

Eagle Eye Application Note - AN019

Eagle Eye VMS User Permissions Best Practices

2022-06-02 Revision 1.2

Target Audience

This Application Note is intended for administrator users of the Eagle Eye VMS. Specifically, admin users who will be adding or editing users and controlling what they have access to. A basic understanding of the VMS is recommended before managing user permissions.

Introduction

The Eagle Eye Cloud VMS offers powerful user access rights to define who can perform which functions within the system. It is important to understand this to avoid any security vulnerabilities within the system and to define clear roles for each user that has access. In addition, there are two levels of users that can have access granted to the system; one for the Reseller Account and one for End User Accounts (end-users). In this App Note, we will explain how to give access to users for each account level, review all different permissions, and will outline associated configuration and camera access as well as recording and more.

User access and permissions are available to all Editions of the VMS (Standard, Professional, Enterprise).

User Access

When Resellers sign up and are given access to the Eagle Eye Networks Cloud VMS, a Reseller account user is created and by default, will have administrator rights. This user has all rights to the system which means they can create new users. These can be on the Reseller account level or the End User account level.

To create a new user to access your **Reseller account**, go to the left menu and select "Users":

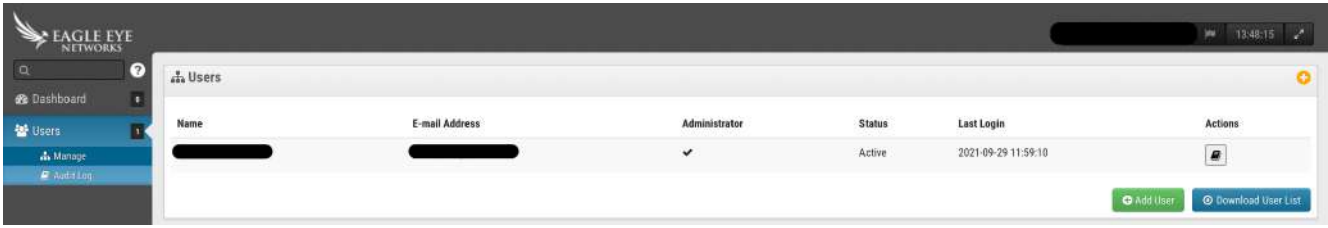


Image 1: An image of where to find the Users window from the left-hand menu

Click on the “+ Add User” button and a new window will popup. Fill in all details such as name, email, access, accounts and permissions. Be aware that this user will be created on the Reseller account level, so be careful of which rights are given to users, which End User accounts they can access, and all permissions provided.

To create a new user account on the **End User account** level, just choose the appropriate account to access by clicking on the “eye” icon as shown below:

Status	Account Name	Bridges/CMVRs	Cameras	Avg. Retention	Users	Last Login	Actions
✓	Account 1				0		<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
✓	Account 2				0		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Image 2: Click on the “eye” icon next to the appropriate account to setup a new user

After entering the End User account, select “Users” from the left menu:

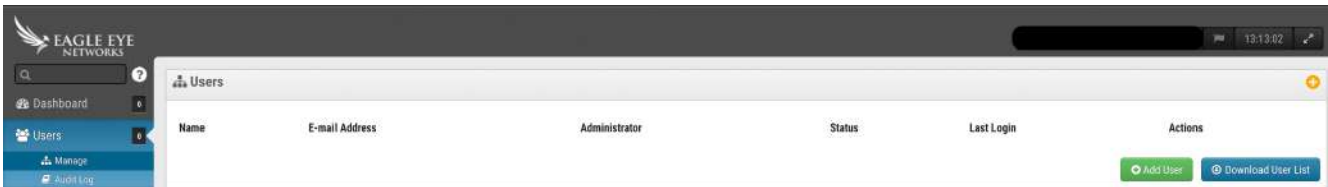


Image 3: Click on the +Add User button to add a new user

Click on the “+ Add User” button and a new window will popup. Fill in all details such as name, email, access, accounts/cameras/layouts and permissions. Be aware that this user will be created on the End User account level, so users will only have access to this account. Access and permissions will be explained below. In addition and depending on which account has been accessed, the Reseller account or the End User account, the popup window will be different.

For the Reseller account, the 3rd menu is about “Accounts” access. For the End User account, the 3rd menu is about “Cameras” access. There is also an additional menu called “Layouts.” See below for screenshots which describe menus related to each of the accounts, Reseller and End User.

