

Security Awakens: Defending Against the First Order

Irvin Hayes Jr.
Autodesk Inc.

Learning Objectives

- Learn how to configure object level security
- Learn how to configure lifecycle state level security
- Learn how object and lifecycle level security work together
- Learn how users are affected by the security settings

Description

The First Order has risen and will stop at nothing to get to your data. Vault security can be complex and confusing if you do not understand how it works. This class is essential for administrators who want to learn the different security models within Vault. The main focus of the class is to cover object and lifecycle level security. Learn how object level security sets or denies access to objects for users or groups. Learn how lifecycle security sets or denies access to objects based on the state of the object. Finally, learn how object and lifecycle state security are combined to work together to control object access, which is new in Vault 2017. Leave with the knowledge needed to awaken your security needs and restore peace and justice to your Vault. Defend against the First Order.

Your AU Expert(s)

Irvin is a Product Manager on the Autodesk Vault team based in Novi, Michigan. He has worked at Autodesk for eleven 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 25 years. He helps partners, consulting, and sales develop Vault deployment plans in enterprise environments and system requirements. You can find multiple classes Irvin has presented at Autodesk University, on a wide range of Vault topics. Irvin is a technology geek and loves sharing with the community on Twitter ([@ihayesjr](#)) and [Flipboard Magazine](#).

Contents

Learning Objectives	1
Description	1
Your AU Expert(s)	1
Introduction	3
Understanding Security	3
Roles and Permission	3
Configuring Object-based Security	5
What is Object-based Security	5
Read\Modify\Delete Permissions	5
Allow & Deny	6
Configuring Lifecycle State Security	10
Lifecycle Based Security	10
Definition Security	10
Combined Security	14
Object-based and State-based Security Working Together	14
Gated Security	15
Effective Access	16
Overriding Security	17
Security Propagation	19
Related Classes	19

Introduction

This class is an overview of the Vault 2017's security model. It is a guideline created to help you understand security and how to configure security in different ways.

Understanding Security

Roles and Permission

Roles

Roles are a group of permissions combined and assigned to a user or group so that they can perform specific commands or actions within Vault. A few examples of roles shown below.

TABLE 1. ROLES

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

A permission authorizes users or groups 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 only to Read a file, but a Document Editor can check-in and modify a file.

Examples:

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

When multiple roles are assigned to a user or group, they act like a union combining all permissions together allowing the user to perform all permissions that each role gives them the authorization to perform. For example, if a user is assigned the Document Consumer and Document Editor Level 1 roles, he has all the permissions of both roles.

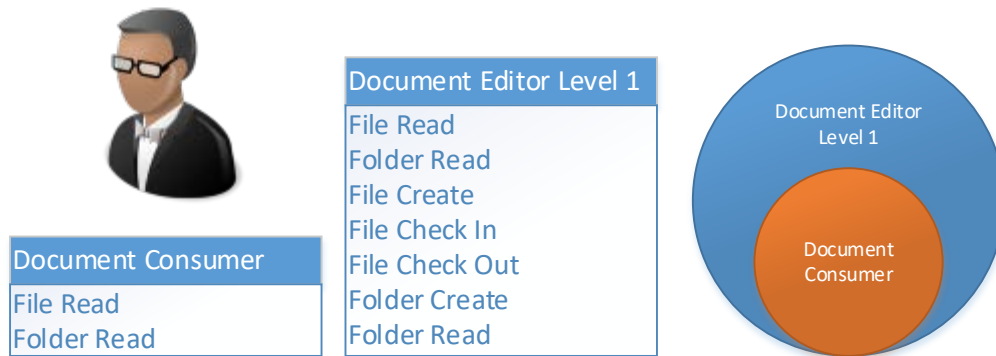


FIGURE 1. COMBINED ROLES

Configuring Object-based Security

What is Object-based Security

Object-based Security (OBS) is an ACL which controls whether the user or group can view, modify or delete the object.

Read\Modify\Delete Permissions

TABLE 2. READ\MODIFY\DELETE PERMISSIONS

Permission	Access
Read	<ul style="list-style-type: none">• Allow – grants Read permission on the object• Deny – explicitly denies Read permission on the object.• Null – implicitly denies Read permission on the object
Modify	<ul style="list-style-type: none">• Allow – grants Modify permission on the object• Deny – explicitly denies Modify permission on the object.• Null – implicitly denies Modify permission on the object
Delete	<ul style="list-style-type: none">• Allow – grants Delete permission on the object• Deny – explicitly denies Delete permission on the object.• Null – implicitly denies Delete permission on the object

Allow & Deny

As shown in Table 2, selecting Allow on a permission grants the user the ability to perform the permission. There are two types of denied security, implicit and explicit denies. An implicit deny is when a user or group is not granted a specific permission in the security settings of an object, but they are not explicitly denied either. If the administrator does not add the user or group to the object's Access Control List (ACL) or doesn't select the Allow or Deny options for any of the permissions, the user or group gets implicitly denied the permission to the object. Using the implicit deny can be an advantage because you can add an individual to the object and allow them specific permissions if needed. For example, if you have the Management group with Read permission on a file but you want to allow one user in the Management group to Modify the file, you can add the individual user to the files ACL and select the Allow option for the Modify permission. Using this method allows the individual user to modify the file even though the group they are in only has the Read permission. An implicit deny only denies a permission until the user or group is allowed to perform the permission from a different setting.

