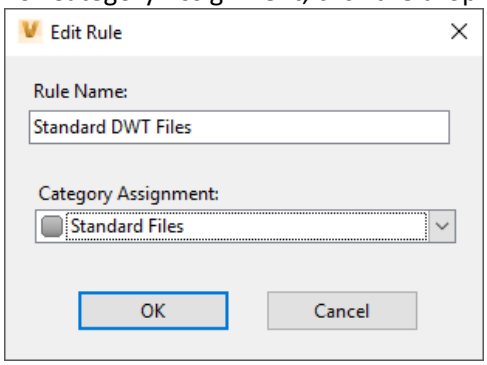
Another thing to factor as you are creating your list of rules and conditions is that rule sets use the AND as the operator. What this means is that you will need to create a separate rule for each file extension. For example, if you create a rule that has the conditions to looks for the file extension “dwt” and “rfa”, it will come back with no results therefore appear as though your rule is not working properly. So, you will need to create a new rule for each file extension that you want to auto-assign to category.




## File Rules

Once you have carefully decided on what conditions you would like to configure a rule for, follow along with the example below to create your File Assignment Rules for. We will be creating a new rule that looks for the “dwt” file extension.

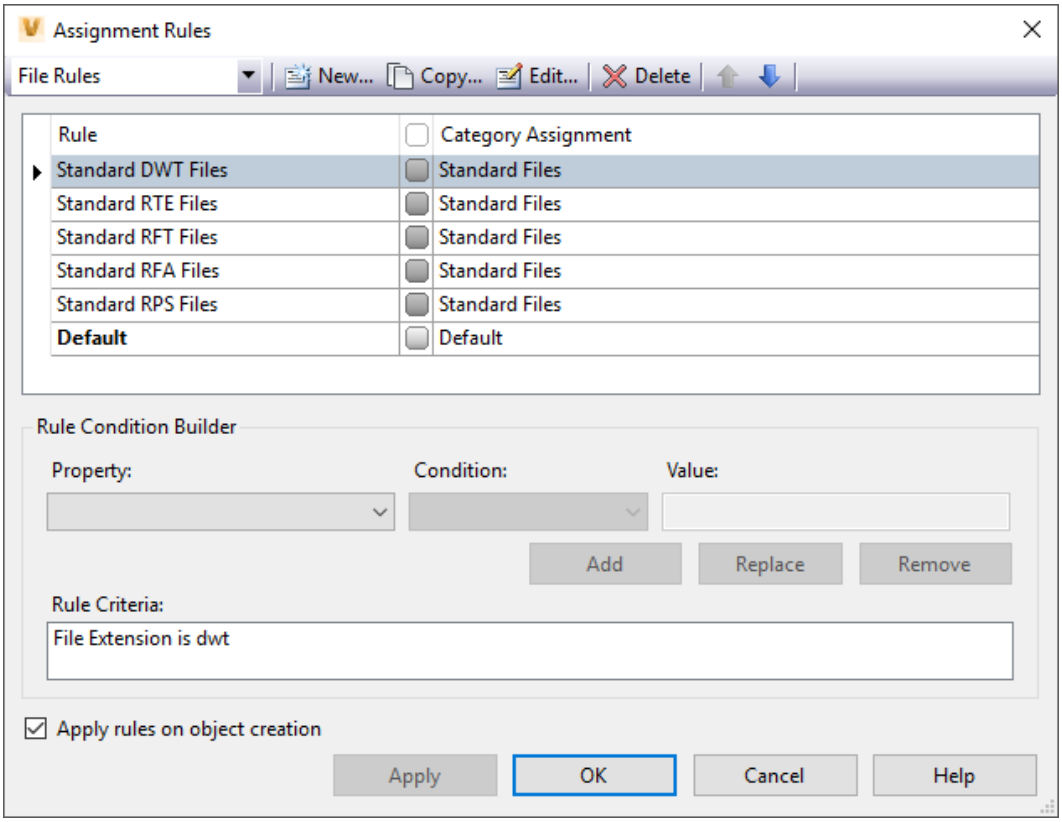
1. Click **Tools** ➤ **Administration** ➤ **Vault Settings**
2. On the Vault Settings dialog box select the **Behaviors** tab ➤ **Rules**
3. Select **Files Rules** from the drop-down list in the top left
4. Check the “*Apply rules on object creation*” toggle in the bottom right
5. Click **New…** to open the Edit Rule dialog box
6. For the Rule Name, use something like “Standard DWT Files”
7. For Category Assignment, click the drop-down and select “*Standard Files*”




8. Click **OK**

9. In the Rule Condition Builder section, set the following:
    a. File Extension:
        i. Property: *File Extension*
        ii. Condition: *is*
        iii. Value: *dwt (OR the extension you are configuring)*
10. Click **Apply** to save the changes
11. Optionally, you can create a rule that looks for files that have been assigned the "*Standards Lifecycle*" by using the following condition:
    a. Lifecycle Definition:
        i. Property: *Lifecycle Definition*
        ii. Condition: *is*
        iii. Value: *Standards Lifecycle*
12. Repeat steps 5-9 for every file extension type you want to configure
13. Click **OK**

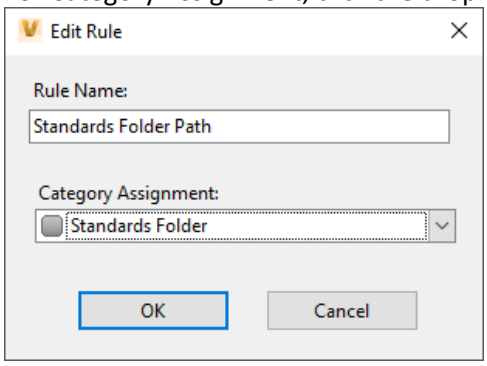
NOTE: If you want to reorder the list, select a rule and then use the **Up** and **Down** arrow keys to move it where would you want it to be in the list.