New user window for Reseller account:

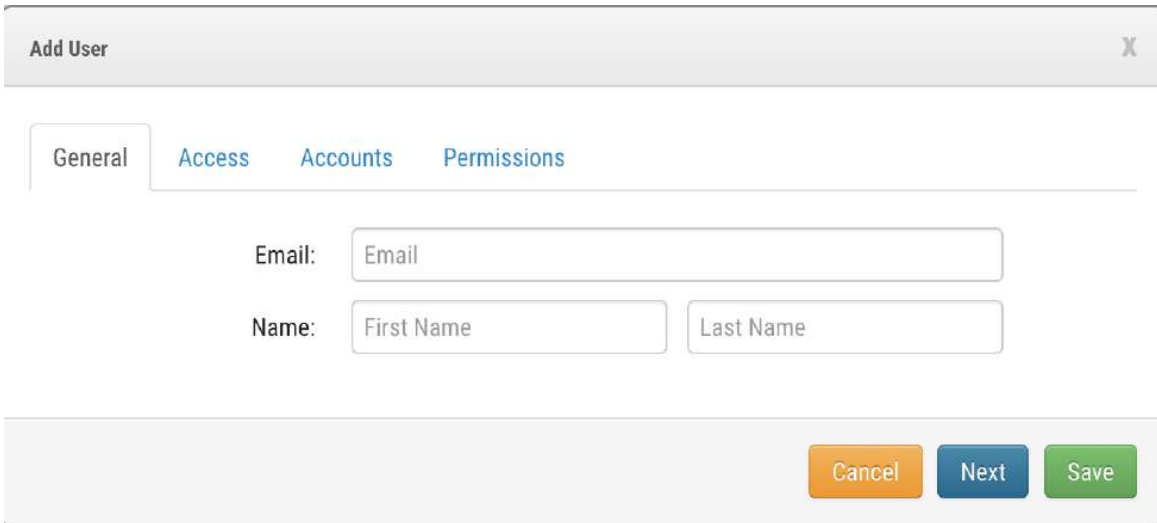


Image 4: Adding a new User window for the Reseller account

New user window for End User account:

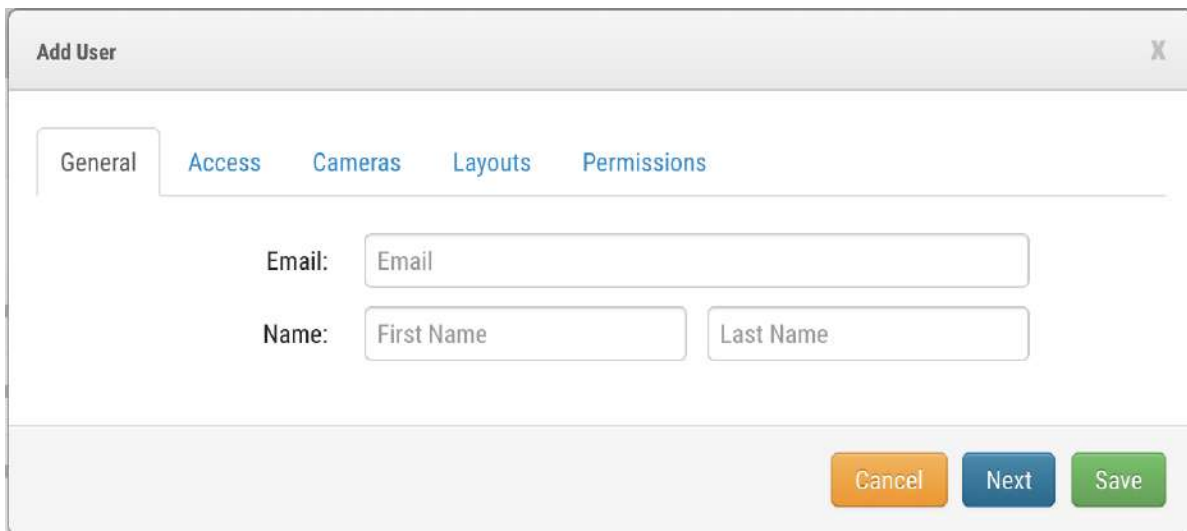


Image 4: Adding a new User window for the End User account

1. General

This is the same menu for both the Reseller and End User accounts. Fill in the First Name, Last Name and Email address. All information must be relevant and the VMS will send an email automatically so the user will be able to create their own password once received.

After filling in all fields, click Next.

Add User [X]

General | Access | Accounts | Permissions

Email:

Name:

[Cancel] [Next] [Save]

Image 5: Click Next to continue with the setup and move to granting Access

2. Access

This is the same menu for both the Reseller and End User accounts. In this menu, choose when the user can access the system depending on the days and times defined within the Access Period menu. Choose default times or create a custom access period. Employee ID is a custom field used to associate employee IDs so to easily identify them on Audit Logs when needed, then click Next.

Add User [X]

General | Access | Accounts | Permissions

Access Period: (US/Central) [?]

Employee ID:

[Cancel] [Next] [Save]

Image 6: Choose when the user can access the system and associate an Employee ID which will be seen in Audit Logs

3. Accounts (Only for the Reseller account)

Choose which End User account this user will have access to. Drag and drop from left to right and note that all accounts can be added by clicking the “Add All” button.

