Commercial Portal – Administration Tutorial

1. Administration Tutorial Overview

This tutorial focuses on administration activities for your portal. There is a separate User Tutorial that covers most end-user features of the portal.

For additional information refer to the User Tutorial and the system help. You can access the help system by clicking on the **help** button at the top right of the screen. You can also run this tutorial at any time from your home page.

For each topic in this tutorial a description is provided followed by a ‘Show Me’ section. The ‘Show Me’ section explains where to go in the portal for different actions.

Administration activities are usually performed by Administrators or Managers with the appropriate set of permissions. Activities described in this tutorial include managing users, user groups, permissions and item groups. There are additional sections focused on managing departments.

2. Users

Every individual who uses or is notified by the system is a user. This includes individuals who log in for administrative reasons, to run reports, perform dispatch operations or simply locate items. Users also include those individuals who do not need to log in but should be notified when an event, such as a panic or speeding violation, occurs.

Users must belong to user groups. The user group to which the user belongs determines what permissions the user has and what actions they can perform. For each user you can choose whether to make that user available as a contact. In addition, you can prevent individual users from logging in by revoking their login permission.

2.1 Contacts

Contacts do not exist separately from users. For each user, you can select whether the user will also be available as a contact. In some cases you may want to create users that are not used for contact purposes. For example, a manager may need to log into the portal and run reports but does not need to be notified. For this case, the user account for the manager would not be enabled as a contact. You can maintain contact information for users even if those users are not available as contacts. This allows you to maintain contact information, including phone numbers and email addresses, for all your users.

When a user is available as a contact, their contact information can be used for the following:

- Notification for scenarios
- Scheduled reports
- Maintenance notification
- Vehicle, asset or personnel contact

2.2 Login Permission

You can choose whether to allow or disallow login for each user. You may want to disallow login permission for users who do not need to access the portal, but do need to be contacted by the system. Disallowing login permission can also be used to temporarily disable access to the portal for employees. For example, while employees are on vacation, you can disable their login access.

Unlike other permissions (see the Permissions section for more information), login permission is managed for individual users and not for a user group. A user with login permission can log in to the portal. What they can do after they log in is determined by the permissions of their user group. Even if the user group has not been granted any permissions, a user with login permission can log in and access their user account information. This allows users to update their account and contact information and periodically change their password. Such a user will not see not have access to any other features in the portal.

2.3 Password Change

For security reasons, it is recommended that users periodically modify their passwords.

Every user with login permission can access their user account information and modify their current password. When a password is modified an email message containing the new password is sent to the user email account.

2.4 Show Me

To **add**, **edit** or **delete** users go to Administration → Users

To **modify the information** of a specific user go to → Administration → Users → select the user to be modified

To **enable contact** functionality for a user go to Administration → Users → select the user to be modified → select the ‘Available as contact’ checkbox

To **disable login** for a user go to Administration → Users → select the user to be modified → deselect the ‘Allow login’ checkbox

To **modify permissions** for the user go to Administration → User Groups → select the

user group of the user → select the permissions for this user group

3. User Groups

A user group is a collection of users who share the same permissions. Every user must belong to a user group. Users can only belong to one user group. You can create user groups to match the different user roles you want to support. A user added to a user group would automatically take on the permissions of the user group.

Note that user groups are different from notification groups. While user groups contain the actual user account, notification groups are collections of just the contact information for users. User groups define what a user can see and do in the portal. Notification groups are used for notification purposes only.

You may want to create user groups for roles, such as:

- Managers
- Dispatchers

Each user group created has a corresponding Parent user group. The new user group is referred to as the Child group. The Child group cannot exceed the permissions of the Parent group. Users in the Child group cannot do more than users in the Parent group. For example, Manager Jane creates a new user group called Dispatchers. The Dispatchers group is now limited to the permissions that Jane has. This ensures that users are never allowed to do more than what their managers can do.

3.1 Default User Groups

By default, two user groups are available:

- Administrators
- Users

The Administrators user group is unique because it is granted all available permissions and it does not have a parent user group. This means that users in the Administrators group can do anything in the portal. In fact, the permissions of the Administrators group cannot be reduced. You may want to limit membership in the Administrators group only to those users who truly need this level of access.

Only the Administrators group can access and modify the Profile page and manage Departments (see the Administrators Group permissions section for more information).

The Administrators group cannot be empty and must always contain at least one user. This ensures that at least one user can always log in and perform all possible actions in

the portal. The Administrators group cannot be deleted.