The explicit deny is when the administrator has selected the Deny option for a permission for a user or group. This Deny takes precedence over all allowed settings. The administrator has explicitly set the permission, and there is no way around it. Only use the Deny option if you mean to deny the user or group at all cost. If the administrator has set the Deny Read option on an object for a group, all members of that group are not able to read the object. If the administrator adds a user to the ACL and gives them the Allow Read permission and that user is a member of that group, they still are not able to read the object. See Figure 2 below.

Permission Precedence

1. Deny
2. Allow
3. No permission

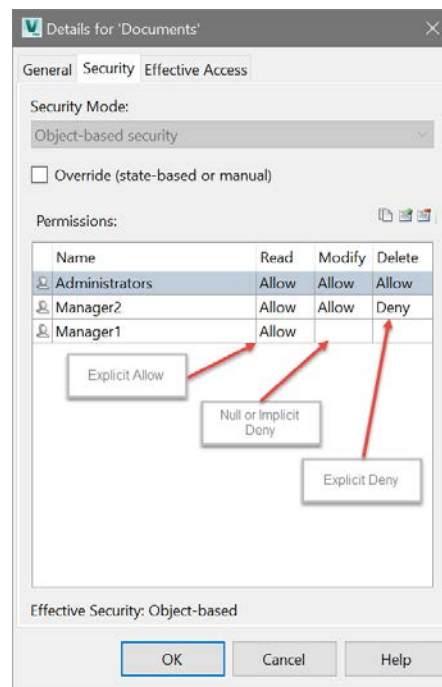


FIGURE 2 – SECURITY TAB

Folder Security

In new Vault, folders do not have entries in the security ACL. Without a security ACL, all users or groups are granted all permissions on all folders. After an ACL gets added to a folder, the ACL permissions combine with the role based permissions to create a more restrictive and more focused security model. For example, a user with a read-only role never has more than read-only access regardless of the ACLs settings which give them more permissions. Conversely, if a user is assigned a role with full permissions, an ACL can be used to restrict that user within a specific folder. 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.

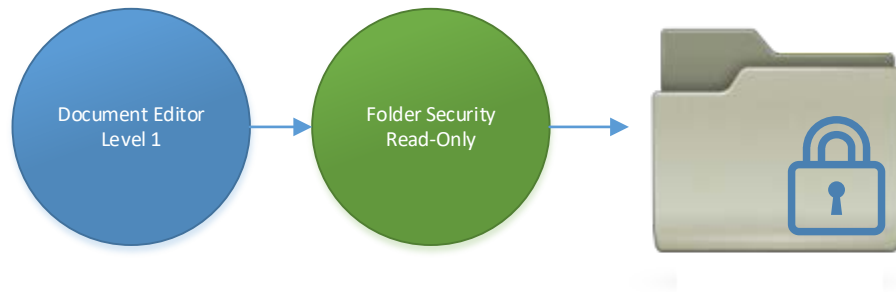


FIGURE 3. FOLDER SECURITY

By default, the Administrator role has read access to all folders. It is recommended to create an administrator group containing all of the administrator user accounts. Add the administrator group to the ACL of the topmost folder in the vault and set the Allow option for all permission giving them full access. Once the administrator group gets granted access, create groups based on business roles or functions that suit your design process and assign users to the groups. By assigning users to groups and then adding the group to the folder ACL, you can easily manage users and their access to the vault folders. All users belong to a built-in group named Everyone. If the Everyone group is added to the folder ACL and allowed permissions to that folder, all new users have access to that folder. Files inside of the folder share or inherit the security of the folder until a different security setting gets set on the file.

TABLE 3. OBJECT PERMISSIONS

Permission	Access
Read	<ul style="list-style-type: none"> • Allow – the folder and files in the folder can be viewed • Deny – the folder and files in the folder cannot be viewed, and this overrides any Read Allow permission. • Null – the folder and files in the folder cannot be viewed.
Modify	<ul style="list-style-type: none"> • 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. • Null – the folder and files cannot be modified.
Delete	<ul style="list-style-type: none"> • Allow – the folder and files can be deleted. • Deny – the folder and files cannot be deleted. This overrides any Delete Allow permission. • Null – the folder and files cannot be deleted.