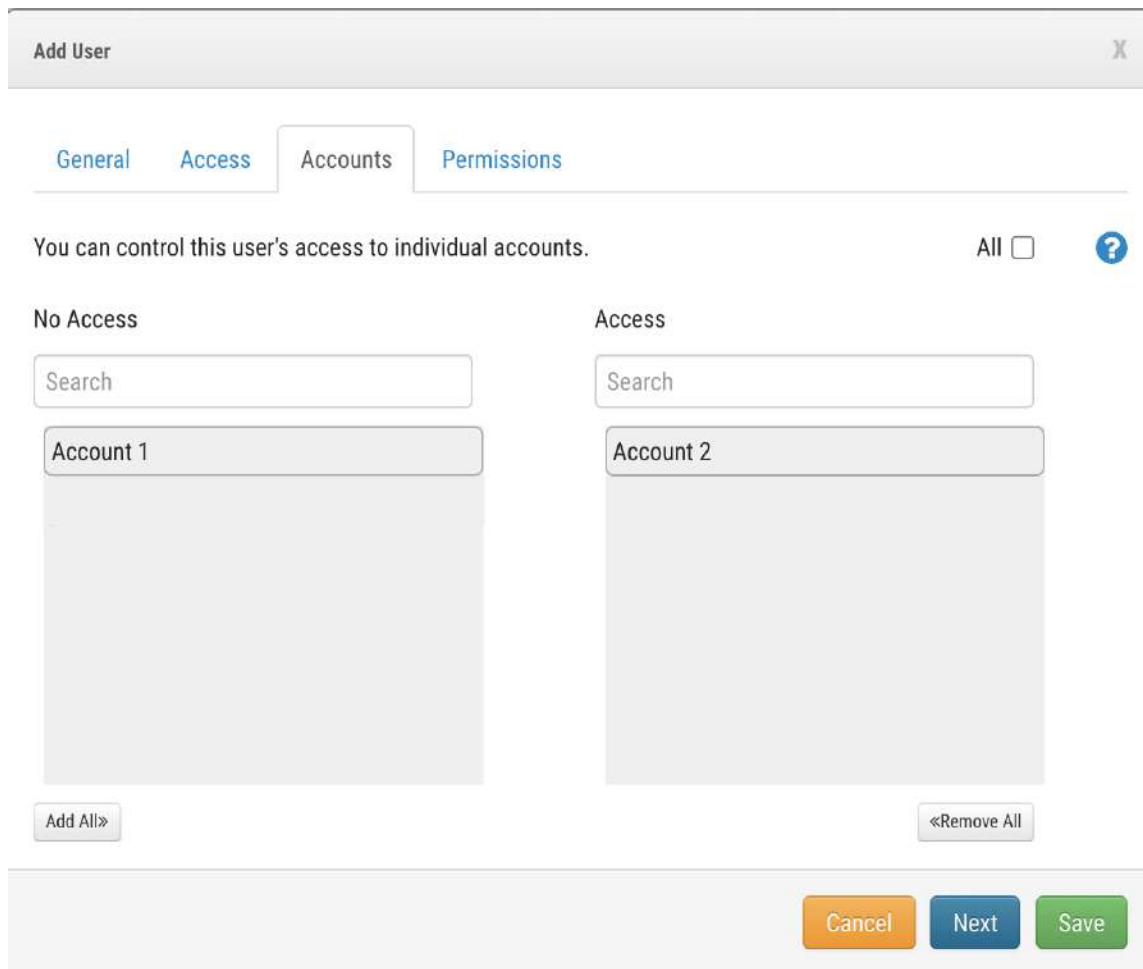


Image 7: How to determine which users have access to which cameras using the drag and drop tool. Use the Add All button if needed

If this user should have access to all accounts and all new accounts in the future, then check the tick-box in the upper-right named “All.” This allows access to existing as well as new accounts in the system.