The **Users** user group is available by default. The permissions of this group can be modified and the group can be deleted.

3.2 User Groups and Departments

For more information on departments see the Departments section.

If you are not using departments, simply granting permissions to a user group is sufficient to allow users to log in and start working. However, when using departments, a user group must have both permissions and be assigned to a department in order to see and use any features in the portal. This is because departments segment your organization into different sections and you need to define which department a user group can access. Until you do so, users in these groups will not be able to access features in the portal regardless of the permissions granted.

3.3 User Group Examples

You may choose to create the following user groups:

Dispatchers – these users need to access information about individual items, locate them and run fleet view. The Dispatchers group would be granted the **Locate permission**.

Fleet Managers – these users need to access information about individual items, run management reports and schedule maintenance. The Fleet Managers group would be granted **Run Reports** and **Use Maintenance** permissions.

External Contacts – you may choose to create a group for users who do not need to log in and are only used for notification purposes. This group would not be granted any permission.

Managers – if you are using departments (see the Departments section for more information) you may choose to create a user group for managers of each department. You may want these users to have full control of their own department but to limit them from accessing organization-wide features and other departments. These users would need to add and remove items and would need access to manage users, landmarks, beacons, etc. This group would be granted all permissions, perhaps with the exception of the **Trigger Output** permission. These users would then be able to fully manage their own department, items and beacons and add their own user groups and users. Users and user groups they add would be limited to this department (see the User Groups section for more information on limiting permissions of Child user groups).

Department Users – if you are using departments (see the Departments section for

more information) you may choose to create a group for standard users in each department. This group would be a child group of the **Managers** group described above, so that its permissions would never exceed those of the **Managers** group. You could use the permissions for any of the example groups described above (**Dispatchers**, **Fleet Managers**) for this user group.

3.4 Show Me

To **add a user group** go to Administration → User Groups → select 'add user group'

To see the **current members** of a user group go to Administration → User Groups → select the user group you want to view → the members are listed under the 'User Group Members' section

To **add or remove users** from a user group go to Administration → User Groups → select users to add from the left hand window and users to remove from the right hand window

To **modify the permissions** of a user group Administration → User Groups → select the user group you want to view → permissions can be modified in the 'Permissions' section

To **change the parent user group** go to Administration → User Groups → select the user group you want to modify → under the 'Primary Information' section select the 'Parent User Group' field

To **change the departments** a user group can access go to Administration → User Groups → select the user group you want to modify → under the 'Department Assignment' section select departments to add from the left hand window and departments to remove from the right hand window

4. Permissions

Permissions define what a user can and cannot do. Each user group has an associated set of permissions. Users in that group are limited by the permissions granted to the user group.

Permissions include 'Use' level permissions, 'Manage' level permissions and the Trigger Output permission. The Login permission is managed for individual users and not for user groups.

4.1 Use Permissions

The following 'Use' level permissions are supported:

- **Locate** permission – allows locating and tracking items individually and through Fleet View
- **Run Reports** permission – provides access to the Reports Module and permission to run real-time reports and manage scheduled reports
- **Use Maintenance** permission – provides access to the Maintenance Module and permission to manage maintenance for items

4.2 Trigger Output Permission

The **Trigger Outputs** permission – allows triggering an output for an item once a Manual Output has been configured in the scenario manager. Note that it is also possible to trigger outputs by creating a scheduled output scenario in the scenario manager. This would require Manage permission and not Trigger permission.

4.3 Manage Permission

Manage permission provides access to most of the Administration Module features. In addition, Manage permission allows creating, modifying and deleting items, assets and personnel. Users not granted Manage permission can only view items, assets and personnel but not create, modify nor delete them.

Manage permission provides access to the following Administration Module features:

- Scenario Manager
- Landmarks
- Users
- User Groups
- Notification groups
- Item Groups
- Beacons

Manage permission does not provide access to the Administration Module Profile page. The Profile page can only be accessed by users in the Administrators user group.

4.4 Administrators Group permissions

Certain features in the portal can only be accessed by users in the Administrators user group. These include:

- Profile page
- Departments feature (if enabled)

The Profile page contains information about your company and the default contact

person. The Departments feature (see Enabling Departments for more information) can only be enabled by a user in the Administrators user group from within the Profile page.

