FacilityPro5
management software for
FacilityPro platform
User Manual

TABLES

FIGURES

1 INTRODUCTION

This is the FacilityPro5 user manual.

FacilityPro5 (or FP5 for short) is the back-office software designed to support the administrator of a site and guarantee easy and effective site management. A site is a location, for example a university or hospital, possibly spread out over several buildings, where the facilities management platform FacilityPro is in use. People can purchase products or gain access by presenting a card/ID at a FacilityPro terminal. Examples of such electronic transactions are purchasing coffee or snacks from a vending machine, making photocopies, or gaining access to the parking garage with their card/ID. The amount due for such a transaction is subtracted from the balance of the card/ID, which can be either the balance of a FacilityPro account in the back office (online systems) or the balance of the e-purse on the card/ID (off-line systems).

1.1 SITES

The majority of items in the system are managed on a per-site basis. Each site has a separate user base, card/ID base, and terminal base.

1.2 MULTI-SITE

FacilityPro5 (FP5) is capable of managing multiple sites on the same system. FP5 users may have access to any number of these sites, or be restricted to only see a single site on the system.

A new installation of FP5 will be pre-populated with an initial system administration site or meta-site, generally given the name "System administration". This is not a functional site with cards/IDs and terminals, but rather the abstract entity that owns all configurations that can be shared across all sites in the system.

For example, roles (used for determining access permissions to FP5) defined within the system administration site (generic roles) can be assigned to FP5 users for other sites, whereas roles defined within a site (site roles) can only be assigned to FP5 users for that specific site.

Also, terminal groups defined within the system administration site can contain terminals from different sites whereas a terminal group defined within a site can only contain terminals from that specific site.

1.3 ROLE-BASED ACCESS

Access to FP5 is controlled by permissions. FP5 has a fixed set of permissions that control access to specific functions.

These permissions can be combined into roles. These roles are subsequently assigned to FP5 users for particular sites. Therefore an FP5 user ultimately receives a set of permissions to execute a particular function in the context of a particular site.

1.4 TRANSACTIONS

Ultimately the function of the system is to facilitate transactions between users (that hold cards or IDs) and another party at terminals.

In these transactions the user provides value (either monetary or preloaded privilege) and receives a product or service. The other party receives the value provided by the user and provides the product or service.

2   USER INTERFACE CONCEPTS

2.1   WEB-BASED

Whether FacilityPro5 is used as a hosted service, or as a private install, the FP5 interface is accessed in a web browser using the URL provided.

In this document we'll use https://www.mcfpp.net/ as the location of the service. In your setup this may be different.

2.2   MENU

The menu gives access to FP5's functions.

Depending on the access permissions of an FP5 user, some parts of the menu may not be visible. In this manual we show the complete menu as it would be visible to an FP5 user with all permissions.

There is one menu which shows your FP5 user name. This menu allows you to change your profile, change the UI language for the present session, and log out (§5.2.4).

To select from the menu:

1. Hover over the main menu item. A pop-up menu will appear.
2. Click on a sub-item.
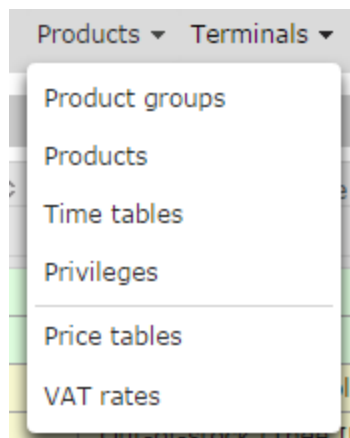
2.3   LONG LISTS

Most menu options open a 'list' page that contains a list of items. This is usually a list of all items in the system, but limited to only show the first few.

2.3.1   Searching/filtering

Some screens, namely those that show long lists, have a "Search" section, that you can view or hide by clicking the "+Search users" (or "+Search privileges" etc.) button. You can use the search section to easily find the item or items that you want to view.

To list a specific selection of items:

1. Open the search section by clicking the "+Search users", "+Search privileges" (or similar) button.
2. Enter data or choose data from the drop-down list in one or more of the search fields that are shown .
3. Click the "Search" button. The matching items will be shown.

To clear the search:

1. Click the "Clear" button. The search fields are cleared and the (beginning of the) entire list of items is shown.

2.3.2 Paging

A paging bar is shown at the bottom of the screen under lists.

The bar shows:

- (X of Y) The current page number (X) and the number of pages (Y)
- Controls to navigate to (consecutively) the first page, the previous page, any page number in between, the next page and the last page
- A drop-down which allows the FP5 user to control the size of the page (25, 50, or 100 items).

2.3.3 Sorting

The column headers of a list may have triangular controls that indicate that the sort order of the list. The sort order can can be changed by clicking on the triangular controls.

Figure 2-1: Unsorted column

Figure 2-2: Column in ascending order (A->Z)
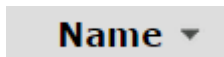
Figure 2-3: Column in descending order (Z->A)

2.4 ACTION BUTTONS
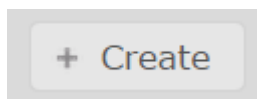
Figure 2-4: Action button

Big buttons (action buttons) typically lead to a pop-up screen that modifies the current item, or creates a new item.

In lists, a smaller style is used to initiate an action because otherwise the list rows would expand too much.

Here you may just see a trash can icon   , or a link that leads to another page.
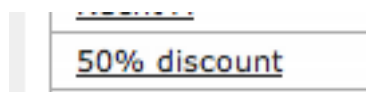
Figure 2-5: Link

2.5 INTERNATIONALISATION

FP5 is capable of handling multiple languages at the same time. At any time, the current language of the user interface may be changed using the language selection drop-down menu in the top right-hand corner of the screen. This changes the language used on the pages of FP5, and also the names of items in the system if multiple languages were entered.

When editing, you will see multiple text prompts, one for each site language.

Figure 2-6: Multilingual name entry

When multiple languages are entered, the user interface will show the name in the chosen language if available. If not available the first language available will be shown marked by an asterisk.
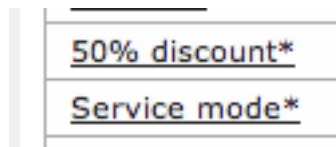
Figure 2-7: First available language shown when chosen language not available

3 LOG IN

3.1 LOG IN PAGE

When the FP5 user browses to the URL provided, a log in page is displayed.

The log in page prompts for a user name and password.
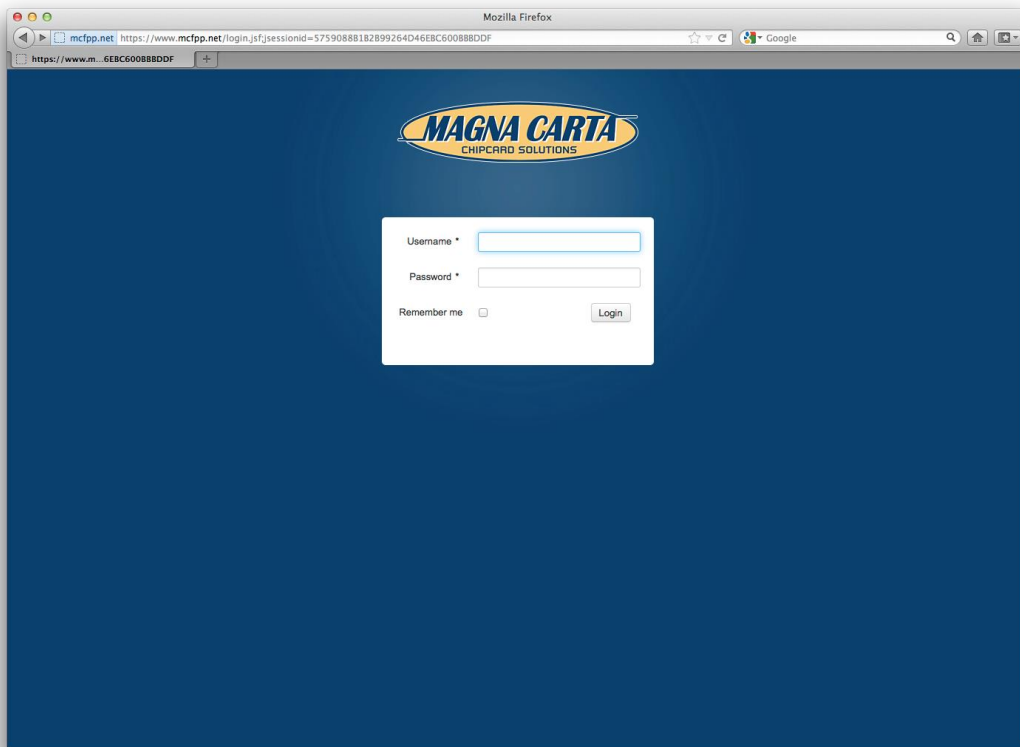
3.2   SESSION TIMEOUT

After a period of inactivity, the login is timed out. The timeout period is determined by your system administrator. The default session timeout period is 30 minutes.

3.3   SINGLE SESSION PER FP5 USER

FP5 allows each FP5 user to be logged in only once. An FP5 user can however have multiple tabs open to the FP5 interface in the same browser. You can also log in as different FP5 users from different browsers.

3.4   ACCESS ROLES

The roles assigned to the FP5 user determine which menu options and functions are visible.

3.5   LOG OUT

To close the session immediately, click the "Log out" menu option.

3.6   LANGUAGE SELECTION

To change the user interface language, select the desired language option from the menu of your user name. You change the default language for future logins in your user profile (§5.2.4).

4 HOME PAGE

4.1 SITE SELECTION

Any operation in the FP5 interface is in the context of a particular site. System wide configurations and operations are available in the system administration site.

The Home page contains the "Site selector" that allows the FP5 user to choose a site. When a site is selected, the choice is reflected in the banner of the page.

To choose another site, click on the drop-down arrow which is the leftmost menu-item (site selector) and select another site.

If the FP5 user only has access to a single site, the site selector will not be visible and that single site will be automatically selected.

4.2 ALERTS

Also visible on the Home page is a list of the most recent alerts that occurred. If the system administration site is selected, alerts from all sites are shown in order of occurrence. If a specific site is selected, only alerts from that site are shown.

5 SYSTEM ADMINISTRATION

Each installation of FP5 has system-wide settings and configurations that are maintained by an administrator with access to the system-wide system administration site.

For some types of objects system-wide defaults can be defined that can be replaced on a per-site basis.

The following table lists the types of objects maintained by FP5 and shows at which level they can be defined.

Table 1: System vs Site object types

Object type	System administration	Site administration
Site	Defined in system	
FP5 user	Owned by system	Owned by specific site
Role	System-wide roles	Site-specific roles
Report template	System-wide templates	Site-specific templates
Magnabox	Assigned to site by admin	
Email template	System-wide default templates	Site-specific templates
Terminal group	System-wide terminal groups can span terminals in multiple sites	Site-specific terminal groups can only contain terminals within that site
Picklist	System-wide picklists serve system terminal groups (spanning multiple sites)	Site-specific picklists can only serve terminal groups within that site

Objects defined at the system level are visible to all sites configured on the system (if the FP5 user has the appropriate permissions for that type of object). Objects defined within a particular site are only visible when that site is selected.

When an object is created, it is created in the site that is selected at that time. If the selected site is the system administration site then the object will be a system-wide object. If the selected site is a normal site, then the object will be 'owned' by that site only.

5.1 ROLES

Roles are in effect sets of permissions, and are used to determine which tasks an FP5 user can perform. You can assign multiple roles to an FP5 user.

FP5 comes preconfigured with some default roles. If given the default role "Administrator", an FP5 user has all permissions and can create new FP5 users and new roles. These preconfigured roles can be modified and even removed after installation of FP5.

The following table lists the predefined roles with their semantics.

Table 2: Default roles

Role name	Description
Administrator	A role that has all permissions. Assigning the administrator role to an FP5 user for a particular site gives that FP5 user access to all functionality for that site. The default FP5 user "admin" has the administrator role for the system administration site.
Site management (functional administrator)	A role that has all permissions typically assigned to a functional site administrator. The role gives access to all functions within a site, including setting up FP5 users, assigning roles, configuring reports etc.
Service desk	A role that has enough permissions to perform service desk functions like creating users and cards/IDs
Reporting	Ability to configure and run reports
Logistics user	Ability to service terminals and restock them
Logistics officer	Ability to create picklists and finalise stock quantities
Site visibility	Simple role that only allows operations to objects of type site. This role is added by default to the current FP5 user when a site is created.

5.1.1 Creating a role

Permissions required: Role| Retrieve, Role | Create

When you create a new role, it will be either a system-wide role, or a site-specific role, depending on which site is selected when you create the role. Bear in mind that in order to be able to do almost any task one will need the permission Site | Retrieve, without which the site is not visible to the FP5 user.

To create a new role:
1. To create a system-wide role, that will be available for selection within all sites, ensure the system administration site is selected before continuing. To create a site-specific role, ensure that site is selected before continuing.
2. Select the "Roles" (from within the system administration site) or "Site roles" (from within a specific site) option from the "Administration" menu.
3. Click "Create".
4. Enter the role name in the site languages and a description of the role in the appropriate fields.
5. Click the "Add" button to add permissions to the role.
6. Select one or more permissions to be added to this role. Multiple permissions may be selected at once by holding the Shift-key (to select a range) or the Ctrl-key (to select separate individual permissions).
7. Click the "Add selected" button.
8. Repeat the three previous steps until you have added all the permissions for this role.
9. To remove a permission, click the "Delete" link to the right of the permission.
10. Click the "Save" button to create the role.

5.1.2 Updating a role

Permissions required: Role | Retrieve, Role | Update

To update a role:

1. Select the "Roles" or "Site roles" option from the "Administration" menu.
2. Click the name of the role.
3. Edit any fields you wish to update (name and/or description).
4. If you wish to add permissions to the role:
   a. Click the "Add" button.
   b. Select one or more permissions. Multiple permissions may be selected at once by holding the Shift-key (to select a range) or the Ctrl-key (to select separate individual permissions).
   c. Click the "Add selected" button.
   d. Repeat the previous three steps if you wish to add more permissions.
5. To remove a permission, click the "Delete" link to the right of the permission.
6. Click the "Apply" button to save the changes.

Changes to permissions will be reflected upon the next login of FP5 users with this role. Currently logged in FP5 users will not be affected by the role change.

5.1.3 Reviewing the permissions assigned to a role

Permissions required: Role | Retrieve

To review the permissions assigned to a particular role:

1. Select the "Roles" or "Site roles" option from the "Administration" menu.
2. Click the "List permissions" link to the right of the role. A pop-up screen will show the permissions that have been assigned to that role.

5.1.4 Reviewing the FP5 users that have been assigned a role

Permissions required: Role | Retrieve, FP5 user | Retrieve

To review the FP5 users that have been assigned a particular role:

1. Select the "Roles" or "Site roles" option from the "Administration" menu.
2. Click the "Show FP5 users" link to the right of the role. A pop-up screen will show the FP5 users that have been assigned that role, and for which site they have that role.

5.1.5 Deleting a role

Permissions required: Role | Retrieve, Role | Delete

☞ NOTE: A role can only be removed if it is no longer assigned to any FP5 users.

To delete a role:

1. Select the "Roles" or "Site roles" option from the "Administration" menu.
2. Click the trash can icon 🗑 to the right of the role to be deleted. A pop-up screen will prompt for confirmation.

3. Conform deletion.

5.2 FP5 USERS

FP5 users log in to FP5 and have access to functionality depending on the permissions assigned to them through roles. This role-based access model allows FP5 users to have different roles for each site on the system.

Initially, FP5 is set up with an FP5 user "admin" that has the role "Administrator" for the system administration site.

Depending on the configuration of FP5 there can be two types of FP5 users:

- Local FP5 users that are created by an administrator and that have roles assigned manually
- Domain FP5 users that exist in an LDAP directory (e.g. Microsoft Active Directory). Their login is validated against the data in a directory and the roles assigned are retrieved from that directory.

To set up authentication of FP5 users with an LDAP directory, consult the FP5 installation manual.

Once an FP5 user is authenticated by the LDAP directory, a shadow copy will be created in FP5, and the FP5 user will be visible in the administration pages. For these FP5 users, some functions (like password change, blocking/unblocking) must be performed in the LDAP directory and are not available in FP5. FP5 users authenticated by the LDAP directory are always owned by the system administration site.

Each FP5 user has a unique user name that is used to log in from the log in screen and to identify the FP5 user in other screens. When an FP5 user is retrieved from an LDAP directory, it will also have the LDAP FP5 user DN set. A unique user name is still generated for LDAP FP5 users to satisfy system requirements. If the user name retrieved from the directory is not unique, a serial number is appended to the name to ensure a unique user name.

5.2.1 Creating a local FP5 user

Permissions required: FP5 user | Retrieve, FP5 user | Create

Ensure the correct site is selected when creating a new FP5 user. The FP5 user will be 'owned' by the site that was selected when the FP5 user was created. When an FP5 user is created in the system administration site, only FP5 users (administrators) with permission to edit FP5 users in the system administration site will be able to manage the FP5 user. When an FP5 user is created within another site, FP5 users (functional administrators) with permission to edit FP5 users for that site will be able to manage the FP5 user.

To create a local FP5 user:

1. Select the "FP5 users" option from the "Administration" menu.
2. Click the "Create" button.
3. Enter the details for the new FP5 user in the appropriate fields.
4. In the tab "Sites/terminal groups", add the sites and system-wide terminal groups that will be visible to this FP5 user.
5. In the tab "Roles", add the roles for this FP5 user. For each role:
   a. Click the "Add" button.
   b. Select the combination of site and role to assign.
   c. Check the "Grant option" checkbox if desired (see below).
   d. Click "Add".
   To delete a role, click the "Delete" link to the right of the role.
6. Click the "Save" button to create the FP5 user.

The "Grant option" checkbox determines whether the FP5 user will be able to assign that same role to another FP5 user (if the FP5 user also has the FP5 user | Update permission for that site).

Effectively, an FP5 user with FP5 user | Update permission can only assign the roles he has been assigned himself, and for which the checkbox "Grant option" is checked, to other FP5 users.

5.2.2 Updating an FP5 user

Permissions required: FP5 user | Retrieve, FP5 user | Update

To update an FP5 user:
1. Select the "FP5 users" option from the "Administration" menu.
2. Click the name of the FP5 user to be updated. If the desired FP5 user is not shown, ensure the correct site is selected first. The screen will show the FP5 user details.
3. Edit the fields you wish to update.
4. If you wish to edit the sites and/or system-wide terminal groups that will be visible to this FP5 user, add or delete sites and/or system-wide terminal groups on the tab "Sites/terminal groups".
5. If you wish to edit the roles for this FP5 user, add or delete roles on the tab "Roles" (see §5.2.1 for info on adding roles and the "Grant option" checkbox).
6. Click the "Apply" button to save the changes.

5.2.3 Changing an FP5 user's password

Permissions required: FP5 user | Retrieve, FP5 user | Update

To change an FP5 user's password:
1. Select the "FP5 users" option from the "Administration" menu.
2. Click the name of the FP5 user. If the desired FP5 user is not shown, ensure the correct site is selected first.
3. On the FP5 user detail screen, click the "Change password" button.
4. Enter the desired password twice.
5. Click "Set".
6. Click the "Apply" button to save the changes.

5.2.4 Changing an FP5 user's profile

Permissions required: none

Whenever an FP5 user is logged in, he can change his own FP5 user profile, i.e. the default UI language that will be shown whenever he logs in, his profile picture and his password.

To change your FP5 user's profile:
1. Select the "Profile" option from the menu with your login name.
2. If you want to change the default UI language that will be shown whenever you log in, choose the preferred language from the drop-down list in the field "Language".
3. If you want to add or change your profile picture, click the "Choose file" button and select a file. The file name will be shown behind the "Choose file" button.
4. If you wish to change your password, click the "Change password" button.
5. Enter the desired password twice.
6. Click "Set".
7. Click the "Apply" button to save the changes.