## Folder Rules

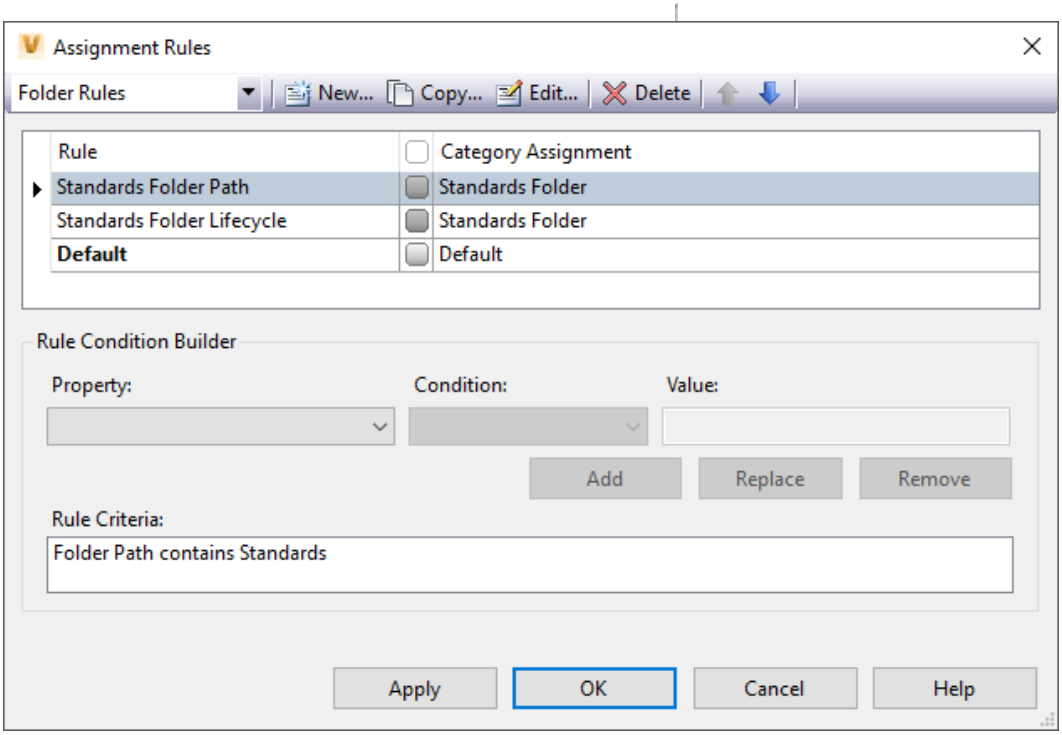
The available properties for folder is far less compared to files, so I find that "*folder path*" is the gem to use and will be what you use to create a Folder Assignment Rule that looks for the value "Standards" using the folder path property.

1. Click **Tools** ➤ **Administration** ➤ **Vault Settings**
2. On the Vault Settings dialog box select the **Behaviors** tab ➤ **Rules**
3. Select **Files Rules** from the drop-down list in the top left
4. Check the "*Apply rules on object creation*" toggle in the bottom right
5. Click **New…** to open the Edit Rule dialog box
6. For the Rule Name, use something like "Standards Folder Path"
7. For Category Assignment, click the drop-down and select "*Standards Folder*"




8. Click **OK**
9. In the Rule Condition Builder section, set the following:
    a. File Extension:
        i. Property: *File Extension*
        ii. Condition: *is*
        iii. Value: *dwt (OR the extension you are configuring)*
10. Click **Apply** to save the changes
11. Optionally, you can create a rule that looks for folders that have been assigned the "*Standards Folder Lifecycle*" by using the following condition:
    a. Lifecycle Definition:
        i. Property: *Lifecycle Definition*
        ii. Condition: *is*
        iii. Value: *Standards Folder Lifecycle*
12. Repeat steps 5-10 for every folder rule you want to configure
13. Click **OK**

NOTE: If you want to reorder the list, select a rule and then use the **Up** and **Down** arrow keys to move it where would you want it to be in the list.




## Properties

Properties are attributes associated with a file, item, folder, and custom objects. There are two types of property definitions: system-defined properties and user-defined properties (UDPs). System-defined properties are those that are derived from the vault. The vault has a global set of properties that are applied to files in the vault. User-defined properties are created by a user using the administrative tools.

When a new user-defined property is created, it does not have to be associated with any categories. However, even if the property is associated with an entity (file, folder, custom object, change order, item, etc.) and is not associated with any categories, it will not appear in the properties grid for that entity type. I suggest assigning them to categories during the process of creating them so it's easier.

Note: Once a property definition is created, the data type cannot be modified. So, think ahead of what you want to create and create a thought-out list prior to creating any new properties. Also, view the Properties Administration page offered by Autodesk to familiarize yourself with common terms, data types, attributes, and icons that will be referenced.

