# User Configuration


- User Types
- Limiting Active Vehicles
- Manage User Departments
- Locker User Types
- Login Sources (SSO)

# User Types

> The User Types feature allows administrators to categorize system users (such as Student, Staff, or Public) and control various aspects of their interaction with the system. Its primary purpose is to tailor the user experience by defining access to specific lots, available payment options, and the visibility of specific fields on their profile based on their assigned group. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing user accounts and system permissions.

## Setup and Configuration

This feature requires administrative access to manage user groups and system master categories.

**Admin Side:** Administrators must have the appropriate system role permissions to access the user configuration tools and create new user types.

**User Side:** Depending on your configuration, end-users can select their user type during the initial portal registration process.

### Creating a New User Type

1. Hover over **System Configuration**, click **Users**, then **Types** to open the User Type Administration page.
2. Click the **Create New User Type** button.
3. Enter the desired name into the **Type Name** field (e.g., Public Parker).

4. Select the appropriate internal master category from the **Grouping** drop-down menu. New user types must be assigned to one of four hardcoded categories: **Staff**, **Student**, **Public**, or **Athletics**.
5. Enable the **Visible to Users** toggle if you want to make this user type selectable by end-users during registration.
6. Enter a numerical value into the **Extra Active Vehicles** field. By default, users can have one active vehicle; this specifies how many additional active vehicles are allowed. Detailed instructions can be found on the *Limiting Active Vehicles* page.
7. Enable the checkbox next to each allowed payment method under the **Allowed Payment Types** section.
8. Click the **Create User Type** button to finalize the addition.

> You can also create specific user types to categorize your archived users. This grouping is crucial as it links to internal master categories, which heavily govern access to other system items and the appearance of profile forms.

## Using this Feature

Administrators can use the following instructions to apply user types to profiles, manage lot access, and execute specific searches.

### Applying a User Type to a User

A user type can be assigned to a user when their account is first created or changed at any time later.

1. Hover over **User Management** and click **User Search**.

2. Search for the specific user you want to edit.
3. Edit the user profile and click the **User Type** drop-down menu.
4. Choose the desired user type.
5. Click the **Submit Profile Information** button.
6. Review the submission and click the **Information Correct** button to save the changes.

## Configuring Access to Lots with User Types

User types play a critical role in controlling backend and user-side access to parking lots.

1. Hover over **Parking Management**, click **Lot Administration**, then **Pricing & Lot Admin**.
2. Click on the **Lot Name** of the lot you wish to configure.
3. Ensure **User Type Lot** is selected on the **General Tab** under the **Lot Access** section.
4. Select the specific user types you wish to allow access to this lot from the **Lot Types** drop-down menu. You can press Ctrl + Click to select multiple types simultaneously.

> When a user logs into the system and attempts to purchase a permit, the portal will only display lots that are explicitly configured for that user's specific user type. For example, a user assigned a student user type will not see staff-only lots during the checkout process

## Available Actions and Buttons

- **# of Users:** Click this button located beside a user type in the main list to automatically perform a system search for all users assigned to this group.
- **# of Payment Types:** Click this button to immediately view a list of all payment types associated with each user type.
- **Show/Hide Lot User Types:** Click this link when viewing the list of lots in the Lot Administration module to quickly see exactly which user types a lot is configured to accept.
- **Delete User Type:** Click this button on an existing user type to permanently remove it. A user type can only be deleted or archived if no active or inactive users are currently assigned to it.

---

## Best Practices and Considerations

- **Align with your organizational structure: Create user types that directly reflect the categories of individuals interacting with your system.** Using clear names like Faculty, Undergraduate, Graduate, or Visitor makes management intuitive.
- **Enforce granular access control: Leverage user types in Lot Administration to precisely control who can access and purchase permits for specific parking areas.** This enhances security and ensures proper resource allocation (e.g., restricting student access to a faculty lot).
- **Understand the impact on profile fields: Remember that the internal Grouping (Staff, Student, Public, Athletics) you assign to a user type dictates the visibility of fields in the registration form.** For instance, student users might see specific student ID fields

that staff users will not.

- **Control vehicle limits securely: Use the Extra Active Vehicles setting to carefully manage the number of vehicles associated with specific user groups.** This directly impacts parking availability and overall system load.
- **Apply payment type restrictions: Utilize the Allowed Payment Types setting to ensure only relevant payment methods are available to specific user groups.** For example, you can safely restrict internal payroll deduction options to staff user types only.