File Security

You can specify user and group access to specific files by modifying the ACLs on that file. The security set on the specific file gets combined with the folder permissions providing an improved level of security for the file. Alternatively, you can override the folder level security on the file.

TABLE 4. FILE SECURITY

Permission	Access
Read	<ul style="list-style-type: none"> • Allow – files can be viewed. • Deny – files cannot be viewed. This overrides any Read Allow permission. • Null – files cannot be viewed.
Modify	<ul style="list-style-type: none"> • Allow – files can be modified. • Deny – files cannot be modified. This overrides any Modify Allow permission. • Null – files cannot be modified.
Delete	<ul style="list-style-type: none"> • Allow – files can be deleted. • Deny – files cannot be deleted. This overrides any Delete Allow permission. • Null – files cannot be deleted.

Override Security Settings

Folder, file and custom objects security can be manually overridden at any time. When you override the security on a folder, files in that folder inherit the folder security ACLs as long as there is 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 model. Selecting an option from the drop-down does not remove the override but gives the administrator the ability to see what got overridden.

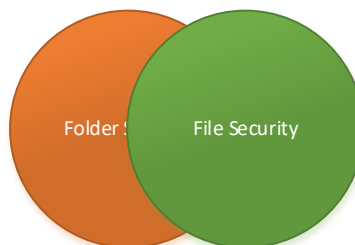


FIGURE 4. OVERRIDDEN FILE SECURITY

Configuring Lifecycle State Security

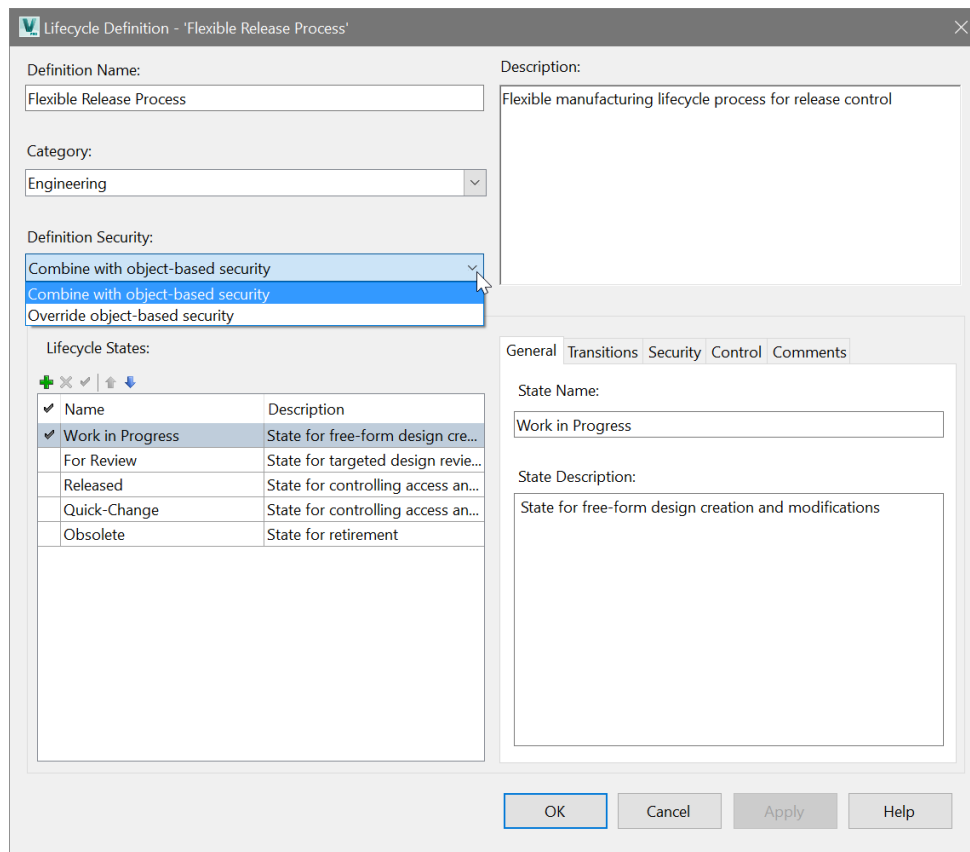
Lifecycle Based Security

A Lifecycle State can contain security settings to control access to an object within a state. The security controls who can read, modify and delete a file based on the lifecycle state.

Definition Security

The Definition Security drop-down has two options which dictate how the Lifecycle Security works with the object-based security settings.

- Combine with object-based security – the Lifecycle Security combines with the object-based security to make a flexible security model. New definitions have this as the default setting.
- Override object-based security – the Lifecycle Security overrides the object-based security making a less flexible security model. Lifecycles migrated from the previous releases have this option selected so that it does not change the workflow.



