//USER MANUAL

SALTO SPACE |
Access Control Software
Management Innovations

ProAccess SPACE Version 2.0

Manual Version 3.0

SALTO SPACE

SALTO
inspiredaccess

MAN-SOFT-SPACE-04-14

TABLE OF CONTENTS

1. INTRODUCTION

This chapter contains the following sections:

1. 1. About this Manual

This manual is a guide for system administrators (operators with administration rights, generally referred to in this manual as admin operators) as well as day-to-day users of the SALTO ProAccess application. It describes the installation procedures for the SALTO system components, as well as how to set up, configure, and use the various features of ProAccess SPACE.

1. 2. Intended Audience

This manual is aimed at organizational staff responsible for site access control, who use ProAccess SPACE on a regular basis. Organizations are defined as hotel or non-hotel sites such as universities.

Routine access tasks such as assigning and deleting of keys, and check-in and check-out are usually performed by a standard (non-admin) operator. The admin operator is generally responsible for higher administrative functionality such as installation and configuration tasks.

1. 3. Manual Roadmap

This manual is divided into the following chapters:

To check which chapters in the manual are relevant to your role, you can refer to the following table.

Table 1: Chapter relevance

Chapter	Non-Hotel Admin Operator	Non-Hotel Operator	Hotel Admin Operator	Hotel Operator
Introduction	Yes	Yes	Yes	Yes
System Overview	Yes	Yes	Yes	Yes
Installation	Yes		Yes	
Getting Started	Yes	Yes	Yes	Yes
Access Points	Yes	Yes	Yes	
Cardholders	Yes	Yes	Yes	
Visitors	Yes	Yes	Yes	
Hotels			Yes	Yes
Keys	Yes	Yes	Yes	Yes
Monitoring	Yes	Yes	Yes	
ProAccess SPACE Configuration	Yes		Yes	
ProAccess SPACE Tools	Yes		Yes	
ProAccess SPACE System Configuration	Yes	Yes	Yes	
ProAccess SPACE General options	Yes	Yes	Yes	
Peripherals	Yes		Yes	
Glossary	Yes	Yes	Yes	Yes

2. SYSTEM OVERVIEW

This chapter contains the following sections:

2. 1. About ProAccess

SALTO ProAccess is an access control management system that is used to manage online and offline access points. An operator with administration rights configures entries such as access points and users to control access to a site. Other operators can then manage access permission changes within the system.

2. 1. 1. SALTO Virtual Network

The SALTO Virtual Network (SVN) uses access control technology that was developed to solve stand-alone access control problems. Access control data is put on an encrypted radio frequency identification (RFID) card, rather than a stand-alone lock. Cards can then be updated anywhere in the building by using an SVN wall reader. The SVN removes the need to hardwire every door. If the online connection is interrupted, the battery-powered locks can continue to work offline.

2. 1. 2. SALTO Data-on-Card

SALTO data-on-card means access data is stored on each RFID card (referred to in the applications and in this manual as a 'key') rather than on the lock as in other access systems. The advantage of this is that the keys can be used to collect and circulate access data throughout a site as a user moves around. This functionality allows you to add or remove a user's access permissions to SALTO access points that are offline without having to visit the door. When a user presents their key to an SVN wall reader, changes in their access permissions are retrieved from the SALTO database and written to the key.

2. 1. 3. Transferring and Updating Access Information

When a user joins an organization, they are presented with a key with their appropriate access permissions. However, these permissions can change frequently and keys may become quickly out of date.

In the SALTO system, access information is transferred from the operator's PC to an online wall reader. When a user presents their key to the SVN wall reader, the latest up-to-date access information is automatically transferred to the key. As the key is used to access doors throughout a building, it updates each door's blacklist – see *About Blacklists* for more information. At the same time, the lock transfers information such as audit trail events and, if the battery is low, the lock battery status. When the user presents their key to an online wall reader again, the wall reader uploads the new information back to the system. In this way, access information is continually updated and circulated throughout the site.

2. 2. SALTO Network Components

The SALTO network typically consists of the following components: the SALTO server, client PCs, SALTO peripherals, and access point devices. The following diagram shows the relationship between these components.

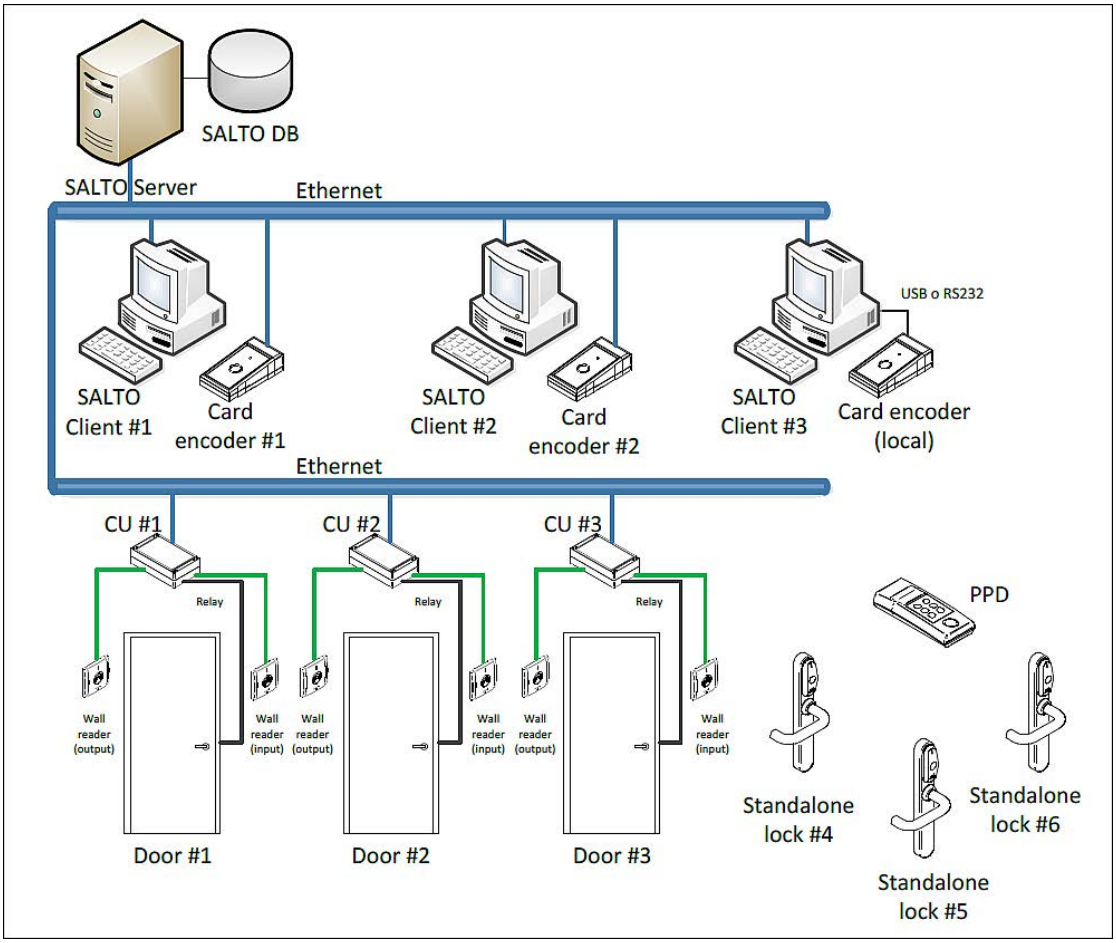
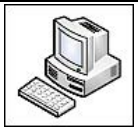
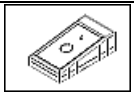
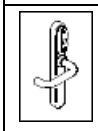
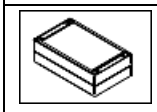


Figure 1: Relationship between SALTO components

The network components are described in the following table.

Table 2: Component icons

Icon	Description
 SALTO server	Contains the SALTO Service and the SQL database (SQL DB). See *SALTO Service* and *SQL Server and Database* for more information. It manages and controls, in real-time, all SALTO online devices, for example, online doors that are operated using radio frequency (RF) technology. It also processes requests from SALTO clients.
 SALTO client	Runs client applications, for example, ProAccess SPACE and the Local IO Bridge. See *ProAccess SPACE* and *Local IO Bridge* for more information.
 Card encoder	Writes access permissions onto cards (keys). A card encoder is an external device that reads and updates keys with access information. Encoders can be enabled for USB or Ethernet connections.

Icon	Description
 Standalone electronic escutcheon and cylinder	Allows or denies access, based on the permissions of the presented key. These access point devices are offline and battery-powered. However, they can be equipped with RF technology to allow online capability.
 Portable Programming Device (PPD)	Communicates information to the lock such as door identification and configuration details. This device, which can be physically connected to a lock, is used to initialize and update offline doors. See *PPD* for more information.
 Online control unit (CU)	Provides real-time access control. Managed by the SALTO server, the CU works as both an online IP door and as a card updater.

2. 3. ProAccess System Components

The system is composed of five components:

- ProAccess SPACE
- SQL Server and database
- SALTO Service (and the ProAccess SPACE Configurator that controls it)
- Local IO Bridge
- Card Printing

The following diagram shows the various components of the SALTO system.

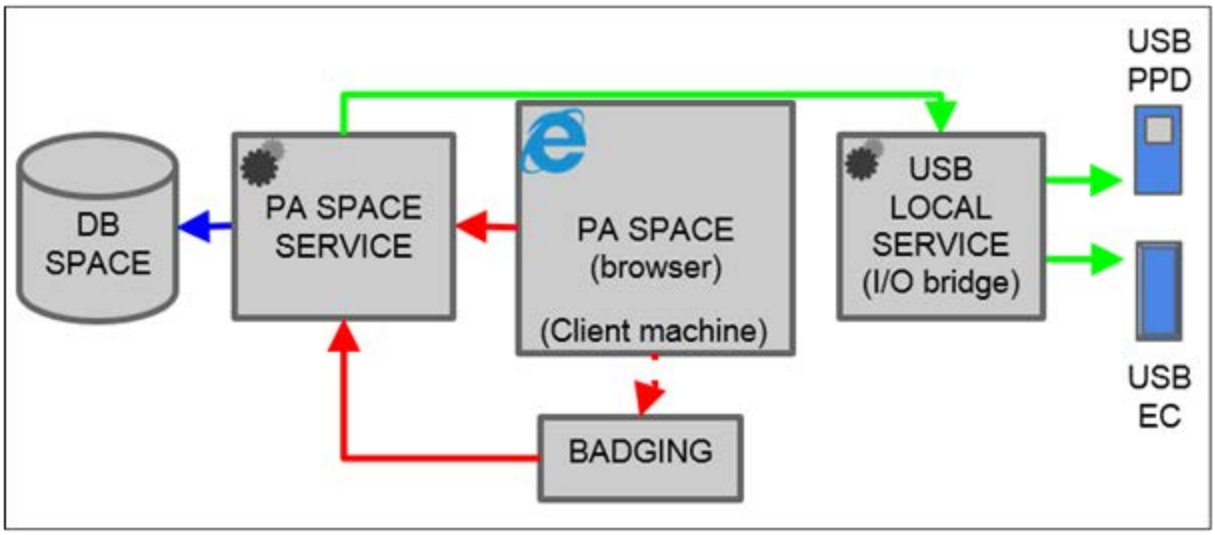


Figure 2: SALTO system

NOTE: All of the components in this figure represent SALTO components except for the Property Management System (PMS) and the Software Integration. Badging is embedded in ProAccess SPACE, but it is only added to the software if this license option is selected.

These components are described in the following sections.

2. 3. 1. ProAccess SPACE

ProAccess SPACE is an online access control management application. It contains the menus that allow admin operators and other operators to set up user profiles, add and delete access points, customize company calendars, obtain audit trails etc.

These menus and functionality are only available where all the appropriate licensing options are selected. See *Registering and Licensing SALTO Software* for more information. To activate particular functionality in ProAccess SPACE, you may also have to enable a specific parameter in ProAccess SPACE General Options. See ***Error! Reference source not found.*** for more information about enabling parameters.

The main menu options are described in the following table.

