AUTODESK **UNIVERSITY** 2013

The Rock, Paper, Scissors of Autodesk Vault Security

Irvin Hayes Jr., Autodesk, Inc.
Adam Luttenbacher, Autodesk, Inc.
Rob Stein, Autodesk, Inc.

PL2082 Have you ever wondered about the details of the Autodesk Vault software security model and how it works? If so, then this class is for you. During this class, we show you what beats what in the Vault security model. We discuss Vault roles and the "role" they play in security. We cover folder permissions, lifecycle state-based security, ACLs and OACLs. After this class, you will be able to win every time with Vault security.

Learning Objectives

At the end of this class, you will be able to:

- Describe Vault roles and their use
- Correctly apply folder-level permissions
- Explain state-based security
- Apply Vault security to real-world scenarios

About the Speaker

Irvin Hayes Jr. is a product manager for the data management group at Autodesk in Novi, Michigan. Irvin has worked at Autodesk for eight years starting in product support and as a user experience designer. Irvin is a Microsoft® Certified Professional, and has been working in the information technology field for more than 19 years.

Introduction

Understanding how to apply security to users and groups inside of a Vault environment can be like playing Rock, Paper, Scissors if you don't understand how it works. Understanding what security is set on an object at any given time needs to be easy to understand and easy to configure once you have the understanding. This class is meant to help you understand how permissions and security work inside of Vault so that you can configure your environment to work for your security needs.

Roles and Permissions

Users/Groups

Users - user account that allow individuals to log into vault. These accounts are created and administered in the User Management dialog box.

Groups - a collection of users that can be configured together with specific permissions. Groups are created and administered in the Groups dialog box.

Roles

Role - A name associated to a group of permissions which allows the user to perform specific actions. Roles vary depending on the edition of Vault you are using.

Role	Details
Custom Object Consumer	Read-only access to Custom Objects only.
Custom Object Editor Level 1	Basic Custom Object adding and editing privileges within the vault, and add/remove Custom Object user-defined properties privileges. Cannot delete Custom Objects. Does not have administrative privileges on the server.
Custom Object Manager Level 1	Privileges to change category, lifecycle, and revision assignments, and to edit user-defined properties.
Document Consumer	Read-only access to files and folders only, including the job server queue.
Document Editor Level 1	Basic file adding and editing privileges within the vault, also add/remove file and folder user-defined properties, but cannot delete files and folders. No administrative privileges on the server.

Document Editor Level	Full privileges within the vault, also add/remove file and folder user-defined properties, but no administrative privileges on the server.
Document Manager Level 1	The privileges to change category, lifecycle, and revision assignments, and to edit user-defined properties.

Permissions

Permissions - authorization to perform specific actions such as checking in a file, creating a change order or editing a custom object. For instance, a Document Consumer has the permission to only Read a file but a Document Editor can create and check-in a file. When multiple roles are assign to a user or group, the user has the ability to perform all actions that the roles give them authorization to perform. The roles act as a union by combining all permissions together for the user or group.

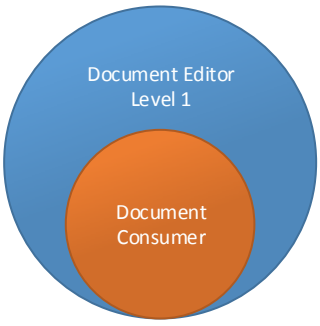
Examples:

- File Check In
- File Check Out
- File Create
- File Delete Conditional
- File Delete Unconditional
- File Read
- File Rename

When users are assigned to multiple roles, the effective permissions for the user is the combined permissions from all of the roles the users are assigned. For example if a user is assigned the Document Consumer and Document Editor Level 1 roles, he will have all the permissions of both roles.

Document Consumer
File Read
Folder Read

Document Editor Level 1
File Read
Folder Read
File Create
File Check In
File Check Out
Folder Create
Folder Read



Object Security

Object security is based on an Access Control List (ACL) which controls whether the member can only view the content, modify the content and delete the content. There are three ways to define the security of an object. They are role-based security, object-based security, and state-based security. If an object has no security defined, then security is determined by role. State-based security overrides object-based security. If the object has no security, then the permissions are defined by role.

This level of security is available in Vault Workgroup and Professional editions.

The lack of a user appearing in the ACL will result in the user having “No Permission”. This is not a deny of permission, they are just not allowed to perform the specific permission.

