For any questions or troubleshooting please call:

CTC Business

208-229-9000

6. CARDHOLDERS

This chapter contains the following sections:

* *About Cardholders*
* *Cardholders Process*
* *Users*
* *User Access Levels*
* *Limited Occupancy Groups*
* *Cardholder Timetables*

# 6. 1. About Cardholders

Card is a generic term in the SALTO system that refers to a key, bracelet, watch, or phone. A cardholder is a person who accesses a SALTO site by using one of these access devices. A cardholder can be a user (usually a member of staff), a visitor (someone who only requires access once or just occasionally), or a guest (someone staying temporarily at a hotel who requires access to an assigned room for a fixed period of time).

This chapter describes how to create users. It also describes the management options associated with cardholders. See *Visitors* for information about visitors and *Hotels* for information about hotel guests.

The information contained in this chapter applies to non-hotel sites only. See *Hotels* for information about hotel guests who also use keys. Note that guests are treated differently from other types of cardholders.

**NOTE:** Keycards are generally referred to as keys, both in this manual and in the system itself.

## 6. 1. 1. About Cardholder Configuration

You must perform certain cardholder configuration tasks in ProAccess SPACE General options. You can use the **User** tab to do the following:

* Enable and amend options for users and user keys
* Delete users permanently
* Configure user IDs

See *Users Tab* for more information.

You can also go to **Users** tab to enable and configure tracks for user keys.

# 6. 2. Cardholders Process

Cardholders are generally created and managed by an operator with admin rights. References are made to the admin operator throughout this chapter. However, this can mean any operator that has been granted admin rights.

The following example shows a simple way of completing this process:

### 1. Users created and configured

The admin operator creates user profiles and configures the user options.

### Users associated

The admin operator associates access points, user access levels, zones, outputs, and locations/functions with the specified users.

### User access levels created and configured

The admin operator creates user access levels and configures the user access level options.

### User access levels associated

The admin operator associates access points, zones, users, and outputs with the specified user access level.

### Limited occupancy groups created and configured

The admin operator creates limited occupancy groups and configures the limited occupancy groups options.

### Limited occupancy groups associated

The admin operator associates users and limited occupancy areas with the specified limited occupancy groups.

### Cardholder timetables created and configured

The admin operator creates cardholder timetables and configures the timetable options.

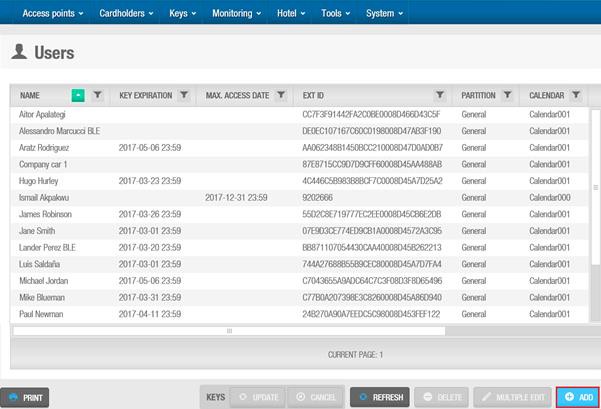
# 6. 3. Users

A user is typically a member of staff who needs access to and within your site’s buildings. They are differentiated from other cardholders by the fact that they need regular, rather than occasional, access. Usually, they also have a greater level of access than other types of cardholders such as visitors.

## 6. 3. 1. Creating Users

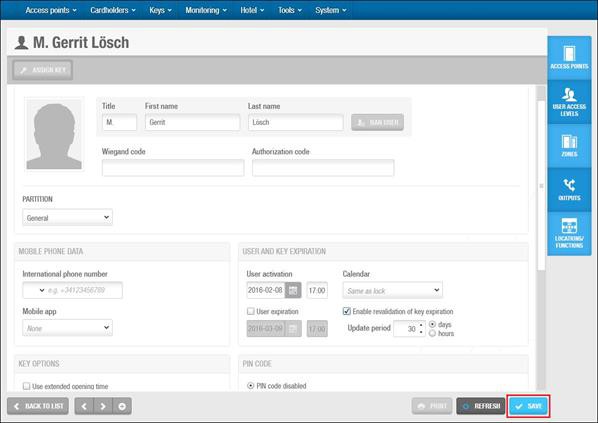
To create a user, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.



**Figure 89: Users screen**

Click **Add User**. The **User** information screen is displayed.



**Figure 90: User information screen**

Type a title, first name, and last name for the user in the **Identification** panel.

**NOTE:** You can activate system restrictions for user names by enabling the INHIBIT\_USER\_NAME\_CHANGE parameter in **System** > **General options** > **Advanced**. If you enable this parameter, you cannot edit the **Title**, **First name**, and **Last name** fields on the **User** information screen if you have assigned a key to the user at any point. An **Error** pop-up message is displayed when you try to save any changes to these fields. This ensures that the audit trail data for users is accurate. See *Advanced Tab* for more information.