Lifecycle Definition - 'Flexible Release Process'

Definition Name: Flexible Release Process

Category: Engineering

Definition Security: **Combine with object-based security**

Description: Flexible manufacturing lifecycle process for release control

Lifecycle States:

Name	Description
✓ Work in Progress	State for free-form design cre...
For Review	State for targeted design revie...
Released	State for controlling access an...
Quick-Change	State for controlling access an...
Obsolete	State for retirement

General | Transitions | **Security** | Control | Comments

State Name: Work in Progress

State Description: State for free-form design creation and modifications

OK Cancel Apply Help

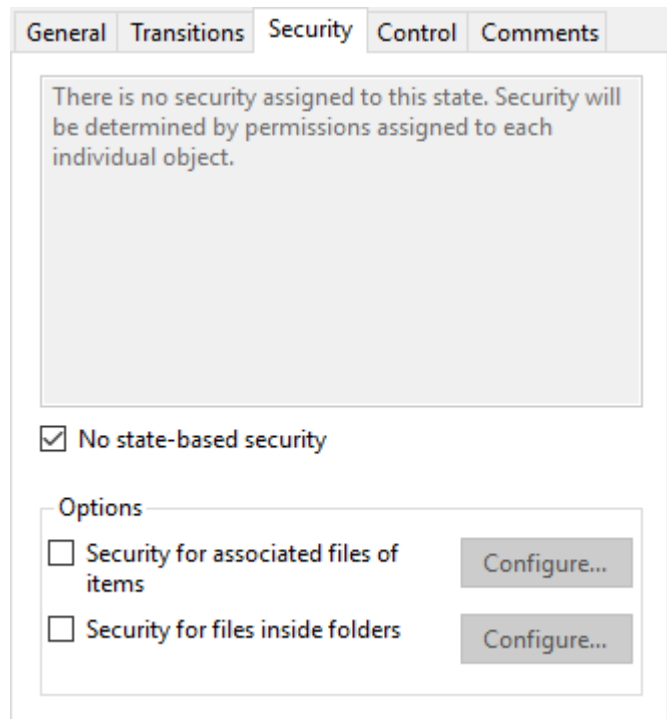
FIGURE 5 - LIFECYCLE DEFINITION

Security Options

The Security tab in the Lifecycle definition is where you modify the ACL settings to set the security for the state.

Note: making security changes do not affect objects that are already in a state. A state change must occur for the security settings to be applied.

- No state-based security – no security is configured for the lifecycle state, so security is determined by the security already set on the object.
- Security for associated files of items – security set on the file's SBS
- Security for files inside folders – security set on the file's SBS



The screenshot shows the 'Security' tab selected in a tabbed interface. The tabs are 'General', 'Transitions', 'Security', 'Control', and 'Comments'. The main content area contains a message: 'There is no security assigned to this state. Security will be determined by permissions assigned to each individual object.' Below this message is a checked checkbox labeled 'No state-based security'. Underneath, there is an 'Options' section with two unchecked checkboxes: 'Security for associated files of items' and 'Security for files inside folders'. Each checkbox has a 'Configure...' button to its right.

FIGURE 6 – SECURITY TAB

Security for Associated Files of Items

When entering a state for an Item the security is set on the Item and the associated files as well. To configure the security for Item associated files, check the Security for associated files of items option and click the Configure button.

The Security for Associated Files of Items dialog has the following options:

- Apply item security to associated files
When selected, the Access Control List (ACL) settings for the item for this state are also applied to the associated file.
- Apply custom security to associated files
When selected, administrators can set an ACL that is different from the one applied to the item for that state.
- Clear security override from associated files
When selected, if there is a current override ACL on the associated file, the security override is removed when the item enters this state