# Limiting Active Vehicles

> The Limiting Active Vehicles feature allows administrators to strictly control the maximum number of active vehicles a user can associate with their portal profile. Its primary purpose is to help manage parking inventory, prevent permit abuse, and ensure users maintain a reasonable number of registered vehicles within the system. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing user configurations and parking regulations.

## Setup and Configuration

Active vehicle limits are controlled and configured through the specific settings of individual User Types.

**Admin Side:** Administrators must have the appropriate system role permissions enabled to access the user configuration menus and modify user type settings. For detailed information on working with user types, refer to the *User Types* wiki article.

**User Side:** Users will directly experience these limits on the user portal when attempting to add new vehicles or change the active status of their existing vehicles.

### Editing Active Vehicle Limits

1. Hover over **System Configuration**, click **Users**, then **Types** to open the **User Type Administration** page.

2. Locate the specific user type you wish to edit from the list and click the **Edit** button.
3. Locate the **Extra Active Vehicles** field.
4. Enter the desired number to reflect the maximum additional active vehicles allowed for this user type.
5. Click the **Update User Type** button to apply your new configuration limit.

> The number entered in the **Extra Active Vehicles** field represents how many *additional* active vehicles a user may have on their profile, beyond their first required active vehicle. For example, if you set this number to 1, the user may have a maximum of 2 active vehicles (their one required active vehicle plus one additional).

## Using this Feature

Once the active vehicle limit is set for a user type, it directly dictates how those specific users can interact with their vehicle information on the portal.

### Standard User Portal Interaction

1. Navigate to the **Vehicle** tab on the user portal to access the vehicle information section.
2. Click the **Add New Vehicle** button.
3. Fill out the required vehicle information and click the **Save Changes** button.
4. Observe the confirmation message and verify the vehicle now appears on the active list.

### Exceeding the Active Vehicle Limit

If a user tries to add a vehicle that would exceed their configured limit (e.g., attempting to add a third vehicle when their limit is set to a maximum of two):

1. Enter the new vehicle information and click the **Save Changes** button.
2. The user will still receive a confirmation message indicating the vehicle was successfully added to their profile.
3. Observe that the newly added vehicle appears on the vehicles page, but it is locked in an inactive state.
4. Attempt to make the vehicle active by toggling its state. The system will block the action and display a message indicating the vehicle cannot be made active due to the limit set for their user type.

### Minimum Active Vehicle Requirement

Conversely, if a user attempts to make all of the vehicles on their profile inactive, the system will block the action. A message will appear indicating that the user must always have at least one active vehicle associated with their profile.

---

## Best Practices and Considerations

- **Understand the additional limit logic: Remember that the Extra Active Vehicles setting represents additional vehicles beyond the one required active vehicle.** A setting of 0 means a user can have a maximum of one active vehicle. A setting of 1 means a maximum of two active vehicles, and so on.
- **Account for grandfathered vehicles: If you reduce the number of allowed active vehicles for a user type, users who currently exceed the new limit will not be immediately affected.** They are

grandfathered in with their current active vehicles. The new, stricter rule will only come into effect when the user attempts to add new vehicles or reactivate previously inactive vehicles in the future.

- **Communicate limits clearly to users: Inform users about active vehicle limits in your FAQs or permit purchasing guidelines to manage expectations.** While the system provides messages when limits are reached, proactive communication prevents user confusion and reduces support tickets.
- **Handle existing system vehicles: Be aware that if a user attempts to add a vehicle that is already present in the system, they will be prompted to claim it.** The exact same active vehicle rules and limits described above will still apply to this claiming process.

# Manage User Departments

> The User Departments feature allows administrators to categorize users based on their departmental affiliation within an organization. Its primary purpose is to enhance user management by enabling better organization, reporting, and potentially targeted communications or access controls, ensuring that user data is structured and easily manageable. This article is intended for OperationsCommander (OPSCOM) administrators responsible for configuring system settings and managing user profiles.

## Setup and Configuration

This feature is a core administrative tool used to structure organizational data within the system.

**Admin Side:** Administrators must have the appropriate system role permissions enabled to access the user configuration menus and manage departmental lists.