Enter a **Wiegand code** if required. See *Wiegand code format* for more information. Enter an **Authorization code** if required

**NOTE:** Only Wiegand interface is supported and requires a third-party ROM-code reader. The user access is based on a white list of ROM codes at the Salto DB. CU42x0 are required. See *Advanced Tab* for more information.

Select the relevant partition from the **Partition** drop-down list, if required. See *Partitions* for more information.

Select the appropriate management options.

The configuration and management fields are described in *Configuring Users*. Click **Save**.

**NOTE:** The **Multiple Edit** button is enabled when you select more than one entry on the **Users** screen. This allows you to enter the appropriate options and configuration details on the **Multiple edit** screen including access rights. The details are then applied to all of the selected entries. See *Configuring Users* for more information about the configuration settings for users.

#### 6. 3. 1. 1. Adding Additional Information

If required, you can use ProAccess SPACE General options to add up to five general purpose fields to the **User**

screens. These fields allow you to add extra data, for example, a passport number or car registration number. To

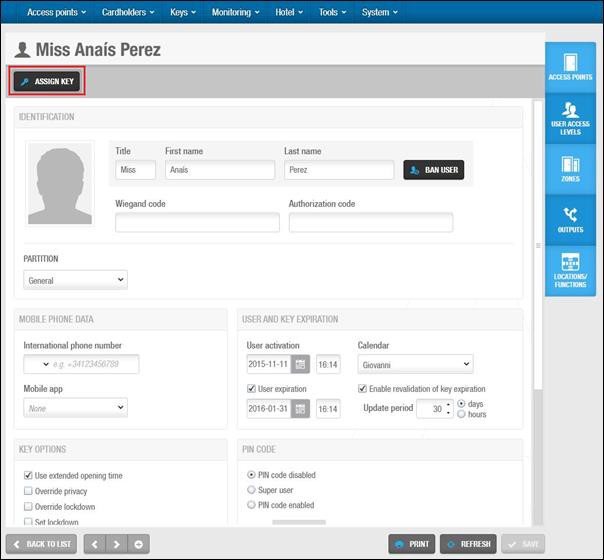
activate a general purpose field, you must select an **Enable field** checkbox in **System** > **General options** > **User**. You can then name the field in accordance with the information that you want to capture.

#### 6. 3. 1. 2. Assigning Keys

After you have created and configured a user, you can click **Assign Key** on the **User** information screen to assign them a key. See *Assigning User Keys* for more information.

When you assign keys to users, different icons are displayed in the **Key status** column on the **Users** screen, depending on the key status. See *Key Status Icons* for more information. The key status is also displayed on the **User** information screen. The period for which keys are valid is shown on the **User** information screen and also in the **Key Expiration** column on the **Users** screen.

**NOTE:** The **Assign Key** button is only available on the **User** information screen after a user profile has been created and saved.



**Figure 91: User information screen**

#### 6. 3. 1. 3. Banning Users

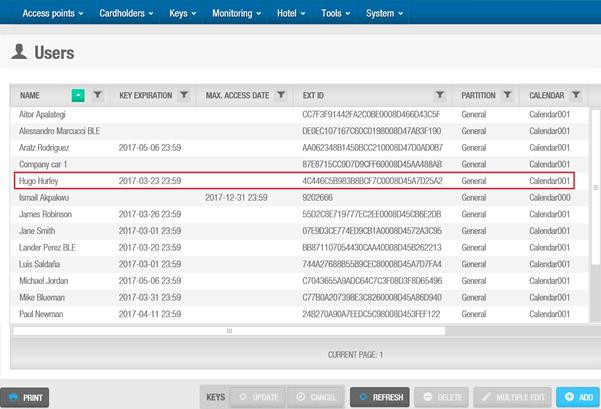
After you have created and configured a user, you can, if necessary, ban a user from accessing any part of a site by invalidating their key. For example, a user who is a member of staff can be banned while they are on vacation.

Unbanning the user when they return from vacation restores their original access data to their key (after presenting the key to an SVN wall reader).

**NOTE:** Banning users is different from cancelling keys. A user’s key can be cancelled, for example, if a user loses their key. See *Cancelling Keys* for more information. The blacklist is a record of cancelled keys. Banned users are not added to the blacklist. See *About Blacklists* for more information.