5.2.5 Blocking an FP5 user

Permissions required: FP5 user | Retrieve, FP5 user | Block

To block an FP5 user:
1. Select the "FP5 users" option from the "Administration" menu.
2. Click the "Block" link to the right of the FP5 user. If the desired FP5 user is not shown, ensure the correct site is selected first. The blocked FP5 user will not be able to log in to FP5. If the FP5 user is currently logged in, the block will be active on the next login.

5.2.6 Unblocking an FP5 user

Permissions required: FP5 user | Retrieve, FP5 user | Unblock

To unblock an FP5 user:
1. Select the "FP5 users" option from the "Administration" menu.
2. Click the "Unblock" link to the right of the FP5 user. If the desired FP5 user is not shown, ensure the correct site is selected first. The FP5 user will now be able to log in again.

5.2.7 Deleting an FP5 user

Permissions required: FP5 user | Retrieve, FP5 user | Delete

To delete an FP5 user:
1. Select the "FP5 users" option from the "Administration" menu.
2. Click the name of the FP5 user to be deleted. If the desired FP5 user is not shown, ensure the correct site is selected first.
3. On the detail screen, click the "Delete" button. A pop-up screen will prompt for confirmation.
4. Confirm deletion.

Because of referential integrity constraints, FP5 users are never actually deleted. They merely become invisible from the list. It is not possible to create a new FP5 user with the same user name as an existing deleted FP5 user.

5.2.8 Assigning permissions based on LDAP groups

When FP5 users are authenticated against an LDAP directory, their permissions are assigned based on the group membership in the LDAP directory.

To create a group-to-role mapping:
1. Ensure the system administration site is selected.
2. Select the "Group-to-role mappings" option from the "Administration" menu.
3. Click the "Create" button to create a new mapping.
4. Enter the group name in the site languages and a description of the mapping in the appropriate fields. The value in the field "Group name" should be the LDAP group common name in all uppercase characters prefixed by the "ROLE_" text. For example, for an LDAP group named "Service-desk", the field "Group name" should be "ROLE_SERVICE-DESK". In future versions of FP5 the group name will just be equal to the LDAP group name.
5. Check the synchronise option if desired. This determines whether this mapping is active. If synchronise is off, FP5 will no longer assign permissions based on this mapping. If synchronise is on (checked), permissions contained in this mapping will be assigned to FP5 users that are a member of a matching group.

7. To add system-wide roles to the mapping, for each role:
    a. Click the "Add" button next to "System-wide roles".
    b. Select the combination of site and role to assign.
    c. Check the "Grant option" checkbox if desired (see §5.2.1).
    d. Click the "Add" button.
    To delete a role, click the "Delete" link to the right of the role.
8. To add site-specific roles to the mapping, for each role:
    a. Click the "Add" button next to "Site-specific roles".
    b. Select the combination of site and role to assign.
    c. Check the "Grant option" checkbox if desired (see §5.2.1).
    d. Click the "Add" button.
    To delete a role, click the "Delete" link to the right of the role.
9. To add sites that FP5 users with this mapping may view, for each site:
    a. Click the "Add" button next to "Sites".
    b. Select the site.
    c. Click the "Add selected" button.
    To delete a site, click the "Delete" link to the right of the site.
10. To add terminal groups to be associated with the mapping, for each terminal group:
    a. Click the "Add" button next to "Terminal groups".
    b. Select the combination of site and terminal group.
    c. Click the "Add" button.
    To delete a terminal group, click the "Delete" link to the right of the terminal group.
11. Click the "Save" button to save the mapping.

Normally, FP5 will only synchronise the permissions of an FP5 user when it detects that the LDAP directory entry for that FP5 user has been updated. When a mapping is added (or modified or deleted), FP5 will force re-synchronisation of all FP5 users.

5.3   SITES

An FP5 user does not always see all the sites on the system. Which sites are visible and selectable is determined on the tab "Sites/terminal groups" of that FP5 user (see §5.2.1). A fresh install will have an initial admin FP5 user that has Administrative access to the system administration site.

5.3.1   Setting up a new site

Permissions required: Site | Retrieve, Site | Create

☞ Before a new site can be set up a unique site code has to be obtained from Magna Carta. This site code is a numeric value that distinguishes card/ID bases worldwide and ensures that terminals within the site will only accept cards/IDs issued by that site. To retrieve a site code for a new site, contact your Magna Carta representative.

To create a new site:
1. Select the "Sites" option from the "Administration" menu.
2. Click the "Create" button.
3. Enter the site details in the appropriate fields. The site code obtained from Magna Carta should be entered in here. Refer to §5.3.2.1 for information on a site's details.
4. Click the "Save" button to create the site.

When a new site is created, the current FP5 user is automatically given initial permission to access the site (otherwise the site would not be visible to that FP5 user). In other words, the "Site management" role for that site is assigned to the current FP5 user.

To define the administrator for the new site:

1. Select the "FP5 users" option from the "Administration" menu.
2. Click the name of the FP5 user to define as administrator for the new site.
3. On the tab "Roles" click the "Add" button next to "General roles for sites".
4. Choose the new site from the drop-down list in the field In the field "Site"
5. Choose "Administrator" from the drop-down list in the field "Role".
6. Check the "Grant option" checkbox if desired (see §5.2.1).
7. Click the "Add" button.
8. Click the "Apply" button to save the changes. If the role was added for an FP5 user logged in at that moment, he must log out and log in again before the new permissions become active.

5.3.2 Updating a site's details

Permissions required: Site | Retrieve, Site | Update

To update the details of a site:

1. Select the "Sites" option from the "Administration" menu.
2. Click the name of the site.
3. Edit the fields you wish to update on the tabs "Details", "Contact", "Servers", "Artwork" and "Parameters". The following paragraphs describe which details can be found on each tab.
4. Click the "Apply" button to save the changes.

Note: All details from the site can be updated. However, it is not advisable to change the site code after a site has been put into production.

5.3.2.1 The tab "Details"

The details on this tab are required details (apart from "Language 2", "Language 3", etc.

- Name: the name of the site as shown in the management interface (in each of the site languages). The languages to be provided here are the languages configured for the system administration site.
- Site code: this is provided by Magna Carta for a new site. The system administration site uses site code 0, demonstration sites use site code 12345. It is not advised to change the site code after a site has been put into production.
- Time zone: the time zone for displaying and entering times. This time zone is also used to determine the schedule for reports run by the site as well as the date ranges contained in those reports.
- Default currency: the default currency for displaying monetary amounts.
- Web domain: the URL to use for managing this site; i.e. the domain name and, optionally, the port and path for the management interface for the site. If a different domain name is set than the main server, ensure that DNS points to the server and that virtual hosts are set up properly. A technical administrator should perform this operation before another host name can be chosen.
- Meta-site (read-only): Indicates (if checked) that this site is the system administration site (meta-site).
- Status (read-only) : Current status of this site: active or blocked
- Language 1..5: the languages that can be used by FP5 users of this site. The language configured as first language (Language 1) will be the default language if a text is not available in the chosen language.

5.3.2.2 The tab "Contact"

For administrators it can be useful to have access to the details of a contact person for a particular site. These details may be entered and retrieved but they are not used by FP5 itself.

- Contact name

- Contact address
- Contact email
- Contact phone 1
- Contact phone 2
- Comments: Arbitrary comments about this site

5.3.2.3 The tab "Servers" (email configuration and secondary database details)

At different points in time FP5 will send emails to FP5 users and users. For instance, reports can be sent by email and site alerts can be emailed to administrators. Each site can have a separate email configuration so that emails may appear to originate from an address specific to that site.

- From address: email address to send mail from
- From name: name to use as 'from' contact
- SMTP server: server host name or IP to connect to
- SMTP port: port to connect to (default is 25)
- SMTP user name: if authentication is required, supply the user name to use
- SMTP password: if authentication is required, supply the password to use

Optionally, the details of a secondary database connection may be supplied. These details will be used by the reporting engine. There are two common scenarios for entering this information:

1. The site is used to report on an 'old' FPM database, in which case the details of the FPM database are provided here.
2. On large scale sites, the reporting may be performed from a read-only synchronised copy of the database. This prevents database locking during reporting. In this case the details of this database connection are provided here.

- 2nd database type: Type of database
- 2nd database url: JDBC URL for this database
- 2nd database user name: User name to log in
- 2nd database password: Password used to log in to the database

5.3.2.4 The tab "Artwork"

On this tab you can select files that will be used as the logo for the site and as the logo on reports. You can choose files with jpg or png format.

5.3.2.5 The tab "Parameters"

This tab at present has one parameter:
- Days to retain transactions – the default value is 1461, which is four years;

5.3.3 Deleting a site

Permissions required: Site | Retrieve, Site | Delete

To delete a site:
1. Select the "Sites" option from the "Administration" menu.
2. Click the trash can icon to the right of the site. A pop-up screen will prompt for confirmation.
3. Confirm deletion.

A site cannot really be deleted if it has been used anywhere in FP5. By deleting a site, it is merely disabled and hidden from view.

5.3.4 Blocking a site

Permissions required: Site | Retrieve, Site | Block

If a hosted site has not paid invoices and the service is temporarily suspended, or alternatively to stop operations before a site is discontinued and deleted, one might need to block access to FP5 for all FP5 users and terminals of a particular site.

To block a site:

1. Select the "Sites" option from the "Administration" menu.
2. Click the "Block" link to the right of the site.

A blocked site will no longer have access to FP5. FP5 users that are 'owned' by a blocked site can no longer log in to FP5 and terminals configured by that site will be refused by FP5.

5.3.5 Unblocking a site

Permissions required: Site | Retrieve, Site | Unblock

To unblock a site:

1. Select the "Sites" option from the "Administrator" menu.
2. Click the "Unblock" link to the right of the site.

Once a site is unblocked, FP5 users and terminals will be able to connect to FP5 again.

5.4 EMAIL TEMPLATES

A system administrator or site administrator may configure different email templates that will be used by FP5 to format emails to FP5 users and users. For each type of message a different template is used. Also, templates may be configured in multiple languages. When you create an email template, you select a language in the field "Language".

Templates configured in the system administration site serve as defaults for all sites in the system. A site's administrator may configure alternate templates.

The following table lists the types of email templates that may be configured.

Table 3: Email template types

E-mail template type	Description
Report with attachment	Used to send a report attachment to an FP5 user. The report will be attached as a document to the text specified by the template.
Report with link (no attachment)	Used to send a link to a report to an FP5 user. The report may also be attached (if desired by the distribution details). The report template should contain a variable that will contain the link. To add the link, the following variable needs to be inserted: https://$site.domain/$site.context/report/report-output/$output.id
Empty report	Used to send a notification in case a report did not produce any data.
SMS report	Used to send a SMS to an FP5 user when a report becomes available. The text resulting from the template should not contain more than 160 characters. An SMS gateway email address can be entered in the field "To address" of the template. Use the ${mobileNumber} or ${mobileNumberNoPlus} parameter in the field "To address" to retrieve the normalized mobile number for the FP5 user.

SMS empty report	Used to send a SMS to an FP5 user when a report did not produce any data. The text resulting from the template should not contain more than 160 characters. A SMS gateway email address can be configured in the field "To" of the template. Use the ${mobileNumber} or ${mobileNumberNoPlus} parameter in the field "To" to retrieve the normalized mobile number for the FP5 user.
Site alert	Not yet in use.
Reservation available	Not yet in use.
Reservation expired	Not yet in use.
User password reset	Used to send a new password generated by FP5 to a user via email.
User password reset SMS	Used to send a new password generated by FP5 to a user via SMS.
FP5 user password reset	Used to send a new password generated by FP5 to an FP5 user via email.
FP5 user password reset SMS	Used to send a new password generated by FP5 to an FP5 user via SMS.

If a template cannot be found for a particular type (in any language), sending the email or SMS will fail. Therefore it is important to ensure that at least these templates exist in the default language.

If a template cannot be found in a particular FP5 user's language, FP5 will use the template configured for the default language.

5.4.1   Creating an email template

Permissions required: Email template | Retrieve, Email template | Create

To create an email template:

1. Select the "Email templates" option from the "Administration" menu.
2. Click the "Create" button.
3. Enter the email template name in the site languages and the type in the appropriate fields.
4. Enter the subject and body text to use for the email (or SMS). The body text is entered as rich text (html). FP5 will automatically convert this text down to plain text for recipients that are not able to process html email texts.
5. Click the "Save" button to create the template.

5.4.2   Updating an email template

Permissions required: Email template | Retrieve, Email template | Update

To update an email template:

1. Select the "Email templates" option from the "Administration" menu.
2. Click the name of the template.
3. Edit the fields you wish to update.
4. Click the "Apply" button to save the changes.

5.4.3   Deleting an email template

Permissions required: Email template | Retrieve, Email template | Delete

To delete an email template:

1. Select the "Email templates" option from the "Administration" menu.
2. Click the trash can icon   to the right of the template to be deleted. A pop-up screen will prompt for confirmation.

3. Confirm deletion.

5.4.4 Variables allowed in email templates

The text specified for the subject line and the body text are interpreted by the Velocity engine.

When sending an email the engine will replace variable names in the subject line and in the body text with a dynamic value. The variable names are recognised because they adhere to specific formatting rules.

For a complete reference of possible constructs in these templates, refer to the Velocity documentation which is available at http://velocity.apache.org/engine/devel/vtl-reference-guide.html.

The following table lists variable names that can be included in the subject or body text of an email template and that will be substituted by the current value when the email is sent.

Table 4: Email template variable names

Variable name	Description
${config.description}	Description of the report configuration
${config.id}	Internal unique ID of the report configuration
${configName}	Name of the report configuration in the language of the email template
${distribution.distributedTo.emailAddress}	If distributed to a FP5 user, the email address for this FP5 user
${distribution.distributedTo.languageId}	If distributed to a FP5 user, the language ID for this FP5 user
${distribution.distributedTo.timeZoneId}	If distributed to a FP5 user, the time zone ID for this FP5 user
${distribution.distributedTo.userDN}	If distributed to an LDAP FP5 user, the user DN for this FP5 user
${distribution.distributedTo.userName}	If distributed to a FP5 user, the login name of this FP5 user
${distribution.emailAddress}	If distributed to an email address, the email address
${distribution.languageId}	If distributed to an email address, the language ID for this email address
${mobileNumber}	The mobile number of the FP5 user that the report is being sent to, normalized including a "+" sign and country code.
${mobileNumberNoPlus}	The mobile number of the FP5 user that the report is being sent to, normalized including country code, but not including a "+" prefix.
${output.adHoc}	Indicates whether the report was scheduled or created ad hoc
${output.byLoginName}	User name of the FP5 user that created the ad hoc report
${output.createdDate}	Date the report was created
${output.id}	Internal unique ID for this report. You can link to a report's page by specifying: https://${site.domain}/${site.context}/report/report-output/${output.id}
${output.parameterValues}	List of parameter values used to create the report
${output.status}	Indicates the current status of the report
${site.contactAddress}	Contact address of the site the report is about
${site.contactEmail}	Contact email address of the site the report is about
${site.contactName}	Contact name of the site the report is about
${site.contactPhone1}	Contact phone number 1 of the site the report is about
${site.contactPhone2}	Contact phone number 2 of the site the report is about
${site.context}	Context path after the domain name of the site the report is about
${site.defaultCurrency}	Default currency of the site the report is about

Variable name	Description
${site.description}	Description provided with the site the report is about
${site.domain}	Domain name (and port) of the site the report is about
${site.id}	Internal unique ID for the site the report is about
${site.siteCode}	Site code for the site the report is about
${site.timeZoneId}	Time zone code of the site the report is about
${siteName}	Name of the site in the language of the email template.
${template.description}	Description of the report template
${template.id}	Internal unique ID for the report's template
${templateName}	Name of the email template in the language of the email template

Images can also be added to the body text of an email template. They can be inserted using the "Insert image" icon ( ) in the rich text editor's toolbar. The image has to be available on a public web server and is inserted by supplying the URL to the image on that server.

5.5 REPORT TEMPLATES

The reporting engine of FP5 uses templates to determine the query and layout of a report. These templates are created using JasperReports. For documentation on how to create report templates, please refer to the JasperReports and iReports site: https://www.jaspersoft.com/ireport-designer.

5.5.1 Report template format

A report template consists of multiple files and is presented to FP5 as a single zip-file of these files.

5.5.1.1 Zip-file contents

FP5 looks in the zip-file for a file with "jrxml" extension. The name of the file is insignificant. A report template may contain multiple sub-reports that are included in the main report. The names of the files that contain the sub-reports must start with the prefix "sub_", otherwise they may be confused with the main report.

Additional files in the zip-file may contain images and language resources, they will be available to the report template as long as no explicit path is specified (from the current directory). Note that iReport by default includes the full path to an image in the template, so it may be necessary to manually edit the template xml to remove these paths.

An example of contents of a report template zip-file is given in the following table.

Table 5: Example of report template zip-file contents

File name	Description
logo.png	Logo image that may be used by a template
texts.properties	Texts in the default language
texts_nl.properties	Texts in the Dutch language
main.jrxml	Main report template XML file
sub_detail.jrxml	Sub-report template XML file

NOTE: A report template contains SQL queries that have the capability to access data across the database (not limited to the selected site) when improperly constructed. Therefore it is strongly advised to give only System Administrators permission to create and update report templates, even when created in a particular site. FP5 will always pass the selected site to the SQL query, but the developer of the report template is responsible for ensuring only data for that site is selected by including the site parameter in the SQL WHERE-clause.

5.5.1.2 Report template languages

A report template can be used to generate a report in each of the site languages.

This is done by including a resource bundle in the report and supplying different translations of the texts as separate Java resource bundle files ending in the ".properties" extension. FP5 will detect the languages supported by the report by decoding the locale identifier in the file name.

Each file name should be formatted as follows:

<resource-bundle-name>_<locale>.properties

Inside the template, strings defined in the resource bundle can be referenced by using the $R{name} construct.

5.5.1.3 Report template parameters

A report template can specify extra external parameters to be supplied when creating the report.

There are built-in parameters that are always supplied by the report engine. Please refer to the JasperReports documentation for a list of these parameters.

There are also parameters that are always supplied by FP5 that can be referenced in a report template.

The following table lists the parameters that are built into each report template.

Table 6: Parameters built-in all report templates

Parameter name	Description
REPORT_LOCALE	The language selected for the report
REPORT_RESOURCE_BUNDLE	A reference to the language resource bundle if one has been supplied in the zip-file
REPORT_TIME_ZONE	The default time zone for the site the report is about
_siteId	The internal unique ID of the site the report is about
_siteName	The site name in the language selected for the report
_reportName	The report name in the language selected for the report
_dateFormat	A date pattern string with the desired date format for the report
_currencyFormat	A number pattern string with the desired number format for currencies in the report
entityId	The internal unique ID of an entity being exported as PDF file (automatically assigned if the exported PDF is used with a system report template type)

In addition, a report template may specify custom parameters to be supplied when configuring or generating the report. These parameters must be declared in the preamble of the report xml and that declaration may contain additional properties that control how the parameter values are selected by FP5.

Custom parameters must not start with an underscore and must define the "class" attribute to be a valid Java class name. The following table lists the parameter types recognised by FP5.

Table 7: Report template parameter's classes

Parameter name	Description
Collection classes	FP5 will allow multiple values to be supplied for collections
java.lang.Long	An integer parameter
java.lang.Boolean	A boolean parameter
java.lang.String	A string parameter
java.util.Date	A date parameter. If the parameter name ends with the "_start" postfix, FP5 will also look for a parameter that ends with "_end" to indicate a date range. Otherwise a single date is expected.

In addition, the template may specify a "type" property that allows further specification of the range of possible values that may be supplied by the FP5 user. The following table specifies the values supported for the type property.