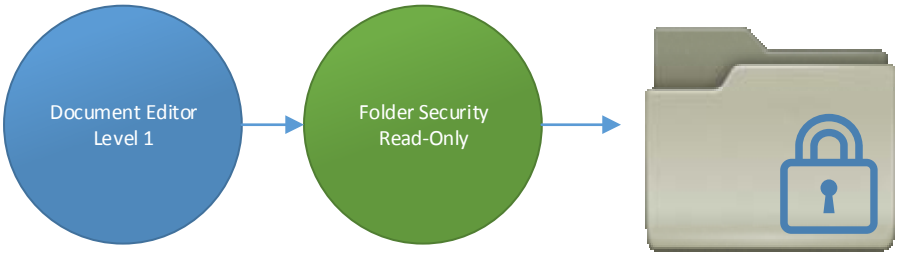
By selecting “Deny” for a specific permission, the user will be explicitly denied to perform the permission overriding any other settings that would explicitly give them “Allow” permission.

Permission Precedence

1. Deny
2. Allow
3. No permission

Folder Security

A folder that does not have an Access Control List defined uses role-based security. By default, no members are assigned to folders, meaning that all users have access to all folders. Once an ACL is defined for a folder, the ACL permissions combine with the role based permissions to create a more restrictive and more focused security model (object-based security). Roles are used first to determine permissions and then the ACL allows you to be more restrictive. For example, a user with a read-only role will never have more than read-only access regardless of the ACLs to which they belong. Conversely, if a user is assigned a role with full permissions, an ACL can be used to restrict that user within specific folders. The ACL can never give a user more permissions than the roles assigned to the user. When adding users to an ACL, consider the roles assigned to the users and restrict the users accordingly within the folder structure.



By default, the Administrator role has read access to all folders. The best practice for creating a vault security model is to first create an administrator group containing all of the administrators. Add the administrator group to the ACL to the top most folder in the vault, giving the group full access. Once the administrator group has been granted access, create groups and assign users to the groups. By assigning users to groups and then granting folder membership to those groups, you can easily manage users and their access to vault folders. By default, every new user is added to the Everyone group. If the Everyone group is granted membership to a folder, all new users will have access to that folder.

Files inside of the folder will share or inherit the security of the folder until a different security setting is set on the specific file.

Permission	Access
Read	• Apply - Vault security to real-world scenarios • Deny - The folder and files in the folder cannot be viewed and this overrides any Read Allow permission. • None - The folder and files in the folder cannot be viewed.
Modify	• Allow - The folder and files in the folder can be modified. • Deny - The folder and files in the folder cannot be modified. This overrides any Modify Allow permission. • None - The folder and files cannot be modified.
Delete	• Allow - The folder and files can be deleted. • Deny - The folder and files cannot be deleted. This overrides any Delete Allow permission. • None - The folder and files cannot be deleted.

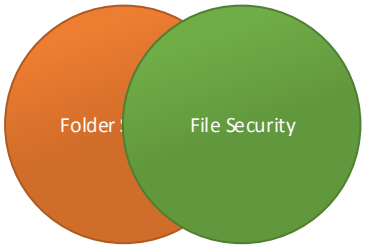
Short-cuts of objects in the folder will follow the permission of the folder where the object is at.

Propagate Folder Permissions

- Do not propagate to child folders–The security settings are used for the current folder only. Changes are not propagated to sub-folders.
- Propagate only changes (append permissions)–Any users or groups that have been added to or removed from the Override Access Control List on the current folder are added to or removed from the sub-folders. Any changes to users or groups assigned to the current folder are propagated to any sub-folders that also have those users and groups assigned. This is the default setting.
- Propagate entirely (replace permissions)–The Override Access Control List and the permissions are used for the current folder and all sub-folders contained in the current folder.

File Security

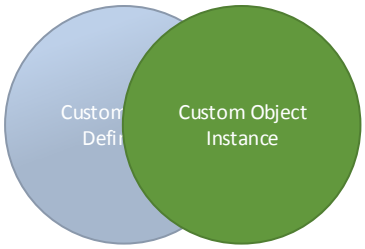
You can specify user and group access on specific files by modifying the ACLs on that file. This will override any folder or state level of security that was previously created.



Permission	Access
Read	• Allow - Files can be viewed. • Deny - Files cannot be viewed. This overrides any Read Allow permission. • None - Files cannot be viewed.
Modify	• Allow - Files can be modified. • Deny - Files cannot be modified. This overrides any Modify Allow permission. • None - Files cannot be modified.
Delete	• Allow - Files can be deleted. • Deny - Files cannot be deleted. This overrides any Delete Allow permission. • None - Files cannot be deleted.

Custom Object Security

When a Custom Object definition is created, the permissions set on the definition will be applied to all instances of the Custom Object. Permissions can be set on an individual Custom Object to override the permission set on the Custom Object definition.



Permission	Access
Read	• Allow - Object can be viewed. • Deny - Object cannot be viewed and this overrides any other Read Allow permission. • None - Object is not visible to the user
Modify	• Allow - Object can be modified. • Deny - Object cannot be modified and this overrides any other Modify Allow permission. • None - Object cannot be modified.
Delete	• Allow - Object can be deleted. • Deny - Object cannot be deleted and this overrides any other Delete Allow permission. • None - Object cannot be deleted.