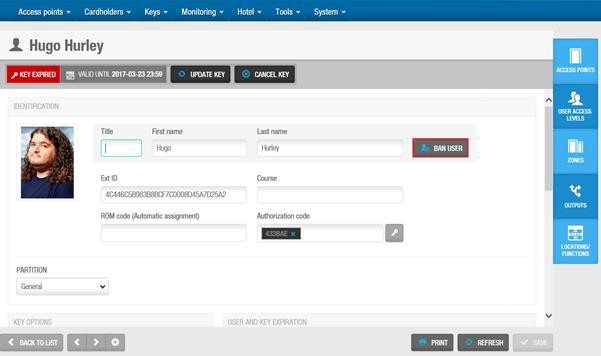
To ban a user, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.



**Figure 92: List of users**

Double-click the user that you want to ban. The **User** information screen is displayed.



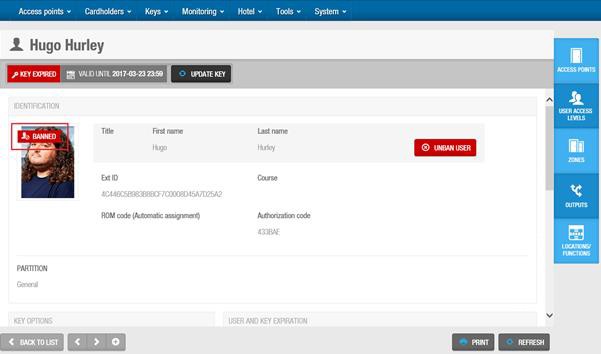
**Figure 93: User information screen**

Click **Ban User**. A pop-up is displayed asking you to confirm that you want to ban the user.



Click **Yes**. The user is banned.

**Figure 94: Ban user confirmation pop-up**



**Figure 95: User information screen**

To unban a user, perform the following steps:

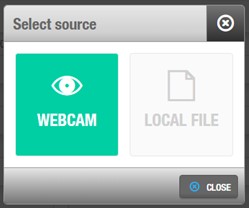
1. Select **Cardholders** > **Users**. The **Users** screen is displayed.

Double-click the user that you want to unban. The **User** information screen is displayed.

Click **Unban User**. A pop-up is displayed asking you to confirm that you want to unban the user. Click **Yes**. The user is unbanned.

#### 6. 3. 1. 4. Adding User Images

You can add images to user profiles in ProAccess SPACE to identify users. You can upload these images from storage devices such as USBs and memory cards, or from camera devices. Images or pictures could be also taken from a webcam:



**Figure 96: User information screen**

The following image formats are compatible with ProAccess SPACE:

* JPEG
* PNG

To add a user image, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.
2. Double-click the user entry to which you want to add an image. The **User** information screen is displayed.
3. Hover the mouse pointer over the image in the **Identification** panel and click the **Select photo** icon. The **Open**

dialog box is displayed.

1. Select the appropriate image and click **Open**. The selected image is displayed on the **User** information screen. Note that the image you add cannot be more than 200 KB in size.
2. Click **Save**.

You can hover the mouse pointer over the image and click the **Remove photo** icon to remove it if required.

**NOTE:** User pictures can also be imported through synchronization *Automatic CSV File Synchronization*, *Automatic Database Table Synchronization* and *Manual Synchronization* for more information.

#### 3. 1. 5. Printing User Profiles

You can print user profiles by clicking **Print** on the **User** information screen. See *Printing and Exporting Data in ProAccess SPACE* for more information. Date and signature fields are automatically included when you print user profiles. You can ask users to sign and date these to confirm receipt of their keys, for example.

#### 6. 3. 1. 6. Deleting Users

You can delete any user by selecting the required user on the **Users** screen and clicking **Delete**. This deletes their profile, and they are no longer displayed on the **Users** screen. If the deleted user had an assigned key, his key will be cancelled through the same process.

## 6. 3. 2. Configuring Users

The following sections describe the various panel options used to configure users.

#### 6. 3. 2. 1. Identification

The **Identification** panel defines the user’s details. Most of the fields in this panel are described in *Creating Users*.

The **ROM** field is generally filled in by synchronization but it can also be filled in manually. This code is used for automatic key assignment. Note that the automatic key assignment functionality is license-dependent. If you do not have access to this in your licensing options, the **ROM** field is not displayed. See *Registering and Licensing SALTO Software* for more information.

You must enable the SHOW\_ROM\_CODE parameter in ProAccess SPACE General options to control the display of ROM codes when you read keys or export audit trail data. See *Advanced Tab* for more information.

**NOTE:** Generally, the system does not allow you to create two cardholders with the same name. You can make user names unique by changing the default format for user IDs in ProAccess SPACE General options. See *Configuring User IDs* for more information.

#### 6. 3. 2. 2. Mobile Phone Data

The **Mobile Phone Data** panel defines what mobile application the user will use.