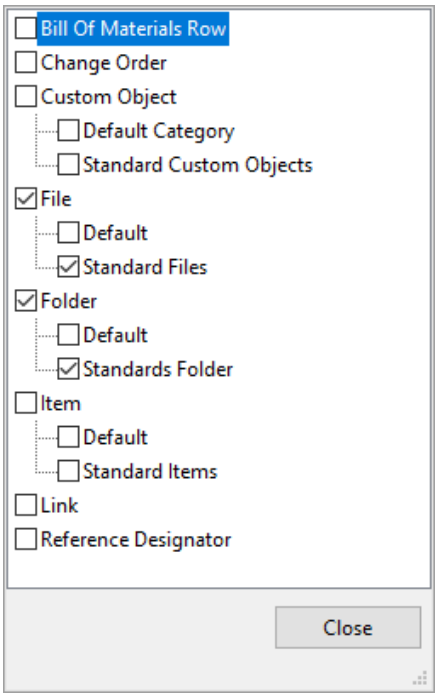
### Product

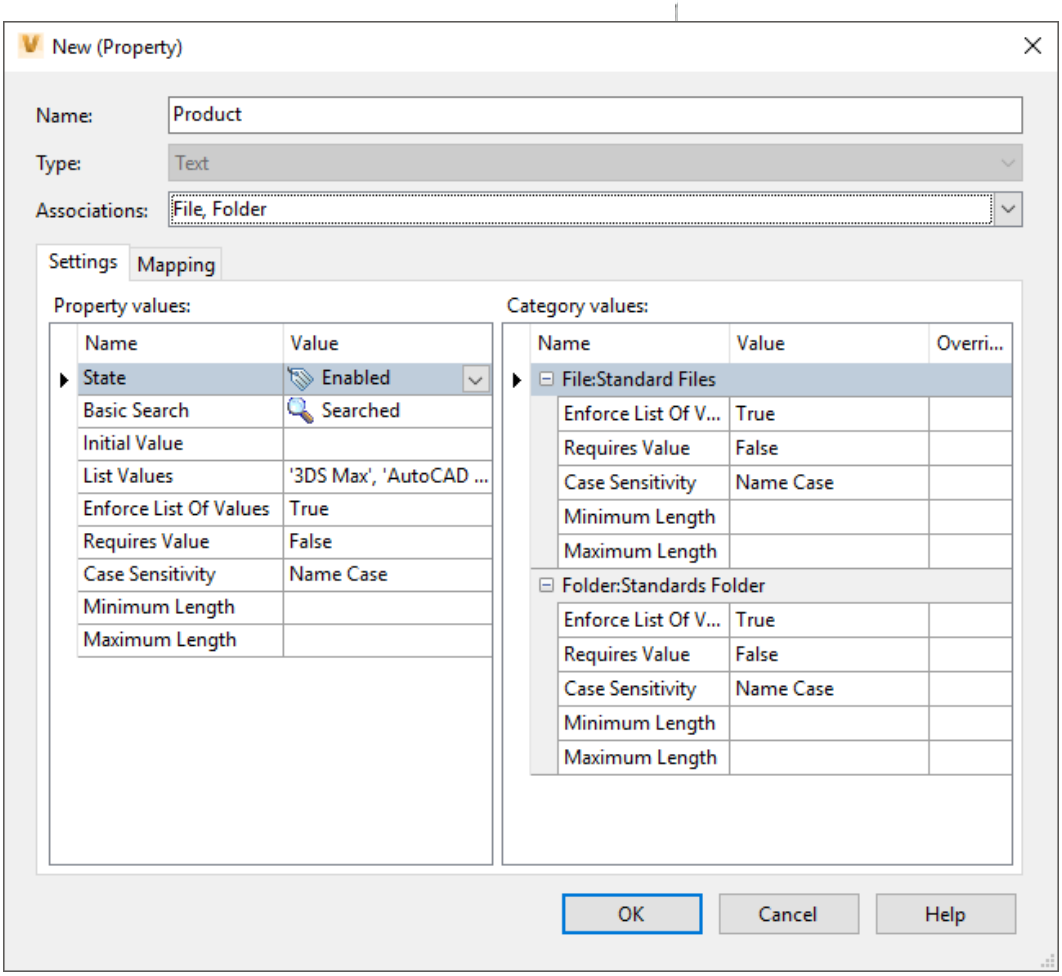
You may want to assign what product your standards are for to help search for or run reports, so will create a "*Product*" property to aid in process like that. Pro Tip: It would be possible to create a User Group and assign specific users to that use a certain product, to only see standards that are applicable to them.

1. Click **Tools** ➤ **Administration** ➤ **Vault Settings**
2. On the Vault Settings dialog box **Behaviors** tab, click **Properties**
3. In the Property Definitions dialog box, click **New…**

4. In the New Property dialog box, in the name field, enter "*Product*"
5. In the Type list, select "*Text*"
6. Expand the Associations drop-down and select "*Standard Files*" under the File section and "Standards Folder" under the Folder Section
7. On the Settings tab, we want to leave the Initial Value empty. Selecting a default value could prove problematic later if you manage multiple products.
8. Click the drop-down beside List Values to expand the Property Values
9. Click within the top line to add a new product name for each product that is managed, then hit **Enter**. (Repeat for each product; AutoCAD, Revit, Inventor, 3DS Max, etc.)

   Note: If you need to restructure the list of products, select a value and click **Move Up** or **Move Down** as needed to arrange the order of the values in the list.
10. Click the area beside Enforce Lost of Values, and choose "*True*"
11. Click the area beside Case Sensitivity, and choose "*Name Case*"
12. Click **Close** to return to the New Property dialog box
13. Click **OK** on the New (Property) dialog
14. If you would like to override the Property Values per category, you can find the category/value under Category Values and select the desired value for each. This will not allow to have different List Values.