**User Side:** Depending on your specific portal configuration, these departments may be selected by end-users during the registration process or when editing their profile, providing a key piece of information for accurate user categorization.

## Using this Feature

Administrators can use the following instructions to navigate the management interface and seamlessly add, edit, or delete user departments.

### Accessing the Management Interface

1. Hover over **System Administration**, click **Users**, then **Manage User Departments**.

### Adding User Departments

1. Click the **Add User Department** button.
2. Enter the desired name into the **Department Name** field.
3. Click the **Save Changes** button to add the new department to the system.

### Editing User Departments

1. Locate the specific user department you wish to modify in the list.
2. Click the **Edit** button next to the department.
3. Update the existing name of that department in the provided field.
4. Click the **Save Changes** button to apply your updates.

### Deleting User Departments

1. Locate the department you wish to remove from the list.
2. Click the **Delete** button next to the department.
3. Click the **Confirm** button to finalize the removal.

> In order to delete a user department, it must not currently be in use by any user in the system. Administrators must first verify that no users are actively assigned to this department before it can be removed.

---

## Best Practices and Considerations

- **Reflect your organizational structure: Create user departments that accurately reflect the specific departments or divisions**

**within your organization.** This significantly helps with accurate reporting and long-term user organization.

- **Maintain consistency in naming: Use clear, consistent, and recognizable names for your departments to avoid confusion.** Avoid using obscure acronyms if they are not universally understood by your user base.
- **Ensure data integrity prior to deletion: Always ensure that no users are assigned to a department before attempting to delete it.** Reassigning users to another department (or to "None" if applicable) is a necessary step to maintain data integrity and prevent system errors.
- **Leverage departments for targeted reporting: Categorizing users by department can be highly valuable for generating targeted reports.** This structural data allows you to easily analyze trends across different parts of your organization, such as departmental permit sales or specific violation distributions.

---

## Related Video

https://www.youtube.com/embed/d57_-PDGFoE?wmode=opaque

# Locker User Types

> The Locker User Types feature allows administrators to categorize user profiles specifically for the purpose of locker management. Its primary purpose is to enable flexible control over who can access and utilize certain locker areas, enhancing organizational efficiency and tailored access to physical resources. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing locker inventory and user permissions.

## Setup and Configuration

This feature requires administrative access to the backend system settings to create and manage the user categorizations.

**Admin Side:** Administrators must have the appropriate system role permissions enabled to access the configuration menus and manage locker user types.

> If you do not see the configuration settings mentioned below, please contact support@ops-com.com to have them enabled for your environment. You will need the authorization of your primary administrator to request this change.

**User Side:** Locker User Types are strictly a backend administrative configuration. They are not editable, selectable, or viewable by end-users on the parking portal.

# Using this Feature

Administrators can use the following instructions to create new locker user types and apply them to specific user profiles and building areas.

## Adding a New Locker User Type

1. Hover over **System Configuration**, click **Users**, then **Locker User Types** to open the management screen.
2. Click the **Add Locker User Type** button.
3. Enter the full name of the user type (e.g., Public User) into the **Name** field.
4. Click the **Save Changes** button. The screen will refresh, and your new user type will automatically appear in the active list.

## Assigning Locker User Types to User Profiles

1. Hover over **User Management** and click **User Search**.
2. Search for the specific user you want to edit.
3. Edit their profile and select the desired group from the **Locker User Type** drop-down menu.
4. Click the **Submit Profile Information** button.
5. Review the submission and click the **Information Correct** button to finalize the assignment.

## Assigning Locker User Types to Locker Areas

Once locker user types are created and assigned to user profiles, they must also be associated with specific locker building areas to actively control user access. Detailed configuration instructions can be found on the *Allocate Lockers* page.

### Key Information Displayed

When viewing the main management screen, the list of existing locker user types typically displays:

- **Name:** The designated name of the locker user type.
- **Number:** The total number of user records currently associated with that specific type.