**Table 21: Mobile Phone Data options**

|  |  |
| --- | --- |
| **Option** | **Description** |
| International phone number | User mobile phone number. The Area code has to be entered first according to the country the mobile phone line is from. |
| Mobile app: JustIN mSVN | Defines the mobile application the user will use. JustIN mSVN allows the user to use the mobile phone as a mobile key updater. Note that this option is currently only compatible with Desfire Evolution 1 keys and Android phones. |

|  |  |
| --- | --- |
| **Option** | **Description** |
| Mobile app: JustIN Mobile | Defines the mobile application the user will use. JustIN Mobile allows the use of a Mobile phone as a credential. The communication between the reader and the phone is Bluetooth.  Note that the lock reader has to be BLE (Bluetooth Low Energy) compatible. |

#### 6. 3. 2. 3. Key Options

The **Key Options** panel defines the user access details.

**Table 22: User key options**

|  |  |
| --- | --- |
| **Option** | **Description** |
| Use extended opening time | Allows extended door opening times if a user has a disability and requires a longer access time when entering a door |
| Override privacy | Allows the user access to a door that has been locked from the inside |
| Override lockdown | Allows the user to open a door closed by lockdown. Note that this option applies to both online doors and offline doors that have AMOK locks. See *Lockdown Areas* for more information. |
| Set lockdown | Allows the user to enable or disable the lockdown mode on a door. This is done by presenting a valid key to the door’s inside reader. This option only applies to offline doors that have AMOK locks. See *Lockdown Areas* for more information. |
| Office | Allows the user to set doors to Office mode. See *Opening Modes and Timed Periods* for more information. |
| Use antipassback | Ensures that a user cannot enter through the same door multiple times until they have first exited the door (or until a specified time period has passed). This is to prevent a key being used by a number of different users. See *Enabling Anti-passback* and *Access Points Tab* for more information. The antipassback functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information. |
| Audit openings in the key | Allows an audit trail of the user’s access point activity to be written to their key. If this option is disabled, the locks will not write any audit information to the key. You must also enable this feature on the required access points by selecting the **Audit on keys** option. See *Door Options* and *Locker Options* for more information. |
| New key can be cancelled through blacklist | Ensures that the user’s key is sent to the blacklist if it is cancelled. To activate this option, you must enable the MORE\_THAN\_64K\_USERS parameter in ProAccess SPACE General options. This checkbox is selected by default for users. If you clear the checkbox, the user’s key is not sent to the blacklist when cancelled. See *Advanced Tab* for more information. |

#### 6. 3. 2. 4. PIN Codes

The **PIN Code** panel defines the user’s PIN code options. In addition to a key, a PIN code may sometimes be required for users to gain access to certain parts of the site.

**Table 23: PIN code options**

|  |  |
| --- | --- |
| **Option** | **Description** |
| PIN code disabled | Disables the PIN code. This denies a user entry to access points that require a PIN code. |
| Super user | Allows a user access using only their key when the door is in Key + PIN mode. See *Opening Modes and Timed Periods* for more information. |
| PIN code enabled | Enables user access using a card and a PIN code |
| PIN | Defines the PIN code. This option is only available if you select the **PIN code enabled** option. |

|  |  |
| --- | --- |
| **Option** | **Description** |
| Confirmation | Confirms the PIN code. This option is only available if you select the  **PIN code enabled** option. |

#### 6. 3. 2. 5. User and Key Expiration

The **User and Key Expiration** panel defines the key activation period.

**Table 24: User and user key expiration options**

|  |  |
| --- | --- |
| **Option** | **Description** |
| User activation | Defines the date and time upon which the user’s key becomes functional and they will be granted access permissions. By default, the activation date is the day on which the user’s key is encoded. |
| User expiration | Defines the long-term expiration date of the user’s data and access permissions. Keys assigned to a user will never exceed this date. Note that you can choose not to assign an expiration date to a user. This means that they can revalidate their card when required. |
| Calendar | Defines which calendar is applied to the user. See *Calendars* for more information. |
| Enable revalidation of key expiration | Enables the user’s key to be revalidated at any time even when the key has not expired. For example, if the user’s update period is seven days, the key is revalidated for another seven days every time the user presents their key to an SVN wall reader even if has been revalidated the day before. |
| Update period | Defines the time period between user validations. If this is set to zero, the user’s key expires at 00:00 on the same day that it is updated.  However, the key can still be updated each day. If 30 days is selected, the user’s key will be valid for 30 days and will need to be revalidated once that time period has expired. You can change the default update period by amending the value in the **Default expiration period** field in **System** > **General options** > **Users** in ProAccess SPACE. See *User Tab* for more information. |

#### 6. 3. 2. 6. Dormitory Doors

You can allow users in your organization to change a door’s keypad code. For example, in a dormitory where there is a high turnover of students, users may need to frequently change a door’s keypad code to prevent unauthorized access.