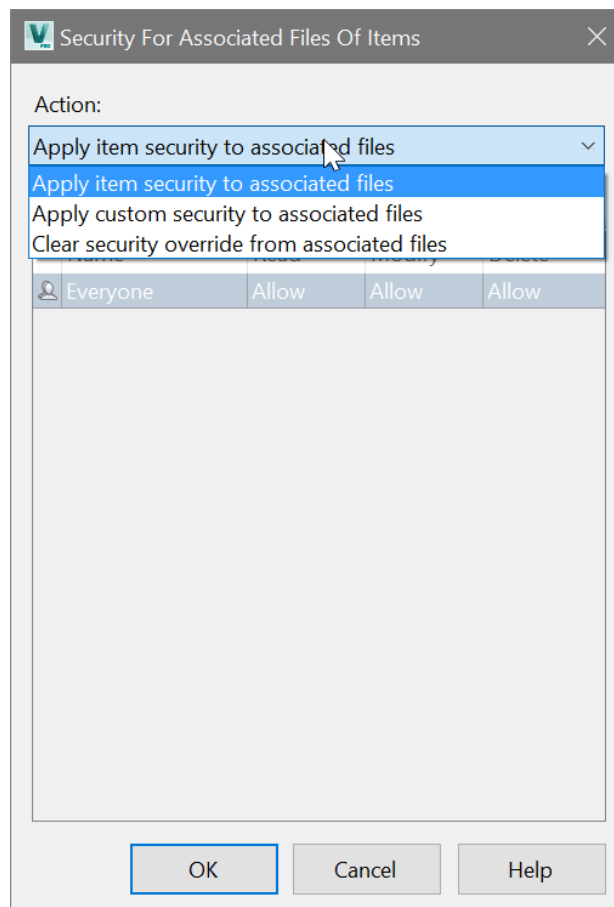


FIGURE 7. SECURITY FOR ASSOCIATED FILES OF ITEMS

Security for Files inside Folders

This setting applies security on files in a folder based on the folder's lifecycle state.

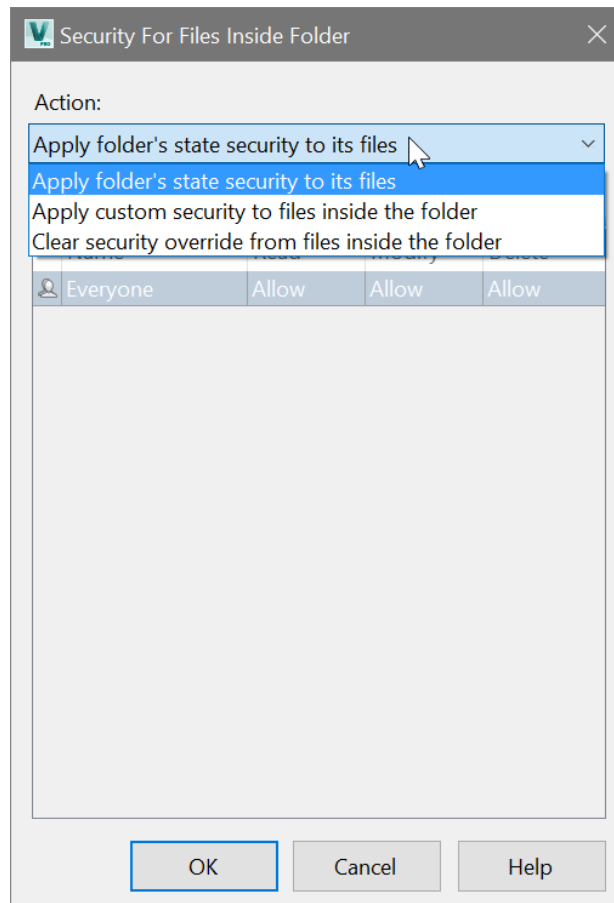


FIGURE 8 - SECURITY FOR FILES INSIDE FOLDER

On the Security for Files Inside Folder dialog, select one of the following actions from the drop-down:

- **Apply folder's state security to its files**
When selected, the Access Control List (ACL) settings for a folder in this state are also applied to the files inside the folder.
- **Apply custom security to files inside the folder**
When selected, administrators can set an ACL for the files in a folder that is different from the ACL applied to the folder in this state.
- **Clear security overrides from files inside the folder**
When selected, if there is a current override ACL on the files inside a folder, the security override is removed from the files when the folder enters this state.

Combined Security

Object-based and State-based Security Working Together

When object-based and state-based security get set on an object, they combine to protect allow or deny users access. You can say that they work like security gates to the object. The users must be able to pass through all permission gates before the user can perform the permission on the object.