Table 3: ProAccess SPACE main menu options

Menu Item	Option
Access points	▪ Doors ▪ Lockers ▪ Rooms ▪ Zones ▪ Locations ▪ Functions ▪ Outputs ▪ Lockdown areas ▪ Limited occupancy areas ▪ Roll-call areas ▪ Access point timed periods ▪ Access point automatic changes
Cardholders	▪ Users ▪ Visitors ▪ Guests ▪ User access levels ▪ Visitor access levels ▪ Guest access levels ▪ Limited occupancy groups ▪ Cardholder timetables
Keys	▪ Read key ▪ Visitor check-in ▪ Visitor check-out ▪ Delete key ▪ Reset locker data ▪ Automatic key update
Monitoring	▪ Audit trail ▪ Online monitoring ▪ Lockdown monitoring ▪ Limited occupancy monitoring ▪ Roll-call monitoring

Menu Item	Option
Hotel	▪ Room status ▪ Check-in ▪ Check-in groups ▪ Check-out ▪ Copy guest key ▪ Cancellation of guest lost keys ▪ One shot key ▪ Programming & spare keys ▪ Edit guest cancelling key ▪ Edit room cleaner key
Tools	▪ Scheduled jobs ▪ Synchronization ▪ Make DB Backup ▪ Event streams ▪ Card printing
System	▪ System auditor ▪ Operators ▪ Operator groups ▪ Partitions ▪ PPD ▪ SALTO network ▪ Calendars ▪ Time zones ▪ General options ▪ SAM & Issuing options ▪ PMS Authorizations ▪ System resources

2. 3. 2. SQL Server and Database

The SQL Server and SQL database (SQL DB) are used to host and manage the SALTO database. This database contains all the access control system information such as user permissions, locking plans, and key data.

2. 3. 3. SALTO Service

The SALTO Service is a Windows service that manages communication between the peripherals, ProAccess SPACE, the database, and any software integrations. It is controlled using the ProAccess SPACE Configurator.

The ProAccess SPACE Configurator is a desktop application used to set up communication between the various components of the SALTO system. It is also used to start and stop the SALTO Service.

NOTE: The SALTO Service remains running in the background. It should not be stopped except for maintenance purposes as ProAccess SPACE will not work without it. Peripherals can continue to operate as stand-alone or offline devices but will not be able to communicate with the database unless the SALTO Service is restarted.

2. 3. 4. Local IO Bridge

The Local IO Bridge is a Windows service. It allows USB devices to be used with ProAccess SPACE by creating a link between the USB device and the browser. The Local IO Bridge must be installed on any client PCs you intend to use with a USB encoder or PPD. See *Encoders* and *PPD* for more information.

3. INSTALLATION

This chapter contains the following sections:

3. 1. About Installing

This chapter describes how to install and configure the software components required to access and use the SALTO system. You need to perform two separate installation processes:

- ProAccess SPACE (which includes the installation of the SALTO Service and the ProAccess SPACE Configurator)
- Local IO Bridge (which you can download from within ProAccess SPACE)

3. 2. Installation Process

The installation process should be performed in the following order by an operator with admin rights, referred to here as the admin operator:

1. **Installation prerequisites are checked**

   The admin operator checks that the correct hardware and software requirements are met before beginning the installation process.
2. **SALTO installation files are obtained**
   a) The admin operator (or other appropriate manager) selects the appropriate licensing options as part of purchasing the SALTO software.
   b) The admin operator registers the SALTO software serial number on the SALTO website.
   c) The admin operator downloads the SALTO software.
3. **SALTO software components are installed**
   a) The admin operator installs ProAccess SPACE.
   b) The admin operator installs the Local IO Bridge.

3. 3. Installation Prerequisites

The following tables outline the minimum hardware and system requirements for the SALTO server and client applications. The client applications are: ProAccess SPACE and the Local IO Bridge.

Table 4: Minimum hardware and system requirements for the SALTO server

Component	Requirement
RAM	4 GB
Processor	1 GHz or higher
Display	1024 x 768 high-colour 32-bit display
Hard Disk Space	10 GB This is the recommended required space to operate a database in a large organization
Operating System	Windows Vista, Windows 7,Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2008R2, or Windows Server 2012 (32-bit and 64-bit)
MS SQL Server	Versions 2005, 2008, 2008R2, 2012, 2014, or LocalDB (all editions, including MS-SQL Express). Note that if the SALTO database was originally created with MS SQL Server 2000 and later migrated to a higher version, you must ensure that the database is in compatibility level 90 (version 2005) or higher.
Machine Name Resolver	Domain Name System (DNS)
Domain Environment	A shared network is required and the domain or work group must be set up by the organization's IT administrator. This is strongly recommended as it simplifies security and permission issues.

Table 5: Minimum hardware and system requirements for ProAccess SPACE

Component	Requirement
RAM	1 GB
Processor	1.6 GHz or higher (x 86 or x 64)
Operating System	Windows Vista (32-bit and 64-bit) or higher
.NET Framework	Version 4.0.2 (included with the installation file)
Plugin	Silverlight 5
Web Browser	Microsoft Internet Explorer (9 or higher) Due to its compatibility with Silverlight, Microsoft Internet Explorer is the only browser recommended for use with ProAccess SPACE.

3. 4. Registering and Licensing SALTO Software

To obtain your SALTO software, you must first purchase it and select the appropriate license options as part of this process. You must then register it on the SALTO website in order to download the required installation files. See *Downloading SALTO Software* for more information about how to register and download the software.

If you need to change your licensing options after registration, you can contact your SALTO representative to do this. You can then update your installation from within ProAccess SPACE to match the new licensing options. See *Updating SALTO Software Licenses* for more information.

3. 5. Downloading SALTO Software

To obtain SALTO software, you must first register the unique SALTO software serial number, received when the SALTO software was purchased, and create a personal password.

To register for your SALTO software, perform the following steps:

1. Register your SALTO software serial number on the SALTO registration site:
   http://softwarearea.saltosystems.com/usuarios/inicio_insertar.php?id=en
2. Type your personal details in the appropriate fields and complete all mandatory fields.
3. Note your personal password.
4. Click **Send**.
   SALTO sends a validation email to the email address you provided.
5. Click the link in the validation email to open the SALTO User Access webpage:
   http://softwarearea.saltosystems.com/usuarios/index.php?id=en
6. Click **Send**.
7. Download the ZIP file containing ProAccess SPACE.

3. 6. Installing SALTO Software Components

To set up the SALTO software system, you need to install three separate files:

- **Setup_ProAccessSpace.exe**: This installs ProAccess SPACE, the ProAccess SPACE Configurator, and the SALTO Service.
- **Setup_SaltoLocalIOBridge:** This installs the Local IO Bridge.
- **Setup_CardPrintingSpace.exe:** This installs Card Printing.

NOTE: Installation instructions are also available within the ProAccess SPACE installation folder (SALTO\ProAccess Space\docs).

3. 6. 1. Installing ProAccess SPACE

ProAccess SPACE, the SALTO Service, and the ProAccess SPACE Configurator are installed together from the one installation file. The ProAccess SPACE installation procedure covers the installation for all of them.

To install ProAccess SPACE, perform the following steps:

1. Unzip the ProAccess SPACE installation file.
2. Right-click the Setup_ProAccessSpace.exe file.

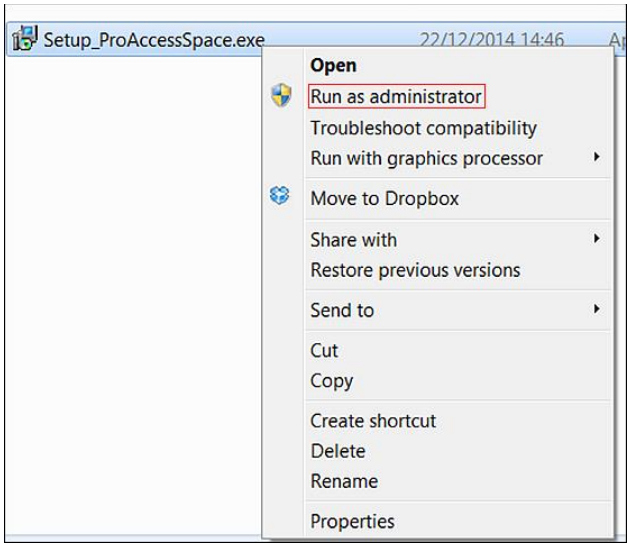


Figure 3: Run as administrator

3. Select **Run as administrator**.
4. Click **Yes** when prompted with the following message:

   Do you want to allow the following program from an unknown publisher to make changes to this computer?

   The initial installation dialog box is displayed.
5. Click **next**. The **license agreement** dialog box is displayed.

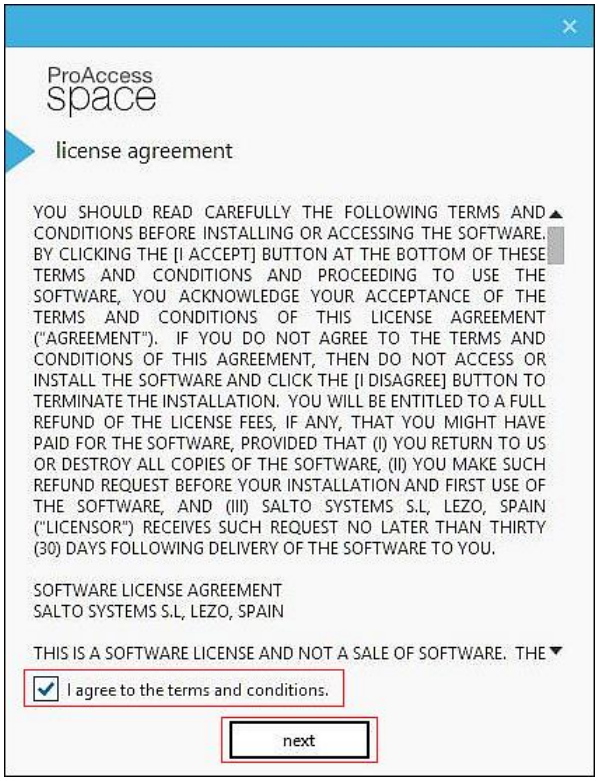


Figure 4: License agreement dialog box

6. Select **I agree to the terms and conditions** and click **next**. The **destination folder** dialog box is displayed.

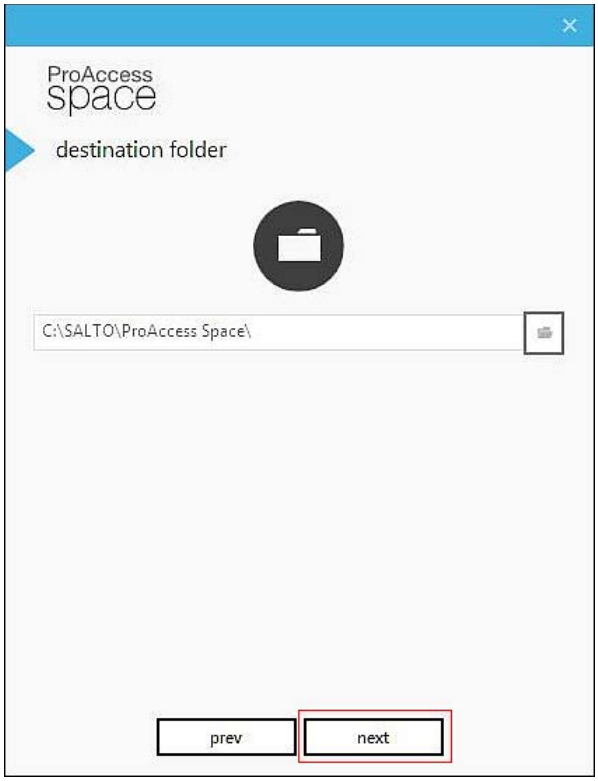


Figure 5: Destination folder dialog box

7. Choose a different location or accept the suggested installation destination folder.
8. Click **next**. The **configure data backend** dialog box is displayed.

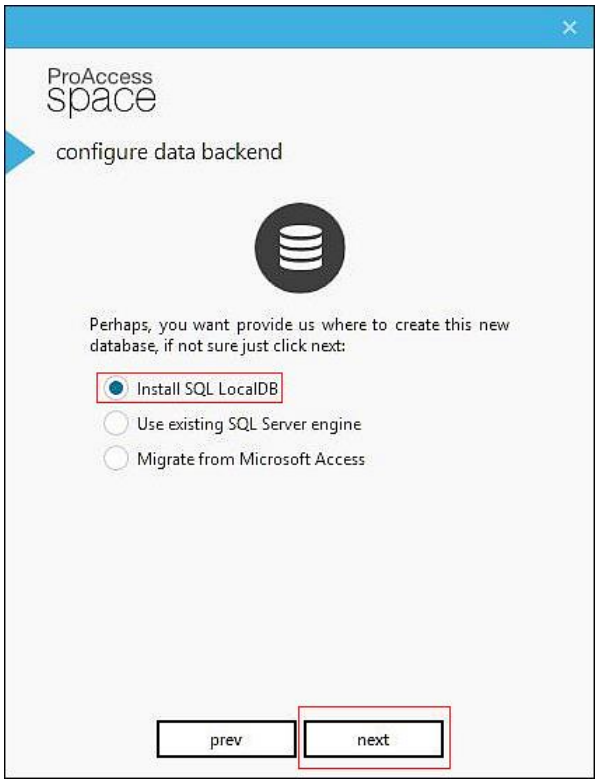


Figure 6: Configure data backend dialog box

9. Select **Install SQL LocalDB**.
   In these steps, it is assumed that you are installing ProAccess SPACE for the first time and that you are selecting the default option of using the SQL LocalDB. However, if you are intending to select an alternative database (or create a new one) from an existing SQL Server engine as part of the installation process, see *Using an Existing SQL Server Engine* for more information.
   If you are intending to migrate data from a Microsoft (MS) Access database as part of the installation process, see *Migrating Data from a Microsoft Access Database* for more information. See ***Error! Reference source not found.*** for more information.
10. Click **next**. The **activate software** dialog box is displayed.