4. Cameras (Only for the End User account)

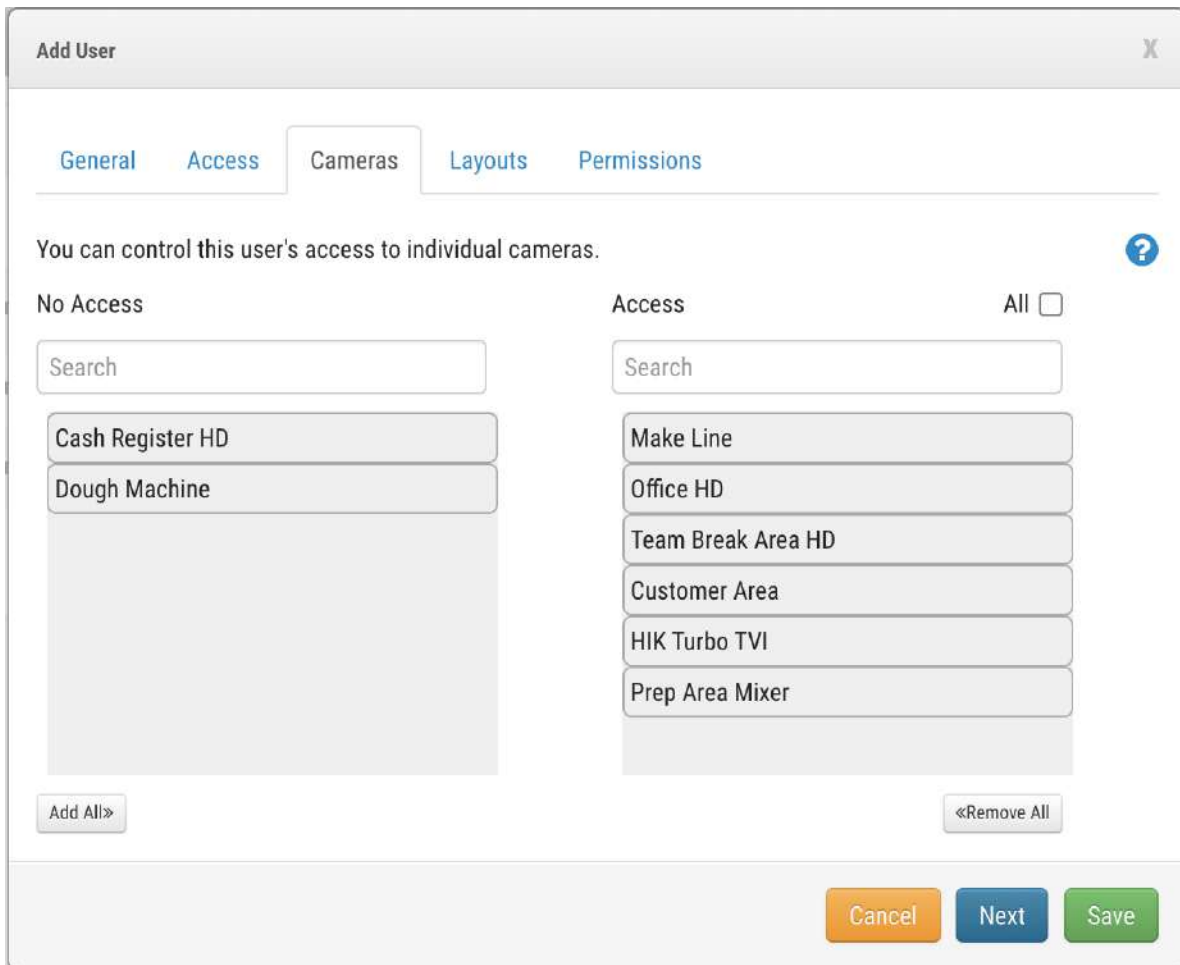


Image 8: How to determine which cameras this user has access to. Use the Add All button if needed

In this menu, choose which cameras this user has access to. The left panel shows the cameras that have not had access granted and the right panel shows which cameras have had access granted. Drag and drop on a camera per camera basis or click on the button “Add All” to allow all cameras to be accessed at once.

If you want this user to have access to all cameras and all new cameras installed in the future, then check the tick-box upper-right corner named “All”. This allows access to existing and new cameras in the system.