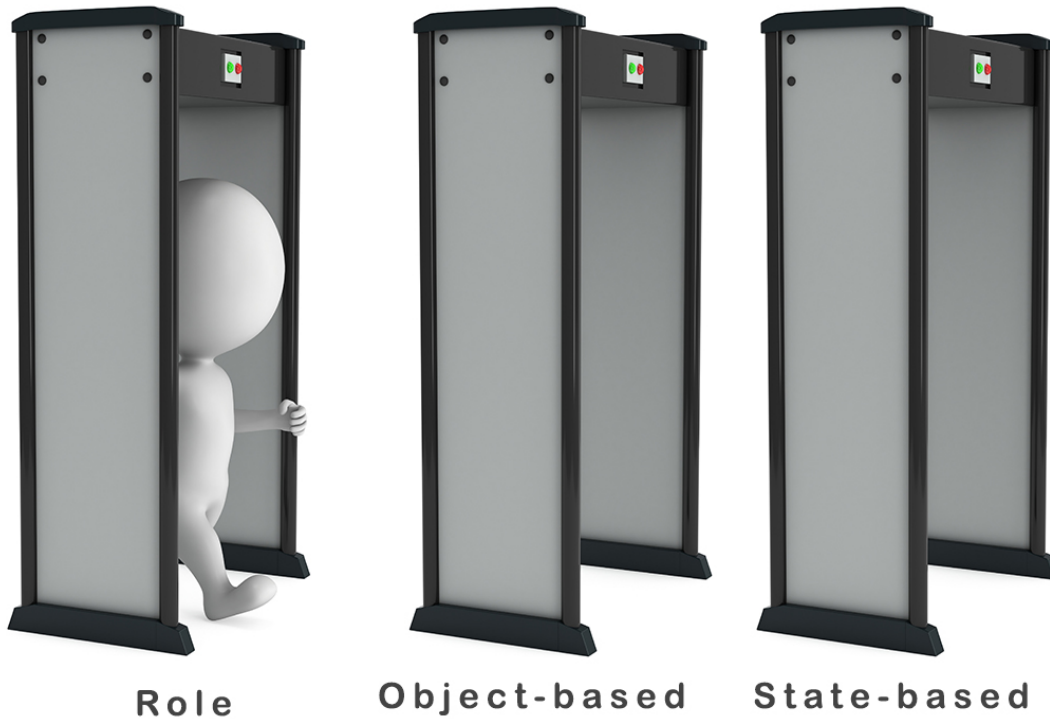


FIGURE 9 - SECURITY GATES

Gated Security

The following table illustrated the effective access for users when object-based and state-based security are combined to work together. Even when the object-based and state-based ACLs are swapped, the effective permission remains the same.

TABLE 5

Object -based	State-Based	Effective Permission
Allow	Allow	Allow
Deny	Deny	Deny
Deny	Allow	Deny*
Null	Deny	Deny
Allow	<i>Null</i>	Deny
Null	<i>Null</i>	Deny
Null	Allow	Deny*
Allow (Group A)	Allow (Group B)	Allow* (intersect group)

* Resulting permission is different from legacy security model.

Note: “Null” means neither Allow nor Deny exists (i.e. “implicit deny”).

Effective Access

The Effective Access tab helps administrators understand the how the configured security of an object affects individual users access to the object. The tab has a drop-down with four different options; Effective Access, State-based security, Overridden security, and Object-based security. Add and remove users from the list and select the different options to see how each security level sets the effective access for the user. You cannot edit the security in this tab. Edits made on the Security tab updates the Effective Access tab, and you see the effects of the change.

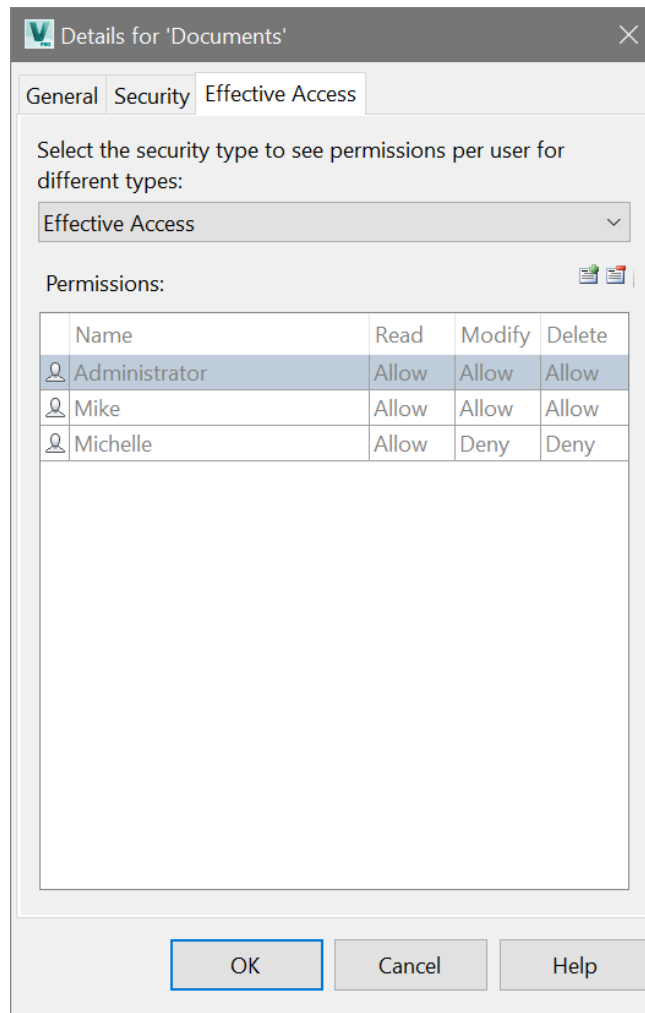


FIGURE 10 – EFFECTIVE ACCESS

Overriding Security

When thinking about object-based and state-based security, it is better to think that the security settings reside in two different layers. Let's call them the lower and upper layers of security. OBS sits in the lower layer and SBS sits in the upper layer. Overridden security settings reside in the upper layer when configured.