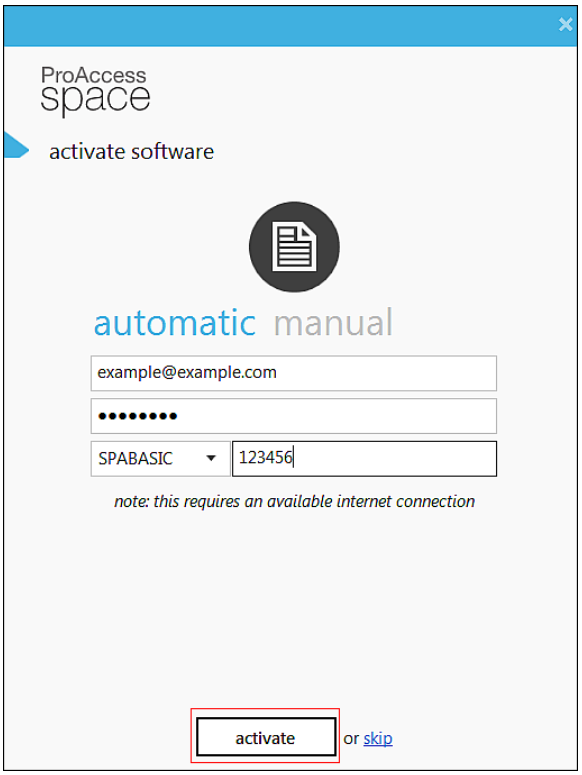


Figure 7: Activate software dialog box

11. Type the email address and password you used to register.
    Note that you can register using the **manual** tab if you have already received the license data (.dat) file.
12. Select your license type from the drop-down list.
13. Type your serial number.
14. Click **activate**. The **Well done!** screen, confirming that ProAccess SPACE is installed, is displayed.

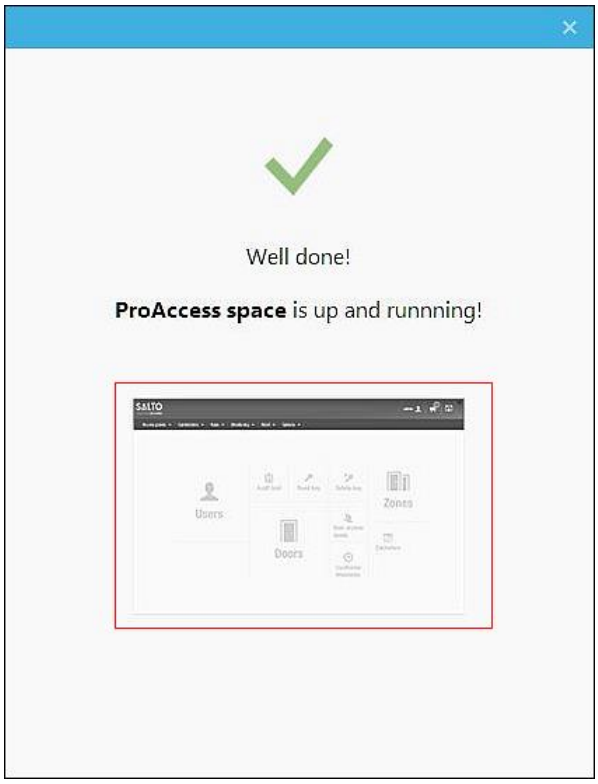


Figure 8: Installation confirmation

You can click the quick-access tile to start using ProAccess SPACE.

3. 6. 1. 1. Using an Existing SQL Server Engine

After you select the installation destination folder in Step 7 of *Installing ProAccess SPACE*, the **configure data backend** dialog box is displayed.

You can choose to use an existing SQL server engine in one of two ways:

- Use an existing database for the installation.
- Create a new database for the installation.

Using an Existing Database

To install ProAccess SPACE using an existing database, perform the following steps:

1. Select **Use existing SQL Server engine**.

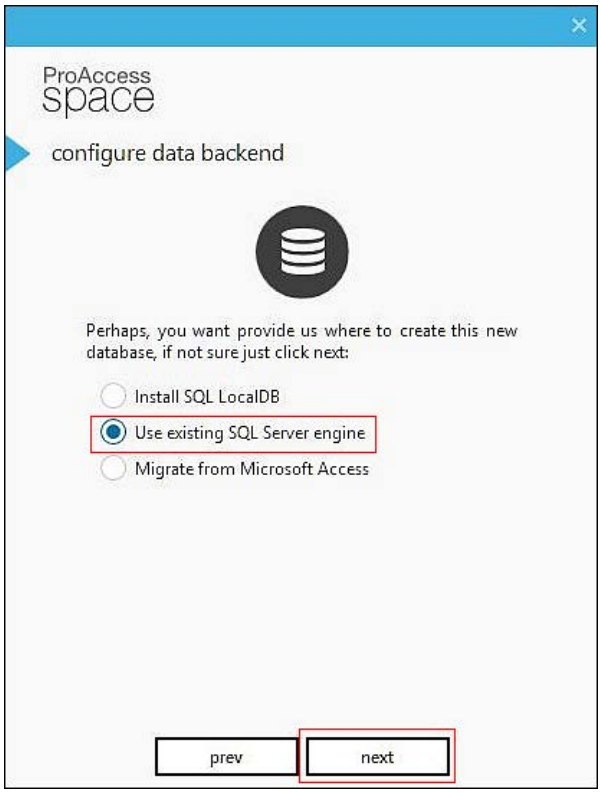


Figure 9: Use existing SQL Server engine

2. Click **next**.

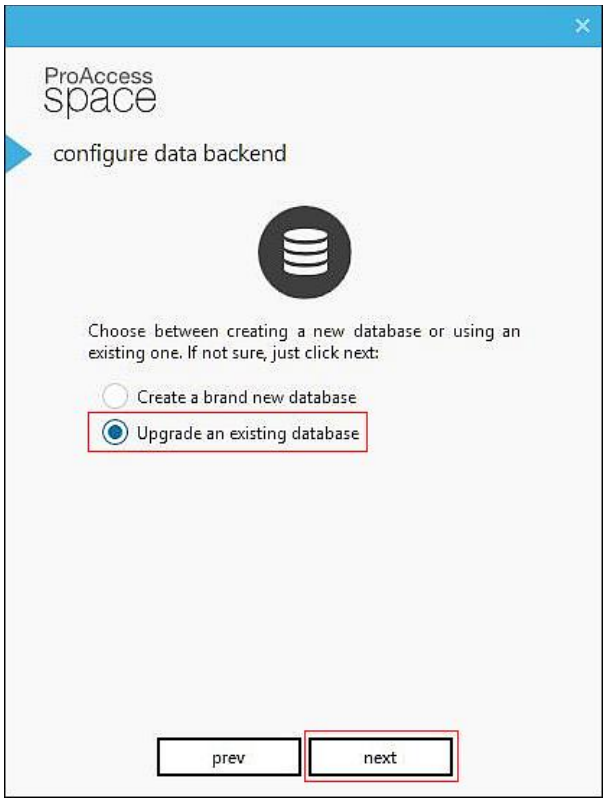


Figure 10: Upgrade an existing database

3. Select **Upgrade an existing database** and click **next**.

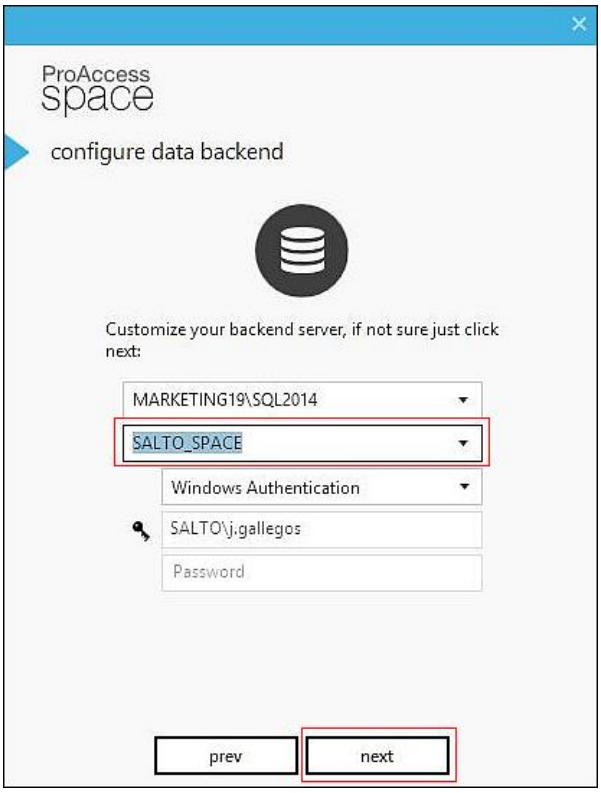


Figure 11: Select the SQL database

4. Select the applicable SQL database and enter the appropriate details.
5. Click **next**.
6. Follow Step 10 in *Installing ProAccess SPACE* to continue with the installation.

Creating a New Database

To install ProAccess SPACE using a new database, perform the following steps:

1. Select **Use existing SQL Server engine**.

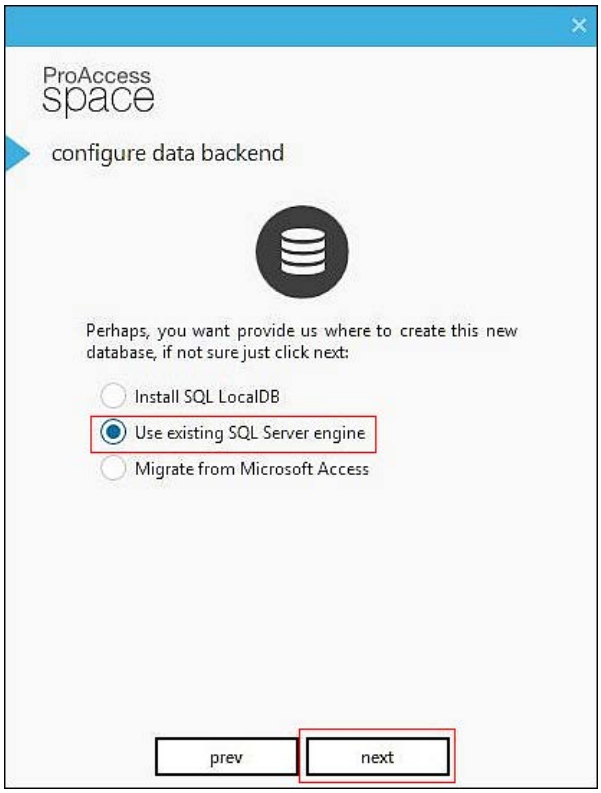


Figure 12: Use existing SQL Server engine

2. Click **next**.

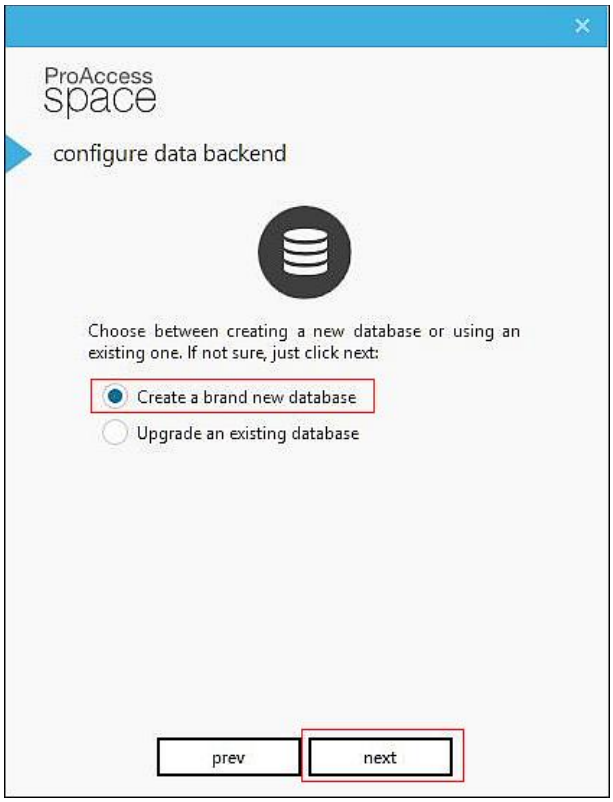


Figure 13: Create a brand new database

3. Select **Create a brand new database** and click **next**.

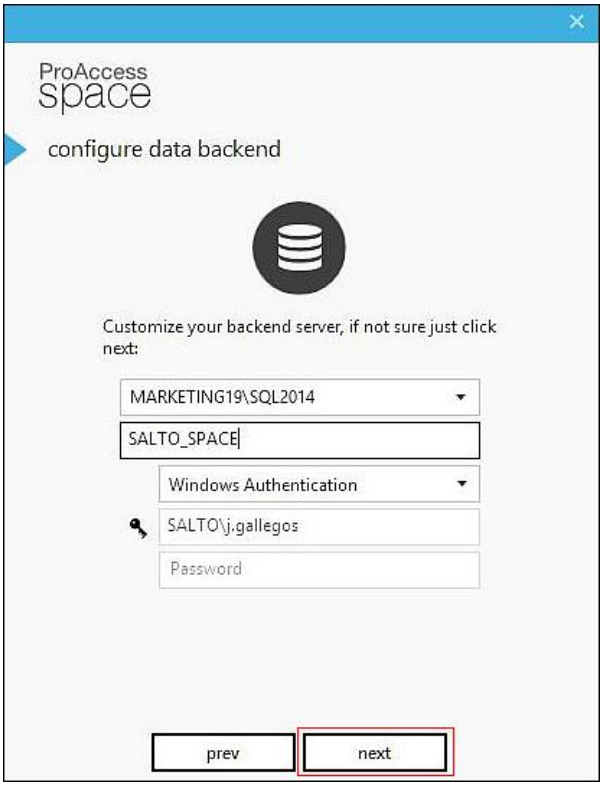


Figure 14: Existing SQL database details

4. Type the name of the new SQL database and enter the appropriate details.
5. Click **next**.
6. Follow Step 10 in *Installing ProAccess SPACE* to continue with the installation process.

3. 6. 1. 2. Migrating Data from a Microsoft Access Database

After you select the installation destination folder in Step 7 of *Installing ProAccess SPACE*, the **configure data backend** dialog box is displayed.

To install ProAccess SPACE by migrating data from an MS Access database, perform the following steps:

1. Select **Migrate from Microsoft Access**.

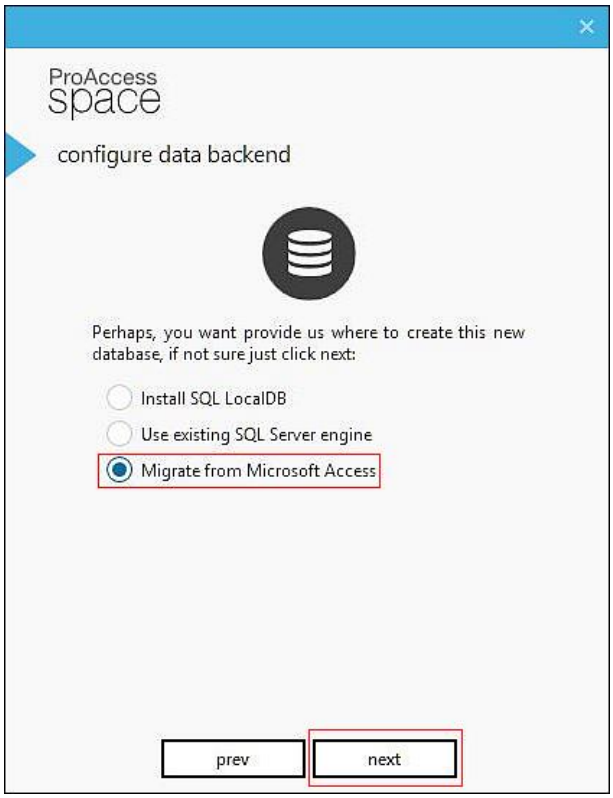


Figure 15: Migrate from Microsoft Access

2. Click **next**.

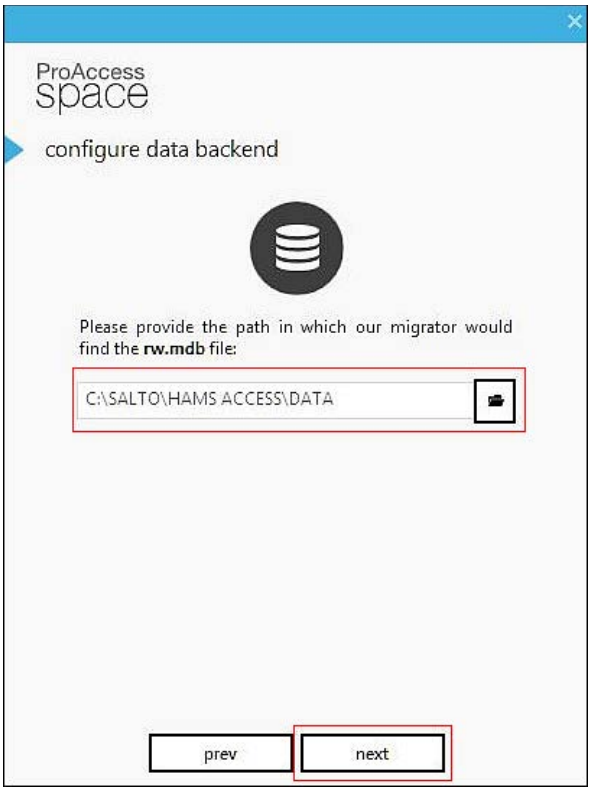


Figure 16: RW.mdb file location

3. Select the location of the rw.mdb file by clicking the folder icon.
4. Click **next**.

5. Follow Step 10 in *Installing ProAccess SPACE* to continue with the installation process.

3. 6. 2. Installing the Local IO Bridge

The Local IO Bridge must be installed on any client PCs you intend to use with a USB encoder or PPD. See *Local IO Bridge* for more information. The Local IO Bridge allows USB devices to be used with ProAccess SPACE by creating a link between the USB device and the browser.

To install the Local IO Bridge, you must first log in to ProAccess SPACE as an operator with admin rights. See *Logging In to ProAccess SPACE* for information about how to log in to ProAccess SPACE. The latest version of the Local IO Bridge can be installed from within ProAccess SPACE in two ways:

- From the **Settings** screen
- From the **About** dialog box

Figure 17: Accessing the Operator Settings screen and the About dialog box

3. 6. 2. 1. Installing from the Settings Screen

To install the Local IO Bridge from the **Settings** screen, perform the following steps:

1. Click **admin** (or other appropriate operator login) on the top right-hand side of the home screen. The **Settings** screen is displayed.

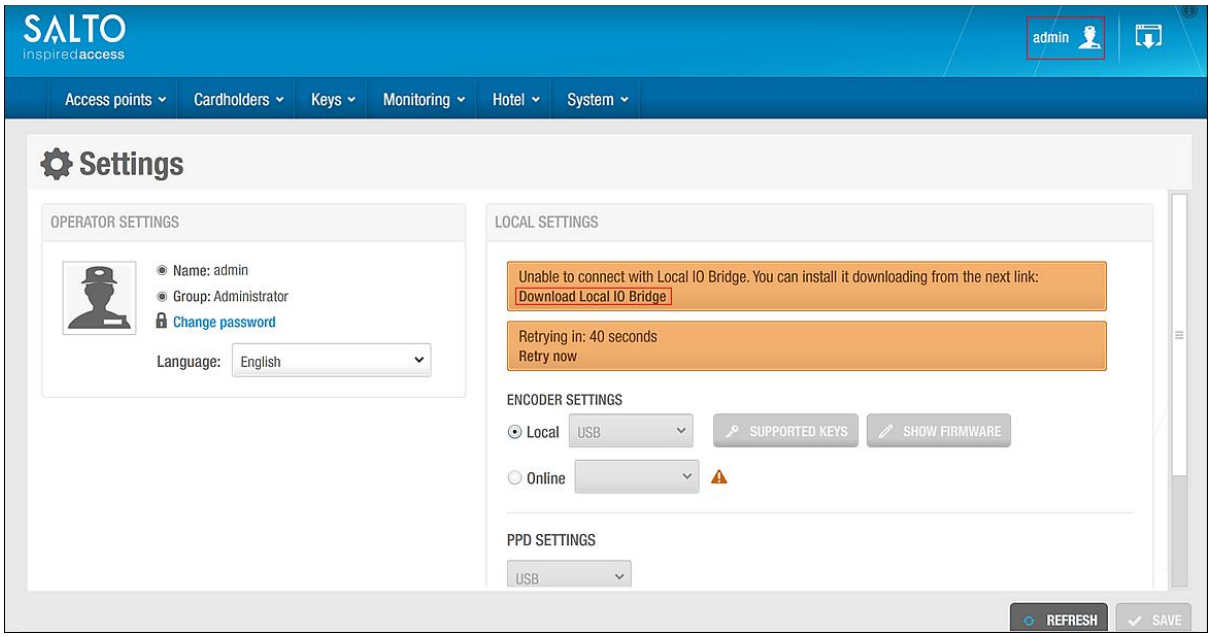


Figure 18: Settings screen

2. Click **Download Local IO Bridge**.
3. Click **Save** when prompted with the following message:

   Do you want to run or save Setup_SaltoLocalIOBridge.exe?
4. Save the Setup_SaltoLocalIOBridge.exe file to your computer and right-click it.

5. Select **Run as administrator**.
6. Click **Yes** when prompted with the following message:

   Do you want to allow the following program from an unknown publisher to make changes to this computer?

   The initial installation dialog box is displayed.
7. Click **next**. The **license agreement** dialog box is displayed.

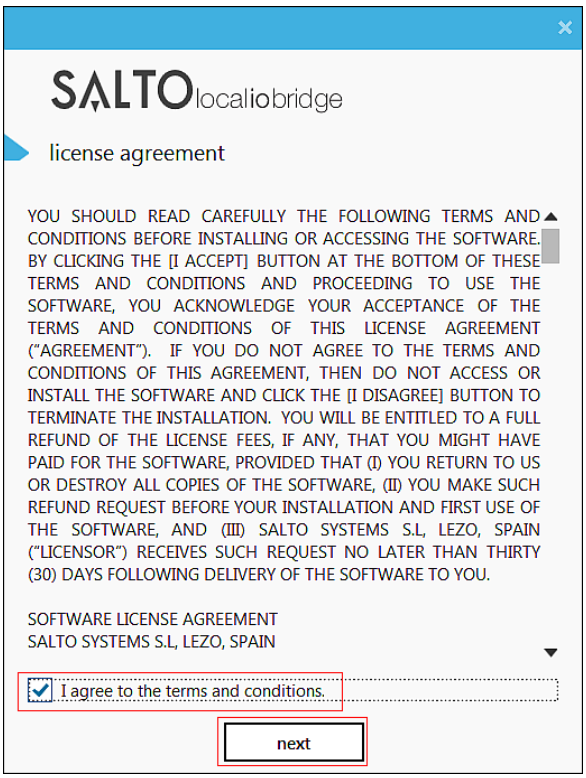


Figure 19: License agreement dialog box

8. Select **I agree to the terms and conditions**.
9. Click **next**. The **destination folder** dialog box is displayed.

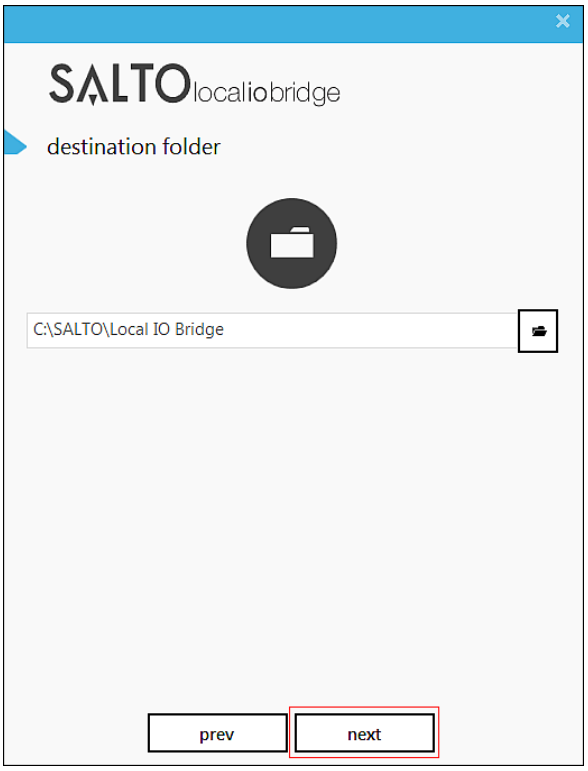


Figure 20: Destination folder dialog box

10. Choose a different location or accept the suggested installation destination folder.
11. Click **next**. The **succeeded** dialog box, confirming that the Local IO Bridge is installed, is displayed.