5. Layouts (Only for End User accounts)

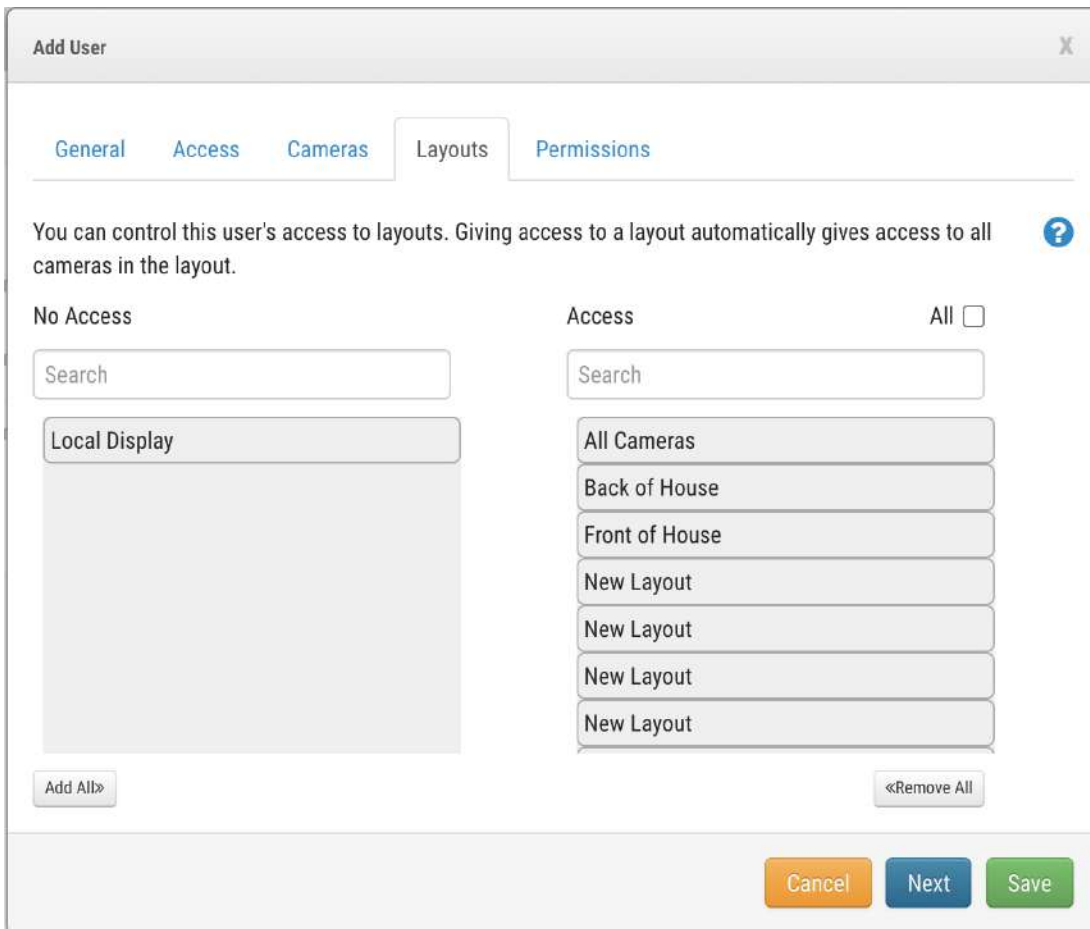


Image 9: How to determine which users have access to which layouts using the drag and drop tool. Use the Add All button if needed

In this section, provide user access to certain layouts configured in the system. Drag and drop from the left panel to the right to grant access and add all of them at once by clicking on the “Add All” button.

If this user should have access to all Layouts and all new layouts created in the future, then check the tick-box in the upper-right corner named “All”. This allows access to existing and new layouts in the system.

NOTE: If a user has NO rights to see a certain camera BUT the camera is included in a Layout that they can access, the user will be able to see the camera so be cautious when implementing this scenario.

6. Permissions

Permissions is where you configure which features users of the VMS have access to. These are divided into several categories as can be seen below and depending on the

access provided, an entire category can be chosen or just specific features within a category as shown below within the “Layouts” menu.

The screenshot shows the 'Add User' dialog box with the 'Permissions' tab selected. The dialog has a title bar 'Add User' with a close button 'X'. Below the title bar are four tabs: 'General', 'Access', 'Accounts', and 'Permissions'. The 'Permissions' tab is active and contains a list of permission categories, each with a checkbox and a description. The 'Layouts' category is expanded, showing sub-options 'Edit Layouts' and 'Create Layouts Only'. At the bottom right of the dialog are two buttons: 'Cancel' (orange) and 'Save' (green).

Permission Category	Description
<input type="checkbox"/> Administrator	All permissions are enabled: create, delete, edit, and view access to all accounts and user settings, bridges, cameras, layouts, audit log and archive
<input type="checkbox"/> Bridges and Cameras	
<input type="checkbox"/> Accounts and Users	
<input type="checkbox"/> View and Download Videos	
<input type="checkbox"/> Layouts	
<input type="checkbox"/> Edit Layouts	Create, delete, edit and view any accessible layouts. All user layouts are visible to admin users
<input type="checkbox"/> Create Layouts Only	Ability to create layouts and edit the layouts created. This does not grant permission to edit layouts created by other users
<input type="checkbox"/> Locations	
<input type="checkbox"/> Audit Log	
<input type="checkbox"/> Archive	
<input type="checkbox"/> Business Portal	

Image 10: The Permissions tab is where you can determine which users have access to which VMS features/categories

User Permissions - Reseller and End User Accounts

As outlined above, there are many different permissions for users and will now review them by section. As seen below, the first category is **Administrator**, which provides full user access with no restrictions on editing, deleting, creating, etc. Eight different categories follow and are described in the next section. Depending on whether it is a Reseller account or End User account, there will be differences on certain permissions. Please note that the “Business Portal” category is only for Reseller account users.