Table 8: Syntax of report template parameter's type property

Parameter name	Description
boolean	FP5 will present a checkbox to supply the value.
integer(*min*,*max*)	FP5 will accept an integer value within the given range
entityref(*"class"*)	FP5 will prompt the FP5 user to select entities of the given class from a list of entities.
daterange	FP5 will prompt with a list box of texts and supply the option name as value. There must be two parameters specified for a date range, ending in _start and _end.
select(*"option"*:*"text"*,…)	FP5 will prompt with a list box of texts and supply the option name as value.
string(*"regex"*)	FP5 will prompt for a string value that must match the given regular expression. Refer to Oracle's documentation for the syntax of these regular expressions: http://docs.oracle.com/javase/tutorial/essential/regex/

If a property is specified with name "mandatory" and value "true", the parameter must be entered by an FP5 user in the report configuration.

Parameters are referenced in the report template xml using the $P{*parameter-name*} syntax. To use a multi-valued parameter in a where clause, use the $X{IN,*sql-variable*,*parameter-name*} syntax.

5.5.1.4 Report types

Most report templates will be used to schedule reports and generate ad-hoc reports from the reports menu. There are some places in FP5 where an entity can be exported from the detail screen. The picklist is one of these entities, there is an "Export PDF" button on the picklist screen that can be used to export the picklist as a PDF file. FP5 uses report types as template for these exports.

The following table lists the report types defined in FP5 by default.

Table 9: Report template types

Report type	Description
<empty> or Custom report	A normal report that is not used explicitly by FP5
Picklist report	Indicates this is a report template to be used to export a picklist as a PDF file. The unique ID for the entity being exported will be supplied as the "entityId" parameter.

5.5.2 Uploading a report template

Permissions required: Report template | Retrieve, Report template | Create

Before adding a new report template, ensure that the appropriate site is selected. If the system administration site is selected, the report template will be visible to all sites on the system. If a particular site is selected, the report template will only be visible to administrators (FP5 users) of that site.

To create and upload a new report template:

1. Select the "Report templates" option from the "Reports" menu.
2. Click the "Create" button.

3. Enter the report template name in the site languages and a description of the report template in the appropriate fields.
4. Select the report type.
5. Select the zip-file with the report template to upload. The name of the selected file will be shown behind the "Choose file" button.
6. Click the "Save" button to create the report template.

5.5.3 Updating a report template

Permissions required: Report template | Retrieve, Report template | Update

A report template can be updated. The names can be changed, but also a new template zip-file can be uploaded.

To update a report template:
1. Select the "Report templates" option from the "Reports" menu.
2. Click the name of the report template.
3. Edit the fields you wish to update and/or upload a new zip-file.
4. Click the "Apply" button to save the changes.

5.5.4 Deleting a report template

Permissions required: Report template | Retrieve, Report template | Delete

NOTE: A report template can only be deleted when it is no longer used by any report configuration.

To delete a report template:
1. Select the "Report templates" option from the "Reports" menu.
2. Click the trash can icon 🗑 to the right of the report to be deleted. A pop-up screen will prompt for confirmation.
3. Conform deletion.

5.5.5 Uploading several report templates at once

Permissions required: Report template | Retrieve, Report template | Create

If several report template zip files (see §5.5.1) are saved together in a report template package zip file, they can all be imported at once. Ensure that the appropriate site is selected. If the system administration site is selected, the report templates will be visible to all sites on the system. If a particular site is selected, the report templates will only be visible to administrators of that site.

To create and upload several new report templates at once:
1. Select the "Report templates" option from the "Reports" menu.
2. Click the "Upload package" button.
3. Select the zip-file with the report templates to upload. A pop-up will show which report templates are in this zip-file.
4. Click the "Import" button. You will return to the list of report templates, and the imported report templates will be shown in the list.

5.6 FP5 ACTIVITY LOG

The FP5 activity log allows the FP5 user to view all previous FP5 activities or a selection. One can narrow down the activities shown by selecting a certain type of entity (card/ID, card/ID configuration, card/ID update, cost centre, email template, FP5 user, FP5 user directory, hardware, picklist, pricetable, privilege, product, product group, product reservation, purse, purse configuration, report configuration, report template, role, site, terminal, terminal configuration, terminal group, terminal product layout, timetable, user, user group,VAT rate), or by entering a specific value for certain fields.

To retrieve a list of FP5 activities:

1. Select the "FP5 activity log" option from the "Administration" menu.
2. If you want to see the activities of a particular kind choose a value from the drop-down list in the field "Entity name" and/or enter values in the other fields.
3. Click the "Search" button. A list of the activities that match the search criteria (if any) will be shown. Some basic data of this activity is shown, and if you click on the "Data" button to the left of an activity you see all the details of that activity, i.e. which fields were modified as a result of the activity, and what the old and new values were.

5.6.1 The "Show revisions" button

On various FP5 detail screens one might see a "Show revisions" button if the FP5 user has access to the system administration site and a role for the system administration site which has the FP5 activity | Retrieve permission . This redirects the FP5 user to the FP5 activities screen with the value of the entity for which the "Show revisions" button was selected already filled in.

6 PRODUCT CONFIGURATION

A product is the unit that is sold/controlled by terminals in the system.

6.1 PRODUCT GROUPS

Products are grouped into product groups. A product can only be in one product group at a time. Organising products into product groups simplifies the configuration of privileges.

The fields of the product group detail screen are listed below. The fields marked * must be assigned a value:

1) Name*
2) Default VAT rate: (default value "Select one" which means no VAT rate has been defined for the product group) the VAT rate for products of this product group. The value must be chosen from a drop-down list which shows the VAT rates that have been defined in FP5 (see §6.5). Individual products can be assigned a VAT rate which will then overrule the product group VAT rate.
3) Description

6.1.1 Creating a product group

Permissions required: Product group | Retrieve, Product group | Create

To create a product group:

1. Select the "Product groups" option from the "Products" menu.
2. Click the "Create" button.
3. Enter the details for the new product group in the appropriate fields.
4. Click the "Save" button to create the group.

6.1.2 Updating a product group

Permissions required: Product group | Retrieve, Product group | Update

To update the details of a product group:

1. Select the "Product groups" option from the "Products" menu.
2. Click the name of the product group.
3. Edit the fields you wish to update.
4. Click the "Apply" button to save the changes.

6.1.3 Deleting a product group

Permissions required: Product group | Retrieve, Product group | Delete

NOTE: A product group can only be deleted if it is not in use by any privilege or product.

To delete a product group:

1. Select the "Product groups" option from the "Products" menu.

2. Click the trash can icon   to the right of the product group to be deleted. A pop-up screen prompts for confirmation.

3. Conform deletion.

6.2 PRODUCTS

The fields of the product detail screen are listed below. The fields marked * must be assigned a value:

1) Name*
2) Short name
3) Product group: products can be grouped into product groups. A product can only be in one product group at a time. Organising products into product groups simplifies the configuration of privileges.
4) Part number
5) Logistic code
6) Weight
7) Length
8) Width
9) Height
10) Default price*: default price in the site's default currency
11) Default VAT rate: (default value "Select one" which means no VAT rate has been defined for the product) the VAT rate for this product. The value must be chosen from a drop-down list which shows the VAT rates that have been defined in FP5 (see §6.5). If a value is entered here, this will overrule the default VAT rate of the product group. If no value is entered here, the default VAT rate of the product group will apply to the product.

6.2.1 Creating a product

Permissions required: Product | Retrieve, Product | Create

To define a new product:

1. Select the "Products" option from the "Products" menu.

2. Click the "Create" button.
3. Enter the details for the new product in the appropriate fields. If a default VAT rate has been defined for the product group the product belongs to, this VAT rate will be used for this product unless you define an alternative VAT rate for this product here, even though the product group's default VAT rate is not shown here.
4. Select a product group to assign this product to (optional).
5. Click the "Save" button to create the product.

6.2.2 Updating a product

Permissions required: Product | Retrieve, Product | Update

To update a product's details:
1. Select the "Products" option from the "Products" menu.
2. Click the name of the product.
3. Edit the fields you wish to update.
4. Click the "Apply" button to save the changes.

☝ NOTE: When product details are updated, FP5 will queue an automatic update to affected terminals. A banner at the top of the screen will indicate when this update will occur.

6.2.3 Deleting a product

Permissions required: Product | Retrieve, Product | Delete

☝ NOTE: It is not possible to delete a product once it has been used in a privilege or transaction.

To delete a product:
1. Select the "Products" option from the "Products" menu.
2. Click the trash can icon 🗑 to the right of the product to be deleted. A pop-up screen prompts for confirmation.
3. Confirm deletion.

6.3 TIMETABLES

When creating privileges, timetables can be chosen, which then define periods in time when the privilege is valid, or points in time when the privilege counter value should increase. A timetable consists of a set of validity intervals defined by a start time and an end time.

A timetable can be repeating, in which case the validity intervals automatically recur each time the selected period (e.g. day, week month) has gone by.

FP5 supports two basic types of timetables:

- Weekly timetable: defines validity intervals based on the days of a week. If the timetable is repeating, the validity intervals repeat each week.
- Yearly timetable: defines validity intervals based on date/time ranges in a calendar year. If the timetable is repeating, the validity intervals repeat each year.

Timetables may be combined by including or excluding validity intervals from another timetable. In this way, yearly and weekly timetables can be combined. For example, it is possible to have a yearly timetable of holidays and exclude them from a weekly timetable of working hours effectively creating a timetable that specifies as validity periods: working hours on non-holidays.

The fields of the timetable detail screen are listed below. The fields marked * must be assigned a value:

1) Name*: We recommend using a name that describes the properties of the timetable.
2) Type*: weekly or yearly. Once selected the type cannot be changed.
3) Repeating: if checked, the timetable will repeat, i.e. the intervals defined automatically recur in each period selected (week or year depending on value of field "Type").
4) Relative: if this field is not checked and the timetable is repeating, e.g. weekly, a privilege assigned this timetable will increase the privilege counter each time a card/ID is presented at an online terminal on condition that another week has passed, calculated from the start time defined in this timetable. If this field is checked, the time the privilege counter was last increased will be used, and not the start time defined in this timetable. If a week has passed since the last increase, the value will be increased. (Example: field not checked and start time Monday 9 am: increase every week at first transaction after Monday 9 am; field checked: increase only if a week has passed since last increase).
5) Start time*: first start time for the timetable. The timetable will not be valid before the given reference time, but if repeating it will be valid indefinitely after the start time.
6) Description
7) Validity intervals: one or several intervals in which timetable will be valid.
8) Exclude timetable: the value must be chosen from a drop-down list which shows the timetables that have been defined in FP5. Any time intervals that would fall within the current timetable, but also fall within the exclude timetable will be excluded from the current timetable
9) Include timetable: the value must be chosen from a drop-down list which shows the timetables that have been defined in FP5. Any time intervals that would not fall within the current timetable, but fall within the include timetable will be included in the current timetable

6.3.1 Creating a timetable

Permissions required: Timetable | Retrieve, Timetable | Create

To create a timetable:

1. Select the "Timetables" option from the "Products" menu.
2. Click the "Create" button.
3. Enter the details for the timetable in the appropriate fields.
4. To add a validity interval, click the "Add" button. A pop-up screen appears in which the interval can be defined (see Figure 6-1 and Figure 6-2).

Figure 6-1: Pop-up screen for defining validity interval for timetables of type "Weekly"

Figure 6-2: Pop-up screen for defining validity interval for timetables of type "Yearly"

5. For a timetable of type "Weekly" select the "From" and the "To" day and time of the interval. For a timetable of type "Yearly" select the "From" and the "To" month, date and time of the interval.
6. Click the "Add" button to add the validity interval to the list.
7. Repeat the previous three steps to add another validity interval.
8. To delete an interval, click the "Delete" link to the right of the interval.
9. Optionally, select an "Exclude timetable". The intervals from the exclude timetable will be excluded from the validity intervals specified for this timetable.
10. Optionally, select an "Include timetable". The intervals from the include timetable will be combined with the validity intervals specified for this timetable.
11. Click the "Save" button to create the timetable.

6.3.2   Updating a timetable

Permissions required: Timetable | Retrieve, Timetable | Update

To update a timetable:

1. Select the "Timetables" option from the "Products" menu.
    Click the name of the timetable.
2. Edit the fields you wish to update. The interval type ("Weekly" or "Yearly") cannot be changed on an existing timetable.
3. Click the "Apply" button to save the changes.

☝ When a timetable is updated, FP5 will queue an automatic update to affected terminals. A banner at the top of the screen will indicate when this update will occur.

6.3.3   Deleting a timetable

Permissions required: Timetable | Retrieve, Timetable | Delete

☝ NOTE: A timetable can only be deleted if it is not referenced by any privileges.

To delete a timetable:

1. Select the "Timetables" option from the "Products" menu.
2. Click the trash can icon 🗑 to the right of the timetable to delete. A pop-up screen will prompt for confirmation.
3. Confirm deletion.

6.4   PRICE TABLES

FP5 allows for multiple prices to be defined for products. This is done by creating price tables and then defining the prices of the products in these price tables. One must also define, for each price table, a privilege of type "Price table" (see § 7.1.6.5), in which the applicable price table is chosen, as well as the products and/or product groups to which the privilege (i.e. the price table) applies, and assign that privilege to one or more user groups or users (see § 7.2.3 and §7.2.5).

The fields of the price table detail screen are listed below. The fields marked * must be assigned a value:

1) Name*: We recommend using a name that describes to whom the price table might apply (e.g. "Guest prices" or "Price table seminar")
2) Description
3) Currency

4) Default VAT rate: the VAT rate that applies when a product is purchased against the price defined for this product for this price table. The value can be chosen from a drop-down list which shows the VAT rates that have been defined in FP5 (see § 6.5).

6.4.1 Creating a price table

Permissions required: Price table | Retrieve, Price table | Create

To create a price table:
1. Select the "Price tables" option from the "Products" menu.
2. Click the "Create" button.
3. Enter the details for the price table in the appropriate fields.
4. Click the "Save" button to create the price table.

6.4.2 Setting product prices for a price table

Permissions required: Product | Retrieve, Product | Update, Price table | Retrieve, Price table | Update

To define the prices for a price table:
1. Select the "Products" option from the "Products".
2. Click the "Edit price table" button.
3. Select the price table to edit. The list of products now contains editable fields for the selected price table.
4. Enter the prices in the "Price in selected price table" column and (optionally) the VAT rates for the products in this price table.
5. Click the "Save price table" button to save the changes. You can now view the list of products with or without the column for the selected price table, by clicking the "Hide price table" and "Edit price table" buttons respectively. You can only see the prices for one price table at a time.

6.4.3 Deleting a price table

Permissions required: Price table | Retrieve, Price table | Delete

A price table cannot be deleted if it is used by a privilege.

To delete a price table:
1. Select the "Price tables" option from the "Products" menu.
2. Click the trash can icon   🗑   to the right of the price table to delete. A pop-up screen will prompt for confirmation.
3. Confirm deletion.

6.5 VAT RATES

FP5 allows multiple tax rates or VAT rates to be defined and assigned to product groups or individual products. The fields of the VAT rate detail screen are listed below. The fields marked * must be assigned a value:

1) Name*
2) VAT percentage*
3) Description

6.5.1 Creating a VAT rate

Permissions required: VAT rate | Retrieve, VAT rate | Create

To create a VAT rate:

1. Select the "VAT rates" option from the "Products" menu.
2. Click the "Create" button.
3. Enter the details for the VAT rate in the appropriate fields.
4. Click the "Save" button to create the VAT rate.

6.5.2 Updating a VAT rate

Permissions required: VAT rate | Retrieve, VAT rate | Update

To update a VAT rate:

1. Select the "VAT rates" option from the "Products" menu.
2. Click the name of the VAT rate.
3. Edit the fields you wish to update.
4. Click the "Apply" button to save the changes.

6.5.3 Deleting a VAT rate

Permissions required: VAT rate | Retrieve, VAT rate | Delete

A VAT rate cannot be deleted if it is used by a product, product group, or price table.

To delete a VAT rate:

1. Select the "VAT rates" option from the "Products" menu.
2. Click the trash can icon 🗑 to the right of the VAT rate to delete. A pop-up screen will prompt for confirmation.
3. Confirm deletion.

7 PRIVILEGES

7.1 INTRODUCTION

A privilege given to a user allows that user to receive the products defined in the privilege at a reduced price or even for free.

Typically, one might allow certain users to obtain a predefined number of certain products for free (e.g. 5 free coffee a day). FP5 must keep track of the number of products obtained through a privilege.

When products are purchased without any specific privilege, the product price is taken from the balance of the card/ID (which is in the related FacilityPro account (online systems) or in the e-purse on the card/ID (off-line systems)). When products are obtained through a privilege, all or part of the product price is subsidised by another party. This party can be billed for the amount thus granted using the reports from FP5 (see chapter 11).

One can also assign more than one privilege for the same products. The privilege which is most advantageous for the user is then always used. One might, for example, define a privilege for three free coffee a day and another for 50% discount on coffee. The former privilege would then be used first, and after the third cup of coffee, the latter would apply.

When creating privileges one will first choose a privilege type, then determine a number of parameter values. Only after saving this basic data of the privilege, one can and must define to which products and/or product groups the privilege pertains.

One can (but need not) also define to which terminals and/or terminal groups the privilege pertains (i.e. only to the products defined in the terminals defined). For an access privilege, one will define which terminals the privilege grants access to. For a service privilege one will define for which terminals the privilege allows the use of the service functions.

Privileges are assigned to user groups.

Which fields are shown on the privilege detail screen depends on the value of the field "Type" of the privilege.

7.1.1   Privilege counter

A privilege may have a value that indicates how many times a privilege can be used or up to which amount a privilege can be used. The value is stored as a counter for the privilege, either in the back office (online systems) or on the Card/ID (off-line systems). Whether the privilege counter represents a number of times or a monetary amount depends on the type of privilege. The value for the privilege counter is determined by the fields "Start value" and "Max value" and by transactions that were carried out against the privilege. The privilege counter is initially set to "Start value". It is topped up at set intervals if the privilege is defined as a privilege with a recurring increase or auto top-up (see §7.1.3), but it will never exceed "Max value". It is decreased when a transaction is carried out against the privilege: If the privilege counter represents a number of times it is increased by 1; if the privilege counter represents a monetary amount it is decreased by the amount subsidised through the privilege for this transaction.

7.1.2   Validity

A privilege can be subject to validity constraints.

To define at which times a privilege is valid, you can enter the following values:

- Start date: a date before which this privilege is never valid
- End date: a date after which this privilege is never valid
- Valid timetable: Select a timetable to control the validity in fine grain intervals.

7.1.3   Recurrence or auto top-up

The privilege counter of a privilege may be increased periodically. This is called auto top-up. To activate auto top-up, you must check the field "Enable auto top-up" and define the auto top-up value (field "Auto top-up") and interval (field "Auto top-up period"). The increase occurs at the terminal when it determines that the card/ID has not received its increase yet in the defined period. A "last top-up date" is stored for the card/ID as part of the privilege, and is updated every time the privilege counter is increased.

When defining a privilege, the default value for the auto top-up interval is 'never', and the privilege is therefore non-recurrent.

7.1.4   Maximum value

A privilege may have a maximum value. The privilege counter can never exceed this maximum value. If an auto top-up would cause the privilege counter to increase above the maximum value, the increase is lessened and the privilege counter is set to the maximum value.

7.1.5 Transparency

The transparency of a privilege controls whether the products to which the privilege pertains may still be obtained should the privilege be depleted, using the user's card/ID balance or another privilege. The following examples should clarify further.

At a school the teachers have a privilege which allows them to make 500 free copies per month. The field "Transparent" will be unchecked, to avoid teachers accidentally making copies for which they pay when they make more than 500 copies in a month.