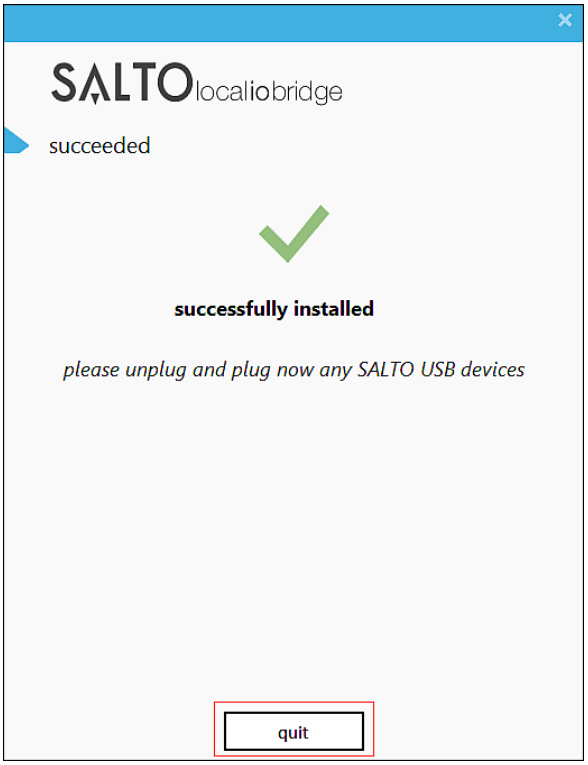


Figure 21: Installation confirmation

12. Click **quit.**

3. 6. 2. 2. Installing from the About Dialog Box

To install the Local IO Bridge from the **About** dialog box, perform the following steps:

1. Click the **About** icon on the top right-hand side of the home screen. The **About** dialog box is displayed.

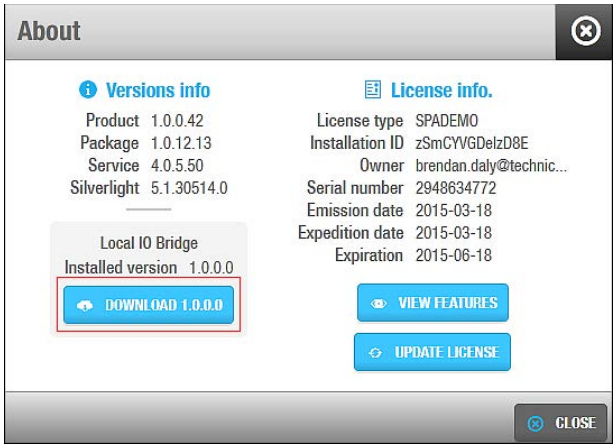


Figure 22: About dialog box

2. Click **Download**.

   Note that the text of the **Download** button varies slightly to reflect the latest available version of the Local IO Bridge.
3. Click **Save** when prompted with the following message:

   Do you want to run or save Setup_SaltoLocalIOBridge.exe?
4. Save the file to your computer and follow the steps in *Installing from the Settings Screen*.

3. 6. 3. Installing Card Printing

To install Card Printing, perform the following steps:

1. Go to **Tools** > **Card printing**. If Card printing was not installed before, the following link will show informing that Card printing is not installed and can be downloaded from the link.

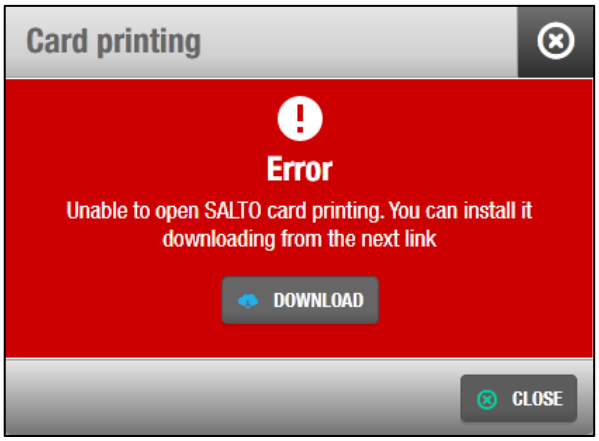


Figure 23: Language selection dialog box

2. Click **Save** when prompted with the following message:

Do you want to run or save Setup_**Setup_CardPrintingSpace.exe**?

3. Save the **Setup_CardPrintingSpace.exe** file to your computer and right-click it.
4. Select **Run as administrator**.

5. Click **Yes** when prompted with the following message:

   Do you want to allow the following program from an unknown publisher to make changes to this computer?

   The initial installation dialog box is displayed.

6. Click **next.** The **license agreement** dialog box is displayed.

Figure 24: License agreement dialog box

7. Select **I agree to the terms and conditions**.
8. Click **next**. The **destination folder** dialog box is displayed.

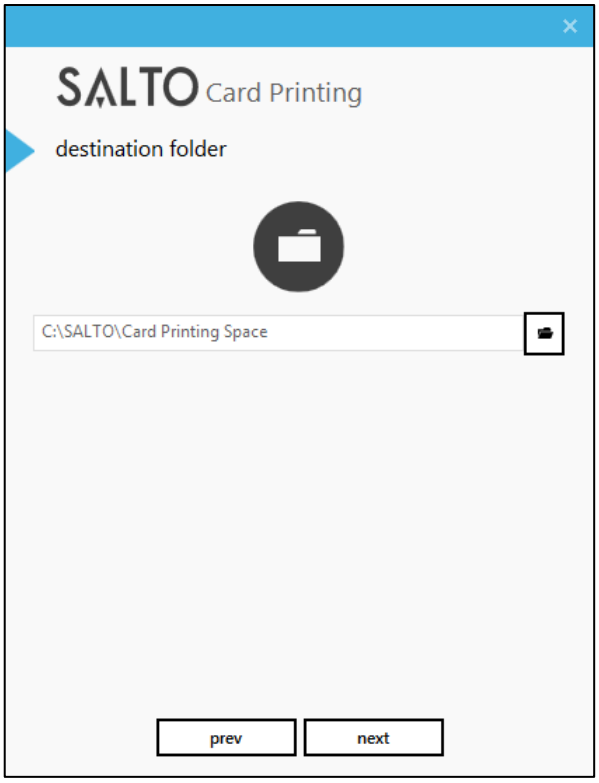


Figure 25: Destination folder dialog box

9. Choose a different location or accept the suggested installation destination folder.
10. Click **next**. The **succeeded** dialog box, confirming that the Card Printing is installed, is displayed.

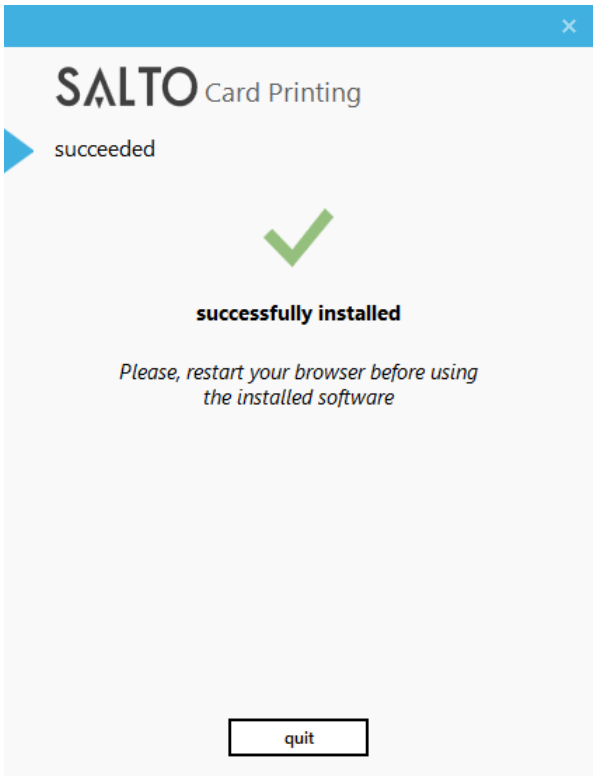


Figure 26: Installation confirmation

11. Click **quit.**

NOTE: You will find more information about how to use Card printing in *Card Printing Templates chapter* and *Using Card Printing Template*.

3. 7. Updating SALTO Software Licenses

Certain SALTO features, for example partitions and visitors, are license-dependent. This means that some functionality will not be enabled in your SALTO installation unless it is covered by your selected license options.

To view the features enabled for your license, perform the following steps:

1. Click the **About** icon on the top right-hand side of the home screen. The **About** dialog box is displayed.

Figure 27: About dialog box

2. Click **View Features**. The **Features** dialog box, listing all features, is displayed.

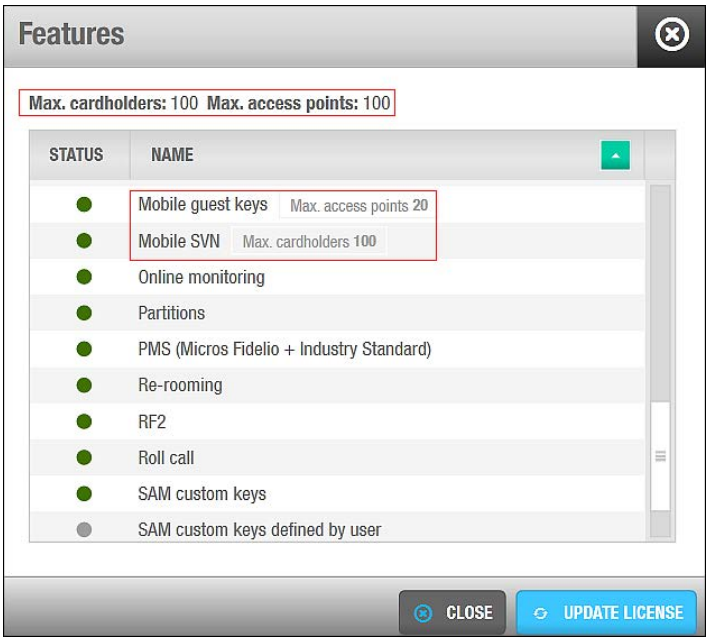


Figure 28: Features dialog box

Enabled features are denoted by a green circle in the **Status** column. Disabled features are denoted by a grey circle.

The **Features** dialog box also lists the license limitations for the following:

- Maximum number of cardholders
- Maximum number of access points
- Maximum number of access points for mobile guest keys
- Maximum number of access points for mobile SVN users who can update their keys with Near Field Communication (NFC) technology

To enable additional license-dependent features, contact your SALTO representative. When these changes are implemented for your registered account, you can update your installation in two ways:

- From the **About** dialog box
- From the **Features** dialog box

3. 7. 1. 1. Updating the License from the About Dialog Box

To update your license from the **About** dialog box, perform the following steps:

1. Click **Update License**. **The Update license** dialog box is displayed.

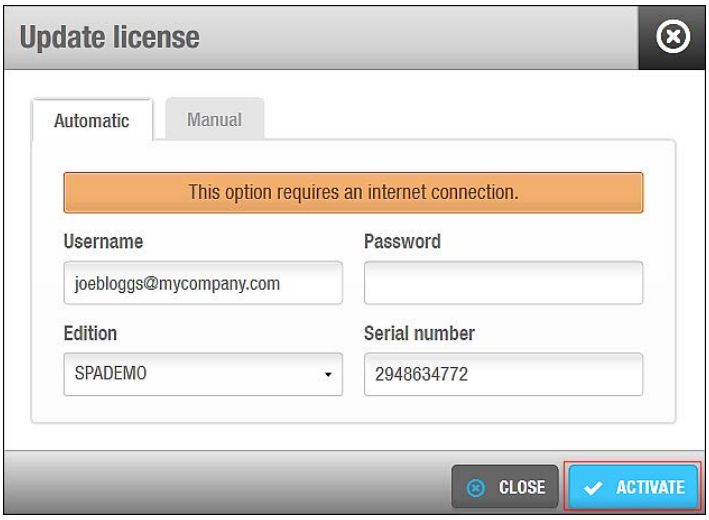


Figure 29: Update license dialog box

2. Type the username and password you entered at registration.

   Note that you can also update your license using the **manual** tab if you have already received the license data (.dat) file. Generally, this file will only be sent to you by a SALTO representative in cases where they are assisting you in testing or demonstrating functionality. This type of license data file has a specific expiration period.
3. Click **Activate**. ProAccess SPACE automatically checks the license status online and enables the applicable features in your database.

   Note that you must restart ProAccess SPACE for the changes to take effect.

3. 7. 1. 2. Updating the License from the Features Dialog Box

To update your license from the **Features** dialog box, click **Update License** and follow the steps in *Updating the License from the About Dialog Box*.