- **Bridges and Cameras**

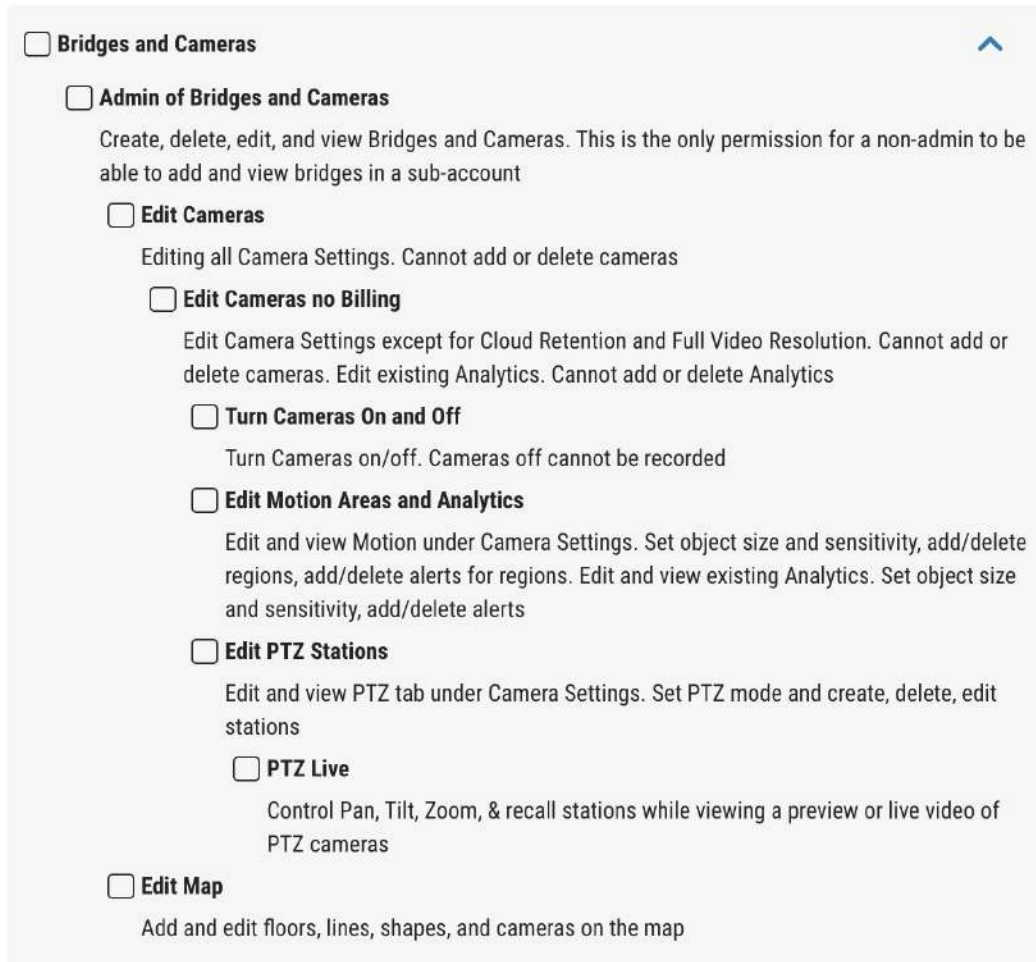


Image 11: Permission categories relating to Bridges and Cameras

These permissions are related to physical devices (Bridges and CMVRs for example) as well as cameras in the system that are installed in any End User account in case users are at the Reseller account level. For End User account users, permissions will only be related to their own account.

Choose if a user can edit cameras, turn them On and Off, set up Motion, Analytics, and more. Map edition is also included in this section as it affects camera placement.

One key parameter named “**Edit Cameras no Billing**” lets the customer configure the cameras but NOT the Cloud retention period and full video resolution for recording, in addition to adding or deleting cameras. This is the same for Analytics, which can be edited but not added or deleted. This allows the customer to configure parameters on cameras that do not affect the billing of the account.

- **Accounts and Users (Reseller account)**

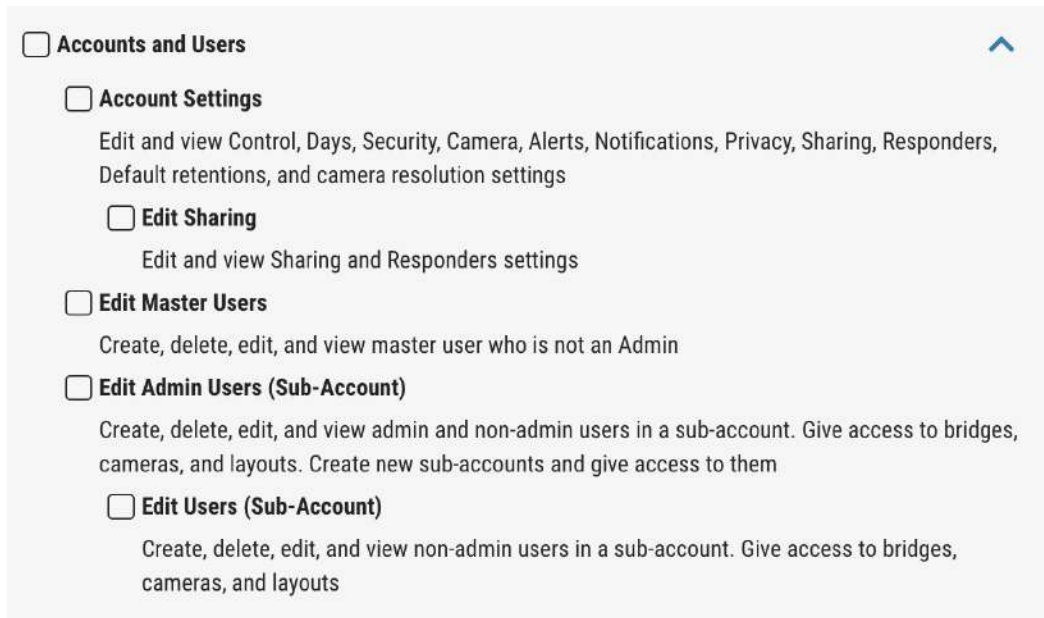


Image 12: Permission categories relating to Accounts and Users (Reseller account)

This section relates to users and account management. It is important to understand that users in the Reseller account are being referenced as can be seen on the picture above that there are rights for “Reseller Users” in addition to rights for the “End User Account” which determines whether this specific user can create such accounts. The “Edit Sharing” parameter allows users to share cameras between accounts and also allows them to use the “First Responders” parameter to share cameras.