A guest who is a speaker at a seminar is given a subsidy privilege allowing him to get lunch for up to €10 per day. But of course, if he wishes to have a €12 lunch, he should be free to pay the extra €2. Therefore, the field "Transparent" will checked.

7.1.6 Privilege types

Some of the fields of a privilege are specific for the type of privilege, and are discussed in the sections below.

The fields all privilege types share are listed below. The fields marked * must always be assigned a value.

- Name*
- Valid timetable (optional): choose a timetable that determines when this privilege may be used
- For terminal access: indicates when this privilege fulfills a terminal access requirement. Each terminal has a configuration parameter "Need privilege to use terminal" (see §9.3.1). If this parameter has the value "On", the terminal will refuse all cards/IDs unless they have a privilege for access to the terminal, i.e. a privilege with the field "For terminal access" checked and with this terminal included in the section "Terminals" or with its terminal group included in the section "Terminal groups". On top of giving access to the terminals in the sections "Terminals" and "Terminal groups" the privilege can have the function of granting a discount, a subsidy, a reduction etc.
- Transparent: controls whether the products to which the privilege pertains may still be obtained should the privilege be depleted, using the user's card/ID balance or another privilege
- Enable auto top-up: this checkbox controls whether the privilege counter is to have a recurring increase (auto top-up). When checked, the number of times or amount of the increase can be entered as well as the period after which the counter is increased.

7.1.6.1 Discount

A discount privilege grants a percentage discount off the price of a product. The user only pays the remaining amount from the balance of card/ID. A discount of 100% renders the product free of charge.

The privilege value (#) of a discount privilege is a counter that controls how many times the discount will be given. When the value is depleted (down to zero), the discount no longer applies. The transparency flag now controls whether the product may still be purchased without this privilege (from the card/ID balance or with another privilege).

The fields of a discount privilege are listed below. The fields marked * must always be assigned a value.

- Type*: must have the value "Discount"
- Discount (%)*: the percentage of the product price that is discounted (subtracted off the product price, 100% = free sale)
- Start value: the initial value of the privilege counter. To grant the privilege without limit, enter 65535 for always. If no start value is entered, the initial value will be 0, meaning no privilege. This would only make sense for a privilege with auto top-up.
- Max value: the maximum value (number of times) for the privilege counter

7.1.6.2 Subsidy

A subsidy privilege allows a product to be bought from a source of funds other than the balance of the card. The subsidy privilege is effectively a second purse that holds an amount of funds.

The value of a subsidy privilege is an amount in the default currency of the site. When an applicable product is purchased, the value is decreased by the default price of the product. If there is no or insufficient value left in the privilege counter, the transparency flag determines whether the remainder of the product price may be paid by other means.

The fields of a subsidy privilege are listed below. The fields marked * must always be assigned a value.

- Type*: must have the value "Subsidy"
- Start amount: the initial amount of the subsidy granted in units of the site's default currency
- Max value: the maximum amount for the privilege value

7.1.6.3 Penalty

A penalty 'privilege' adds a percentage to the price of products when used.

The privilege value (#) of a penalty privilege is a counter that controls how many times the penalty will be given. When the value is depleted (down to zero), the penalty no longer applies. The transparency flag now controls whether the product may still be purchased without this privilege (from the card/ID balance or with another privilege).

Because the order in which privileges have to be used is well defined, a penalty privilege cannot be circumvented until the privilege counter is depleted (the field "Transparent" must then be checked).

The fields of a penalty privilege are listed below. The fields marked * must always be assigned a value.

- Type*: must have the value "Penalty"
- Penalty (%): the percentage of the product price that is added to the default price of the product
- Start value: the initial value of the privilege counter. To define a penalty that will always be applied, enter 65535 for always.
- Max value: the maximum value (number of times) for the privilege counter

7.1.6.4 Reduction

A reduction privilege gives a fixed reduction (a fixed amount in the site's currency) off the sales price of the product. If the reduction amount exceeds the price of the product, the product is rendered free of charge.

The privilege value (#) of a reduction privilege is a counter that controls how many times the reduction will be given. When the value is depleted (down to zero), the reduction no longer applies. The transparency flag now controls whether the product may still be purchased without this privilege (from the card/ID balance or with another privilege).

The fields of a reduction privilege are listed below. The fields marked * must always be assigned a value.

- Type*: must have the value "Reduction"
- Reduction*: the amount of reduction in units of the site's default currency
- Start value: the initial value of the privilege counter. To grant the privilege without limit, enter 65535 for always.
- Max value: the maximum value (number of times) for the privilege counter

7.1.6.5 Price table

A price table privilege allows the user to pay a different amount for a product, as specified in the selected price table (see §6.4).

The value of the price table privilege is the number of times this price table may be used.

7.1.6.6 Service

A service privilege allows the user to use service functions of selected terminals. One such service function allows a logistics user, i.e. a person that services and restocks terminals, to confirm a picklist when at the terminal.

7.1.6.7 Terminal access (not yet implemented in this version)

One may want certain terminals only to be accessible to certain users (e.g. printers outside the staff room for teaching staff only). This requires the parameter "Need privilege to use terminal" of those terminals to be set to "On" (see §**Error! Reference source not found.**).

Terminal access privileges must be defined for those terminals and assigned to the users who may use the terminals. Access to the terminals is blocked to users without a privilege for those terminals.

At present the privilege type "Terminal access" has not yet been implemented. To create a privilege that achieves the same as a terminal access privilege, one must create a privilege of type "Discount" with 0% discount, check the field "For terminal access" of the privilege and add the terminals to which the privilege must grant access to the sections "Terminals" and/or "Terminal groups".

7.1.7 Products

A privilege is typically limited to specific products and/or product groups.

Only after a privilege has been saved with the basic data, the data entry areas "Products" and "Product groups" become visible on the screen. Select the product groups and/or individual products that this privilege pertains to.

Not selecting any products or product groups will render the privilege useless (unless it is a price table, service or access privilege).

7.1.8 Terminals

A privilege may also be restricted to particular terminal groups and/or terminals.

Only after a privilege has been saved with the basic data, the data entry areas "Terminal" and "Terminal groups" become visible on the screen. Select the terminal groups and/or individual terminals that this privilege pertains to.

For a service privilege select the terminal groups and/or individual terminals that may be serviced by users with this privilege.

For a terminal access privilege select the terminal groups and/or individual terminals that may be accessed by users with this privilege. These terminals will be blocked to users who do not have an access privilege for the terminals (see §7.1.6.7).

For all other privileges, select the terminal groups and/or individual terminals that this privilege pertains to. The privilege will only apply to products in those terminals.

7.1.9 Understanding privilege order

When determining which privilege to use for a particular product in a particular terminal, the privileges are checked in a well-defined order. This order is controlled in the privilege list page by clicking the "Sort" button. The top-most privilege will apply first and the bottom privilege will apply last.

When multiple privileges could apply to the same transaction, simple payment terminals will merely choose the privilege with the highest priority (the highest on the sort list). Some terminals with sufficient hardware capacity may prompt the user to select the privilege they would like to use for the transaction.

7.1.10 Terminal configuration

Modifying privileges or the order in which privileges apply requires an update of the terminal configurations of all terminals which are affected by by the change.

NOTE: When privileges are created, modified or deleted, and when the order of priority of the privileges is changed, FP5 will queue an automatic update to affected terminals. A banner at the top of the screen will indicate when this update will occur.

7.2 CREATING, UPDATING, DELETING AND ASSIGNING PRIVILEGES

7.2.1 Creating a privilege

Permissions required: Privilege | Retrieve, Privilege | Create

To create a new privilege:

1. Select the "Privileges" option from the "Products" menu.
2. Click the "Create" button.
3. Enter the privilege name in the site languages and a description of the privilege in the appropriate fields.
4. Choose a type of privilege. Refer to § 7.1.6 for a description of different privilege types. Depending on the type of privilege selected, different fields will show.
5. Enter the details for the new privilege in the appropriate fields.
6. To limit the times the privilege is valid, choose a value from the drop-down list in the field "Validity timetable". Refer to §6.3 for a description of timetables.
7. To only enable the privilege after a particular date, enter a value in the field "Start date". The privilege cannot be used before this date.
8. To only enable the privilege until a particular date, enter a value in the field "End date". The privilege cannot be used after this date.
9. Check the "For terminal access" box if this privilege should also give access to restricted terminals. Restricted terminals are terminals that require a privilege (see §7.1.6.7). Normal terminals, or non-restricted terminals, can handle privileges, but can also be used by users without privileges.
10. Check the "Transparent" box if this privilege is not required to obtain the products it applies to. If a transparent privilege is depleted, the products may still be obtained without applying the privilege.
11. To have the privilege value increase periodically:
    a. Check the "Enable auto top-up" box.
    b. Enter an amount in the field "Auto top-up". If an auto top-up would cause the privilege counter to increase above the maximum value, the increase is lessened and the privilege counter is set to the maximum value.
    c. In the "Auto top-up period" section, select a period (daily, weekly, monthly or yearly) or to use a custom period, select the "Timetable" option.
    d. Enter the time, day and/or date when the value of the privilege counter should increase in the selected period. Or, if you have chosen the "Timetable" option in the previous step, choose a value from the drop-down list in the field "Timetable" which shows the timetables that have been defined in FP5 (see §6.3). This timetable will be uses for the auto top-ups (top-ups will occur at the start of each interval in the timetable).
12. Click the "Save" button to create the privilege. The "Product groups", "Products", "Terminal groups" and "Terminals" sections become visible.
13. If the privilege will apply to particular product groups and/or individual products (most privileges will), select those product groups and products. For each product group/product:
    a. Click the "Add" button in the "Product groups"/"Products" section.
    b. Choose the product group/product from the drop-down list.
    c. Click the "Add" button.
14. If the privilege will be restricted to particular terminal groups and/or individual terminals, select the terminal groups and terminals the privilege applies to. For each terminal group/terminal:
    a. Click the "Add" button in the "Terminal groups"/"Terminals" section.
    b. Choose the terminal group/ terminal from the drop-down list.
    c. Click the "Add" button.
15. Click the "Apply" button to save the changes.

Creating a privilege will require terminals that have any of the targeted products to be reconfigured. A banner at the top of the screen will indicate when this update will occur.

☞ Note: the field "Factor" is obsolete and should not be used. It will be removed from future versions.

7.2.2 Updating a privilege

Permissions required: Privilege | Retrieve, Privilege | Update

To update a privilege:

1. Select the "Privileges" option from the "Products" menu.
2. Click the name of the privilege to edit.
3. Refer to §7.1.1 through §7.1.9 and §7.2.1 for information about the fields to edit.
4. Click the "Apply" button to save the changes.

Updating a privilege will require terminals that have one of the targeted products to be reconfigured. A banner at the top of the screen will indicate when this update will occur.

7.2.3 Assigning a privilege to a user group

Permissions required: User group | Retrieve, User group | Update, Privilege | Retrieve

A privilege can be assigned to multiple user groups.

To assign the privilege to a user group:

1. Select the "User groups" option from the "Cards/IDs" menu.
2. Click the name of the user group to assign the privilege to.
3. For each privilege you wish to assign to this user group:
   a. In the "Privileges" section, click the "Add" button.
   b. Choose the privilege to assign from the drop-down list.
   c. Click the "Add" button to add the privilege to the list of assigned privileges.
4. Click the "Apply" button to save the changes.

☞ When a privilege is assigned to a user group, FP5 will queue an automatic update to all cards/IDs assigned to users that are a member of this The cards/IDs will be updated the next time they are presented at an online terminal. user group.When a privilege is given to (the user of the) card/ID, it will initially receive the value of the field "Start value".

7.2.4 Removing a privilege from a user group

Permissions required: User group | Retrieve, User group | Update, Privilege | Retrieve

A privilege can be removed from a user group.

To remove a privilege from a user group:

1. Select the "User groups" from the "Cards/IDs" menu.
2. Click the name of the user group to remove the privilege from.
3. For each privilege you wish to remove from this user group:
   a. In the "Privileges" section, click the "Delete" link to the right of the privilege.
4. Click the "Apply" button to save the changes.

☞ When a privilege is removed from a user group, FP5 will queue an automatic update to all cards/IDs assigned to users that are a member of this user group. The cards/IDs will be updated the next time they are presented at an online terminal. When a privilege is removed from a card/ID, it will lose its remaining value.

7.2.5   Assigning a privilege to an individual user

Permissions required: User | Retrieve, User | Update, Privilege | Retrieve

A privilege can also be assigned to an individual user.

To assign a privilege to an individual user:
1. Select the "Users" option from the "Cards/IDs" menu.
2. Search the user (see §2.3.1) and click the name.
3. For each privilege you wish to assign (see note below):
    a. In the "Privileges" section, click the "Add" button.
    b. Choose the privilege to assign from the drop-down list.
    c. Click the "Add" button to add the privilege to the list of assigned privileges.
4. Click the "Apply" button to save the changes.

☞ A user can receive privileges through user group membership and through privileges assigned individually. On the user detail screen you see only the individually assigned privileges. To view all privileges currently assigned to a user click the "Show privileges" button. The "User's privileges" screen shows all privileges assigned to the user (and how each privilege was assigned).

☞ When a privilege is assigned to a user, FP5 will queue an automatic update to all cards/IDs assigned to that user. The cards/IDs will be updated the next time they are presented at an online terminal. When a privilege is given to (the user of the) card/ID, it will initially receive the value of the field "Start value".

7.2.6   Removing a privilege from an individual user

Permissions required: User | Retrieve, User | Update, Privilege | Retrieve

To remove a privilege from an individual user:
1. Select the "Users" option from the "Cards/IDs" menu.
2. Search the user (see §2.3.1) and click the name.
3. For each privilege you wish to remove from this user (see note below):
    a. In the "Privileges" section, click the "Delete" link to the right of the privilege.
4. Click the "Apply" button to save the changes.

☞ A user can receive privileges through user group membership and through privileges assigned individually. On the user detail screen you see only the individually assigned privileges. To view all privileges currently assigned to a user click the "Show privileges" button. The "User's privileges" screen shows all privileges assigned to the user (and how each privilege was assigned).

☞ When a privilege is removed from a user will queue an update to all cards/IDs assigned to that user. The cards/IDs will be updated the next time they are presented at an online terminal. When a privilege is removed from a card/ID, it will lose its remaining value.

8 CARDS/IDS AND USERS

8.1 USER GROUPS

Users are grouped in user groups, and privileges may be assigned to a whole user group at once. All the users within this user group will receive the privilege.

The fields of the user group detail screen are listed below. The fields marked * must be assigned a value:

1) Name*
2) External ID: this field can be used to couple user groups to IDs used by an external system for reference purposes
3) Default cost centre: the cost centre that will be registered with the transactions carried out by users of this user group against privileges assigned to this user group
4) Validity period (from): before this date, terminals will not apply privileges that have been assigned through this user group and will not even accept cards/IDs belonging to this user group unless they also belong to another user group for which they are valid
5) Validity period (until): after this date, terminals will not apply privileges that have been assigned through this user group and will not even accept cards/IDs belonging to this user group unless they also belong to another user group for which they are valid
6) Validity (in years): (default value 10)
7) Purse configuration: Here you can choose between the purse configurations that have been defined in FP5 (see §8.2). A purse configuration allows you to define the maximum balance, the start balance and an incurring balance increase for all cards/IDs belonging to this user group.
8) Privileges: shows which privileges have been assigned to the user group. Privileges can be added and deleted.

8.1.1 Creating a user group

Permissions required: User group | Retrieve, User group | Create

To create a user group:

1. Select the "User groups" option from the "Cards/IDs" menu.
2. Click the "Create" button.
3. Enter the details for this new user group in the appropriate fields.
4. If you want to assign privileges to this user group, for each privilege:
    a. In the "Privileges" section, click the "Add" button.
    b. Select the privilege to add from the drop-down list.
    a. Click the "Add" button to add the privilege to the list of assigned privileges.
5. To delete a privilege from the user group click the "Delete" link to the right of the privilege.
6. Click the "Apply" button to create the user group.

8.1.2 Updating a user group

Permissions required: User group | Retrieve, User group | Update

To update a user group:

1. Select the "User groups" option from the "Cards/IDs" menu.
2. Click the name of the user group.
3. Edit the fields you wish to update.

---

4. To assign extra privileges to this user group, for each privilege:
   a. In the "Privileges" section, click the "Add" button.
   b. Select the privilege to add from the drop-down list.
   c. Click the "Add" button to add the privilege to the list of assigned privileges.
5. To remove a privilege from the user group click the "Delete" link to the right of the privilege. The privilege will be removed from all cards/IDs held by users of this user group.
6. Click the "Apply" button to save the changes.

☞ If the privileges assigned to a user group have changed, FP5 will queue an automatic update to all cards/IDs held by users that are a member of this user group. The cards/IDs will be updated the next time they are presented at an online terminal. A privilege that has been assigned is valid with immediate effect. A privilege that the user previously had by virtue of belonging to the user group, but that has been removed, is then no longer valid with immediate effect.

8.1.3   Deleting a user group

Permissions required: User group | Retrieve, User group | Delete

A user group can be deleted, even if there are users that belong to the user group.

To delete a user group:

1. Select the "User groups" option from the "Cards/IDs" menu.
2. Click the trash can icon 🗑 to the right of the user group. A pop-up screen will prompt for confirmation.
3. Confirm deletion.

The privileges assigned to the user group will be removed from all cards/IDs held by users that are a member of this group. The cards/IDs will be updated the next time they are presented at an online terminal. Any privileges that the user previously had by virtue of belonging to the user group, are no longer valid with immediate effect.

8.2   PURSE CONFIGURATIONS

Purse configurations enable you to determine the maximum balance, the start balance and a recurring balance increase for all cards/IDs of a user group. If you create a purse configuration you can then assign this purse configuration to one or several user groups by selecting it in the field "Purse configuration" of the user group (see §8.1.1).

The fields of the purse configuration detail screen are listed below. The fields marked * must be assigned a value:

1) Name*
2) External ID
3) Start balance: the amount that will be the balance when a card/ID is first created within a user group that has this purse configuration.
4) Icon image: you can select a jpg or png file that will be shown to represent this purse configuration.
5) Recurring balance increase: this is a check field. When checked a number of fields will show which you can use to define recurring balance increase for all cards/IDs that belong to a user group that has this purse configuration:
   a. Increase type: "Replace" = when the balance increase is executed the balance will be replaced with the amount you enter in the next step irrespective of the current balance. "Adjust" will add the amount you enter in the next step to the balance. If the adjust value is negative, the balance will be decremented with that amount. The balance will not go below 0 and will not exceed the maximum balance set for this card/ID.

    b.   Amount: the amount with which to replace or adjust the balance.

    c.   Frequency: select a period (daily, weekly, monthly, yearly) or to use a custom period, select the "Timetable" option.

    d.   Enter the time, day and/or date when the value should increase in the selected period or, if you have chosen the "Timetable" option in the previous step, specify a timetable you have created (see §6.3) to use for the increases (the increase will occur at the start of each interval in the timetable).

8.2.1 Creating a purse configuration

Permissions required: Purse configuration | Retrieve, Purse configuration | Create

To create a purse configuration:

1. Select the "Purse configurations" option from the "Cards/IDs" menu.
2. Click the "Create" button.
3. Enter the details for this purse configuration in the appropriate fields.
4. Click the "Save" button to create the purse configuration.

8.2.2 Updating a purse configuration

Permissions required: Purse configuration | Retrieve, Purse configuration | Update

To update a purse configuration:

1. Select the "Purse configurations" option from the "Cards/IDs" menu.
2. Click the name of the purse configuration.
3. Edit the fields you wish to update.
4. Click the "Apply" button.

8.2.3 Deleting a purse configuration

Permissions required: Purse configuration | Retrieve, Purse configuration | Delete

A purse configuration cannot be deleted if it is in use by a user group.

To delete a purse configuration:

1. Select the "Purse configurations" option from the "Cards/IDs" menu.
2. Click the trash can icon to the right of the purse configuration. A pop-up screen will prompt for confirmation.
3. Confirm deletion.