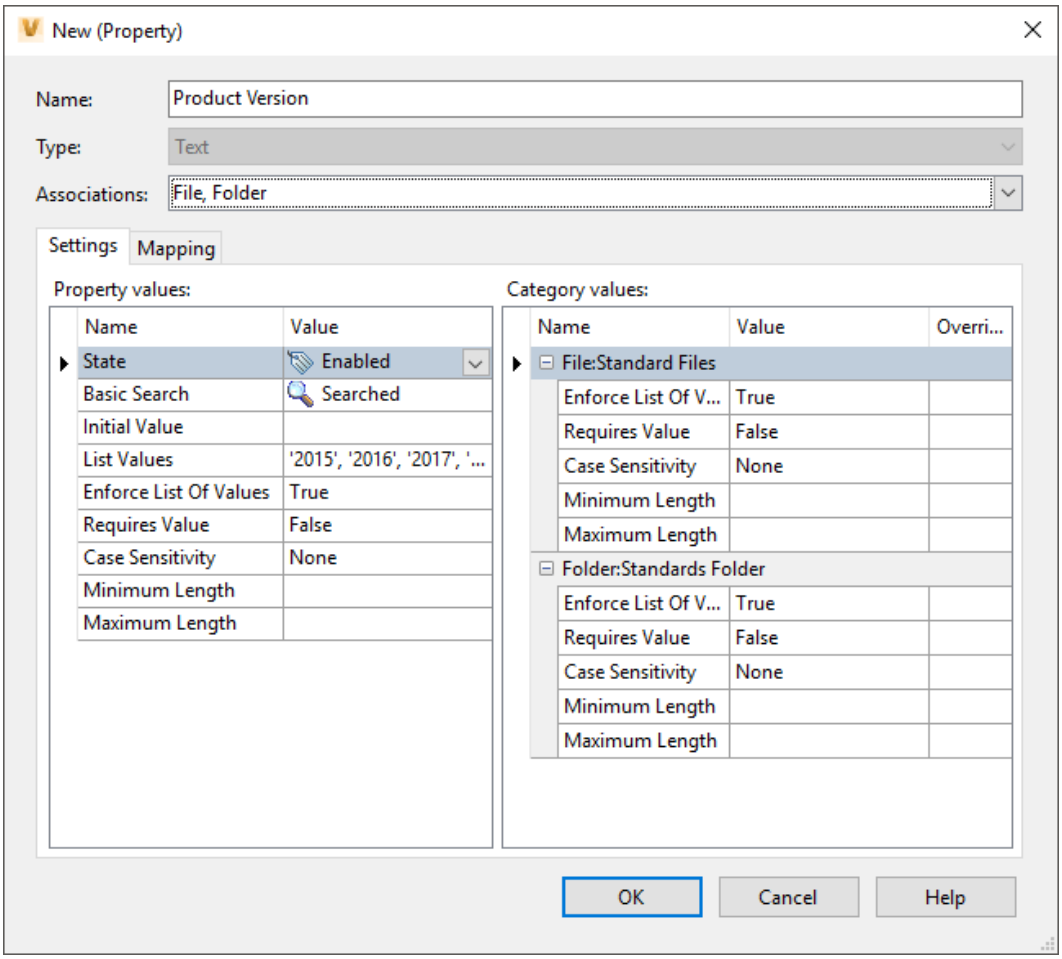

## Product Version

If you manage multiple versions of the same a product, then creating a "*Product Version*" property to aid in tracking what if a certain is standard is compatible with the product it will be used in. The following steps are like the process of creating the "Product" property, just with slight differences for property name and not setting case sensitivity.

1. Click **Tools** ➤ **Administration** ➤ **Vault Settings**
2. On the Vault Settings dialog box **Behaviors** tab, click **Properties**
3. In the Property Definitions dialog box, click **New…**
4. In the New Property dialog box, in the name field, enter "*Product Version*"
5. In the Type list, select "*Text*"
6. Expand the Associations drop-down and select "*Standard Files*" under the File section and "Standards Folder" under the Folder Section
7. On the Settings tab, we want to leave the Initial Value empty. Selecting a default value could prove problematic later if you manage multiple product versions.
8. Click the drop-down beside List Values to expand the Property Values

9. Click within the top line to add a new product name for each product that is managed, then hit **Enter**. (Repeat for each product versions; 2017, 2018, 2019, etc.)

   Note: If you need to restructure the list of products, select a value and click **Move Up** or **Move Down** as needed to arrange the order of the values in the list.
10. Click the area beside Enforce Lost of Values, and choose "*True*"
11. Click **Close** to return to the New Property dialog box
12. Click **OK** on the New (Property) dialog
13. If you would like to override the Property Values per category, you can find the category/value under Category Values and select the desired value for each. This will not allow to have different List Values.




That wraps up everything required to configuring Vault to manage your CAD/BIM standards within Vault, and by far the hardest part of the journey. Now is the time to start testing the different aspects we just set up by dropping some test files in and apply the appropriate category then lifecycle states. If something doesn't work as intended, go back through the steps and verify that you set up each properly.

## Product Configuration

The methods used to configure each product will vary, but the all follow the same concept which is to point any support path at location that we have previously defined within Vault. Some applications, like AutoCAD, will allow you preconfigure all the settings so all the user will have do is copy a modified shortcut and use it to run the application. Others will require the user to manually go into the options and change each path one time, so their application will use those paths from that point forward. Below, we will walk through some of Autodesk's primary products and go through some the basics involved with these processes. It will be up to you to determine what works best for the company standards and adjust accordingly.

### Architecture, Engineering & Construction Collection

In this collection, we will cover both AutoCAD 2019 and Revit 2019, which utilizes different methods when it comes to customizing their support paths. Both have straightforward paths, but the more tech savvy individuals can use lisp or ini files to adjust and append support paths. For simplicity sake, I won't dive into using lisp because it can be an in-depth topic which can be hard to cover due to the diversity of how you can achieve different results. However, utilizing Revit's ini file could be a good method for those that configure Vault to sync this file to the appropriate location on a user's machine. So, let's get started.

#### AutoCAD

This process will be the same for all other flavors of AutoCAD including Architecture, Electrical, Map 3D, Mechanical, MEP, Plant 3D, and Raster Design. We will create a new local profile and modify all the support paths to look at our new standards folders managed by Vault. We will then save this file in Vault along with a modified shortcut that will use this new profile, so the only things users will have to do is pin the shortcut to their taskbar. If there are any changes from that point forward, they will always get them.