- **Accounts and Users (End User account)**

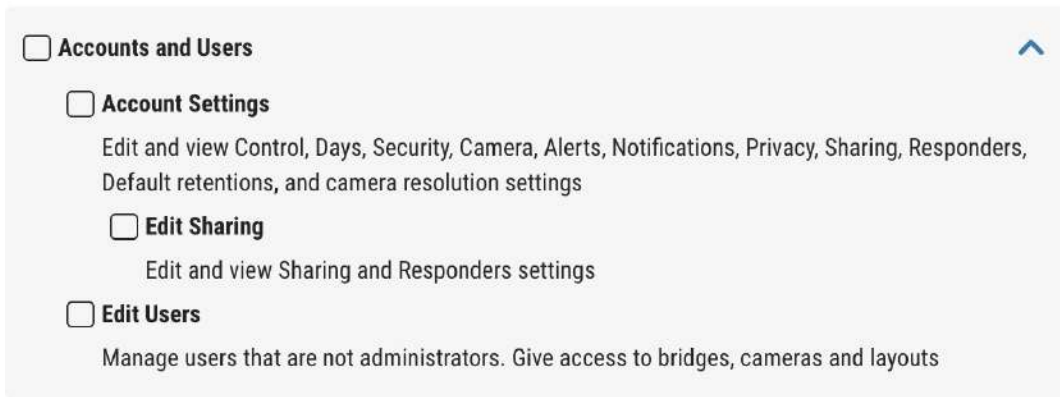


Image 13: Note that permissions are different at the End User account level

As can be seen on the End User account level, permissions are different as we are granting rights on the End User account only.

- **View and Download Videos**

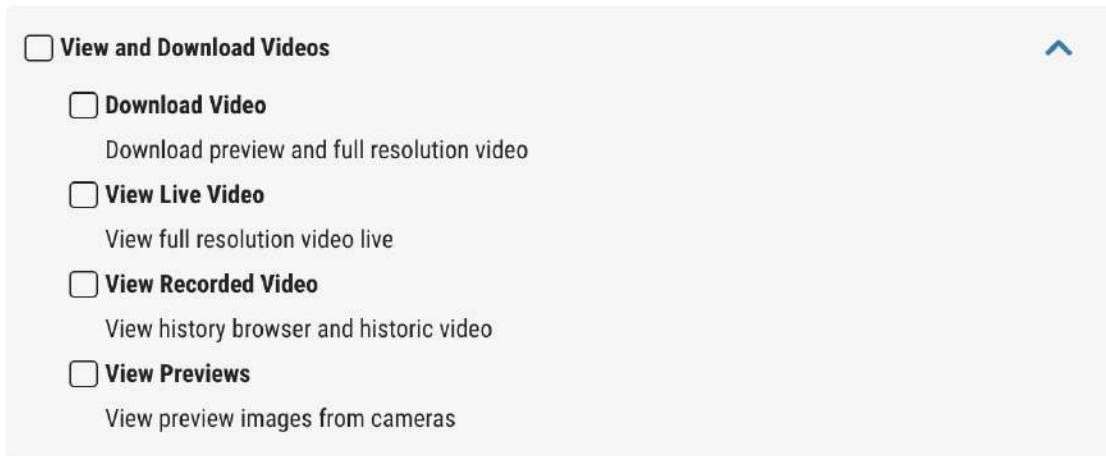


Image 14: Permission categories for viewing and downloading videos

This category determines access to live and recorded video. Within the Reseller account, permissions can be granted for all End User accounts. If in the End User account, these will only be available for this particular End User account. If “View Previews” is enabled, the user won’t be able to view live video or be able to download or view recorded video. Allowing Download, View Live and View Recorded Video will automatically permit the user to view previews.

- **Layouts**

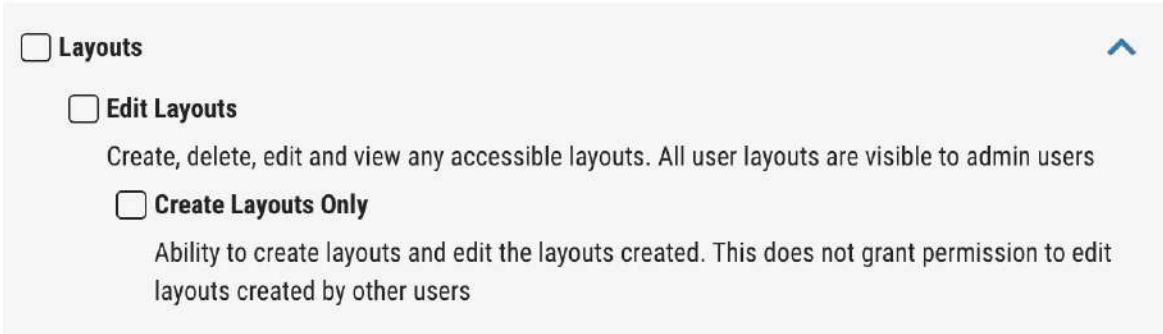


Image 15: Determine who can edit and/or create Layouts

These permissions are related to the creation and addition of Layouts. Depending on the level of permissions granted, users will either be able to create or edit Layouts. If within the Reseller account, grant permissions for all End User accounts. If within the End User account, permissions will only be for this particular account.