8.3 CARD/ID CONFIGURATIONS

A card/ID configurations determines which type of card/ID is used (e.g. Mifare Classic or DESfire) and whether the balance of the card/ID and the value assigned through privileges is stored online or on the card/ID (off-line).

Multiple card/ID types can be used on site, but then require separate card/ID configurations.

The fields of the card/ID configuration detail screen are listed below. The fields marked * must be assigned a value:

1) Name*
2) External ID

3) Status: this is a read-only field. Until a card/ID configuration is activated it will have the status "Editing" and cannot be selected as the card/ID configuration for cards/IDs. Once it has been activated it has the status "Active". Once activated it can be given the status "Expired" and then can again not be selected as the card/ID configuration for cards/IDs.

4) Chip type*: you can select a card/ID type from a drop-down list, e.g. Mifare Classic or DESfire

5) Payment/identification type: you can select a value from a drop-down list. The values have the following meanings:
   a. Online with UID only: all value (balance and privileges) is stored online in a FacilityPro account and ID is through the UID
   b. Online with image and UID: all value (balance and privileges) is stored online in a FacilityPro account and ID is through the UID and the FacilityPro card/ID number
   c. Off-line: all value (balance and privileges) is stored on the card/ID
   d. Combined (on/off-line): value (balance and privileges) is stored partly online in a FacilityPro account and partly on the card/ID and ID is through the FacilityPro card/ID number. NB: this payment/identification type is not yet available.

6) Key set version*: the key set version that was used to create the payment master keys used in the terminals (not shown if "Online with UID only" is chosen as /identification type).

7) Generate activation codes: If this check box is checked, FP5 will generate a random activation code for each card/ID produced with this card/ID configuration. The user needs the activation code to be able to use the FacilityPro user portal. The card/ID producer will receive the activation code and send it to the user. When the user logs in to the user portal he can activate his card/ID with the activation code and then see his transaction history and reload his card/ID through the user portal.
   a. Activation code length: this determines the number of characters for the activation code.
   b. Activation code characters: enter all the characters that may be used to generate the activation code.

8) Icon image: you can select a jpg or png file that will be shown to represent this card/ID configuration.

8.3.1 Creating a card/ID configuration

Permissions required: Card/ID configuration | Retrieve, Card/ID configuration | Create

To create a card/ID configuration:
1. Select the "Card/ID configurations" option from the "Cards/IDs" menu.
2. Click the "Create" button.
3. Enter the details for this Card/ID configuration in the appropriate fields.
4. Click the "Save" button to create the card/ID configuration.

8.3.2 Updating and/or activating a card/ID configuration

Permissions required: Card/ID configuration | Retrieve, Card/ID configuration | Update

To update and/or activate a card/ID configuration:
1. Select the "Card/ID configurations" option from the "Cards/IDs" menu.
2. Click the name of the Card/ID configuration.
3. Edit the fields you wish to update.
4. Click the "Apply" button or, if you want to activate the Card/ID configuration so that it can be selected as the Card/ID configuration for cards/IDs, click the "Activate" button and then the "Apply" button.

8.3.3 Changing the card/ID configuration to status "Expired"

Permissions required: Card/ID configuration | Retrieve, Card/ID configuration | Update

To change the status of a card/ID configuration to "Expired" so it can no longer be selected as the Card/ID configuration for cards/IDs:

1. Select the "Card/ID configurations" option from the "Cards/IDs" menu.
2. Click the name of the card/ID configuration.
3. Click the "Expire" button. This button will only be available if the status of the card/ID configuration is "Active". The status will change to "Expired".

8.3.4 Deleting a Card/ID configuration

Permissions required: Card/ID configuration | Retrieve, Card/ID configuration | Delete

To delete a card/ID configuration:

1. Select the "Card/ID configurations" option from the "Cards/IDs" menu.
2. Click the trash can icon to the right of the Card/ID configuration. A pop-up screen will prompt for confirmation.
3. Confirm deletion.

8.4 COST CENTRES

A cost centre is a bookkeeping account that can 'fund' the purchase of a product or can be used for generating turnover data per cost centre. When a purchase is carried out at a terminal the amount for this purchase might be wholly or partially funded by a cost centre, or simply booked against a cost centre for administrative purposes. This is the case if the user has been assigned a privilege which applies to the product purchased or if the user has been assigned a cost centre, in which case the applicable cost centre is saved as a part of the transaction data. Reports can be generated by FP5 for through-billing to each cost centre or to determine turnover data per cost centre, showing the amount funded through the privileges or booked against a cost centre. FP5 decides which cost centre should be registered with each transaction as follows:

1) If the transaction is granted on the basis of a specific privilege which has been assigned to a user group for which a default cost centre has been defined, the amount not paid from the balance of the card/ID is booked against that cost centre.
2) If the transaction is granted on the basis of a specific privilege which has been assigned to the user directly, and a cost centre has been specifically assigned to that user, the amount not paid from the balance of the card/ID is booked against that cost centre.
3) If the transaction is **not** granted on the basis of a specific privilege, and therefore the total amount is paid from the balance of the card/ID, and a cost centre has been specifically assigned to the user involved, the amount paid is booked against that cost centre.
4) If the transaction is **not** granted on the basis of a specific privilege (and therefore the total amount is paid from the balance of the card/ID), and **no** cost centre has been assigned to the user involved, **no** cost centre is saved with the transaction.

The fields of the cost centre detail screen are listed below. The fields marked * must be assigned a value:

1) Name*
2) External ID: this field can be used to couple cost centres to IDs used by an external system for reference purposes
3) Description

8.4.1 Creating a cost centre

Permissions required: Cost centre | Retrieve, Cost centre | Create

To create a new cost centre:
1. Select the "Cost centres" option from the "Cards/IDs" menu.
2. Click the "Create" button.
3. Enter the details for this cost centre in the appropriate fields.
4. Click the "Apply" button to create the cost centre.

8.4.2 Updating a cost centre

Permissions required: Cost centre | Retrieve, Cost centre | Update

To update a cost centre:
1. Select the "Cost centres" option from the "Cards/IDs" menu.
2. Click the name of the cost centre.
3. Edit the fields you wish to update.
4. Click the "Apply" button to save the changes.

8.4.3 Deleting a cost centre

Permissions required: Cost centre | Retrieve, Cost centre | Delete

A cost centre cannot be deleted if it is in use by user groups or users.

To delete a cost centre:
4. Select the "Cost centres" option from the "Cards/IDs" menu.
5. Click the trash can icon to the right of the cost centre. A pop-up screen will prompt for confirmation.
6. Confirm deletion.

8.5 USERS

A user's details are maintained by FP5.

Some installations will use FacilityPro merely as a cost registration system and use a 3rd party system to maintain their user database. In this case, not a lot of fields need to be entered, ultimately only an identifier is required so that FP5 can tell which cards/IDs are assigned to the same user.

In other installations, however, FacilityPro will be the database of record for user data. For each user FP5 can maintain basic address information as well as phone numbers, email addresses and social media links.

A user may be associated with multiple user groups at the same time, receiving all privileges associated with those user groups. The site's privilege order will determine in which precedence the merged privileges will be interpreted.

8.5.1 Importing users from a CSV-file

> Permissions required: User | Retrieve, User | Create, User | Update, User | Delete,
>
> Card/ID | Retrieve, Card/ID | Create, Card/ID | Update, Card/ID | Delete
>
> Which of these permissions are required depends on the intended result of the file import (see below)

New users and modifications to existing users may be imported from a text file in comma-separated values (CSV). In this way new users can be created, and existing users can be modified or deleted.

8.5.1.1 File format

The file should consist of an initial row with column headers, separated by commas, followed by one row per user or card/ID. Each row contains a number of values separated by commas. If the value is supposed to contain a comma it must be quoted using double quote (") characters.

Each column header specifies for which field the values in that column are. The following table specifies which column headers are understood by FP5, and whether they are mandatory (M), optional (O) or conditional (C) for each of the three opcodes: create (C), modify (M), and delete (D).

Table 10: User / Card/ID import fields

Column header	Data type	C	M	D	Description
opcode	enum	O	M	M	Possible values: "create", "modify", or "delete". When this field is absent a new user will be created. When this field is set to modify or delete one of the following "lookup_" fields is used to look up an existing user and perform the operation.
lookup_id	string(36)	-	C^1	C^1	Modify or delete existing user with this internal unique ID.
lookup_externalid	string(40)	-	C^1	C^1	Modify or delete existing user with this 3rd party ID in field "External ID". The external ID column itself may also be specified to change the external ID.
lookup_cardnumber	number(9)	-	C^1	C^1	Modify or delete existing user associated with the given card/ID number.
lookup_card_externalid	string(50)	-	C^1	C^1	Modify or delete existing user associated with the card/ID with the given external ID.
lookup_cardissuenumber	number(2)	-	C^2	C^2	Modify or delete existing user associated with the given card/ID issue number. If not present (and a lookup_cardnumber is present), the default of 1 will be used.
firstname	string(40)	O	O	O	First name of user
lastname	string(40)	M	O	O	Last name of user
Initials	string(10)	O	O	O	Initials of user
mailaddress	string(80)	O	O	O	Postal address of user
City	string(40)	O	O	O	City of user
State	string(40)	O	O	O	State of user
zipcode	string(20)	O	O	O	Zip code of user
countrycode	string(2)	O	O	O	ISO 3166 country code of user
mobilenumber	string(20)	O	O	O	Mobile phone number of user (needed for SMS functionality)
phonenumber	string(20)	O	O	O	Phone number of user
emailaddress	string(80)	O	O	O	Email address of user
externalid	string(40)	O	O	O	Arbitrary ID from 3rd party system
customergroup	string(50)	O	O	O	Name of the user group in the primary language of the site. If no user group exists with given name, a new user group will be created. The user will no longer belong to user groups he previously belonged to.
addcustomergroup	string(50)	O	O	-	Name of a user group to add to the user. If no group exists with given name, a new user group will be created.
removecustomergroup	string(50)	-	O	-	Name of a user group the user must no longer belong to.

Column header	Data type	C	M	D	Description
costcentre	string(50)	O	O	O	Name of the cost centre in the primary language of the site. If no cost centre exists with given name, a new cost centre will be created.
cardstate	Enum	O	O	-	Desired card/ID state for the card/ID assigned to this user. If not specified, the default value ToBeProduced is used. The card/ID state determines which of the following fields are mandatory. See Table 13 for a description.
cardnumber	number(9)	O	O	O	Card/ID number of card/ID to assign to this user. If a card/ID already exists with the given card/ID number and card/ID issue number, it will be assigned to this user. If the card/ID was assigned to another user, it will be removed from that user.
cardbalance	Decimal number	O	O	-	Adds an amount to the current balance of the card/ID. Decimal separator is always a "."
cardissuenumber	number(2)	C[3]	C[3]	C[3]	Card/ID issue number of card/ID to associate with this user.
cardtype	Enum	C	C	C	Type of card/ID that determined the UID. This field must be present for card/ID states other than "ToBeProduced". Possible values: DESFIRE, LEGIC, MIFARE, JCOP
carduid	hex(40)	C	C	C	UID of card/ID to associate with this user
addprivilege_externalid	string(50)	O	O	-	Assigns the privilege with this external ID of the user.
removeprivilege_externalid	string (50)	O	O	-	Removes the privilege with this external ID from the user.

To import users from a CSV-file:
1. Select the "Users" option from the "Cards/IDs" menu.
2. Click the "Import users…" button.
3. Click the "+ Choose" button. A standard Windows "Open" dialog screen will appear.
4. Select the file to import and click "Open". The file name is shown.
5. Click "Upload" to start importing. The progress bar will indicate the progress. If too many (more than 10%) records in the file cannot be interpreted, the whole import will fail without any records being imported. If over 90% of the imports are successful and less than 10% of the records fail, these failures will be individually reported and the others will be accepted into FP5.

8.5.1.2 Failure codes

The following table lists the validation errors that can occur during the import of user data.

---

[1] If opcode is modify or delete, one of these lookup fields must be specified.

[2] lookup_cardissuenumber number may only be present if lookup_cardnumber is present

[3] cardissuenumber number may only be present if cardnumber is present

Error code	Description
{cardService.duplicateCardIssueNumber}	?
{cardService.duplicateValue}	Value specified violates a uniqueness constraint
{cardService.invalidState}	The requested state is not supported by FP5
{cardService.invalidStateChange}	The current state of the Card/ID cannot be changed to the requested state.
{global.duplicateExternalId}	External ID specified already exists for this site
{global.notNull}	Missing mandatory field
{global.uidNotUnique}	UID specified for a card/ID already exists for this site

8.5.2 Creating a user

Permissions required: User | Retrieve, User | Create

To create a new user:

1. Select the "Users" option from the "Cards/IDs" menu.
2. Click the "Create" button.
3. Enter the details for this new user in the appropriate fields. At this point only the last name is a mandatory field, but entering an email address is advised if reservation or report notification emails are to be sent.
4. If you want the user to belong to one or several user groups:
    a. Click the "Add" button in the "User groups" section.
    b. Select a user group from the drop-down list.
    c. Click the "Add" button.
    d. Repeat the previous three steps to add another user group.
5. If you want to assign privileges to this user on an individual basis:
    a. Click the "Add" button in the "Privileges" section.
    b. Select a privilege from the drop-down list.
    c. Click the "Add" button.
    d. Repeat the previous three steps to add another privilege.
6. Click the "Save" button to create the user.

At this stage, no cards/IDs are assigned to the user.

8.5.3 Updating a user's details

Permissions required: User | Retrieve, User | Update

To update a user:

1. Select the "Users" option from the "Cards/IDs" menu.
2. Search the user (see §2.3.1) and click the name.
3. Edit the fields you wish to update.
4. Click the "Apply" button to save the changes.

8.5.4 Setting or changing a user's password

Permissions required: User	Retrieve, User	Update

To use the FP5 user portal a user must have a password. If the user's password has never been set, i.e. the user does not have a password, you will see the text "No password set" above the "Set pwd…" button on the user detail screen. Otherwise you will see the text "Password set".

To set (or change) a user's password:

You will determine the password for the user. You must ensure that the user is informed what this password is.

1. Select the "Users" option from the "Card/IDs" menu.
2. Search the user (see §2.3.1) and click the name.
3. On the user detail screen, click the "Set pwd" button.
4. Enter the desired password.
5. Click "Set".
6. Click the "Apply" button to save the changes.

The user can log into the user portal with the password.

To have FP5 generate a new password and send it to the user:

In order to use this functionality, an email template must exist of type "User password reset" and/or "User password reset SMS" respectively (see §5.4).

1. Select the "Users" option from the "Card/IDs" menu.
2. Search the user (see §2.3.1) and click the name.
3. On the user detail screen, click the "Reset password" button if you want the password to be sent to the user via e-mail, or click the "Reset password (SMS)" button if you want the password to be sent to the user via SMS. The status shown above the password buttons will change to "Reset will be sent".

The user can log into the user portal with the password, but is required to change this password upon first login.

8.6 CARDS/IDS

Cards and IDs can be created without being assigned to a user (yet). FP5 maintains a record of each card/ID separately from the user. During the life of a card/ID it may be assigned to different users, but only with one particular user at any given point in time.

A user can hold multiple cards and/or IDs at the same time. Each of these cards and IDs will receive all the privileges assigned directly to the user or to any of the user groups the user belongs to.

A card/ID has a card/ID number, which is effectively the account number of the user. When multiple cards/IDs exist with the same card/ID number they are distinguished by different card/ID issue numbers.

A card/ID that has been issued usually has a chip with a unique ID. This chip UID can also be used by FP5 to uniquely identify a card/ID.

The fields of the card/ID detail screen are listed below. The fields marked * must always be assigned a value. Some fields become mandatory depending on the card/ID state (see § 8.6.1):

1) External ID: this field can be used to couple cards/IDs to IDs used by an external system for reference purposes
2) Card/ID number
3) Card/ID issue number
4) Card/ID state (see § 8.6.1)
5) Card/ID confuguration
6) UID*
7) Activation code
8) User

8.6.1 Card/ID states

FP5 tracks the state of each individual card/ID. Cards/IDs may be registered in FP5 before they are assigned to a user (i.e. personalised).

The following table lists the states supported by FP5.

Table 12: Card/ID states

Card/ID state	Description
Initialised	Card/ID is not assigned to a user and is in stock with initial production keys
PrePersonalised	Card/ID is not assigned to a user but applications/security domains have been installed with site specific card/ID keys
ToBeProduced	Card/ID is assigned to a user and should be produced by the manufacturer.
InProduction	The production system has requested application data to be prepared and is currently producing the card/ID. This state prevents other systems from attempting to produce the card/ID at the same time.
Personalised	Card/ID has been produced but may not have been assigned to a user or received by the associated user yet.
Issued	Card/ID has been handed to the user but may need to be activated before it can be used
Active	Card/ID has been activated and transactions can be performed with the card/ID
Transaction lock	A transaction is being executed with this card/ID
Blocked	Card/ID has temporarily been blocked, no transactions can be performed with the card/ID
Withdrawn	Card/ID has been permanently blocked and should be returned to the site administrator. The user association is maintained to allow any remaining balance to be finalised should the card/ID be presented.
Returned	Card/ID has been handed in after having been withdrawn and can either be destroyed or reissued to another user. The relation with the previous user is removed by FP5.
ProductionFailed	Indicates an attempt was made to produce this card/ID, but failed. The card/ID should be destroyed.

The following table lists the possible card/ID fields and their presence depending on the state of the card/ID.

Table 13: Card/ID field presence depending on card/ID state

Card/ID state	Card/ID type	UID	Card/ID number	Card/ID issue number	User
Initialised	M	O	-	-	-
PrePersonalised	M	O	M(G)	M(G)	-
ToBeProduced	-	-	M(G)	M(G)	O
InProduction	-	-	M	M	O
Personalised	M	O	M(G)	M(G)	O
Issued	M	O	M	M	M
Active	M	O	M	M	M
Blocked	M	O	M	M	M
Withdrawn	-	-	M	M	M
Returned	-	-	M	M	-

M indicates a mandatory field, O is an optional field. M(G) indicates a field for which FP5 generates a value if none is provided.