**From within AutoCAD:**

1. Click the **Application** menu ➤ **Options**
2. In the Options dialog box, click the **Profiles** tab
3. Click **Add to List…**
4. In the Add Profile dialog box, set the following:
   a. Profile Name: *AutoCAD 2019*
   *b.* Description: *New company standard AutoCAD 2019 profile*
5. Click **Apply & Close**
6. Now select the new "*AutoCAD 2019*" profile, then click **Set Current**
7. Click the **Files** tab
   Note: The following are examples according to the folder structure I listed previously, so change the values to match your existing Vaults folder structure that you set up.
8. Select Support File Search Path, then:
   a. Click **Add** to add a new support path, then paste the following for the location:
   "*C:\Vault\Standards\AutoCAD Architecture\2019\...*"
   (Adding the "\..." will make AutoCAD search through all the sub-folders)
9. Select Trusted Locations, then:
   a. Click **Add** to add a new support path, then paste the following for the location:

"*C:\Vault\Standards\AutoCAD Architecture\2019\...*"

10. Expand Customization Files, then:
    a. Select Main Customization File
    b. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Menus*"
    c. Select Custom Icon Location
    d. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Menus\Icons*"
11. Expand Printer Support File Path, then:
    a. Select Printer Configuration Search Path
    b. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Plotters*"
    c. Select Printer Description File Search Path
    d. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Menus\PMP Files*"
    e. Select Printer Style Table Search Path
    f. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Menus\Plot Styles*"
12. Expand Template Settings, then:
    a. Select Drawing Template File Location
    b. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Templates*"
    c. Select Sheet Set Template File Location
    d. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Templates*"
    e. Select Default Template File Name for QNEW
    f. Click **Browse** and select or paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Templates\acad.dwt*"
13. Select Tool Palettes File Locations, then:
    a. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Palettes*"
14. Expand Action Recorder Settings, then:
    a. Select Actions Recording File Location
    b. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Action Routines*"
    c. Select Additional Actions Reading File Location
    d. Click **Browse** and paste the following for the location:
    "*C:\Vault\Standards\AutoCAD Architecture\2019\Action Routines*"
15. Make any additional changes you choose on the other tabs according to company standards

16. Click the **Profiles** tab
17. Now select the new "*AutoCAD 2019*" profile, then click **Export…**
18. Save the an arg file in a folder within your standards Local Working folder, such as Profile, so it's easily accessible by the other users
19. Click **Save**, followed by **Ok** back at the Options dialog box

**From the Desktop:**

20. Right-click the "*AutoCAD Architecture 2019 – English*" and choose **Copy**
21. Open Windows Explorer and navigate to "*C:\Vault\Standards\AutoCAD Architecture\2019\Profile*"
22. Right-click and chose **Paste**
23. Select the newly pasted shortcut, right-click and choose **Properties**
24. In the Target field, scroll to the end and paste:
    /p "C:\Vault\Standards\AutoCAD Architecture\2019\Profile\AutoCAD 2019.arg"
    (This is a profile switch that will tell AutoCAD to run load the profile that we just created upon startup)
25. Click **OK**
26. Right-click the shortcut and choose "*Pin to taskbar*"

Now AutoCAD has been fully configured to look at the Vault Standards Folders for most of its content, so once someone performs a Get on any content, their AutoCAD will be updated to the latest and greatest.

## Revit

Revit has two methods that the file locations can be modified; manually and automatically. The manual method will require that someone changing the locations within Options ➤ File Locations, but only allows a limited number of items that can be changed. The automatic method will involve modifying the directory settings in the Revit.ini file but allows more items that can be changed including the interface. Using this method creates a situation where if you decide the change a directory or file location in the future, Revit will not notice a change because it looks for a directory change only once, then loads this into a separate file. A workaround is to script or group policy object (GPO) that would replace the original file with the modified one. So, choose what is best for you and how you would like to manage customizations.

**Manually within Revit:**

1. Click the **Application** menu ➤ **Options**
2. In the Options dialog box, click the **File Locations** tab
3. For each of the Project Templates, do one of the following:
   a. Select the template
   b. Click the (**…**) to the right
   c. Navigate to "*C:\Vault\Standards\Revit\Templates*" and select the appropriate template
4. Beside the "*Default path for family template files*", click **Browse**
5. Navigate to and select "*C:\Vault\Standards\Revit\Family Templates\2019*"
6. Click the **Places…** button, then:
   a. Select Imperial Library path
   b. Paste "*C:\Vault\Standards\Revit\Families\2019*"

c. Select Imperial Library path
d. Paste "*C:\Vault\Standards\Revit\Families\2019*"
e. Click **OK**
f. Then click **OK** again back at the Options dialog box

**Automatically with the Revit.ini file:**

1. Create a custom version of the Revit.ini file, as follows:
   a. Create a copy of Revit.ini, preserving the original version so you can return to it if needed.
   b. Edit the new copy of Revit.ini, changing the values of the desired settings as needed.

   Note: See the "Revit.ini settings for Revit_2019.xls" document that was provided for a full list of available settings that can be modified within the Revit.ini file.
2. Use a text editor such as Notepad or Notepad++ to open the Revit.ini file
3. In the Install section, add the Update setting to indicate the sections and settings that are to be changed for each user who receives the updated Revit.ini file.

   Use this format:
   Update=section|setting;section|setting;section|setting...

   For example:
   [Install]
   Update=Appframe|Theme;Documentation|HelpBrowser;Documentation|OnlineHelpLocale

4. There are three methods you can use to push the updated Revit.ini file to the UserDataCache folder on each user's computer:
   a. Use a script
   b. Use a group policy object (GPO)
   c. Use the IMAGINiT Vault 2019 Utilities to create a Standards Folder sync to copy the file from Vault into the UserDataCache location on the users' machine

   The UserDataCache version of Revit.ini resides in the following location:
   "*%ALLUSERSPROFILE%\Autodesk\RVT 2019\UserDataCache*"
5. Ask users to restart the Revit software.
6. The next time a user starts the software, Revit compares UserDataCache\Revit.ini with the user profile version of the Revit.ini file. When it determines that the Update setting in the UserDataCache version is different than the Update setting in the user profile version (or it does not exist there), Revit copies the settings specified by the Update setting in UserDataCache\Revit.ini from that file to the user profile version of the Revit.ini file, overwriting previous values for those settings. Other values in the user profile version of the Revit.ini file is not changed.

## Product Design & Manufacturing Collection

In this collection, we will cover how to configure Inventor 2019 using an xml file to customize the work environment and support paths.