Override Security Settings

Folder, file and custom objects security can be manually override at any time.

When your override the security on a folder, files in that folder will inherit the folder security ACLs as long as there are no lifecycle or override security set on the file.

You can view the override setting and compare them to the Role or Object based security by clicking the Security Mode drop-down and select the other security mode. This doesn't remove the override but gives the administrator the ability to see what was overridden.

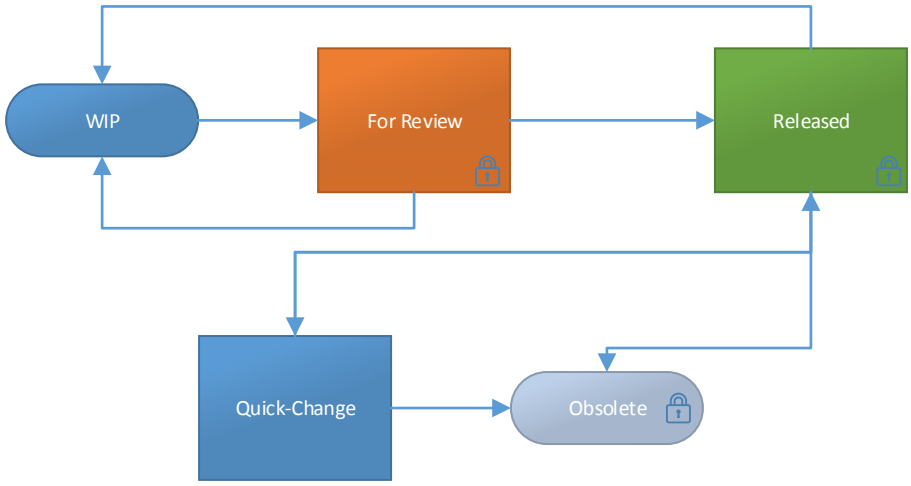
Lifecycle Security

A lifecycle definition 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.

Lifecycles can be used with files, project folders, and custom objects.

State-based Security

State-based security controls which members and groups can read, modify, or delete an object assigned to a state from the Security tab of the Lifecycle Definition dialog box. State-based security can be set by an Item Lifecycle or a file level lifecycle.



Permission	Access
Read	• Allow - States can be viewed. • Deny - States cannot be viewed. If a member is denied read access then they are not allowed Modify or Delete access either. • None - State cannot be viewed.
Modify	• Allow - States can be modified. • Deny - State cannot be modified. • None - State cannot be modified.
Delete	• Allow - State can be deleted • Deny - State cannot be deleted. • None - State cannot be deleted.

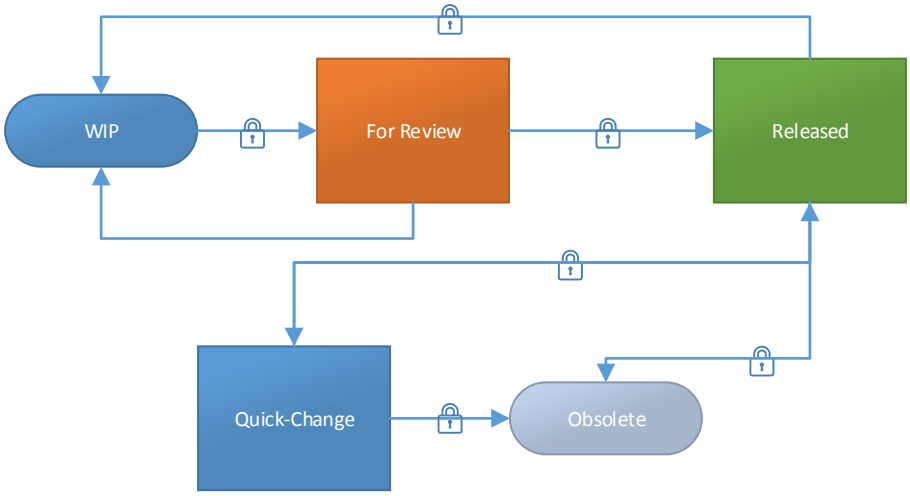
State Transition Security

Defining security for a transition dictates who can make the transition. When no security restrictions are in place for this transition, then anyone with access to the system can invoke the Change State command.

Permission

Allow - User or group is allowed to make the transition.

Deny - User or group is not allowed to make the transition.

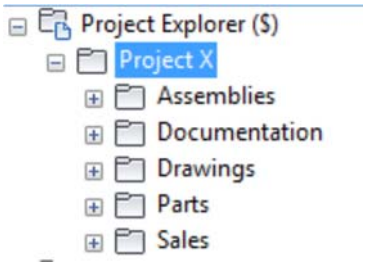


Making it Work for You

Let's look at some real world scenarios to help you understand how security works.