---

## Best Practices and Considerations

- **Establish logical categorization: Create locker user types that directly align with your organization's locker access policies.** Standardizing names like "Student Dorm," "Staff Locker," "Gym Member," or "Public Day Use" makes management much more intuitive.
- **Coordinate with locker areas: Remember that simply assigning a locker user type to a user profile is not enough to grant them access.** You must also actively link the locker user type to the relevant locker building areas to define actual access permissions.
- **Follow the deletion policy: A locker user type can only be deleted if no users are currently assigned to it.** Once a user has been assigned to a locker user type, the system will hide the delete button. You must manually reassign all users from a locker user type before it can be permanently removed.
- **Maintain clear naming conventions: Use clear and concise names for both the full name and short name to avoid administrative confusion.**

- **Train administrative staff: Since locker user types are not visible or editable by users, ensure your administrative staff are properly trained on how to accurately assign and manage them.** Relying on manual backend assignment means staff must proactively apply these types during registration or onboarding.

# Login Sources (SSO)

> The Login Sources SSO feature allows administrators to define the various methods by which users authenticate and sign into the system. Its primary purpose is to provide flexible control over user access, allowing for standard direct logins or integration with external identity providers like SAML or LDAP to enhance convenience and security. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing system access and user authentication.

## Setup and Configuration

This feature is a core administrative tool used to manage how different user populations access the portal.

**Admin Side:** Administrators must have the appropriate system role permissions enabled to access the configuration menus and manage SSO integrations.

**User Side:** Users will interact with the configured login sources when accessing the portal. If a Single Sign-On (SSO) source is enforced, they will automatically be redirected to their institution's secure login page before accessing the system.

## Using this Feature

Administrators can use the following instructions to manage the default login source, add new external identity providers, and modify existing authentication methods.

## Managing the Default Login Source

OPSCOM is the default login source for the system. This means that, by default, users will log in directly to the portal using a standard username and password created within the system itself.

If you disable the OPSCOM default login source, then only your other configured login sources, such as SAML or LDAP, will be active. Users will be forced to authenticate through those external providers.

## Adding Login Sources

The system supports multiple login sources simultaneously, allowing some users to utilize SSO while others log in directly.

1. Hover over **System Configuration** and click **Users** then **Login Sources**.
2. Click the **Add Login Source** button.
3. Enter a descriptive label into the **Name** field.
4. Enter the display identifier into the **Login Source** field. This is what you will see on the user profile to indicate if the user logs in with a special source (e.g., SSO or SAML).
5. Enter the root domain into the **Domain Name for OPSCOM to use** field. This must be the domain without any references to the admin portal (for example, use *CLIENTID.ops-com.com* instead of *CLIENTID.admin.ops-com.com/admin*).
6. Define the **Login Source - Code** field. This is a crucial identifier that the user profile will match against when associating users with this new login source.

7. Complete the remaining SSO fields when you are ready to apply the specific setup instructions provided by your Identity Provider.
8. Click the **Save Changes** button to add the new login source.

> When filling out the configuration form, fields highlighted in red are strictly required before you can save. Fields highlighted in yellow are technically required for the login source to function correctly, but the system will temporarily allow empty or invalid values to be saved initially. Yellow fields can also indicate that an unsaved change has been made to that specific field.

### Available Actions and Buttons

From the main management page, you can manage your configured login sources using the following actions:

- **Edit:** Click this button to modify an existing login source's details. This will bring up the configuration form, allowing you to update its connection properties.
- **Delete:** Click this button to permanently remove a login source from the system.
- **Status Drop-down:** Select a status of Active, Inactive, or Hidden for any login source. If a source is made inactive, users who were previously connected to it will no longer be able to log in and must be manually migrated to a different login source.

---

## Best Practices and Considerations

- **Strategically plan for multiple sources: Carefully plan your login source strategy before implementation.** Determine exactly which user groups will use which login method (e.g., students via SAML, staff via LDAP, and public users via direct login).
- **Manage user provisioning: Consider how users will be created and linked to their login sources.** Decide whether profiles will be auto-created upon their first successful SSO login or if they must be pre-imported. This linkage strictly relies on the exact string match of the **Login Source - Code** field.
- **Test before disabling direct logins: If you intend for all users to access the system via an external SSO, thoroughly test the integration before disabling the default OPSCOM login source in a live environment.**
- **Deactivate instead of deleting: Use the inactive status for temporary deactivation or if you foresee needing to reactivate a login source in the future.** Only use the **Delete** action when a login source is permanently retired and has absolutely no associated active users.
- **Communicate changes to users: Clearly communicate to your users how they are expected to log in.** If you introduce new SSO options or change existing methods, provide clear instructions and direct links on your portal homepage to prevent login confusion.