### Inventor

Customization settings allow you to customize your work environment including the ribbon, keyboard, and marking menu. They allow you to create custom user-defined panels for each of the ribbon tabs. User-defined items display in the User Commands panel., which is created when you first create a custom panel.

1. Click **File** ➤ **Options**.
2. In the Application Options dialog box, click the **File** tab
3. Select each path listed and do the following:
   a. Click **Browse**
   b. Navigate the appropriate standards folder with the local Vault working folder that was configured previously.
   c. Click **Ok**
4. Click the **Content Center** tab
5. Under Access Options, select "*Autodesk Vault Server*"
6. At the bottom of the Application Options dialog box, click **Export**
7. In the Save Copy As dialog box:
   a. Navigate the standards folder in Vault
   b. Specify the name of the .xml file
   c. Click **OK**

   Note: The export operation uses the current settings in Application Options settings, even if you did not yet apply them.
8. Check this file into same location in Vault
9. Each team member will then:
   a. Perform a one-time only Get on the file in Vault
   b. Open the Application Options dialog box in Inventor
   c. Click **Import** at the bottom

## Media & Entertainment Collection

In this collection, we will cover how to configure 3DS Max 2019. This software is like Revit in that it can be configured within the application and outside via an ini file. Choose the path that you are comfortable with taking.

### 3DS Max

3ds Max uses stored paths to locate different kinds of user files, including scenes, images, DirectX effects, photometric, and MAXScript files. Like Revit, we can customize these paths using two methods; manually or automatic. The manual process involves using the Configure User Paths dialog, and only allows configuring

folder paths. This can be useful when you are adding new folders to help you organize your scenes, images, plug-ins, backups, and so on. After the paths have been configured, you can export a MXP (Max Path) file that other users would load. This capability makes it easy for content-creation teams to keep projects organized and work efficiently by using the same paths.

The automatic method uses involves modifying the 3dsmax.ini that stores settings between. In most cases, you don't need to access this file directly. You can make changes to 3ds Max start-up conditions by editing this file. If you do edit the file, be sure to maintain the structure and syntax of the original file.

**Manually within 3DS Max:**

10. Access the Configure User Paths dialog by done one of the following:
    d. Default menu: Customize menu > Configure User Paths
    e. Alt menu: Customize menu > Customization > Configure User Paths
11. Click a path entry to highlight it
12. Click **Modify**
13. Use the Choose Directory dialog to either:
    f. Enter a path in the Path field
    g. Navigate to locate a path
14. Optional step (3rd Party Plug-Ins panel only): Edit the description of the path in the Label field. This description then appears in the path list.
15. Click **Use Path**
16. Click the **Save As** button and then use the Save Paths To File dialog to save the path configuration as an MXP file in a Vault Standards folder, such as:
    "*C:\Vault\Standards\3DS Max\2019\Paths*"
17. Each team member will then:
    h. Perform a one-time only Get on the file in Vault
    i. Open the Configure User Paths dialog in 3DS Max
    j. Use Load or Merge to open the path configuration file

    Note: Using Load eliminates the existing path configuration; using Merge overwrites only paths that exist in both the current configuration and the new one.

**Automatically with the 3dsmax.ini file:**

1. Create a custom version of the 3dsmax.ini file, as follows:
    a. Create a copy of 3dsmax.ini, preserving the original version so you can return to it if needed.
    b. Edit the new copy of 3dsmax.ini, changing the values of the desired settings as needed.
2. Use a text editor such as Notepad or Notepad++ to open the 3dsmax.ini file
3. After changing the directory path to look at a Vault standards folder, and any other settings you had decided on, perform a check-in on the file to Vault
4. There are three methods you can use to push the updated 3dsmax.ini file to each user's computer:
    a. Use a script
    b. Use a group policy object (GPO)

c. Use the IMAGINiT Vault 2019 Utilities to create a Standards Folder sync to copy the file from Vault into the UserDataCache location on the users' machine

The UserDataCache version of Revit.ini resides in the following location:
"*C:\Users\%USERNAME%\AppData\Local\Autodesk\3dsMax\2019 - 64bit\ENU*"

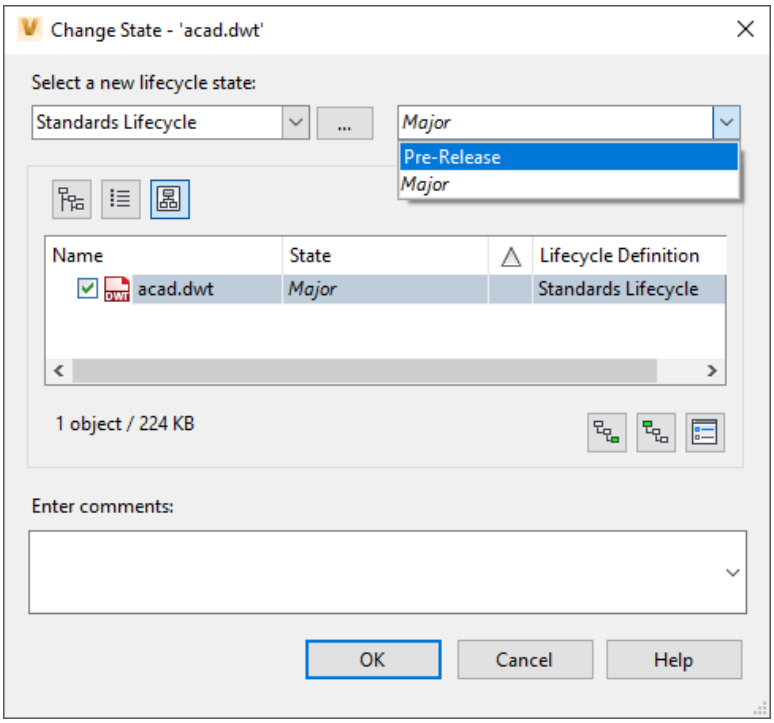
## Workflows for Updating Content

When there is a need to modify/update content, the file(s) will need to go through the workflow we configured. It will get moved into a state that will allow members of the "Support Team" to check the files out, adjust locally, and then check the files back in. When this process is complete, members of the "Pilot Team" will be able to get the files and test on their local systems to verify that intended changes have been made and that there is no bugs or issues within the content. Once they confirm that everything was properly adjusted, a member of the "Support Team" will then approve the content by changing the file state of the content to the appropriately. Then everyone will either perform a Get on the content, or if the correct utilities are installed, the affected files will automatically be downloaded from the Vault once the user opens Vault after the changes are made.