The following figure describes the card/ID states and which transitions are allowed by FP5.
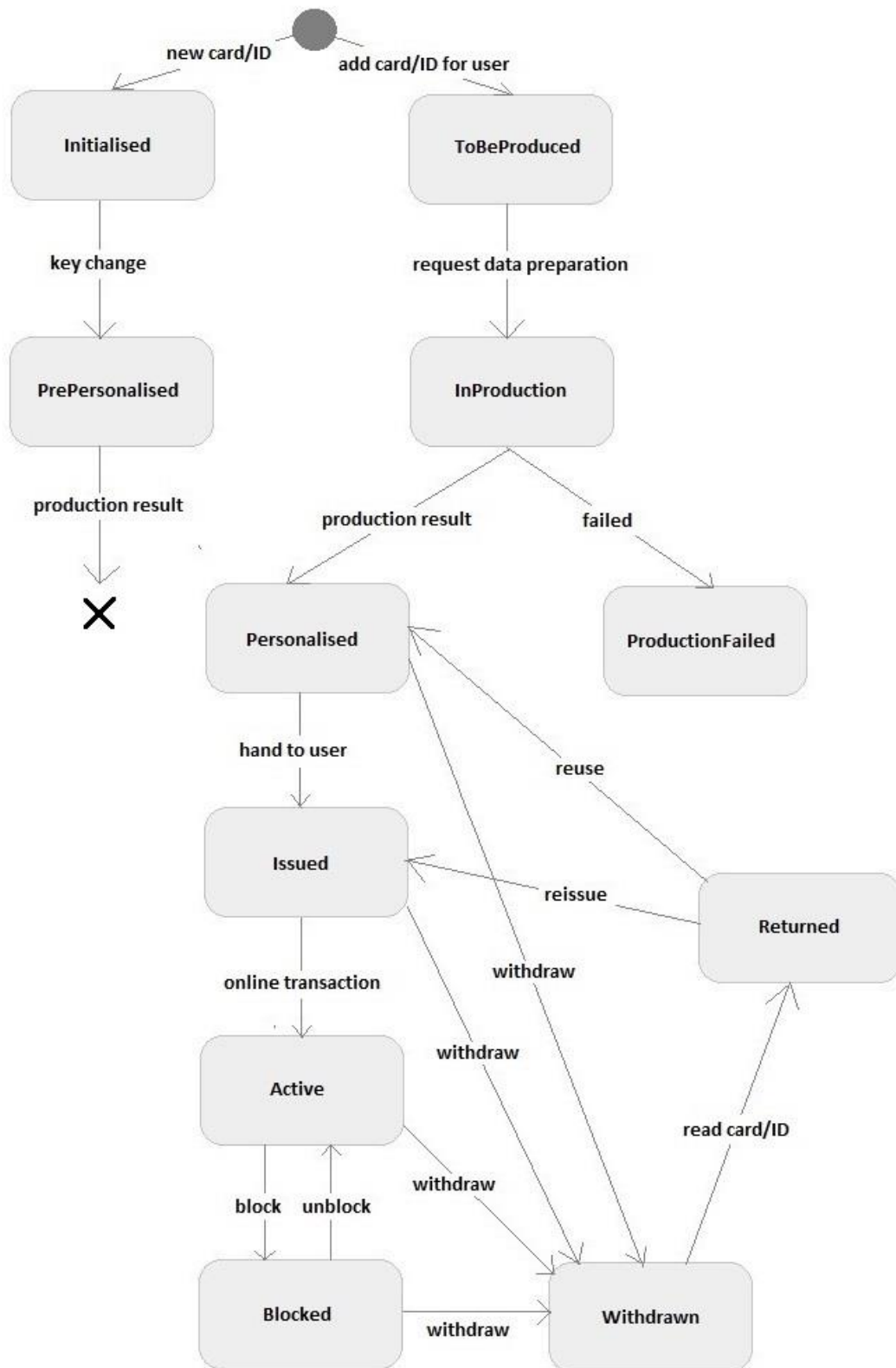
Figure 8-1: Card/ID state transitions

8.6.2 Creating a card/ID

Permissions required: Card/ID | Retrieve, Card/ID | Create

To create a new card/ID:
1. Select the "Cards/IDs" option from the "Cards/IDs" menu.
2. Click the "Create" button.
3. Enter a unique card/ID number and issue number combination, and the configuration and UID of the chip of this card/ID in the appropriate fields.
4. To assign the card/ID to a user at this time, select a user by entering (part of) the last name of an existing user.
5. Click the "Save" button to create the card/ID.

8.6.3 Assigning a card/ID to a user

Permissions required: User | Retrieve, User | Update, Card/ID | Retrieve

To assign a card/ID to a user:
1. Select the "Users" option from the "Cards/IDs" menu.
2. Search the user (see §2.3.1) and click the name.
3. In the "User's cards/IDs" section, click the "Assign" button.
4. Select an unassigned card/ID.
5. Click the "Save" button.

The card/ID will receive all the privileges assigned directly to the user or to any of the user groups the user belongs to. The privilege counters will be set to the start values of the privileges. The balance of the card/ID will be set to the highest start balance of any of the associated user groups. The next time this card/ID is presented at an online terminal it will be initialised.

8.6.4 Removing a card/ID from a user

Permissions required: User | Retrieve, User | Update, Card/ID | Retrieve

To remove a card/ID from a user:
1. Select the "Users" option from the "Cards/IDs" menu.
2. Search the user (see §2.3.1) and click the name.
3. In the "User's cards/IDs" section, click the trash can icon 🗑 to the right of the card/ID to be removed from the user.

8.6.5 Blocking a card/ID

Permissions required: Card/ID | Retrieve, Card/ID | Update

Blocking a card/ID is an example of a post-issuance update. The card/ID has been issued, and one wants the card/ID to be updated, in this case blocked, when it is next presented at an online terminal.

To block a card/ID:
1. Go to the card/ID detail screen of the card/ID you want to block. To get there, either
   a. Select the "Users" option from the "Cards/IDs" menu.
   b. Search the user (see §2.3.1) and click the name.

c. Click the card/ID number from the "User's cards/IDs" section.

or

a. Select the "Cards/IDs" option from the "Cards/IDs" menu.
b. Search for a card/ID by Card/ID number, UID or User name (see §2.3.1).
c. Click the card/ID number.

2. Change the field "Card/ID state" to value "Blocked".
3. Click the "Apply" button to save the changes.

8.6.6   Replacing a card/ID

At this time, there is no separate function in FP5 to replace a card/ID. To replace a card/ID with a new one, assign the new card/ID (§8.6.3) and remove the old card/ID (§8.6.4).

8.6.7   Performing post-issuance updates to a card/ID

Permissions required: Card/ID | Retrieve, Card/ID | Update

Any change to a card/ID after it has been issued is a post-issuance update. The change to the card/ID is entered in FP5 and the card/ID will be updated when it is next presented at a terminal.

Changes to the Card/ID state, such as blocking the card/ID, are done from the Card/ID detail screen.

Changing which privileges the user associated with the card/ID is entitled to is done from the user detail screen for individually assigned privileges (see §7.2.5 and §7.2.6) and from the user group detail screen for other privileges (see §7.2.3 and §7.2.4). As long as such changes are pending they can be seen in the "Card/ID update" section of a card/ID.

To change to the value of the card/ID balance or the privilege counters or change the start and/or end date:

1. Go to the card/ID detail screen of the card/ID you want to update. To get there, either
    a. Select the "Users" option from the "Cards/IDs" menu.
    b. Search the user (see §2.3.1) and click the name.
    c. Click the card/ID number from the "User's cards/IDs" section.

   or

    d. Select the "Cards/IDs" option from the "Cards/IDs" menu.
    e. Search for a card/ID by Card/ID number, UID or User name (see §2.3.1).
    f. Click the card/ID number.

   On the card/ID detail screen, the field "Card/ID status" shows the last known status of the card/ID. The "Card/ID update" section shows the current start date, end date, PIN code and balance of the card/ID. If a manual update is scheduled, the "Requested time" shows the time the update was requested. If an update was queued because of changes to privileges, user groups or user group membership, then no requested time is shown.

4. To change the start date and/or end date:
    a. Click the "Edit" button next to the field you wish to edit.
    b. Select the desired new date value.
    c. Click the "Save" button.

5. To change the PIN code:
    a. Click the "Edit" button next to the field "Current PIN code".
    b. Enter the new PIN code.
    c. Click the "Save" button.

6. To clear the PIN code:
    a. Click the "Edit" button next to the field "Current PIN code".
    b. Click the "Reset PIN code" button.

7. To change the balance:
    a. Click the "Edit" button next to the field "Current balance".

b. Select the balance update type: "Replace" = the balance will be replaced with the amount you enter in the next step when the update is executed irrespective of the current balance. "Adjust" will add the amount you enter in the next step to the balance. If the adjust value is negative, the balance will be decremented with that amount. The balance will not go below 0 and will not exceed the maximum balance set for this card/ID.

c. Enter the amount.

d. Click the "Save" button.

The "Privileges" table shows the privileges assigned to the user to which this card/ID is assigned. Each privilege shows the current value of the privilege counter and the date of next recurring increase (if applicable). If an update to the privilege and/or the value of the privilege counter is pending, the update type shows the type of update. The table below shows the possible update types.

8. To adjust the value of a privilege counter:

a. Click the "Edit" link to the right of the privilege.

b. Select either "Replace" or "Adjust" from the update type drop-down. "Replace" = the privilege counter will be replaced with the amount you enter in the next step when the update is executed. "Adjust" will add the amount you enter in the next step to the privilege counter.

c. Enter a value in the field "Update amount".

d. Click the "Save" button.

e. Click the "Apply" button to queue the update. The update will be executed the next time the card/ID is presented at an online terminal.

Table 14: Balance/privilege update types

Update type	Description
New	The privilege was assigned (either through a user group the user of this card/ID belongs to or to this user directly) and the privilege counter will be set to the start value.
Replace	The privilege counter will be replaced with the new value shown.
Adjust	The privilege counter will be increased with the value shown. If a negative value is shown, the privilege counter will be decremented.
Remove	The privilege was removed (either from the user group through which the holder of this card/ID had been assigned this privilege or from this user directly).

9 TERMINALS

The terminal detail screen has multiple tabs showing different aspects of a terminal's configuration. When a terminal is first created the details on the tab "General" can be entered and the terminal must then be saved before the other tabs can be opened and edited.

The fields of the tab "General" of the terminal detail screen are listed below. The fields marked * must be assigned a value:

1) Name*
2) External ID: this field can be used to couple terminals to IDs used by an external system for reference purposes
3) Description
4) Last know config status: (read-only) shows the last known status of the terminal, which is one of the following:
   a. Unknown
   b. Firmware will be updated

c. Updating firmware...
d. New configuration will be sent
e. Configuring...
f. Configuration has been received
g. Configuration error
h. Terminal data will be collected
i. Terminal data will be collected before firmware update
j. Collecting terminal data...
k. Collecting terminal data before firmware update...
l. Almost ready
m. Terminal OK (Ready)

NB: To the right of the field "Availability" the date and time of the last known config status are shown.

5) Availability: (read-only) shows the current status of the terminal, which is one of the following:
a. Not known: current terminal status could not be determined
b. Off-line: terminal has not been online in the last 2 minutes
c. Online (polling): terminal is online en communicating with FP5 (polling the server) at regular intervals

To the right of the field "Availability" the date and time of the last known config status are shown.

6) Address
7) Machine serial no.
8) Connection type: one of the following: HTTP, HTTPS, TCP, UDP, SAMBA
9) Time zone

9.1 CREATING A TERMINAL – THE TAB "GENERAL"

Permissions required: Terminal | Retrieve, Terminal | Create

Before creating a terminal, ensure the correct site is selected. The terminal will be created within the current site and will only be visible within that site.

To create a new terminal:

1. Select the "Terminal groups" option from the "Terminals" menu.
2. Click the "Create terminal" button.
3. Enter a name for the new terminal in the site languages.
4. Click the "Create terminal" button. The terminal detail screen is opened.
5. Enter the details for this new terminal in the appropriate fields on the tab "General".
6. Click the "Save" button to create the terminal.

9.2 TERMINAL HARDWARE

The system distinguishes between the dispenser which is a machine that controls access to products and the terminal that is installed in or near the machine to connect it to the FacilityPro platform.

Each terminal has an associated main device that connects to the TMS (Terminal Management System) module of FP5. This main device is typically a Magnabox. In addition, peripheral devices may be connected. For each device the firmware version and status can be reported to FP5.

A terminal can be created in FP5 before the hardware has been installed or turned on. When hardware is installed (and when hardware is replaced), that hardware unit is associated with the terminal after which it will automatically receive the correct firmware and configuration.

In the current version of FP5, firmware is not automatically installed in hardware units. An operator must manually download firmware to the devices. Refer to the Magnabox installation and configuration manual for documentation on this procedure.
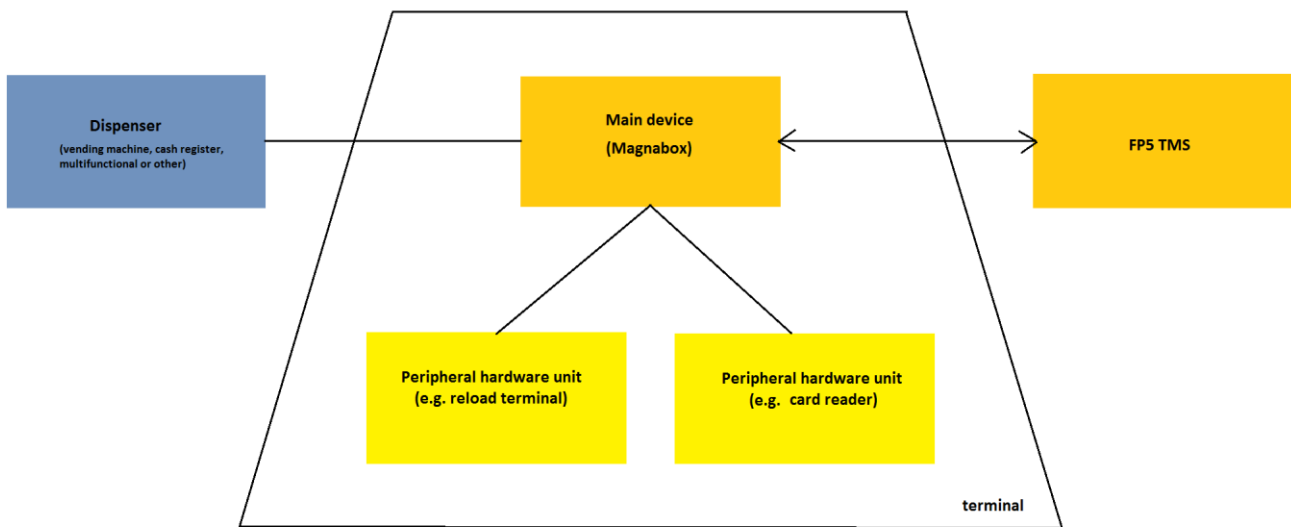
9.2.1 Preparing a Magnabox for connection to FP5

A Magnabox needs to be manually configured before it can connect to FP5. The configuration consists of the TMS URL (which is used to connect to the TMS module of FP5) as well as a certificate thumbprint for the SSL certificate used by the TMS server.

Refer to the Magnabox documentation on how to configure these settings.

The typical TMS URL is https://domain:port/.

When a Magnabox is correctly set up it will automatically attempt to connect to FP5. When an unknown Magnabox connects, FP5 adds the information of this Magnabox to the database and assigns the Magnabox to the system administration site. A system administrator can then assign the Magnabox to the specific site where it is actually installed. Once a Magnabox is assigned to a particular site, it can finally be assigned to the correct terminal by a site administrator.

9.2.2 Assigning a Magnabox to a site

Permissions required: Hardware unit | Retrieve, Hardware unit | Assign

To assign a Magnabox to a site:

1. Select the "Hardware units" option from the "Administration" menu. You are automatically connected to the system administration site (meta-site). A list of Magnaboxes is presented. If the Magnabox to be assigned is not in the list it may not have successfully connected to FP5 yet (see § 9.2.1 on how to configure a Magnabox to connect to FP5). For Magnaboxes that have already been assigned to a site, the column "Site" shows to which site they have been assigned and the "Release" link is available. Magnaboxes that are available to assign to a site have the system administration site (meta-site) in the column "Site" and an "Assign" link.
2. To assign a Magnabox click the "Assign" link to the right of the list entry for that Magnabox.
3. Select the site to assign the Magnabox to from the drop-down list.
4. Click the "Assign" button. The Magnabox is now shown as assigned to that site and can be selected for a terminal.

9.2.3 Releasing a Magnabox from a site

Permissions required: Hardware unit | Retrieve, Hardware unit | Release

You might want to release a Magnabox from a site, for instance because it is defect or (unlikely) so that it can be used for another site.

To release a Magnabox from a site:
1. If the Magnabox is coupled to a terminal (otherwise, go directly to the next step):
   a. Ensure the site the terminal belongs to is selected.
   b. Select the "Terminal groups" option from the "Terminals" menu.
   c. Click the name of the terminal in the "Terminals" section. If the list of terminals is too long you can select a terminal group first and then select a terminal.
   d. On the terminal detail screen, select the tab "Hardware".
   e. Click the "Revoke" button.
2. Select the "Hardware units" option from the "Administration" menu. You are automatically connected to the system administration site (meta-site). A list of Magnaboxes is presented. For Magnaboxes that have already been assigned, the column "Site" shows to which site they belong and the "Release" link is available.
3. To release the Magnabox click the "Release" link to the right of the list entry for that Magnabox. The Magnabox is now shown as available to be assigned. The system administration site (meta-site) is shown in the column "Site" and there is an "Assign" link available.

9.2.4 Associating a Magnabox with a terminal

Permissions required: Terminal | Retrieve, Terminal | Update, Hardware unit | Retrieve

After a terminal has been created, it has to be associated with a Magnabox. Ensure you have the correct serial number of the Magnabox installed for this terminal.

To associate a terminal with a Magnabox:
1. Ensure the site the terminal belongs to is selected.
2. Select the "Terminal groups" option from the "Terminals" menu.
3. Click the name of the terminal in the "Terminals" section. If the list of terminals is too long you can select a terminal group first and then select a terminal.
4. On the terminal detail screen, select the tab "Hardware". If the terminal does not already have a Magnabox associated, the "Select main device" section will show the available Magnaboxes for this terminal. If there are no available Magnaboxes, i.e. Magnaboxes that have been assigned to this site but not yet to a terminal, you will not see the "Select main device" section. If the terminal already has a Magnabox associated, it will be shown here with a "Revoke" link.
5. Associate a Magnabox from the list with the terminal by clicking the "Select" link to the right of the Magnabox with the correct serial number.

9.2.5 Associating a replacement Magnabox with a terminal

Permissions required: Terminal | Retrieve, Terminal | Update, Hardware unit | Retrieve

When a terminal is already associated with a Magnabox but this Magnabox has been replaced with another Magnabox, the new Magnabox needs to be associated.

To associate a replacement terminal with a Magnabox:
1. Select the "Terminal groups" option from the "Terminals" menu.

2. Click the name of the terminal in the "Terminals" section. If the list of terminals is too long you can select a terminal group first and then select a terminal.
3. On the terminal detail screen, select the tab "Hardware".
4. Since the terminal already has a Magnabox associated, click the "Revoke" button to disassociate the current Magnabox.
5. Associate the replacement Magnabox from the list by clicking the "Select" link to the right of the Magnabox with the correct serial number.

The disassociated Magnabox will remain assigned to the site.

9.3 APPLICATION CONFIGURATION

A terminal has an application type. This application type relates directly to the firmware loaded in the Magnabox. The application type is determined by the interface of a the vending machine, multifunctional, cash register or other dispenser as well as by the type of payment system provided. The application type of a terminal is determined when the terminal first connects to the TMS. The application configuration will then in first instance be the default application configuration for that application type. Only once the application type is known, can the application configuration be modified, or can one be imported from a CSV-file or copied from another terminal.

Current application types are:

- MDB: cashless interface for vending machines using the MDB protocol
- EXEC: cashless interface for vending machines using the Executive protocol
- Totaliser: payment system that controls access through configurable signal lines
- COPR: controls access to a variety of multifunctionals, printers and photocopiers
- Access: controls physical access (doors, barriers)
- Bank: terminal for reloading

Each of these applications has a number of configuration settings that control the function of the application. These settings are presented as name/value pairs.

FP5 maintains the current configuration of a terminal for review, which can be modified. When a configuration has been modified, FP5 will queue an automatic update to all affected terminals in a few minutes. Whenever another configuration change is made, this update time will be reset to another few minutes. When no changes have been made during this timeout, FP5 will automatically reconfigure the terminals (i.e. execute the update) the next time they connect to the TMS.

9.3.1 Application configuration parameters

This paragraph explains some of the application configuration parameters that are not application specific. We refer to the installation and user manual for the application concerned (vending, POS, etc.) for an explanation of the parameters that are specific to an application.