3. 8. Checking ProAccess SPACE Configuration

To check the configuration settings for ProAccess SPACE, perform the following steps:

1. Ensure that the appropriate database has been set up in ProAccess SPACE.
2. Double-click the **ProAccess SPACE Configurator** icon on your desktop. The ProAccess SPACE Configurator launches and the **Database** tab is displayed.

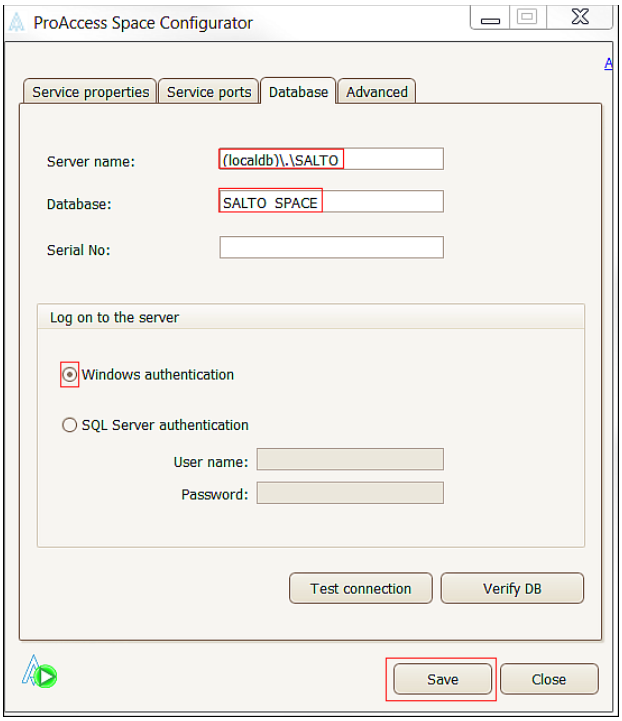


Figure 30: Database tab

3. Ensure the server name in the **Server name** field is correct. You can verify the data in Microsoft SQL Management Studio if installed.
4. Ensure the database name in the **Database** field is correct. You can verify the data in Microsoft SQL Management Studio if installed.
5. Ensure the **Windows authentication** option is selected if you are working in a Windows domain.

   If you are not working in a Windows domain, select the **SQL Server authentication** option. You must enter the appropriate SQL Server username and password.
6. Click **Save**.

   Note that the SALTO Service must be stopped to save any change on the **Service properties** tab and then restarted.
7. Click the **Service properties** tab.

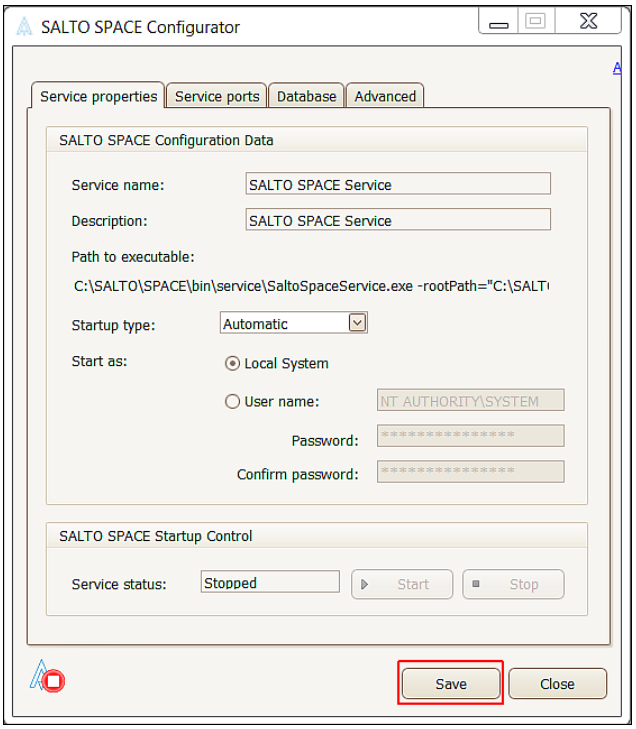


Figure 31: Service properties tab

8. Ensure that **Automatic** is selected as the **Startup type** option.

   This value is selected so that when the PC reboots, the SALTO Service starts automatically.

9. Ensure that the **Local System** option is selected.

   If you select this option, it means that the SALTO Service starts with local rights. If you select the **User** option, the SALTO Service starts with that particular user's rights. The **User** option might be required if the SALTO Service has to perform tasks with files located on a different PC.

10. Click **Save**.
11. Click the **Service ports** tab.

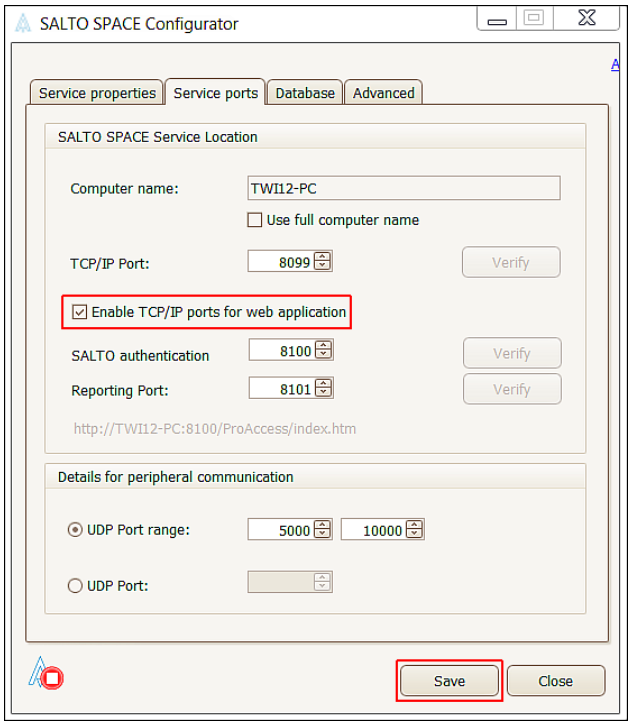


Figure 32: Service ports tab

12. Select the **Enable TCP/IP ports for web application** checkbox.

    The default ports can be changed in accordance with your requirements. In some cases, ports can be limited to one rather than a range.

13. Click **Save**. The ProAccess SPACE link on this tab should now become active.

    See *Logging In to ProAccess SPACE* for information about how to log in to ProAccess SPACE and set up bookmarks in your browser for easy access.

NOTE: The **Advanced** tab manages the tracing level, which can be set to Low, Medium, or High. The default tracing level is Low. Leave the tracing level at Low unless your SALTO technical support contact recommends that you change it. If the tracing level is set to High, this creates a more detailed report but the log file rapidly increases in size. Tracing should only be set to High during troubleshooting, for example, and reset to Low afterwards.

4. GETTING STARTED

This chapter contains the following sections:

4. 1. About Getting Started

This chapter describes the basic functionality of ProAccess SPACE. It includes a brief overview of the main features of both applications. It also provides a process workflow checklist for hotels and non-hotel sites.

4. 2. Logging In to ProAccess SPACE

For the purposes of this chapter, it is assumed that it is an operator with admin rights (admin operator) who is logging in. See *Admin Interface* and *Hotel Interface* for more information.

To log in to ProAccess SPACE, perform the following steps:

1. Double-click the **ProAccess SPACE Configurator** icon (for Windows 7 or XP).

   Or
   Select **Start** > **Programs** > **ProAccess SPACE Configurator** (for Windows 7 or XP).
   Or
   Search for **ProAccess SPACE Configurator** (for Windows 8).
2. Click **Yes** if prompted with the following message:

   Do you want to allow the following program from an unknown publisher to make changes to this computer?
   The ProAccess SPACE Configurator launches and the **Database** tab is displayed.
3. Click the **Service ports** tab.

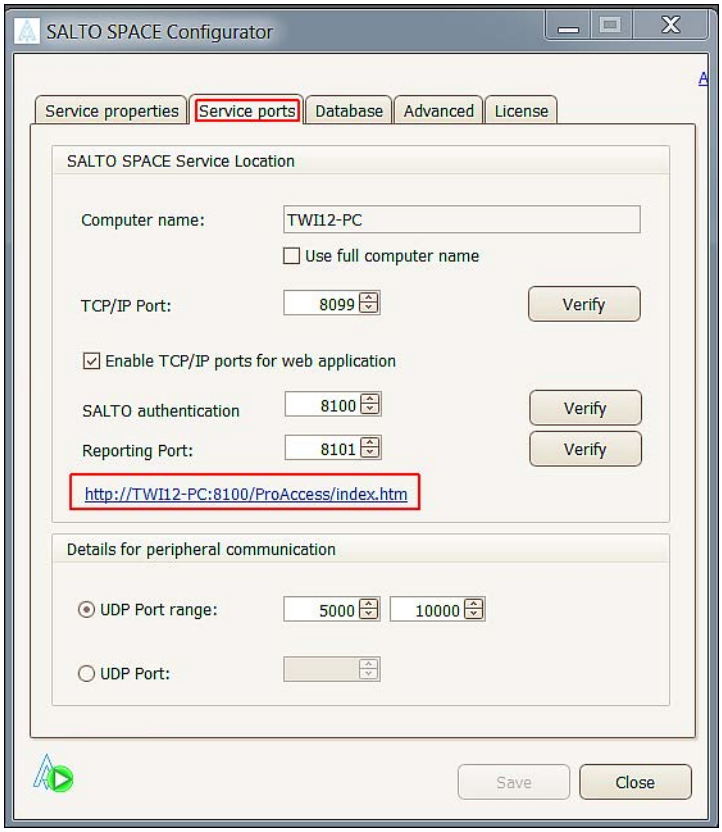


Figure 33: ProAccess SPACE link

4. Click the ProAccess SPACE link. The ProAccess SPACE login screen is displayed in your browser.

NOTE: You can copy the ProAccess SPACE link and create a browser shortcut. This means that you do not have to open the ProAccess SPACE Configurator each time to access the link.

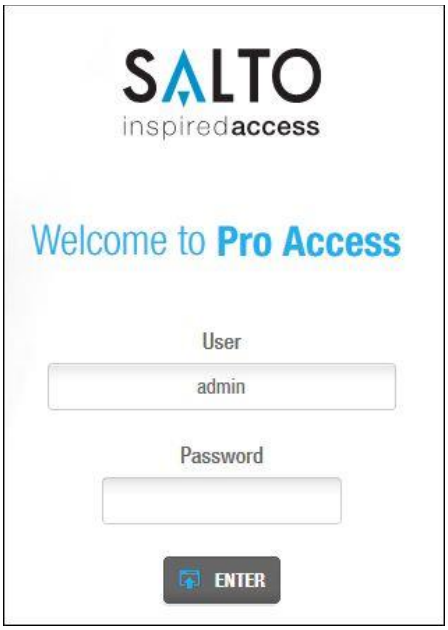


Figure 34: ProAccess SPACE login

Note that the ProAccess SPACE link is only active when the SALTO Service is running. If it is not active, check the **Service Properties** tab and restart the SALTO Service if required.

5. Type **admin** in the **User** field.

   The first time that you log in to ProAccess SPACE, you must use the admin login.

6. Type your password in the **Password** field.

NOTE: You can leave the **Password** field empty the first time you log in. However, it is recommended that you create a password as soon as possible afterwards. See *Managing Passwords* for more information about creating a password.

7. Click **Enter**. The ProAccess SPACE home screen is displayed.

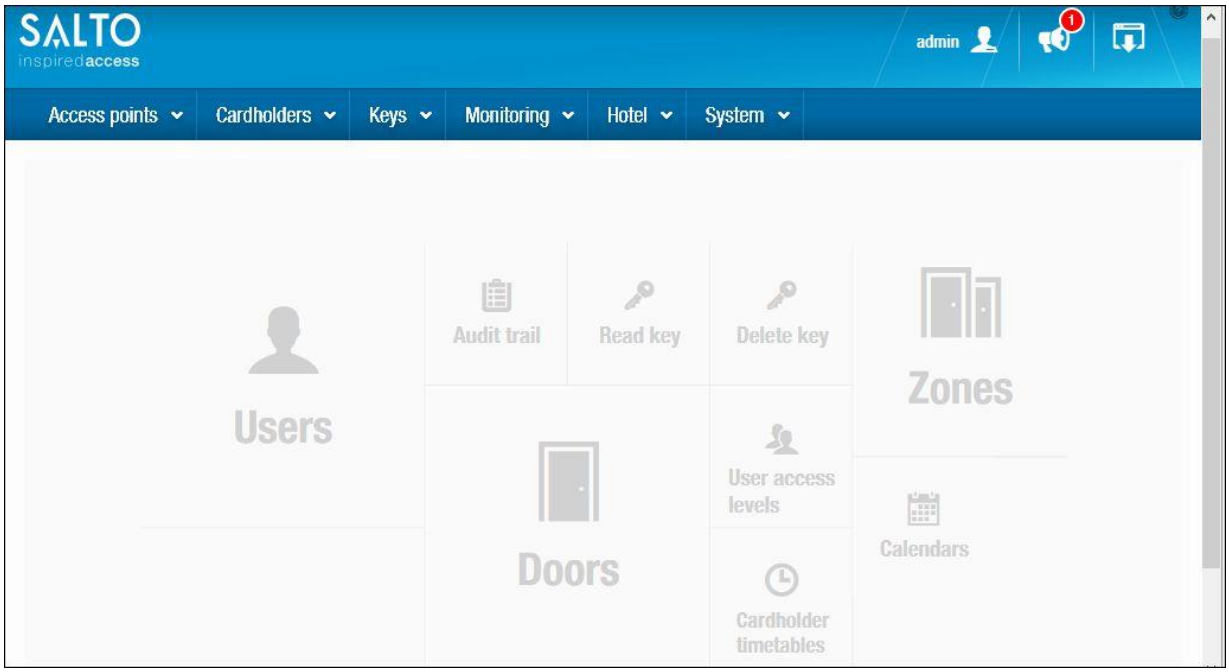


Figure 35: ProAccess SPACE home screen

4. 2. 1. Admin Interface

The Admin interface contains the necessary menu options to perform a wide range of tasks, for example, configuring access points and cardholders. It can be accessed by using the default login: admin.