### Modifying Content

When there is a need to modify/update content, a member of the "Support Team" will need to do the following:

1. Select one or more of the standard files that you would like to modify/update. (To select multiple objects, hold down SHIFT while selecting objects from the main grid.)
2. Do one of the following:
   a. Click **Actions** ➤ **Change State**
   b. From the Lifecycle Management toolbar, click **Change State**
   c. From the selected objects, right-click and then click **Change State**
3. In the Change State dialog box, select the "*Pre- Release*" state from the Select new lifecycle state list. The new state is highlighted in bold in the State column. When related objects are displayed in the table, the new state also applies to those them. Non-released biased revision relationships determine which children are affected. If a file is not the leading version of the leading revision, then the check box is disabled next to it.
   Note: Only items with BOM rows that are turned on are displayed.
4. The comment will default to "Issued for pre-release testing", but you can clear the comment and insert your desired comment.



5. Click **OK**.
6. With the file(s) still selected, right-click and select **Get** to open the Get dialog box
7. Verify that the "*Check Out Files*" button is selected, then click **OK**
8. Make the intended changes to the files, then check the files in through the appropriate application
9. If the testing phase fails, and there are corrections to me made, repeat steps 6-7 until.

## Testing Content

A member of the "Support Team" should notify a member of the "Pilot Team" that they need to test the changed content and provide them with a testing script that lists of the affected files and what areas they need to test.

1. Depending on the content that has been changed, there may be a need to close the application that the files will be affecting. This is only for files that the application references throughout the duration it is running. If it is drawing files or families, closing the application is not needed.
2. Select one or more of the standard files that has been modified/updated. (To select multiple objects, hold down SHIFT while selecting objects from the main grid.)
3. Right-click and select **Get** to open the Get dialog box
4. Click **OK** to proceed with getting the file(s)
5. If it was previously required to close the application, reopen it now to load the changed file(s)
6. Test the affected content to verify the intended changes have been made and that there is no issues or adjustment that need to be made.
7. If everything is correct, notify a member of the "*Support Team*" letting them know they can approve the content and provide them the results of the testing script.
8. If there an issue with content was found, notify a member of the "*Support Team*" letting them there is corrections that need to be made to the content and provide them the results of the testing script.

## Approving Content

When all the content has been tested and verified by the "*Pilot Team*", a member of the "*Support Team*" will do the following:

1. Select affected content that is currently in the "*Pre-Release*" file state. (To select multiple objects, hold down SHIFT while selecting objects from the main grid.)
2. Do one of the following:
   a. Click **Actions** ➤ **Change State**
   b. From the Lifecycle Management toolbar, click **Change State**
   c. From the selected objects, right-click and then click **Change State**
3. In the Change State dialog box, select the appropriate file state according to:
   a. "*Major*" – when incompatible changes are made, such as newly designed features
   b. "*Minor*" – when functionality in a backwards-compatible manner was added, such as adjustments to pre-existing features

c. "*Patch*" – when backwards-compatible bug fixes are made, such as minor changes to fix problem content

4. The default comment will be added according to the file state selected, but if you want to change this to something different the clear the comment and insert your desired comment. It may be time consuming depending on the number of files changed, but I suggest for individual or small collections of files that you add a specific comment per file, or to a group of similar files, stating what was exactly changed to help other team members to track changes throughout the version history.
5. Click **OK**.
6. With the file(s) still selected, right-click and select **Get** to open the Get dialog box, then click **OK**

   Note: This is to update the "historical version" status icon that you will receive after making the last state change on the affected files.

By following the workflows for updating content, you and your team will be able to efficiently make changes to content and be able to track exactly what was changed throughout the history of the files. You will also prevent any unapproved users from being able to get ahold of any files that are being tested, which could lead to big problems within the production environment.

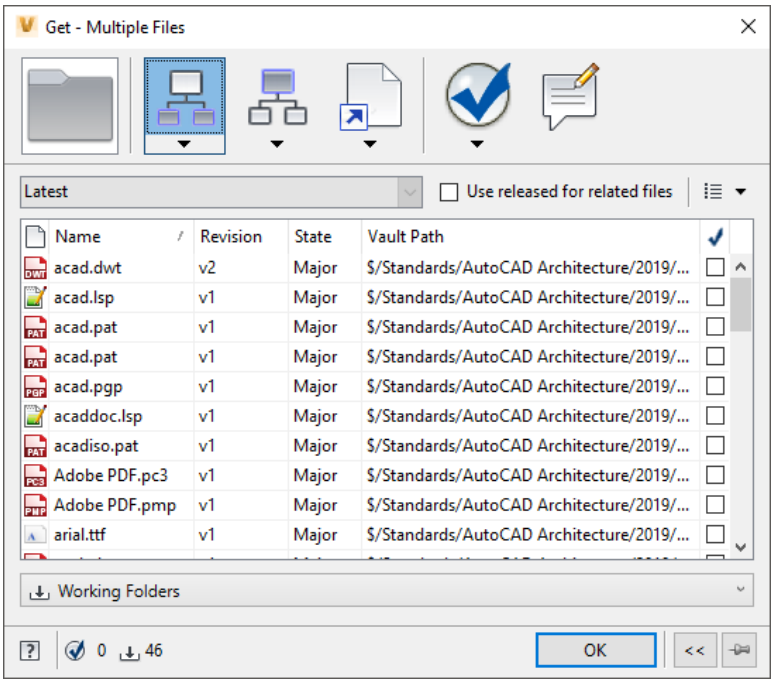
## Methods for Deploying Updates

There are two methods for how you can deploy updates to standard content; manually or automatic. As stated previously, depending on the content that has been changed, there may be a need to close the application that the files will be affecting. This is only for files that the application references throughout the duration it is running. If it is drawing files or families, closing the application is not needed.