Table 15: Application configuration parameters

Parameter	Description
Functional parameters	
Card image on server	On: this is an online system. The card/ID balance and other data of the card/ID are stored in a FacilityPro account in the back office.
	Off: this is an off-line system. The card/ID balance and other data of the card/ID are stored on the card/ID itself.
Need privilege to use terminal	On: a privilege is needed to use the terminal; this privilege must give access to this terminal
Product sale possible without privileges	On: no privilege is needed to purchase the products in this terminal
	Off: a privilege is needed to obtain the products in this terminal; this privilege must pertain to the products in this terminal
Tap&Go antenna(s)	None: Card/ID must be inserted to execute a transaction
	Bottom: Transaction can be executed by holding the card/ID at a short distance from the card/ID reader (Tap&Go); only the bottom antenna is activated
	Top: Transaction can be executed by holding the card/ID at a short distance from the card/ID reader (Tap&Go); only the top antenna is activated
	Top&Bottom: Transaction can be executed by holding the card/ID at a short distance from the card/ID reader (Tap&Go); both the top and the bottom antennas are activated
Tap timeout	Number of milliseconds within which a transaction must be started after presenting the card/ID at a Tap&Go terminal before the terminal returns to idle state
User interface parameters	
Show date/time	On: The current date and time will be shown on the display when the terminal is in idle state
Idle timeout (msec)	Number of milliseconds after which the display switches in idle state. When the terminal is not active, two or three alternating screens will be shown on the display. This parameter defines after how many ms the display switches between the screens. If it has the value 0 the screen will not alternate, only the first screen will be shown (default: WELCOME, YOUR CARD PLEASE). The date and time will then not be shown.
service timeout (msec)	The maximum time (in ms) that the machine may take to vend a product. If this time is exceeded the amount paid is put back in the balance of the card/ID and the transaction fails.
Display balance	On: When card/ID is presented the balance is displayed
Price display timeout	On: the chosen product and its price will be shown on the display after a choice has been entered

Single vend	On: there can only be one transaction (one product sold) with a presented card/ID. In order to effect a second payment with the same card/ID, it must be presented again. Off: the terminal can execute multiple transactions for the same card/ID without the card/ID being presented for each transaction;
User confirmation	On: Ask for user confirmation before payment.
Welcome text 1	When the terminal is not active, two alternating screens will be shown on the display of the terminal. This field contains the first line of text of the first screen. If this field is not filled in the default value 'WELCOME' will be used. The second line will always be 'YOUR CARD PLEASE'. The second screen will show the date and the time.
Welcome text 2	If this field is given a value, when the terminal is not active, three alternating screens will be shown on the display of the terminal instead of two (see above). The third screen will show the text filled in in this field. To control the way lines are shown (the position of lines) commands can be placed in the text. The Magnabox will interpret these commands and implement them. The commands for a line of text must be placed at the beginning of that line. The commands are: a) '\c' center the text on the display b) '\l' left-align the text c) '\r' right-align the text d) '\n' new line e) '\1' this text must be on the 1st line f) '\2' this text must be on the 2nd line g) '\3' this text must be on the 3rd line h) '\4' this text must be on the 4th line

9.3.2   Modifying an application configuration

Permissions required: Application configuration | Retrieve, Application configuration | Update

To edit an application configuration:

1. Select the "Terminals" option from the "Terminals" menu.
2. Click the name of the terminal.
3. Select the tab "Configuration".
4. Click the "Edit" button.
5. Edit the application configuration parameter values (see the installation and user manual for the application concerned (vending, POS, etc.) for an explanation of the parameters).
6. Click the "Save" button.

FP5 will queue the configuration update. It will be automatically executed the next time the terminal connects to the TMS.

9.3.3   Copying an application configuration from another terminal

Permissions required: Terminal | Retrieve, terminal | Update

An application configuration can be copied from another terminal, as long as it has the same application type. The terminal with the configuration you want to copy is referred to as the source terminal. The terminal(s) which you want to have the same configuration as the source terminal is/are called the target terminal(s). You must first create a so-called shared config (application configuration) which contains the application configuration of the source terminal. For each target terminal you must select this shared config.

To create a shared application configuration from the source terminal:

1. Select the "Terminals" option from the "Terminals" menu.
2. Click the name of the source terminal.
3. Select the tab "Configuration".
4. Click on the "New shared config" button.
5. Enter a name and a description for the new shared config.
6. Click the "Save" button.

To assign this shared application configuration to a target terminal:

1. Select the "Terminals" option from the "Terminals" menu.
2. Click the name of the target terminal.
3. Select the tab "Configuration".
4. Click on the "Select" button next to "Configuration:".
5. Select the shared application configuration from the dropdown-list, which shows all the shared application configurations for the application type of this target terminal. If the application configuration you wish to share does not yet exist, first create it (see instructions above).
6. Click the "Save" button.

9.3.4 Importing an application configuration from a CSV-file

Permissions required: Terminal | Retrieve, Terminal | Update

To import a configuration from a CSV-file:

1. Select the "Terminals" option from the "Terminals" menu.
2. Click the name of the terminal.
3. Select the tab "Configuration".
4. Click the "Import config" button.
5. Select the file delimiter (which character is used to separate parameter names and parameter values in the CSV-file) from the drop-down list.
6. Select the file character set used from the drop-down list.
7. Click the "+ Choose" button.
8. Select the CSV-file to be imported.
9. Click the "Import" button to upload and process the file.

The following table lists the field names that are used in a terminal application configuration CSV-file.

Table 16: Application configuration field names

Column name	Data type	Description
parametername	string(255)	Name of the parameter
parametervalue	string(255)	Value to be assigned to the parameter
description	string(255)	Description of the parameter

9.3.5 Exporting an application configuration to a CSV-file

Permissions required: Terminal | Retrieve

The current configuration of a terminal can be exported as a CSV-file. This file can be used to import the configuration for a terminal in another site or another system.

To export the application configuration of a terminal to a CSV-file:

1. Select the "Terminals" option from the "Terminals" menu.
2. Click the name of the terminal.
3. Select the tab "Configuration".
4. Click the "Export config" button. The browser will download the file and saved it in the download directory.

9.4 PRODUCT LAYOUT

The current product layout shows the products configured for sale in this terminal and their current assumed stock levels.

For each product in the layout, we configure the following properties:

1) Selection ID: the internal ID within the application (e.g. in MDB this is the selection number as provided by the vending machine, in printing and copying applications the ID is the decimal representation of the binary value for the three status lines that produce the product specified)
2) Label: the label as visible to and entered by the user
3) Product: the product at this position in the machine
4) Normal stock: the normal stock level that this product must be refilled to
5) Machine capacity: the maximum capacity of item dictated by the machine
6) Always top up?: determines whether the machine will be refilled with instructed quantity or whether the machine will be refilled up to the normal stock level at the time of the service
7) Low-water mark: the quantity of stock that triggers a low-water mark warning. If all selections of the same product reach this level a warning is issued.

9.4.1 Creating a product layout

Permissions required: Terminal | Retrieve, Terminal | Update

To create a product layout:

1. Select the "Terminal groups" option from the "Terminals" menu.
2. In the "Terminals" section, click the name of the terminal. If the list of terminals is too long you can select a terminal group first and then select a terminal.
3. Select the tab "Product layout". If there has been no previous product layout you will see the message "Product layout has not been created". Otherwise you will see the current product layout. See §9.4.2 for instructions to modify it.
4. Select the tab "Next". You will see the message "Product layout has not been created".
5. Click the "Create" link.
6. To add a product to the layout:
   a. Click the "Add product" button.
   b. Enter the choice label (used by the user to select the product), internal ID (depends on the application and type of machine connected to the terminal) and other details in the appropriate fields.
   c. Click the "Save" button to add the product to the layout.
   d. Repeat the previous three steps if you wish to add more products.
7. To remove a product from the layout, click the trash can icon 🗑 to the right of the product.
8. To edit a product in the layout:

a. Click on the ID or label.
b. Edit the field values.
c. Click "Save".
9. To remove the whole layout, click the "Delete all products" button.

You do not have to save the product layout as such. The product layout as you see it on the tab "Next" will be sent to the terminal and become active after the next picklist is serviced.

9.4.2   Modifying a product layout

Permissions required: Terminal | Retrieve, Terminal | Update

As long as a product layout has not been used in a picklist yet, it can be modified.

To modify a product layout:
1. Select the "Terminal groups" option from the "Terminals" menu.
2. Click the name of the terminal.
3. Select the tab "Product layout". You will see the current product layout.
4. Select the tab "Next".
5. To create the new product layout based on the current layout, click the "Create" link. The current product layout will be copied and can now be modified. To copy a product layout from another terminal see §9.4.3.
6. To edit a product in the layout:
    a. Click on the ID or label.
    b. Edit the field values.
    c. Click "Save".
7. To add a product to the layout:
    a. Click the "Add product" button.
    b. Enter the choice label (used by the user to select the product), internal ID (depends on the application and type of machine connected to the terminal) and other details in the appropriate fields.
    c. Click the "Save" button to add the product to the layout.

You do not have to save the product layout as such. The product layout as you see it on the tab "Next" will be sent to the terminal and become active after the next picklist is serviced.

☞   The updated product layout will become active after the next picklist is serviced.

9.4.3   Copying a product layout from another terminal

Permissions required: Terminal | Retrieve, Terminal | Update

To copy a product layout from another terminal:
1. Select the "Terminal groups" option from the "Terminals" menu.
2. In the "Terminals" section, click the name of the terminal. If the list of terminals is too long you can select a terminal group first and then select a terminal.
3. Select the tab "Product layout". If there has been no previous product layout you will see the message "Product layout has not been created". Otherwise you will see the current product layout.
4. Select the tab "Next".
5. Click the "Clone" link. If a new product layout was already created, the "Clone" link will not be visible. First click the "Delete all products" button to remove the current new product layout. The "Clone" link will become visible.
6. Select the terminal from which to copy the layout from the drop-down list.

7. Click the "Save" button. The new product layout will be visible on the tab "Next".

👆 The updated product layout will become active after the next picklist is serviced.

9.4.4 Importing a product layout from a CSV-file

Permissions required: Terminal | Retrieve, Terminal | Update

To import a product layout from a file:
1. Select the "Terminal groups" option from the "Terminals" menu.
2. Click the name of the terminal.
3. Select the tab "Product layout".
4. Select the tab "Next".
5. Ensure there is no new product layout visible on this tab. The "Create" and "Clone" links should be visible. If a new product layout was already created, these links will not be visible. First click the "Delete all products" button to remove the current new product layout. The "Create" and "Clone" links will become visible.
6. Click the "Import layout" button.
7. Select the file delimiter (which character is used to separate parameter names and parameter values in the CSV-file) from the drop-down list.
8. Select the file character set used from the drop-down list.
9. Click the "+ Choose" button.
10. Select the CSV-file to be imported.
11. Click the "Import" button to upload and process the file. The imported product layout is now visible on the tab "Next".
12. Click the "Close" button.

The following table lists the field names that are used in a CSV-file with a terminal product layout.

Table 17: Product layout field names

Column name	Data type	Description
label	string(255)	Name of the parameter
id	string(255)	Value to be assigned to the parameter
type	string(40)	Name of the product in this slot
normalstock	integer	Normal stock level to be maintained in this slot
machinecapacity	integer	Maximum stock level to be validated for this slot
lowwatermark	float	Low-water mark for this slot.
alwaystopup	true or false	Indicates whether service always supplies to the normal stock level when items have been sold between creation of the picklist and the time of the service.

9.4.5 Exporting a product layout to a CSV-file

Permissions required: Terminal | Retrieve

To export a product layout to a file:
1. Select the "Terminal groups" option from the "Terminals" menu.

2. Click the name of the terminal.
3. Select the tab "Product layout".
4. Select the tab "Current".
5. Click the "Export layout" button. A download will start. The product layout is saved in a file with the name "terminalLayoutProducts" in the download directory. You are advised to rename the file to indicate which product layout it contains.

9.5   TERMINAL GROUPS

To ease administration of sites that have large numbers of terminals, terminals can be organised in terminal groups. A terminal group is defined by the system administrator and may contain any number of terminals. Terminal groups themselves can be organised in hierarchies to allow more detailed drill down.

Multiple hierarchies can be created. Terminals can be in multiple terminal groups, but only one per hierarchy.

For example, a hierarchy of terminals may be created based on location. At the top of the location hierarchy may be larger regional areas (North-East, South-West), within a regional area terminals may be grouped by office location and then by floor. A parallel hierarchy can group terminals by type of products they contain (Soda, Snack, Coffee).

A terminal group may also be used when configuring a privilege to control access to terminals (§7.1.6.7).

Most terminal groups will be defined within a site and only be visible to FP5 users of that site. However, there are also system-wide terminal groups. These are created by the system administrator and contain terminals from different sites. For example, a logistics party may use system-wide terminal groups to plan restocking and servicing of terminals at multiple sites. Access to picklists and terminals may be configured by system-wide terminal group.

9.5.1   Creating a terminal group hierarchy

Permissions required: Terminal group | Retrieve, Terminal group | Create

If you create a terminal group at the highest hierarchical level, you also create a new hierarchy. If the system administration site is selected, the terminal group will be a system-wide terminal group. If another site is selected, the terminal group will only be available within the site.

To create a new root of a terminal group hierarchy:
1. Select the "Terminal groups" option from the "Terminals" menu.
2. Ensure no terminal group is selected by clicking the "Unselect" button.
3. Click the "Create" button.
4. Enter the terminal group name in the site languages.
5. Click the "Save" button. The new terminal group will be visible in the list of terminal groups at the highest level ("Root terminal groups").

9.5.2   Creating a terminal group in a hierarchy

Permissions required: Terminal group | Retrieve, Terminal group | Create

If the system administration site is selected, the terminal group will be a system-wide terminal group. If another site is selected, the terminal group will only be available within the site.

To create a terminal group within an existing terminal group:
1. Select the "Terminal groups" option from the "Terminals" menu. In the left column you will see the previously created terminal groups which are the roots of the existing hierarchies. If you see an arrow to the left of such a terminal group, it means that terminal groups have been created at a lower level in the hierarchy.

2. Click the name of the terminal group in the hierarchy to create the new terminal group in.
3. If you want to create the terminal group at a lower level in the hierarchy than directly under the root, click the arrows next to the terminal group names to show a lower level in the hierarchy until you can see the terminal group in which you want to create a new terminal group and click the name of that group.
4. Ensure the terminal group you want the new terminal group to belong to is selected (highlighted).
5. Click the "Create" button.
6. Enter the terminal group name in the site languages.
7. Click the "Save" button.

9.5.3 Assigning a terminal to a terminal group

Permissions required: Terminal | Retrieve, Terminal | Update, Terminal group | Retrieve

To assign a terminal to one or several terminal groups:
1. Select the "Terminal groups" option from the "Terminals" menu.
2. Click on a terminal name in the "Terminals" section.
3. To assign the terminal to system-wide terminal groups:
   a. Select the tab "Meta-site groups".
   b. Check the check boxes to the right of the system-wide terminal groups you want the terminal to be a member of.
   c. Click the "Save" button.
4. To assign the terminal to terminal groups within the site:
   a. Select the tab "Terminal groups".
   b. Check the check boxes to the right of the terminal groups you want the terminal to be a member of.
   c. Click the "Save" button.

9.5.4 Giving FP5 users access to a system-wide terminal group

Permissions required: FP5 user | Retrieve, FP5 user | Update, Terminal group | Access all

☞ An FP5 user can only assign terminals to system-wide terminal groups if he has been configured to have access to those terminal groups (i.e. terminal groups of the system administration site (meta-site)). See §5.2.1, step 4.

To give an FP5 user access to a system-wide terminal group:
1. Select the "FP5 users" option from the "Administration" menu.
2. Click the name of the FP5 user.
3. Select the tab "Sites/terminal groups".
4. In the "Terminal groups" section, click the "Add" button.
5. Select the terminal group you wish this FP5 to have access to from the drop-down list, which shows only system-wide terminal groups.
6. Click the "Add" button to add the terminal group to the list.
7. Click the "Apply" button to save the changes.

10 LOGISTICS

Although FP5 was not designed as an inventory tracking system, some simple functions allow for a basic estimation of machine inventory as well as a way of controlling the supply of the machines (e.g. vending machines).

10.1 PICKLISTS

A picklist contains instructions to a logistics user about how many of a particular product to retrieve from a warehouse (section "Picklist totals") and which products to supply to which machines (section "Picklist terminals"). The quantities are determined based on assumed stock levels in combination with the configured normal stock levels which are determined in the terminals' product layout (see §9.4).

When configuring a product layout for a terminal, the "normal stock level" is set. This is the stock level that a picklist will set out to reach for that terminal. Any additional product that is sold between the creation of a picklist, and the time the logistics user arrives at the terminal with supplies, is not taken into account in the picklist. To allow the logistics user to always supply the product up to normal stock level at the time of the service, the field "Always top-up" should be ticked. This will cause FP5 to assume the stock was refilled up-to normal level at the time of the service. The "Picklist totals" section of a picklist will show a "Grab more" flag to indicate more supplies may be required than the quantity shown in the picklist.

10.1.1 Creating the service privilege

Permissions required: Privilige | Retrieve, Privilige | Create

To confirm the restocking according to a picklist from FP5 at a terminal, the logistics user needs a Card/ID with a special "service" privilege (§7.1.6.6).

To create the service privilege:

1. Select the "Privileges" option in the "Products" menu.
2. Click the "Create" button.
3. Give the privilege a name like "Service privilege".
4. In the field "Type" select the value "Service".
5. If you want to limit the times that a service card/ID can be presented, select a validity timetable in the field "Validity timetable" or enter a start date and/or end date.
6. Click the "Save" button to create the privilege. The sections "Product groups", "Products", "Terminal groups" and "Terminals" become visible.
7. To limit the service privilege to only certain terminal groups or terminals:
    a. In the "Terminal groups" or "Terminals" section click the "Add" button.
    b. Select the terminal group/ terminal from the drop-down list.
    c. Click the "Add" button.
    d. Repeat the three previous steps until you have added all the terminal groups/terminals to which the service privilege must apply.

    The service privilege does not apply to product groups or products, these do not have to be specified.

8. Click the "Apply" button.

Refer to §7.2.3 and §7.2.4 for instructions on assigning the privilege to logistics personnel.

10.1.2 Creating a picklist

Permissions required: Picklist | Retrieve, Picklist | Create

Picklists are made for one terminal group at a time. You will only be able to create a picklist for a terminal group if the normal stock level for every product in each of the terminals in that terminal group has been set in the product layout.

To create a picklist:

1. Select the "Picklists" option from the "Logistics" menu. FP5 shows a list of most recent picklists and their status.
2. Click the "Create" button to create a new picklist.
3. Select the terminal group for which to create a picklist. This can be either a site-specific terminal group or a system-wide terminal group (should one be available and accessible).
4. Click "Select". A picklist is created for the terminals in the terminal group and the picklist detail screen for that picklist is opened. When you return to the picklists screen it will also appear in the list of recent picklists.

You can export the picklist to a PDF-file (see §10.1.3).

10.1.3 Exporting a picklist as PDF-file

Permissions required: Picklist | Retrieve

A picklist can be exported from the picklists list screen or from the picklist detail screen.

To export a picklist as PDF-file:
1. Select the "Picklists" option from the "Logistics" menu.
2. Click the "Export PDF" link to the right of the picklist to be exported or click the name of the picklist you wish to export and then click the "Export PDF" button on the picklist detail screen. The browser will download the file with the name (scan code) of the picklist to the download directory.

10.1.4 Withdrawing a picklist

Permissions required: Picklist | Retrieve, Picklist | Delete

If a picklist was created in error, it is best deleted before any of the terminals have been restocked.

If some terminals on a picklist have already been restocked, a picklist may still be withdrawn, causing it to become invalid for the terminals that haven't yet been restocked.

To withdraw a picklist:
1. Select the "Picklists" option from the "Logistics" menu.
2. Click the name of the picklist to be withdrawn to open the picklist detail screen.
3. Click the "Withdraw" button.

10.1.5 Restocking according to a pick-list

Permissions required: Picklist | Retrieve, Picklist | Adjust

To let FP5 know that a logistics user is at a particular terminal and restocking the terminal according to a picklist, a service card/ID has to be presented at this terminal. A service card/ID is any card/ID that has a service privilege assigned to it (i.e. to the user).