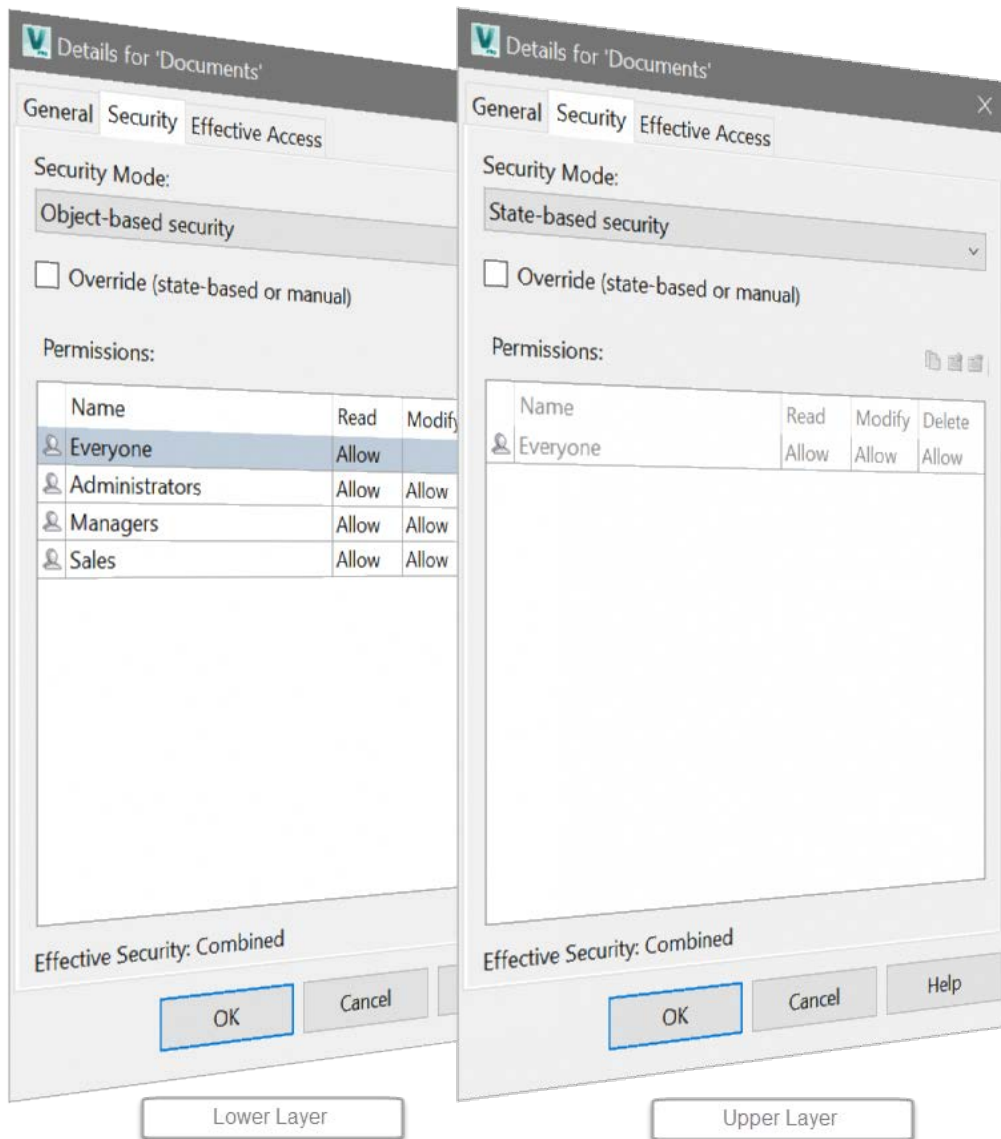


FIGURE 11 - SECURITY LAYERS

When you need to override security settings temporarily on a file or folder, select OBS or SBS in the Security Mode drop-down list in the Security tab. Click the Override checkbox and the settings start with the security settings from the option you selected. Modify the security as needed but before you click the OK button, go to the Effective Access tab and add users so that you can see the effects of your change. The changes are not committed until you click the OK button.