To activate this functionality, you must enable the DORM\_KEYPAD parameter in ProAccess SPACE General options. See *Advanced Tab* for more information. When you enable this parameter, a **Dormitory Door** panel is added to the **User** information screen, and you can select a door from the drop-down list.

You must change the keypad code for the door by using the **Keypad Code** field on the **Door** information screen. See *Opening Modes and Timed Periods* for more information. The new keypad code is transferred to the user’s key when they update their key at an SVN wall reader. When the user presents their key to the door, the door is updated with the new keypad code, and the previous keypad code is invalidated.

#### 6. 3. 2. 7. Limited Occupancy Groups

You can add a user to a limited occupancy group by selecting the required limited occupancy group in the **Limited Occupancy Group** panel. Limited occupancy groups are used to manage restricted car parks, for example. See *Creating Limited Occupancy Groups* for more information. See *Limited Occupancy* for more information about controlling limited occupancy groups.

#### 6. 3. 2. 8. Card Printing Templates

You can create card templates for different users in your organization. For example, you could create one template for day staff and a different template for night staff. When you create card printing templates, they are added to the **Card Printing Template** drop-down list. The template that you select in the **Card Printing Template** panel is used when you print the user’s keycard. To print the card, select the appropriate template from the drop-down list and click the **PRINT** button.

Card printing templates must be created in ProAccess SPACE under **Tools** > **Card printing**. See *Card Printing* and

*Using Card Printing Templates* for more information.

## 6. 3. 3. Associating Users

After you have created a user, you must associate access points, user access levels, zones, outputs, and locations/functions with the specified user. The following sections describe how to associate users with the various entries.

#### 6. 3. 3. 1. Access Points

See *Access Points* for definitions and information about how to create and configure access points.

**NOTE:** You would generally only associate individual users with access points if they do not belong to a user access level. User access levels allow you to group users with the same access permissions for easier access management. See *User Access Levels* for more information. However, there may be cases where you need to give individual users access to doors or zones that are not associated with their user access level.

To associate a user with an access point, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.

Double-click the user name that you want to associate with an access point. The **User** information screen is displayed.

Click **Access Points** in the sidebar. The **Access points** dialog box is displayed.

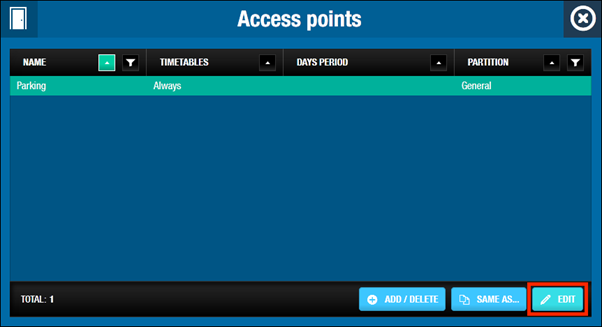
Note that the dialog box will be blank because you have not yet associated a user with this particular access point.

Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.

Select the required access point in the left-hand panel and click the chevron. The selected access point is displayed in the right-hand panel.

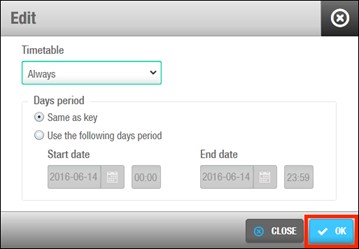
Click **Accept**. The access point is associated with the user.

Select the access point in the **Access points** dialog box if you want to select a cardholder timetable to be used. See *Cardholder Timetables* for more information.



**Figure 96: Users dialog box**

Click **Edit**. The **Edit** dialog box is displayed.



**Figure 97: Edit dialog box**

Select the appropriate timetable using the drop-down list. Alternatively, you can also select the **Always** or **Never**

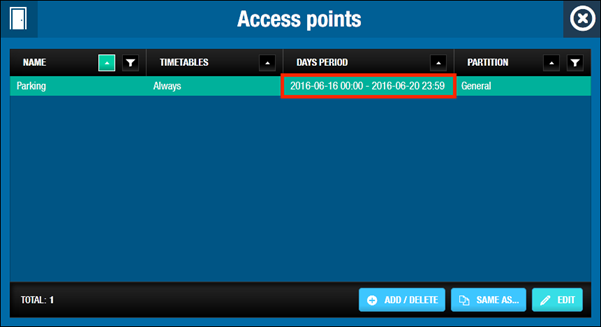
drop-down list option.

The **Always** option is selected by default. This means that the user always has access to the access point, as you have not specified a timetable. Note that the system calendars do not apply if the **Always** option is selected. If you select **Never**, they do not have access to the access point at any time.

In Days period, **Same as key** is selected by default. It means the user will have access to the door while the key is valid.