4.5 Show Me

To **see what permissions** a user group has go to Administration → User Groups → select the user group to view → the 'Permissions' section shows what permissions the user group currently has

To modify permissions for a user group go to Administration → User Groups → select the user group to modify → you can check and uncheck individual permissions

5. Item Groups

An item group is a collection of vehicles, assets or personnel. Item groups can contain one or many items and can include items of mixed types, such as assets and vehicles.

Item groups are used in:

- Scenario assignment
- Real-time reports
- Scheduled reports

When running reports you can select which item group to run reports for. Scenarios can be assigned to items or to item groups. Assigning a scenario to an item group automatically assigns the scenario to each item in the group. This saves having to individually assign the scenario to each item. In addition, if an item is then added to the group it is automatically configured with the scenarios assigned to the item group. An item that is removed from the group loses scenario information assigned to the item group.

For example, you can create an item group called Vans containing several vehicles. The beacons assigned to the vehicles in this item group do not need to be of the same type. You then create a speed violation scenario to notify you if vehicles exceed 80 mph and assign the scenario to the Vans item group. All the vehicles in this group are now configured with the speed violation scenario. If you later add a new vehicle to this group, it will automatically be assigned the speed violation scenario.

In some cases an item group may contain beacons that do not support the scenario you want to assign. You can still assign the scenario as long as at least one item in the group can support it. Items that do not support the scenario will not have the scenario assigned.

5.1 Item Group Scenario Conflicts

The scenarios assigned to an item group cannot conflict with the scenarios assigned to individual items in the group. Conflicts include schedule conflicts and Output configuration conflicts. A schedule conflict exists if a scenario with a similar event type is assigned to both an item group and an individual item with conflicting schedules.

For example, a manager wants to define a 60 mph speed violation scenario for work hours and assign it to the Vans item group. In addition, the manager wants individual items in the Vans group to have another 70 mph speed violation in off hours. One scenario is assigned to the item group and the other to several items in the item group. In this case a schedule conflict does not exist. If, however, the schedules for the two scenarios overlapped, it would not be possible to assign both scenarios. In this case, only the pre-existing scenario would be assigned.

In another example, several cars have an output scenario to automatically lock their doors every day at 5:00 PM. This is configured on output 1 as a toggle event. These vehicles are also in the item group Sales Cars. A second output scenario is created to disable ignition as a pulse for output 1. It would not be possible to assign the second scenario to the Sales Cars group. Since both scenarios use output 1 differently, one as a pulse and the second as a toggle, there would be a conflict.

5.2 Show Me

To **add, edit or delete an item group** go to Administration → Item Groups → select ‘add item group’ to create a new group, select the item group to be modified to edit, or select the item group and the ‘delete’ function to remove an item group

To **add or remove items** from an item group go to Administration → Item Groups → select the item group to be modified → in the ‘Item Group Members’ section items in the left window can be added and items in the right window can be removed from the item group

To **assign a scenario to an item group** go to Administration → Scenarios → select ‘add scenario’ → you will need to define the event, schedule and notification. In the ‘Items and Item Groups’ section item groups available for selection are shown in the left window with the item group icon

6. Departments

Imagine you wanted to create separate administrative departments in your organization and decide which users can access which department. The departments feature allows you to do just that. You can segment your organization into geographical or functional departments and decide which user groups will be able to access these departments.

Note that the departments feature is a power-user feature and should only be enabled after reading this tutorial. Turning this feature on modifies the appearance and functionality of your portal. While it is possible to disable departments, depending on how many modifications you have made, it can be time consuming to undo.

Reasons to enable departments include:

- Separating the organization into geographical branches
- The number of items and users has grown significantly and you want to divide management activities to match your organization structure
- Merging with another company, but wanting to separate user access

Using departments, you can control who (users and user groups) can access what (items, landmarks, scenarios…) and how (permissions).

6.1 Resources

Each department contains its own set of resources. When a user group is assigned to a department they can access and use these resources.

Resources include:

- Items: vehicles, assets and personnel
- Beacons
- Landmarks
- Scenarios
- Item groups
- Notification groups

Once departments are enabled, only those users who have been granted access can see and use the resources in a department.

6.2 User Groups and Departments

In order to specify which users can access which department you need to assign user groups. After departments have been created, you can assign each user group to one or more departments. When a user group is assigned to a department, the users gain access to the resources in the department. They cannot see nor use resources in departments they have not been granted access (assigned) to.

User groups can be assigned to one, none or many departments. The Administrators group is always assigned to all departments.