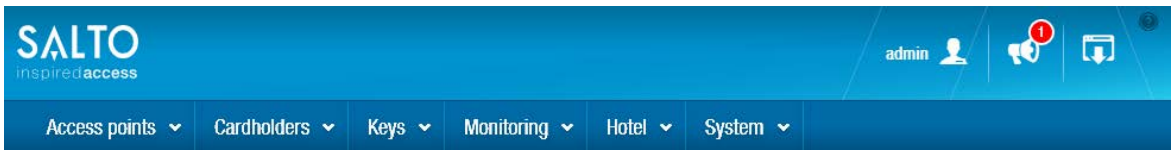


Figure 36: Admin interface menu options

Admin operators can create other logins with access only to a specified subset of ProAccess SPACE functionality. The menu options and associated features visible to other operators within the ProAccess SPACE interfaces depend on the permissions granted to them by the admin operators. See *Operator Group Global Permissions* for more information.

4. 2. 2. Hotel Interface

The Hotel interface contains a subset of the Admin interface, and is intended for use by hotel site operators. Its menu options are related to guest activities such as checking in and out, and cancellation of guest keys, as well as other hotel management options. See *Hotels* for more information. It also displays the quick-access tiles that are specific to hotel sites. Operators can be given access to the Hotel interface by the admin operators. See *Operators* and *Operator Groups* for more information.

Figure 37: Hotel interface menu options

4. 3. Configuring Operator Settings

This section provides information about default operators and operator groups. It also describes how to change the default language displayed in and manage encoder and PPD settings and passwords in ProAccess SPACE.

4. 3. 1. Default Operators

One default system operator is created on the system during installation: (Admin). See *Operators* for more information.

4. 3. 2. Default Operator Groups

One default system operator group is created on the system during installation: Administrator. See *Operator Groups* for more information.

4. 3. 3. Managing Passwords

To create or change a password, perform the following steps:

1. Click **admin** (or other appropriate operator login) on the top right-hand side of the home screen. The **Settings** screen is displayed.

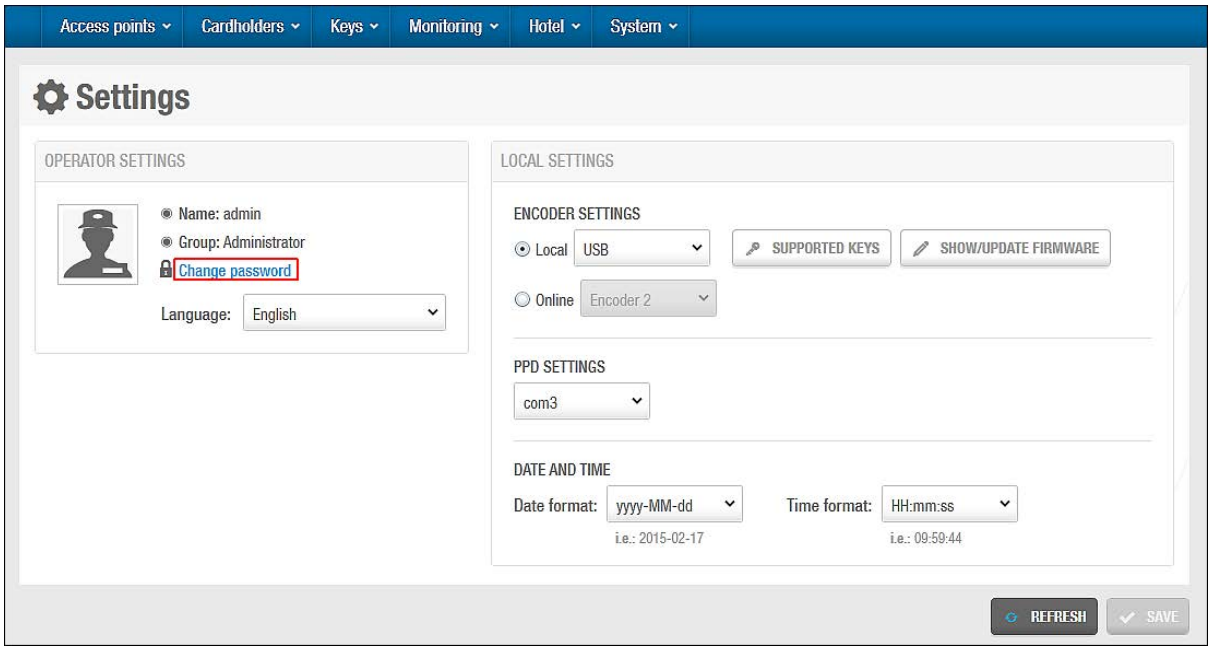


Figure 38: Settings screen

2. Click **Change password**. The **Change password** dialog box is displayed.

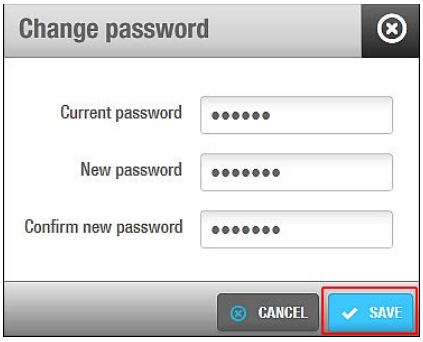


Figure 39: Change password dialog box

3. Type your current password in the **Change password** dialog box.
   Leave the **Current password** field blank if you have not already created a password.
4. Type your new password and confirm it.

   Passwords are case-sensitive. There are no restrictions on password length or complexity.
5. Click **Save**.

4. 3. 4. Changing the Default Language

You can change the language display in ProAccess SPACE to a language of your choice. To change the language display for other operators, see *Adding Operators*.

4. 3. 4. 1. Changing the Default Language in ProAccess SPACE

To change the default language, perform the following steps:

1. Click **admin** (or other appropriate operator login) on the top right-hand side of the home screen. The **Settings** screen is displayed.

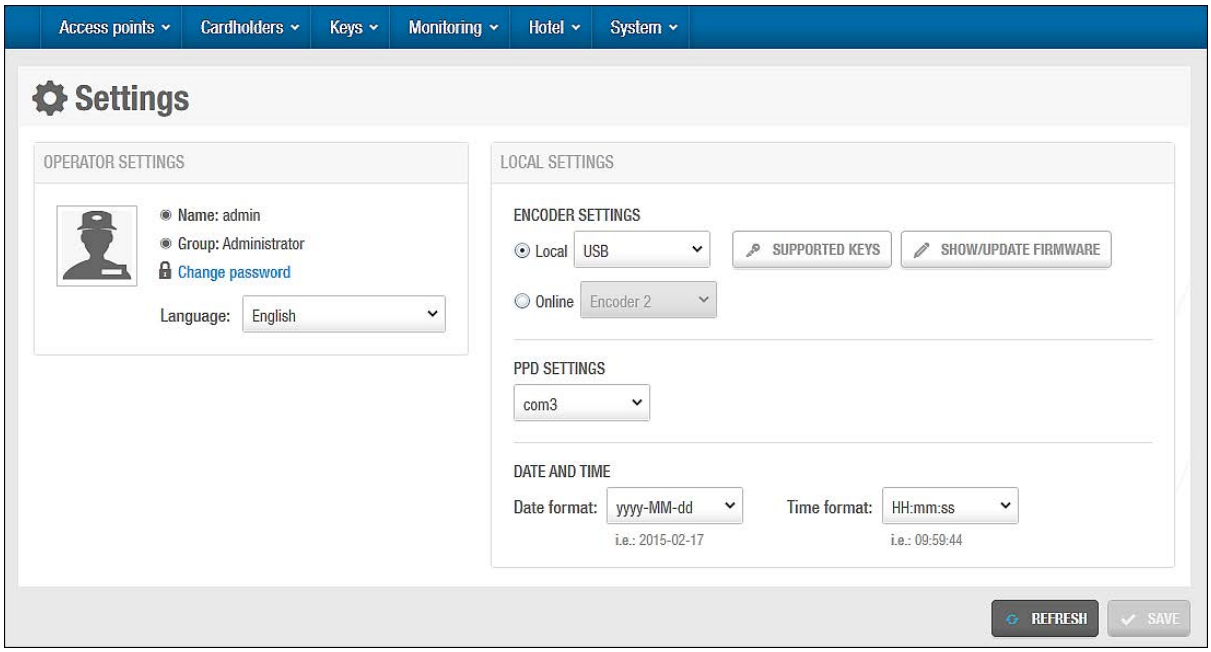


Figure 40: Settings screen

2. Select your preferred language from the **Language** drop-down list.
3. Click **Save**. The language displayed in ProAccess SPACE changes to the language selected.

4. 3. 5. Managing Local Settings

On the **Settings** screen, you must specify how your encoder and PPD connect to the system. Operators use encoders to transfer data to keys, and PPDs to perform various maintenance tasks such as updating offline doors with configuration changes or checking a lock's battery status. See *Encoders* and *PPD* for more information.

You can also use the **Settings** screen to change the date and time format, determining how it displays across the site.

4. 3. 5. 1. Encoder Settings

Encoders can be connected in two ways:

- **Local:** This is used for encoders that are physically connected to the local computer. Using this setting specifies that the encoders can transfer data through a USB connection or a serial connection through a COM port. Ensure that you select the appropriate encoder type from the drop-down list.
- **Online:** This is used for encoders that are connected using an Internet Protocol (IP) address. Using this setting specifies that the encoders transfer data through an Ethernet connection. Ensure that you select the appropriate Ethernet connection from the drop-down list.

When you select either **Local** or **Online**, the following buttons are enabled:

- **Supported Keys**
- **Show Firmware**

These are described in the following table.

Table 6: Encoder setting buttons

Button	Description
Supported Keys	If **Local** is selected, this button shows a list of available technologies the encoder can read from, for example, Mifare and Desfire. If **Online** is selected, this button still shows a list of available technologies the encoder can read from, but the encoder uses an Ethernet connection to communicate with the local computer.
Show Firmware	This button shows the encoder's firmware version and allows you to update the firmware. See *Updating Encoder Firmware* for more information.

NOTE: You can use the **Supported Keys** button on the **Settings** screen in ProAccess SPACE to SAM local encoders. See ***Error! Reference source not found.*** and *General options*

See General options section.

SAM and Issuing Data for more information.

4. 3. 5. 2. PPD Settings

PPDs can connect to the system using either a USB connection or a serial connection through a COM port. Simply select the appropriate option here.

4. 3. 5. 3. Date and Time

You can change the date and time display using the **Date format** and **Time format** drop-down lists. Changing the date and time display here determines how the date and time is displayed in all instances of ProAccess SPACE used within the SALTO installation site.

4. 4. Using ProAccess SPACE

This section describes how to use the main components of the ProAccess SPACE interface.