Select **Use the following days period** if you want the user to have access to that specific door only during a period of time. Select a **Start date** and an **End date**.

**NOTE:** The key validity takes precedence over the door access. If the access to the door is set for a future date than the key expiration, the access will be denied according with the key expiration date.



**Figure 98: Edit Days Period dialog box**

#### 6. 3. 3. 2. User Access Levels

See *User Access Levels* for a definition and information about how to create and configure a user access level. To associate a user with a user access level, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.

Double-click the user name that you want to associate with a user access level. The **User** information screen is displayed.

Click **User Access Levels** in the sidebar. The **User access levels** dialog box is displayed.

Note that the dialog box will be blank because you have not yet associated a user access level with this particular user.

Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of user access levels, is displayed.

Select the required user access level in the left-hand panel and click the chevron. The selected user access level is displayed in the right-hand panel.

Highlight the **Access Level** and click **Edit**. In Days period, **Same as key** is selected by default. It means the user will have access to the access level while the key is valid.

Select **Use the following days period** if you want the user to have access to that specific access point only during a period of time. Select a **Start date** and an **End date**.

Click **Accept**. The user access level is now associated with the user.

**NOTE:** The key validity takes precedence over the **Access Level** access. If the access to the access level is set for a future date than the key expiration, the access will be denied according with the key expiration date.

#### 6. 3. 3. 3. Zones

See *Zones* for a definition and information about how to create and configure a zone. To associate a user with a zone, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.

Double-click the user name that you want to associate with a zone. The **User** information screen is displayed. Click **Zones** in the sidebar. The **Zones** dialog box is displayed.

Note that the dialog box will be blank because you have not yet associated a zone with this particular user. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of zones, is displayed.

Select the required zone in the left-hand panel and click the chevron. The selected zone is displayed in the right-

hand panel.

Highlight the **Zone** and click **Edit**. In Days period, **Same as key** is selected by default. It means the user will have access to the zone while the key is valid.

Select **Use the following days period** if you want the user to have access to that specific access point only during a period of time. Select a **Start date** and an **End date**.

Click **Accept**. The zone is now associated with the user.

Note that you can also select which cardholder timetable is used. See *Access Points* for more information and a description of the steps you should follow.

**NOTE:** The key validity takes precedence over the **Zone** access. If the access to the zone is set for a future date than the key expiration, the access will be denied according with the key expiration date.

#### 6. 3. 3. 4. Outputs

See *Outputs* for a definition and information about how to create and configure an output. To associate a user with an output, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.

Double-click the user name that you want to associate with an output. The **User** information screen is displayed. Click **Outputs** in the sidebar. The **Outputs** dialog box is displayed.

Note that the dialog box will be blank because you have not yet associated an output with this particular user. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of outputs, is displayed.

Select the required output in the left-hand panel and click the chevron. The selected output is displayed in the

right-hand panel.

Click **Accept**. The output is now associated with the user.

#### 6. 3. 3. 5. Locations/Functions

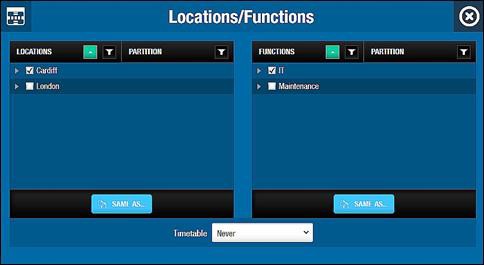
See *Locations* and *Functions* for definitions and information about how to create and configure a location and function.

To associate a user with a location/function, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.

Double-click the user name that you want to associate with a location/function. The **User** information screen is displayed.

Click **Locations/Functions** in the sidebar. The **Locations/Functions** dialog box is displayed.



**Figure 99: Locations/Functions dialog box**

Select the checkbox for the required location in the **Locations** panel. Select the checkbox for the required function in the **Functions** panel.

Select a cardholder timetable to be used from the **Timetable** drop-down list. Alternatively, you can select the

**Always** or **Never** drop-down list option.

The option you select is applied to both the selected location and function. You cannot select a different option for both. The **Always** option is selected by default. This means that the user always has access to the location and function, as you have not specified a timetable. If you select **Never**, they do not have access to the location or the function at any time.

For systems with a lot of functions and/or locations it’s possible to filter by Location or Function name and also by status “Selected” or “not Selected”.



# 6. 4. User Access Levels

User access levels are used to define a group of users with the same access permissions, for example, all staff in a department or all managerial staff. This means that if you are configuring a door entry on the **Door** information screen, you can allow access permissions for that door to all users who belong to a specific user access level.