### Manually Using the Get Command

Using the manual method only involves notifying all members that use the content that they there have been changes, along with providing them a list of the new features and/or bug fixes, and that they can Get the files. If you have a proper folder structure, then they will only need to navigate to a single folder and perform a Get on this location only.

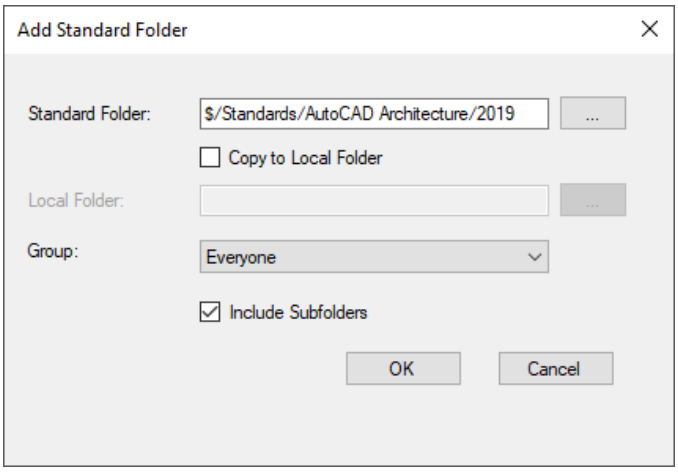
1. Close the affected application, if necessary
2. Navigate to the desired standards folder
3. Right-click and select **Get** to open the Get dialog box, then click **OK**
4. Reopen the application, if necessary

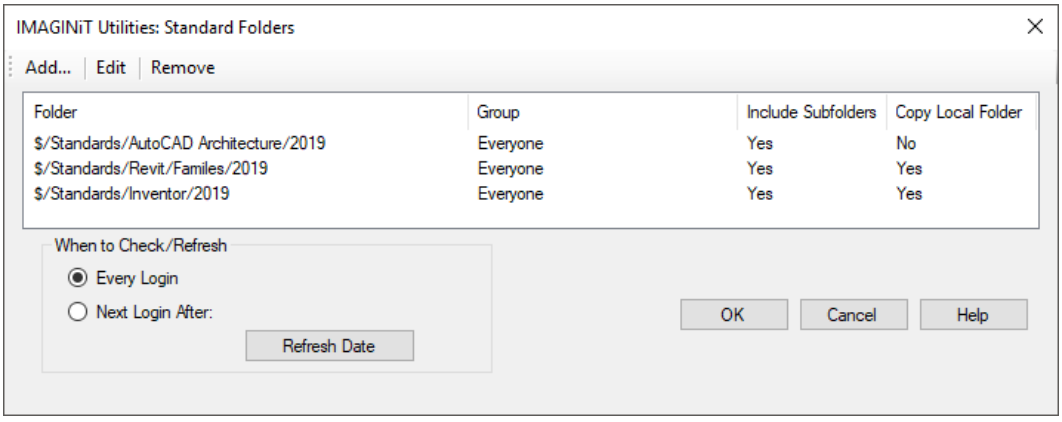


## Automatically Using Standards Folder

The Automatic method requires having the IMAGINiT Vault 2019 Utilities and configuring a sync with their Standard Folders utility. This will allow an administrator to configure a folder of standards that are updated whenever someone logs into Vault. They can create as many syncs as they need to efficiently manage multiple products, locations, and content types and even schedule a time for it start checking for or refresh files. After the user logins into Vault, the utility will scan their local files, then update any files that it finds out of date. They will receive a notification telling them how many files they just received an update for when the process completes. When using the Lifecycle Notification utility, it enables the ability to setup an automatic email notification to be sent to a selected user group that will notify them of all the files that has a had predetermined file state change, like moving from "Pre-Release to Major".

1. Click **Tools** ➤ **IMAGINiT Utilities** ➤ **Standards Folder: Admin**
2. On the Standard Folders dialog box, click **Add…**
3. In the Property Definitions dialog box, click **New…**
4. In the Add Standard Folder dialog box, select the (**…**) button beside Standard Folder
5. Navigate to and select the standards folder in the Folder Browser
6. Click **Ok**
7. If you want the content to be saved outside of the Local Working Folder defined within Vault, then do the following:
   a. Check the "Copy to Local Folder" toggle
   b. Click the (**…**) button beside Local Folder to open the Browse For Folder dialog box
   c. Navigate to and select the desired local folder
   d. Click **Ok**
8. Back at the Add Standard Folder dialog box, click the Groups dialog box and select the "*Everyone*" user group
9. Click **Ok**



Note: If using the "Copy to Local Folder" option, be aware that the "*Support Team*" will have to adjust their workflow for modifying content. They will then have to Get the content from Vault in their Local Working Folder and copy to it to the Local Folder location before starting to modify it. Then copy it back to check-in the changes that have been made so members of the "*Pilot Team*" can then test the content.

Deploying the content is simplified using either method to deploy it. The manual method does not involve anything outside of the typical workflows of getting regular content, and the automatic takes very little time to configure. Both options will make updating or modifying content a breeze compared to the legacy methods. Any content manager will rest easy and no longer having to using network drives and trying to keep the files protected and backed up to safeguard against accidently modifications. Plus, rolling back files to previous versions is a breeze with Vaults version history. Using the new lifecycle states and comments allow them to go back to right version every time.

## References

1. Preston-Werner, Tom (2013). Semantic Versioning 2.0.0. Creative Commons. Retrieved from http://semver.org/spec/v2.0.0.html

2. Autodesk Inc. (2018). Creative Commons. Retrieved from http://help.autodesk.com