For example, two departments exist: the West and East departments. An administrator

creates a new user group West Managers and assigns it to the West Department. Another user group East Supervisors is created and assigned to the East Department. Users in the West Managers group can see and use all the resources in the West Department. However, they cannot see nor use any resources in the East Department. The Administrator, being a member of the Administrators group, can see resources in both the West and East departments.

Once a user group is assigned to a department, child user groups (see the User Groups section for more information) can also be assigned to the department. To continue the example, John, a user in the West Managers group now creates a new user group West Dispatchers. Since West Managers has been assigned to the West Department, John can also assign the West Dispatchers group to this department. John cannot assign the group to the East Department since he cannot see nor access this department.

6.3 Default Department

One department is selected to be the default department. When new beacons are registered to you they will appear in the default department. They can then be moved to other departments.

You can choose which department will be the default department. Or, you can create a separate department with no other resources to use as the default department for new beacons.

6.4 Enabling Departments

Departments is a power-user feature that impacts the functionality and appearance of the portal. Please read this tutorial before enabling departments.

Enabling the departments feature is done in the Profile page. Only users who are members of the Administrator group can enable departments. Once enabled, a new ‘Departments’ tab will appear in the Administration module. This tab is only accessible to Administrators.

To enable departments select the ‘enable departments’ function in the Profile page. Once selected you will be taken to the Edit Department interface where you can rename the default department and assign user groups. This department is now the first department in your organization. All the resources in your portal will now appear in this department. After the first department is created you will be able to assign user groups to this department (see the User Groups and Departments section for more information).

After creating more than one department you may want to move some resources between your departments. See the Moving Resources section for more information.

6.5 Moving Resources

Some resources can be moved between departments. Resources that can be moved include:

- Beacons
- Items (vehicles, assets and personnel) with assigned beacons
- Items (vehicles, assets and personnel) without assigned beacons
- Landmarks

To move a resource, select the resource and then use the ‘change department’ button to select a new department.

The following resources cannot be moved:

- Scenarios
- Item groups
- Notification groups

While scenarios cannot be moved between departments, they can be copied to a new department. Copying a scenario does not copy the contacts, notification groups, items or item groups used for the scenario. It does, however, copy the event information for the scenario. For example, two departments have been created: West and East. You would like to create zone scenarios for customers that are visited by vehicles in both departments. You could create the scenario in one department, say East, first and then copy the scenario to the West department. This would ensure that the same zone information is used in both departments.

6.6 Deleting a Department

To delete a department you must first move or delete items, beacons and landmarks in the department. Items and landmarks must either be moved to another department or deleted. Beacons cannot be deleted and therefore must be moved to another department. After the department no longer contains any beacons, items or landmarks you can delete the department. Deleting the department will delete the following:

- Scenarios and schedules
- Item groups (these will now be empty)
- Notification groups

User groups assigned to the department will no longer be assigned after it is deleted. This will affect what users in these user groups can see can do.

6.7 Disabling Departments

The department feature can be disabled only when there is one department. To disable departments you must delete each department (see Deleting a Department for more information) until only one department is left. After disabling departments all the resources in this department will still be available. The Departments tab in the Administration module will then become hidden.

6.8 Show Me

To **enable departments** go to Administration → Profile page → select the 'enable departments' button

To **add a department** go to Administration → Departments → select the 'add department' function

To see which **user groups are assigned to a department** go to Administration → Departments → select the department to view → In the 'User Group Assignment' section the groups with a checkmark are those assigned to the department

To see which **departments a user group is assigned** to go to Administration → User Groups → select the user group → in the 'Department Assignment' section the list of departments on the right shows assigned departments

To **modify user group assignment** for a department go to Administration → Departments → select the department → in the 'User Group Assignment' section check user groups to be assigned and uncheck those that should not be assigned to the department

To **set the default department** go to Administration → select the department to be the default department and use the 'set default button

To **move resources** between departments → select the resource(s) to be moved and then the 'change department' button (for example, in the Administration → Landmarks interface) → you will now be able to select the new department for the resource. You can also move a resource by selecting the resource and changing the 'department' field (for example, in the Administration → Landmarks → select the landmark to be moved)

To **copy a scenario to another department** go to Administration → Scenarios → select the scenario to be copied and the 'copy scenario' button → in the 'copy scenario' interface in the 'department' field select the new department for the scenario

To **delete a department** first delete or move all the items, beacons and landmarks in the department then go to Administration → Departments → select the department to be deleted and the 'delete department' button

To **disable departments** when only one department exists go to Administration → Departments → select the 'disable departments' button