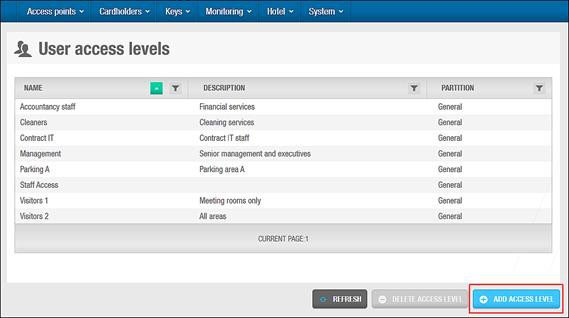
Without user access levels, you would have to associate each individual user with that particular door. The following sections describe how to create and configure a user access level.

**NOTE:** User access levels allow you to group users for easier access management. Unlike zones, user access levels do not save memory space on a key.

## 6. 4. 1. Creating User Access Levels

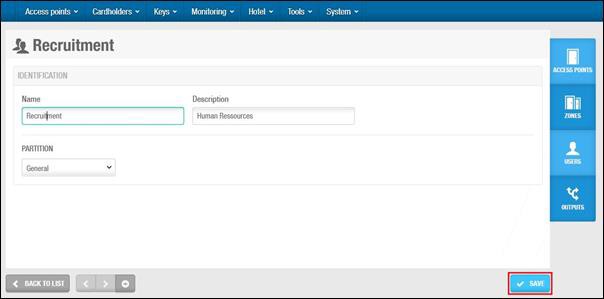
To create a user access level, perform the following steps:

1. Select **Cardholders** > **User Access Levels**. The **User access levels** screen is displayed.



**Figure 100: User access levels screen**

Click **Add Access Level**. The **User access level** information screen is displayed.



**Figure 101: User access level information screen**

Type a user access level name in the **Name** field.

Type a description for the user access level in the **Description** field. Select the relevant partition from the **Partition** drop-down list, if required.

See *Partitions* for more information. Click **Save**.

## 6. 4. 2. Associating User Access Levels

After you have created a user access level, you must associate access points, zones, users, and outputs with the specified user access level. The following sections describe how to associate user access levels with the various entries.

#### 6. 4. 2. 1. Access Points

See *Access Points* for definitions and information about how to create and configure the various types of access points.

To associate a user access level with an access point, perform the following steps:

1. Select **Cardholders** > **User access levels**. The **User access levels** screen is displayed.

Double-click the user access level that you want to associate with an access point. The **User access level**

information screen is displayed.

Click **Access Points** in the sidebar. The **Access points** dialog box is displayed.

Note that the dialog box will be blank because you have not yet associated an access point with this particular user access level.

Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.

Select the required access point in the left-hand panel and click the chevron. The selected access point is displayed in the right-hand panel.

Click **Accept**. The user access level is now associated with the access point.

Note that you can also select which cardholder timetable is used. See *Access Points* for more information and a description of the steps you should follow.

#### 6. 4. 2. 2. Zones

See *Zones* for a definition and information about how to create and configure a zone. To associate a user access level with a zone, perform the following steps:

1. Select **Cardholders** > **User access levels**. The **User access levels** screen is displayed.

Double-click the user access level that you want to associate with a zone. The **User access level** information screen is displayed.

Click **Zones** in the sidebar. The **Zones** dialog box is displayed.

Note that the dialog box will be blank because you have not yet associated a zone with this particular user access level.

Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of zones, is displayed.

Select the required zone in the left-hand panel and click the chevron. The selected zone is displayed in the right- hand panel.

Click **Accept**. The user access level is now associated with the zone.

Note that you can also select which cardholder timetable is used. See *Access Points* for more information and a description of the steps you should follow.

#### 6. 4. 2. 3. Users

See *Users* for a definition and information about how to create and configure a user. To associate a user access level with a user, perform the following steps:

1. Select **Cardholders** > **User access levels**. The **User access levels** screen is displayed.

Double-click the user access level that you want to associate with a user. The **User access level** information screen is displayed.

Click **Users** in the sidebar. The **Users** dialog box is displayed.

Note that the dialog box will be blank because you have not yet associated a user with this particular user access level.

Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.

Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right- hand panel.

Click **Accept**. The user access level is now associated with the user.

#### 6. 4. 2. 4. Outputs

See *Outputs* for a definition and information about how to create and configure an output. To associate a user access level with an output, perform the following steps:

1. Select **Cardholders** > **User access levels**. The **User access levels** screen is displayed.

Double-click the user access level that you want to associate with an output. The **User access level** information screen is displayed.

Click **Outputs** in the sidebar. The **Outputs** dialog box is displayed.

Note that the dialog box will be blank because you have not yet associated an output with this particular user access level.

Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of outputs, is displayed.

Select the required output in the left-hand panel and click the chevron. The selected output is displayed in the right-hand panel.

Click **Accept**. The user access level is now associated with the output.