- **Locations**

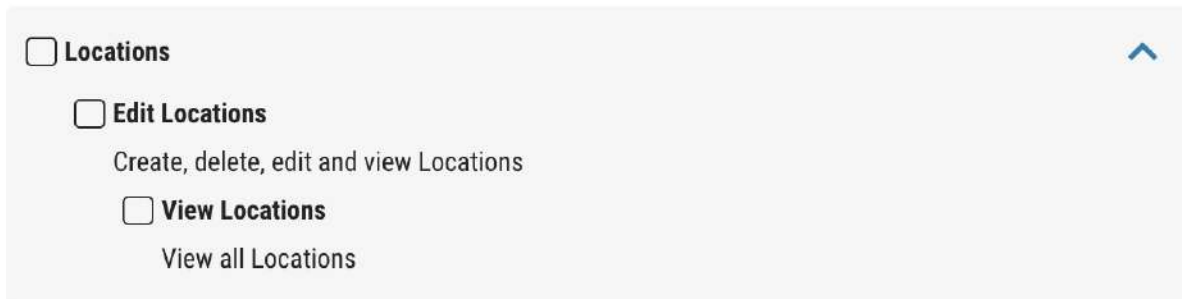


Image 16: Determine who can edit and/or create Locations

This category allows users to edit and/or view Locations. If enabled, the “Edit Locations” category of “View Locations” will be enabled by default. If within the Reseller account, grant these permissions for all End User accounts. If within the End User account, it will be only for this particular account.

- **Audit Log**

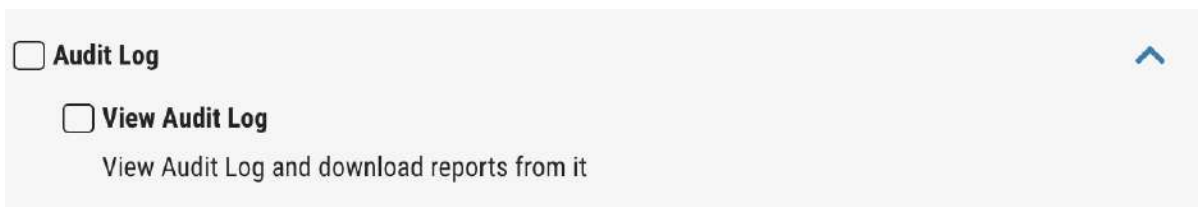


Image 17: Determine which users can view the audit log and download reports

This category allows users to view the audit log of the system. Data is kept for 1 year and includes records of all actions per user, date, time, events, etc. Data can be exported as a CSV file so that it can be filtered and customized as needed. If within the Reseller account, grant these permissions for all End User accounts. If within the End User account, it will be only for this particular account.

- **Archive**



Image 18: Determine which users can edit, delete and view folders within the Archive Vault

This category provides access to Archive functionality and determines which users can edit, delete, and view files and folders within the Archive Vault. If within the Reseller account, grant these permissions for all End User accounts. If within the End User account, it will be only for this particular account.

- **Business Portal (Only for the Reseller account)**

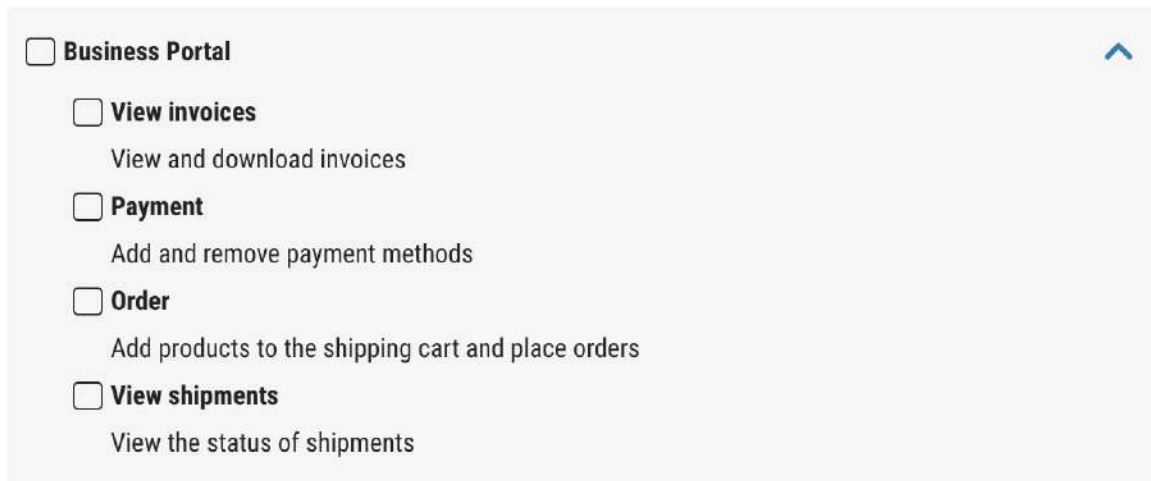


Image 19: Determine which Reseller users can interact with the Business Portal

The Business Portal is only available for users on the Reseller account. It allows users to view invoices, add/remove payment methods, place orders and view the status of shipments. Depending on the hierarchy implemented, limit users as needed to interact with the portal from a business perspective.