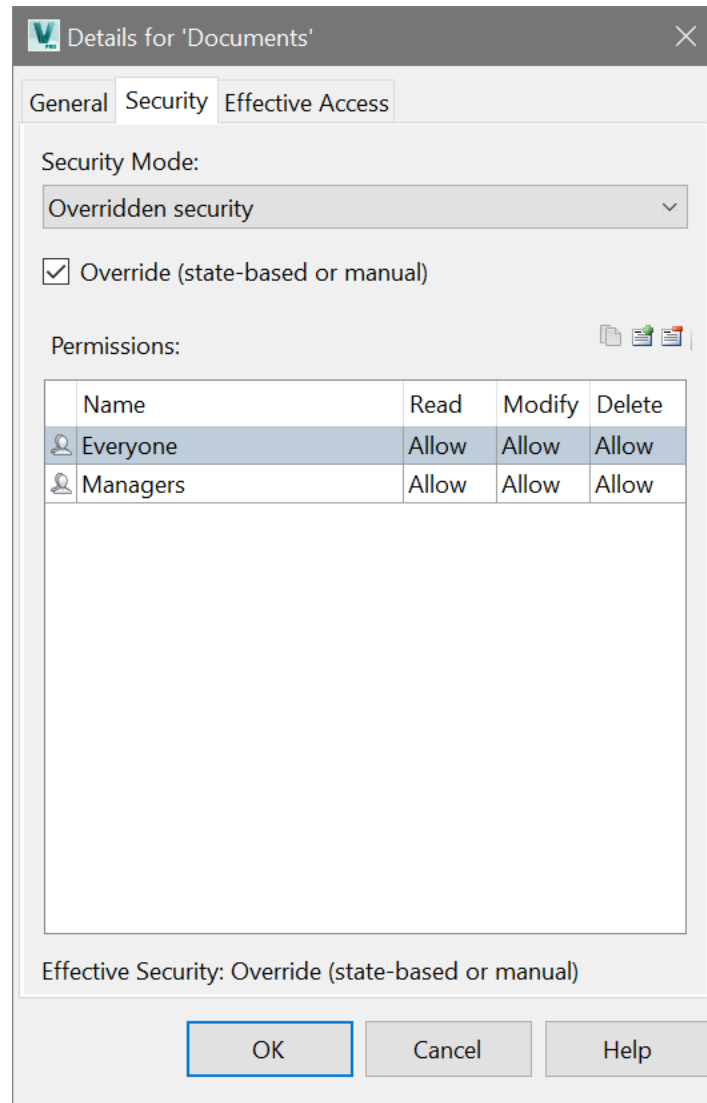


FIGURE 12 - OVERRIDE SECURITY

Security Propagation

Now that you have an understanding of security, you need to understand how the propagation of security settings work. After you have modified the ACLs on a folder, a prompt appears with propagation options for the new settings.

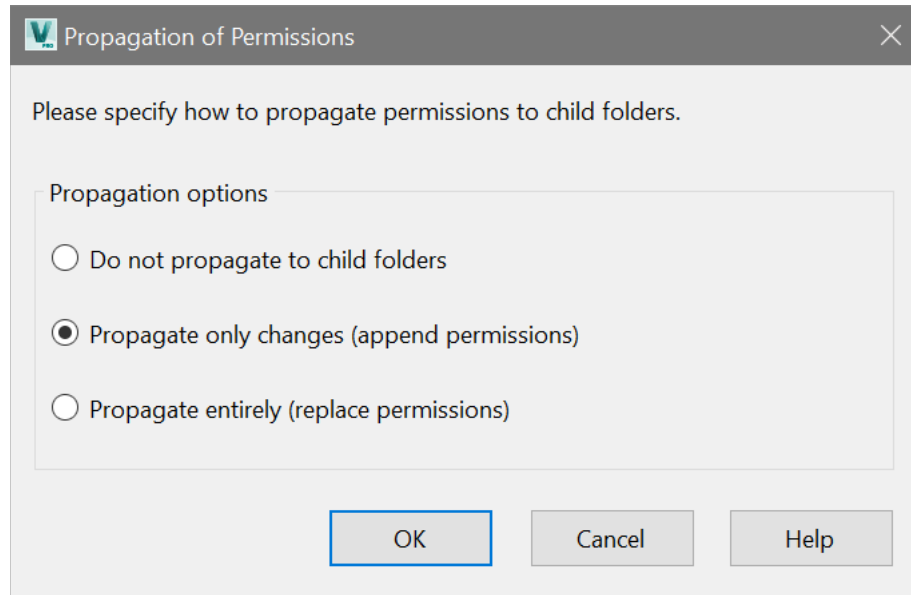


FIGURE 13 - PROPAGATION OF PERMISSIONS

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

When the security is propagated to lower level folders and files within the folder, the OBS, or lower layer, settings get updated settings on those objects. The SBS, or upper layer, is not changed nor the overridden security settings on those objects. If the effective security is combined, the effective permissions get updated with the change of the object-based security.

Related Classes

[PL11664 – Behaviors 301 for the Jedi Master](#)

[PL2082 – The Rock, Paper, Scissors of Autodesk Vault Security](#)