# 6. 5. Limited Occupancy Groups

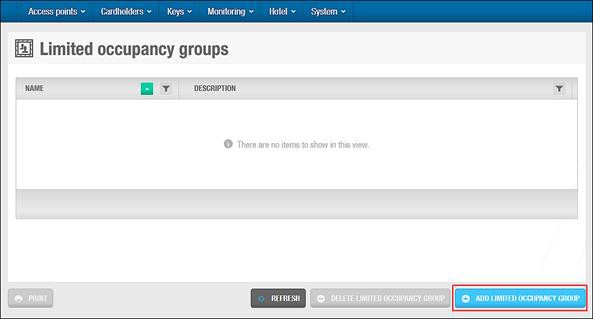
A limited occupancy group is a group of users who require access to a specified limited occupancy area, for example, a restricted car park. See *Limited Occupancy Areas* for information about limited occupancy areas.

The limited occupancy functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

## 6. 5. 1. Creating Limited Occupancy Groups

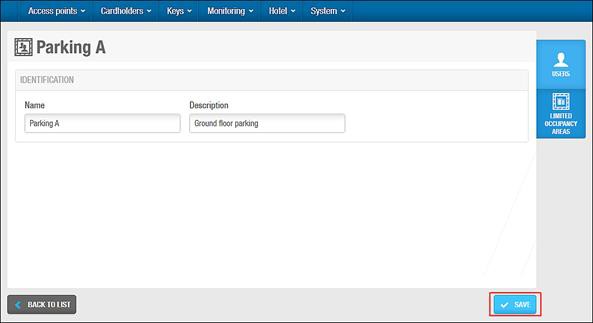
To create a limited occupancy group, perform the following steps:

1. Select **Cardholders** > **Limited occupancy groups**. The **Limited occupancy groups** screen is displayed.



**Figure 102: Limited occupancy groups screen**

Click **Add Limited Occupancy Group**. The **Limited occupancy group** information screen is displayed.



**Figure 103: Limited occupancy group information screen**

Type a name for the limited occupancy group in the **Name** field.

Type a description for the limited occupancy group in the **Description** field. Click **Save**.

## 6. 5. 2. Associating Limited Occupancy Groups

Once you have created a limited occupancy group, you must associate users and limited occupancy areas with that limited occupancy group. The following sections describe how to associate limited occupancy groups with the various entries.

#### 6. 5. 2. 1. Users

To associate a user with a limited occupancy group, perform the following steps:

1. Select **Cardholders** > **Limited occupancy groups**. The **Limited occupancy groups** screen is displayed. Double-click the limited occupancy group that you want to associate with a user. The **Limited occupancy group** information screen is displayed.

Click **Users** in the sidebar. The **Users** dialog box is displayed.

Note that the dialog box will be blank because you have not yet associated a user with this particular limited occupancy group.

Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.

Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right- hand panel.

Click **Accept**. The limited occupancy group is now associated with the user.

**NOTE:** You can also add users to limited occupancy groups by selecting the required limited occupancy group in the **Limited Occupancy Group** panel on the **User** information screen.

#### 6. 5. 2. 2. Limited Occupancy Areas

To associate a limited occupancy area with a limited occupancy group, perform the following steps:

1. Select **Cardholders** > **Limited occupancy groups**. The **Limited occupancy groups** screen is displayed. Double-click the limited occupancy group that you want to associate with a limited occupancy area. The **Limited occupancy group** information screen is displayed.

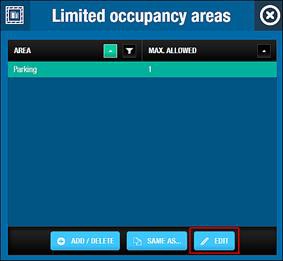
Click **Limited Occupancy Areas** in the sidebar. The **Limited occupancy areas** dialog box is displayed.

Note that the dialog box will be blank because you have not yet associated a limited occupancy area with this particular limited occupancy group.

Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of limited occupancy areas, is displayed. Select the required limited occupancy area in the left-hand panel and click the chevron. The selected limited occupancy area is displayed in the right-hand panel.

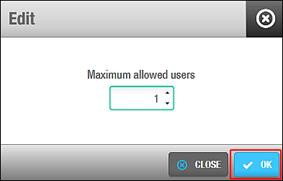
Click **Accept**. The limited occupancy group is now associated with the limited occupancy area.

Select the limited occupancy area in the **Limited occupancy areas** dialog box if you want to change the maximum number of users allowed in the area. The default number of users is 1.



**Figure 104: Limited occupancy areas dialog box**

Click **Edit**. The **Edit** dialog box is displayed.



**Figure 105: Edit dialog box**

Select the maximum number of users allowed using the up and down arrows. Alternatively, you can type the appropriate number in the **Maximum allowed users** field.

Click **OK**.