Scenario 1

Truetechnology is beginning to deploy Autodesk Vault and they have users in manufacturing, engineering, shop floor, sales and marketing and technical publishers. His users are divided into the appropriate groups inside of Vault and he needs to setup a project with specific security on each folder. All users are given the Document Editor Level 2 role which gives them the enough permissions to work with files under the project folders. He creates the following folder structure.



On the Project X folder, he is going to add the Administrators, Engineering, Product Design, Manufacturing, Sales & Marketing and TechPubs groups. He will give the Administrators group Read, Modify and Delete Allow permissions and Read Allow permissions to the other groups. The ACLs that are created are now propagated down to the sub-folders. At this point on the Administrator has the permission to make any changes to files or folders within the Project X structure. To change this, he will now edit the Assemblies, Drawings and Parts folders and give the Modify and Delete Allow permissions to the Manufacturing and Engineering groups. On the Documentation folder he will give the TechPubs and Product Design groups Modify and Delete Allow permissions. On the Sales folder he gives the Sales & Marketing group Modify and Delete Allow permissions.

Effectively he has given all groups Read permissions to each folder but only certain groups can modify the folder contents. The ACLs placed on the folders will restrict the group's permissions on the folders although their Role gives them more capabilities.

Effective permissions for each group:

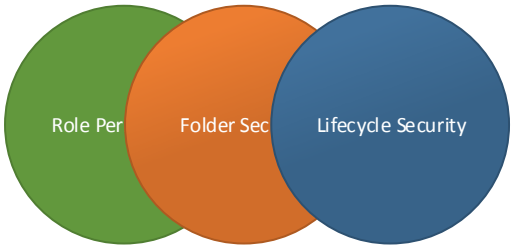
	Assemblies	Documentation	Drawings	Parts	Sales
Administrators	R/M/D	R/M/D	R/M/D	R/M/D	R/M/D
Engineering	R/M/D	R	R/M/D	R/M/D	R
Product Design	R	R/M/D	R	R	R
Manufacturing	R/M/D	R	R/M/D	R/M/D	R
Sales & Mkt	R	R	R	R	R/M/D
TechPubs	R	R/M/D	R	R	R

Scenario 2

Now that the folder permissions are set it is time to modify the lifecycles so that they can be used on the files in the project folder. He is going to modify the Basic Release Process lifecycle definition for files that will be in the Assemblies, Drawings and Parts folders. He has also added a new group called Reviews which can markup files that are in the Review state.

	Work in Progress	For Review	Released	Obsolete
Administrators	R	R	R	R
Engineering	R/M/D	R	R	R
Product Design	R	R	R	R
Manufacturing	R/M/D	R	R	R
Sales & Mkt			R	
TechPubs		R	R	R
Reviewers	R	R/M/D	R	

When files are assigned a category and the Basic Release Process lifecycle, the lifecycles ACLs will override the folder security and restricts the role based permissions.



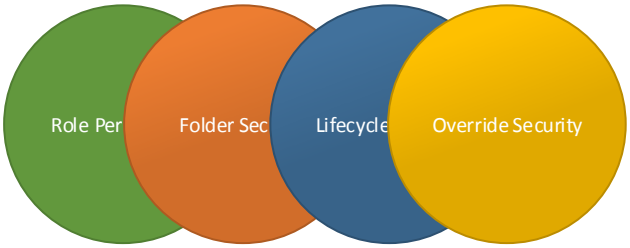
Now he creates a new lifecycle for the documents that are added to the documentation folder.

	Work in Progress	For Review	Released	Obsolete
Administrators	R	R	R	R
Engineering		R	R	R
Product Design	R/M/D	R	R	R
Manufacturing		R	R	R
Sales & Mkt	R/M/D	R/M/D	R	R
TechPubs	R/M/D	R	R	R
Reviewers	R	R/M/D	R	

Scenario 3

A member of the Product Design group has add a Word document to the documentation folder and has placed it in the For Review state. He has been told that a member of the Engineering group has read the document but would like to add some comments to it. Due to the lifecycle security currently on the file, this member has Read-Only permissions to the document and therefore cannot add comments. The Product Design member asks an Administrator to override the security on the file, add the Engineering member and give him Modify permissions to the file. Since the file's security is overridden the lifecycles ACLs no longer applies to the file.

This override will remain until the override has been removed manually or the file is placed into a different lifecycle state.



Vault Family and Security

Basic – Users/groups and roles.

Workgroup - Users/groups, roles, ACLs, and state security

Professional – Users/groups, roles, ACLs, state security, Item and Change Order security.

Conclusion

You should now have a good understanding of how Vault security works and when to know which security ACL is controlling your Vault object. With this knowledge you should be able to implement security at any level inside of Vault and take ultimate control of your data.