When a service card/ID is presented, the terminal will show a logistics menu that allows the logistics user to select the picklist according to which he is restocking the terminal.

10.1.6 Adjusting a picklist

Permissions required: Picklist | Retrieve, Picklist | Adjust

After the restocking of a terminal according to a picklist has been completed (the field "Status" on the picklist detail screen will show the value "Restocking complete"), the results of the restocking can be adjusted manually.

To adjust the results of a picklist:

1. Select the "Picklists" option from the "Logistics" menu.
2. Click the picklist to adjust to open the picklist detail screen.
3. Click the "Adjust" button. FP5 will suggest default final quantities supplied.
4. Edit the final quantities as desired.
5. Clilck the "Finalise" button. The new stock levels become visible throughout FP5. The field "Status" on the picklist detail screen will show the value "Finalised".

10.1.7 Deleting a picklist

Permissions required: Picklist | Retrieve, Picklist | Delete

To delete a picklist:

1. Select the "Picklists" option from the "Logistics" menu.
2. Either click the trash can icon to the right of a picklist to delete, or click the name of the picklist to go to the detail screen and click the "Delete" button.

Only picklists with the "Created", "Finalised" or "Withdrawn" status can be deleted. Picklists that are still being executed or adjusted may not be deleted.

11 REPORTS

Reports may be scheduled or created ad-hoc. Report templates determine the layout and contents of a report. Report templates are created by the system administrator and are available to other FP5 users to be selected as the template for a report. Refer to §5.5 for a description of report templates.

11.1 REPORT CONFIGURATIONS

A report configuration determines the report template and the parameters to be used to generate a particular report. Before a report can be generated, a report configuration has to be created that can determine fixed values for the report's parameters. A report configuration can also contain a schedule that will cause the report to be generated automatically.

A report configuration can also contain a distribution list of FP5 users or email addresses to send the report to once it has been generated.

A report configuration can define that some parameter values are fixed and cannot be changed when generating an ad-hoc report. If an FP5 user has access to report history and the ability to generate ad-hoc reports, that FP5 user can still be restricted from running any kind of report by not giving the report configuration create/update permissions.

11.1.1 Creating a report configuration

Permissions required: Report config | Retrieve, Report config | Create

To create a new report configuration:

1. Select the "Report configurations" option from the "Reports" menu.
2. Click the "Create" button.
3. Select the report template to base the report configuration on.
4. Enter the name for the report configuration in the site languages, a description and a number of days that the report must be kept ("Retention time in days") in the appropriate fields.

5. Click the "Save" button. The sections "Report parameters", "File types", "Report schedule" and "Report distributions" become visible.

The "Report parameters" section

The report configuration is initialised with parameters from the report template. Initially, no values are assigned to the parameters. Parameters can be mandatory (as declared by the report template) in which case they have to be given a value before the report configuration can be saved. Parameters that are mandatory will have the checkbox in the column "Mandatory" checked. For other parameters values can be entered but do not have to be. Typically these optional parameters will restrict the report to a single card/ID, terminal or other entity.

6. To assign a value to a parameter:
    a. Click on the name of the parameter.
    b. Enter a value or a range of values. It will depend on the type of parameter whether you choose a value from a drop-down list or enter a value yourself. See below for possible values for a date range parameter.
    c. Click the "Save" button.
7. To return a parameter to its initial status of "No value specified"
    a. Click on the name of the parameter.
    b. Click "No value".

Date range parameters, like usually the report time range, may be assigned a value that is replaced by FP5 at the time of generating the report. The following table lists the possible values for date ranges. The date ranges are computed in the time zone configured for the site that the report is run for.

Table 18: Reporting date range choices

Date range choice	Replaced by
Today	Midnight at the start of the current date to midnight at the end of the current date
YESTERDAY	Midnight at the start of the day before the current date to midnight at the start of the current date
THIS_WEEK	Midnight at the start of Sunday in the current week to midnight at the end of Saturday in the current week
THIS_MONTH	Midnight at the start of the first day of the current month until midnight after the end of the last day of the current month
THIS_QUARTER	Midnight at the start of 1 January, 1 April, 1 July or 1 October in the current quarter until midnight at the start of the next quarter
THIS_YEAR	Midnight at the start of 1 January of this year until midnight at the end of 31 December of this year
LAST_WEEK	Midnight at the start of Sunday before last Sunday to midnight at the start of last Sunday
LAST_MONTH	Midnight at the start of the first day of the previous month until midnight after the end of the last day of the previous month
LAST_QUARTER	Midnight at the start of 1 January, 1 April, 1 July or 1 October in the previous quarter until midnight at the start of the this quarter
LAST_YEAR	Midnight at the start of 1 January of last year until midnight at the end of 31 December of last year
CUSTOM	Not a dynamic value. The FP5 user is prompted for a start and end date.

The "File types" section

8. Click the check boxes next to each of the format types you wish the report to be generated in.

The "Report schedule" section

FP5 can automatically generate the report on a preset schedule.

9. To run a report automatically:
    a. Check the check box "Run report automatically".
    b. Select the type of schedule (daily, weekly, monthly or yearly).
    c. Enter the month/day/time within that period to run the report at.

The "Report distributions" section

FP5 can also distribute reports by email automatically.

A recipient can be:

- A FP5 user. The report will be emailed to the FP5 user's email address.
- A specific email address. The report will be emailed to that email address.
- All FP5 users with a specific role. The report will be emailed to all FP5 users that have been assigned that role.

To each recipient you can select one or more of the following to send:

- Email notification: Send an email using the "ReportWithLink" template, which contains a link to the report's page. This allows tracking of which FP5 users have clicked the link and downloaded the report.
- Email PDF attachment: Send an email using the "Report" template with the report attached in PDF format
- Email CSV attachment: Send an email using the "Report" template with the report attached in CSV format
- Email as inline: Send an email using the "Report" template with a plain text version of the report presented inline.
- Email notification when empty: Send an email to notify the recipient that a report contains no data.
- SMS notification: Send a SMS to the FP5 user's mobile phone number when the report is ready.
- SMS notification when empty: Send a SMS to the FP5 user's mobile phone number to notify the recipient that a report contains no data.

10. To add a recipient for the report:
    a. Click the "Add" button in the "Report distributions" section.
    b. Select the type of recipient.
    c. Select one or more distribution types.
    d. Click the "Add" button to add the recipient to the distribution list. You will see a table showing which recipients have currently been selected and which distribution types they will receive.
    e. Repeat the four previous steps to add another recipient. You can add as many recipients as you like.
11. To delete a recipient click the "Delete" link to the right of the recipient.

When you have finished configuring the report parameters, file types, schedule and distribution list:

12. Click the "Apply" button to save the report configuration.

If a schedule was selected it will become active immediately.

11.1.2 Updating a report configuration

Permissions required: Report config | Retrieve, Report config | Update

To update a report configuration:
1. Select the "Report configurations" option from the "Reports" menu.
2. Click the name of the report configuration.
3. Edit the fields and parameters you wish to change. See §11.1.1 for a description of a report configuration's details.
4. Click the "Apply" button.

11.1.3 Deleting a report configuration

Permissions required: Report config | Retrieve, Report config | Delete

A report configuration may be deleted. It will no longer be generated automatically and is no longer visible in the list of report configurations. Report history for this report configuration will remain available.

To delete a report configuration:
1. Select the "Report configurations" option from the "Reports" menu.
2. Click the trash can icon   to the right of the report configuration to delete. A pop-up screen will prompt for confirmation.
3. Confirm deletion.

11.1.4 Retrieving the history of revisions of a report configuration

Permissions required: Report config | Retrieve, Report config | Update

☞ The "Show revisions" button is only available to FP5 users who have access to the system administration site. They must have a role for the system administration site which has the FP5 activity | Retrieve permission .

To see a list of previous activities with a particular report configuration:
1. Select the "Report configurations" option from the "Reports" menu.
2. Click the name of the report configuration.
3. Click the "Show revisions" button (you might need to scroll down). You will be diverted to the system administration site and see the FP5 activities (e.g. create, update) for that report configuration in chronological order.

The same can be achieved using the "Show revisions" button on the "Run report" screen (see §11.2.1).

11.2 REPORTS

FP5 stores the reports that have been generated.

11.2.1 Generating an ad-hoc report

Permissions required: Report config | Retrieve, Report config | Update, Report config | Run,

Report history | Retrieve

It is possible to run a report on demand, even if a schedule exists for the report.

To manually generate a report:

1. Select the "Report configurations" option from the "Reports" menu.
2. Click the "Run" link to the right of the desired report configuration. The "Run report" screen will show you which constraints to the report parameters have been defined in the report configuration and which formats (file types) the report will be created in.
3. If you wish to run the report with additional constraints to the parameter values on top of those specified in the report configuration:
    a. Click on the name of the parameter you wish to specify values for. Only parameters that have not been supplied with a value by the report configuration (column "Value" shows "No value specified") can be selected. Depending on the type of parameter you will see a different pop-up screen where you can enter constraints for the parameter.
    b. Enter the desired value(s) or value range(s).
    c. Click the "Save" button.
4. If you wish to change the formats that the report will be generated in, click in the check boxes in the "File types" section to check or uncheck each file type.
5. If you wish the ad-hoc report to be sent to the recipients defined in the report configuration, click in the check box "Distribute ad-hoc report to recipients" to check it.
6. Click the "Run" button to generate the report. You will see a report screen with the status of the report's generation. You may have to refresh the screen a few times until you see the details of this report generation. You can see for which parameter values the report was generated and to whom the report was distributed and in which form. The report files created according to the "File types" section in step 4 can be downloaded by clicking on the "CSV", "PDF", "TXT" and "XML" buttons available.

11.2.2 Retrieving a generated report

Permissions required: Report history | Retrieve

To retrieve reports that have been generated:

1. Retrieve reports for a particular report configuration:
    a. Select the "Report configurations" option from the "Reports" menu.
    b. Click the "History" link to the right of the report configuration. FP5 will show the reports generated (including the date and distribution status).

   or retrieve reports for all report configurations:

    a. Select the "Report history" option from the "Reports" menu. FP5 will show the reports generated (including the date and distribution status).
2. To limit the number of reports shown:
    a. Enter search details such as start and/or end date.
    b. Click the "Search" button.
3. Click the "Details" link to the right of a report to view the report files.
4. Click the "CSV", "PDF", "TXT" or "XML" buttons to download the generated reports of in these formats. Which formats are available (were generated) depends on the values chosen in the "File types" section in the report configuration, which was possibly adjusted if the report was not generated automatically, but run on an ad-hoc basis

11.2.3 Deleting a generated report

Permissions required: Report history | Retrieve, Report history | Delete

To delete a report:

1. Select the "Report history" option from the "Reports" menu. FP5 will show the reports generated (including the date and distribution status).

2. Click the trash can icon ⬛ to the right of the report you wish to delete. A pop-up screen will prompt for confirmation.
3. Conform deletion.

12 USER PORTAL

Users can easily reload their cards, manage their privileges, view their transactions or block their lost or stolen cards/IDs anywhere and anytime, on the user portal site.

In the future, students and other users will also be able to use the portal to give feedback. To share their opinion of product quality and whether they are satisfied with the available range of products and services.

The user portal is a web application. It requests payment for the amount of the purse reload or for the value of the privilege increase before the reload or privilege increase is implemented. Payment can be done via an online payment system. At present iDEAL and PayPal are supported.

The user portal is represented by a terminal in FP5. (We suggest you name the terminal 'User portal'). The product layout of this fictitious terminal defines which purse or privilege reloads can be bought through the user portal.

For the users, there is a separate user manual for the user portal, although the user interface is so simple that a user should not need it. In this chapter you can read which kind of 'products' can be sold through the user portal, how to define them in FP5, and some other administrative functions are explained.

There is a separate installation manual for the user portal where you can read all about the FP5 set-up necessary for the user portal to function, such as creating the user portal 'terminal' and products, assigning the correct privileges for the user portal administrator to be able to log into the user portal and change settings, etc.

The FacilityPro user portal enables users to:

• manage and reload e-purses

• manage and upgrade privileges

• block lost or stolen IDs

• view transactions

In the future, they will also be able to:

• give their opinion on product quality

• give their opinion on the range of products and services

12.1 USER PORTAL SETTINGS

The site administrator can decide which functionality will be available to the users of his site from the user portal. These settings are found on the FP5 user directory page, "FP5 user portal permissions" section (Figure 12-1).

FP5 user directory

Name	Local cardholders
	Local cardholders

☐ Allow password change
☐ Allow password reset
☐ Allow self-enrollment
☐ Connect to LDAP server

FP5 user portal permissions

Enable account holder login	☑
Allow holder to see balance	☑
Allow holder to see privileges	☑
Show recent transaction summary	☑
Number of recent transactions to show	5
Allow holder to browse transactions	☑
Holder can buy top-ups	☑
Allow holder to block account	☑
Allow holder to unblock account	☑
Allow holder to grant access to others	☐
Allow holder to revoke access from others	☐

Figure 12-1

The configurable settings are:

- Enable account holder login: when this box is not checked users cannot use the portal.
- Allow holder to see balance: the balance is shown only when this field is checked.
- Allow holder to see privileges: the privileges are shown only when this field is checked.
- Show recent transaction summary: the recent transaction summary is shown only when this field is checked.
- Number of recent transactions to show: determines how many transactions to show in "Recent transactions" section of the user portal home page.
- Allow holder to browse transactions: when this box is checked there is a "See more" link in the "Recent transactions" section which enables him to browse through the entire transaction history. When this box is not checked the user can only see the recent transaction summary and there is not a "See more" link.
- Holder can buy top-ups
- Allow holder to block account
- Allow holder to unblock account
- Allow holder to grant access to others: not yet in use
- Allow holder to revoke access from others: not yet in use

To change the user portal settings:

1. Select the "FP5 user directory" option from the "Administration" menu.
2. Click the name of the FP5 user directory that contains the users for which you wish to change the user portal functionality.

3. Check or uncheck the fields in the section "FP5 user portal permissions" and/or change the value of the field "Number of recent transactions to show" to reflect the functionality you wish the user portal to have for the users in this FP5 user directory.
4. Click the "Apply" button to save the changes.

12.2 CREATING THE RELOADS AVAILABLE THROUGH THE USER PORTAL

The user portal can offer any product defined in FP5 which has a value in at least one of the fields of the "Account product details" section (Figure 12-2). These products are either top-ups to the e-purse balance or to a privilege that has been assigned to the user.

<div align="center">
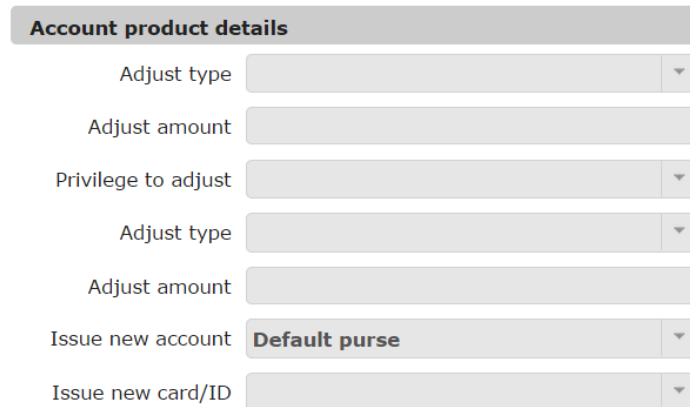
Figure 12-2

</div>

We advise that you assign all the products that are to be available through the user portal to the same product group that you name "User portal" or "Account products" or something similar.

For instructions on creating a new product group, see §6.1.1. For instructions on creating new products see §6.2.1.

The fields of the "Account product details" section of a product are listed below and have the following significance:

1. Adjust type: leave empty or choose between
   a. Add amount: to top-up the e-purse balance
   b. Subtract percentage from price: functionality not yet implemented. Do not use.
   c. Subtract amount from price: functionality not yet implemented. Do not use.
2. Adjust amount or percentage: the amount to add to the e-purse balance (choice a. above) or the percentage to subtract from the price (choice b. above) or the amount to subtract from the price (choice c. above).
3. Privilege to adjust: choose a privilege from the drop-down list
4. Privilege adjust type:
   a. Add amount: to increase the privilege counter for a privilege that is limited by a counter
   b. Subtract percentage from price: functionality not yet implemented. Do not use.
   c. Subtract amount from price: functionality not yet implemented. Do not use.
5. Privilege adjust amount or percentage: the amount to add to the privilege counter (choice a. above) or the percentage to subtract from the price (choice b. above) or the amount to subtract from the price (choice c. above).
6. Issue new account: functionality not yet implemented. Do not use.
7. Issue new card/ID: functionality not yet implemented. Do not use.

Below are some examples of products you might want to define for your user portal.

12.2.1 E-purse top-up

Product

Name	10 euro opwaarderen
	Top-up 10 euros
Short name	
Product group	User portal
Part Number	
Logistic code	
Weight	
Length	
Width	
Height	
Default price *	10
Default VAT rate	Select one
Privileges	Show privileges

Product image

Account product details

Adjust type	Add amount
Adjust amount or percentage	10
Privilege to adjust	
Privilege adjust type	
Privilege adjust amount or percentage	
Issue new account	
Issue new card/ID	

Figure 12-3 Product definition for a €10 top-up

By filling in a lower value in the field "Default price" than in the field "Adjust amount or percentage" you can create a type of discount. The user gets more money in his e-purse than he actually pays. The value in the field "Default price" is the amount the online payment system will charge when the user purchases this product in the user portal and it must be greater than €0. The value in the field "Adjust amount or percentage" is the amount that will be added to the e-purse.

12.2.2 Privilege top-up

Figure 12-4 Product definition for a top-up for a privilege counter

Privilege top-ups can be used for example to:

- allow users that have a certain privilege, such as 1000 free prints/copies a month, but have depleted their privilege counter to purchase more free prints/copies for a dummy amount such as €0.01,
- allow users to buy value which is stored in a privilege counter, so that it can only be used for the products available through that privilege.

By filling in a lower value in the field "Default price" than the value of the amount in the field "Privilege adjust amount or percentage" you can create a type of discount. The user gets more value in his privilege counter than he actually pays. The value in the field "Default price" is the amount the online payment system will charge when the user purchases this product in the user portal and it must be greater than €0. The value in the field "Privilege adjust amount or percentage" is the amount that will be added to the privilege counter of the chosen privilege, which may represent a monetary amount or a number of transactions. E.g. in the example above the privilege counter is the number of prints/copies that can be made, which is increased by 500. For a privilege such as "€5 a day cantine budget" the privilege counter would represent a monetary amount. In the example below, €5 is added to the privilege purse (counter) that can only be spent in the cantine. One can imagine for instance, a parent wanting to top-up his child's allowance for lunch, but not for soft drinks and sweets from the vending machines.

Product

Name	Kantinebudget opladen €5	**Product image**	
	Top-up cantine budget €5		
Short name			
Product group	Select one ▾	+ Choose	
Part Number			
Logistic code		**Account product details**	
Weight		Adjust type	▾
Length		Adjust amount	
Width		Privilege to adjust	€5 a day cantine budget ▾
Height		Adjust type	**Fixed amount** ▾
Default price *	5	Adjust amount	5
Default VAT rate	Select one ▾	Issue new account	▾
Privileges	Show privileges	Issue new card/ID	▾

Figure 12-5 product definition for a top-up for a privilege counter

12.3 MAKING THE RELOADS AVAILABLE THROUGH THE USER PORTAL TERMINAL

The products defined for the user portal must be added to the product layout of the terminal (tab "Next") that represents the user portal. We suggest calling this terminal "User portal".

For instructions on creating a terminal, see §9.1. In principal the terminal will have been created when the user portal was installed. For the terminal to be recognised as the user portal terminal you must ensure that the field "External ID" has the same value as the field "FP5 Terminal external id" in the general settings of the user portal (see FP5 user portal installation manual).