4. 4. 1. Interface Components

The interface is divided into three sections:

- Operator area
- Main menu bar
- Quick-access tiles

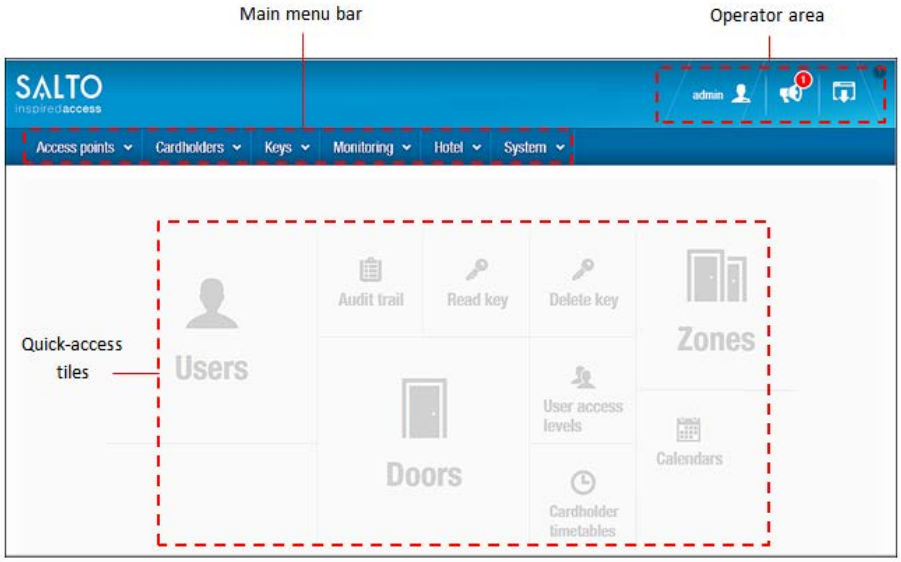


Figure 41: ProAccess SPACE home screen

4. 4. 1. 1. Operator Area

The operator area is on the top right-hand side of the home screen. The screen icons are described in the following table.

Table 7: Operator area icons

Icon	Description
 Operator	Used to change the login password and edit local settings. Note that this changes depending on the login used. For example, if a hotel operator logs in, this could display 'hotel'. Each operator can customize specific settings, for example, their preferred language or, if using an Ethernet encoder, the encoder to use.
 Alerts	Displays alerts so that you can see specific system-related issues, for example, unfinished tasks
 Logout	Used to log out of ProAccess SPACE

4. 4. 1. 2. Main Menu Bar

The main menu bar options are described in the following table.

Table 8: Main menu bar options

Menu	Description
Access points	Creates and controls access to access points, for example, doors, lockers, and rooms. It also enables the creation of zones to group and manage these access points.
Cardholders	Controls who has permissions to use a key, for example, users and visitors. This menu also controls when and where the key can be used through the use of timetables.
Keys	Enables keys to be added and deleted from the system. It is also used to check visitors in and out.
Monitoring	Provides an audit trail of the site by tracking access point activity

Menu	Description
Hotel	Enables guest check-in, check-out, and key control, for example, cancelling keys, for hotels
System	Provides system audit functionality, tracking event and object modifications. This menu also contains specific administration functionality such as managing peripherals and scheduled jobs, and adding and deleting operators, operator groups, and partitions. There is also a calendar option that can be used to control access in different geographical areas, and configure holiday and special day periods.

4. 4. 1. 3. Quick-Access Tiles

The home screen contains shortcuts for quick access to the most commonly used options. The quick-access tiles that are displayed vary according to whether you are accessing the Admin interface or the Hotel interface.

The Admin interface quick-access tiles are listed in the following table.

Table 9: Admin interface quick-access tiles

Quick-Access Tile	Alternative Access Path
Users	**Cardholders** menu
Audit trail	**Monitoring** menu
Read key	**Keys** menu
Delete key	**Keys** menu
Zones	**Access points** menu
Calendars	**System** menu
User access levels	**Cardholders** menu
Cardholder timetables	**Cardholders** menu
Doors	**Access points** menu

The Hotel interface quick-access tiles are listed in the following table.

Table 10: Hotel interface quick-access tiles

Quick-Access Tile	Alternative Access Path
Check-in	**Hotel** menu
Check-out	**Hotel** menu
Copy guest key	**Hotel** menu
Read key	**Keys** menu
Room status	**Hotel** menu

4. 4. 2. Common Screen Tasks

This section describes some common screen tasks.

4. 4. 2. 1. Using the Sidebar to Associate Entries

You can associate or disassociate entries with other system elements, for example, users, access levels, and zones, by clicking the sidebar links at the right-hand side of an information screen. The sidebar links available vary according to the information screen displayed.

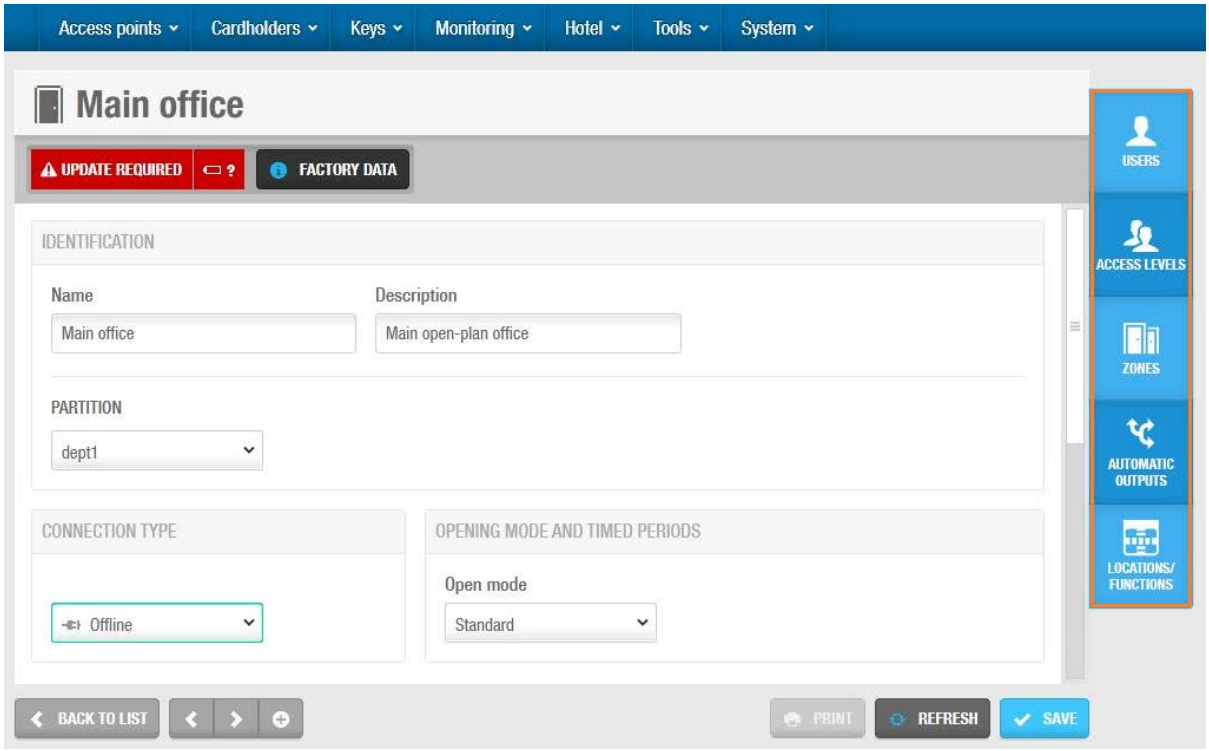


Figure 42: Sidebar links

4. 4. 2. 2. Adding and Deleting from Selection Lists

You can use the chevrons and arrows in an **Add/Delete** dialog box to move items from one side of the screen to the other.

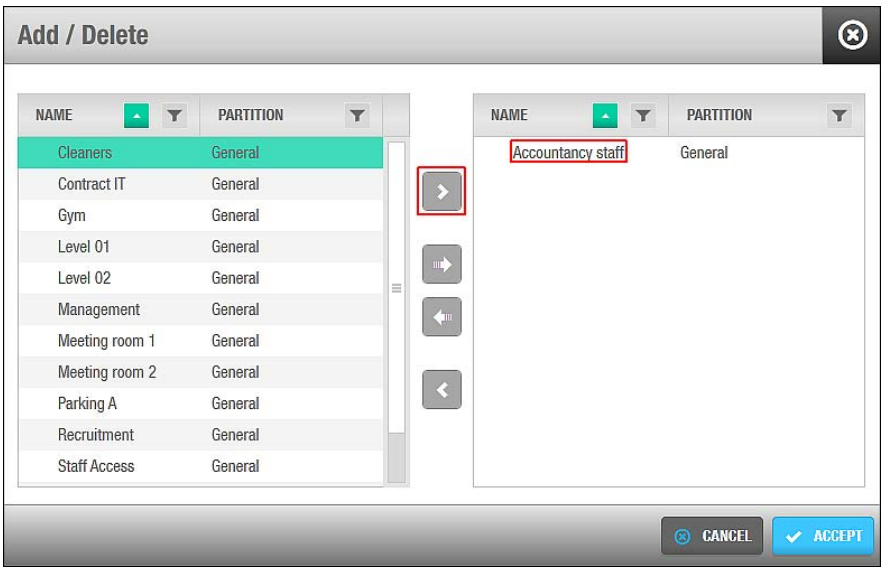


Figure 43: Chevron single selection

Select the required item in the left-hand panel and click the chevron. The selected item is displayed in the right-hand panel. Double-clicking on an item also moves it between the panels. Holding down the Shift key allows you to select several consecutive items to move at a time. Alternatively, you can hold down the Ctrl key while clicking the items to make multiple selections.

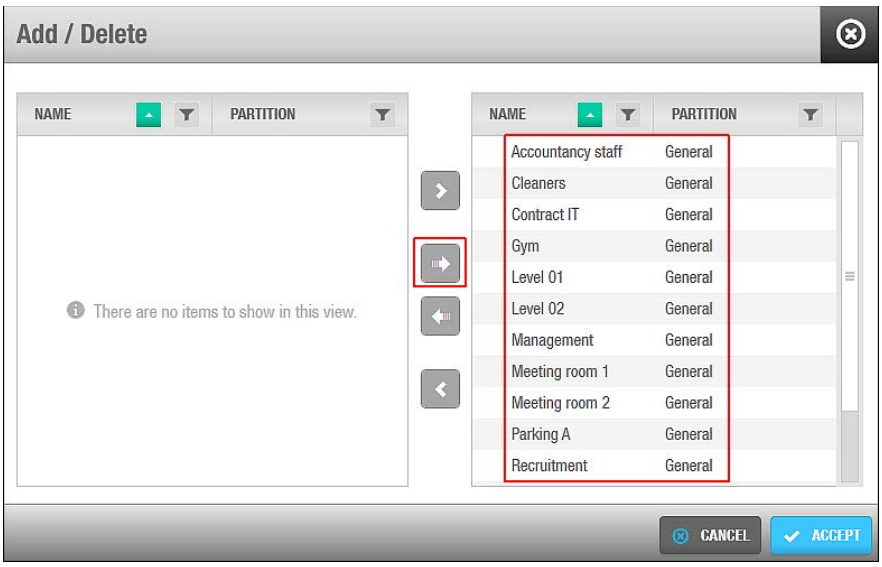


Figure 44: Selection lists

Click the arrows in the middle of the screen to move all items from the left panel to the right panel and vice versa.

4. 4. 2. 3. Copying Information Using Same As…

You can copy information when associating sidebar links by clicking the **Same As…** button in an information screen. For example, if you are associating a door with a user, you can copy the users already associated with another door to the current door by clicking the **Same As…** button.

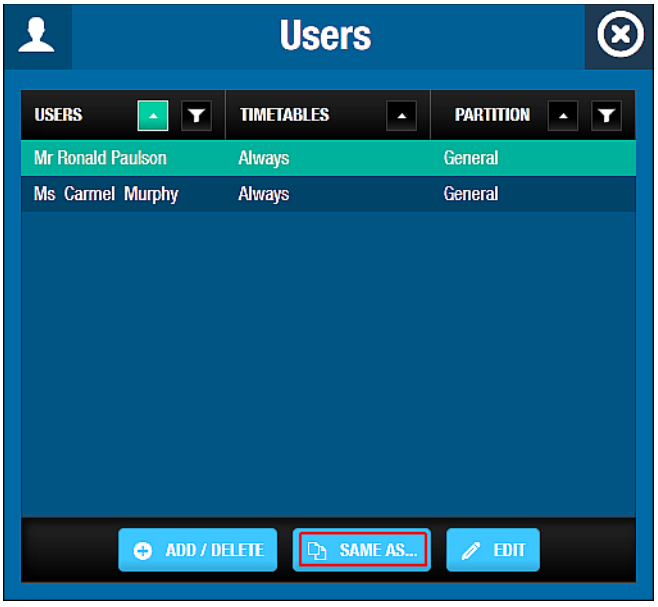


Figure 45: Same As… button

4. 4. 2. 4. Filtering Data by Search Term

You can use the **Funnel** icon to search for specific data. The filtering options vary according to the screen that is displayed. Common filters include user name, operator name, event, and locations.

To search for specific data, click on the **Funnel** icon and enter your search term. The following figure shows an example of a **Users** screen with the search dialog box displayed.

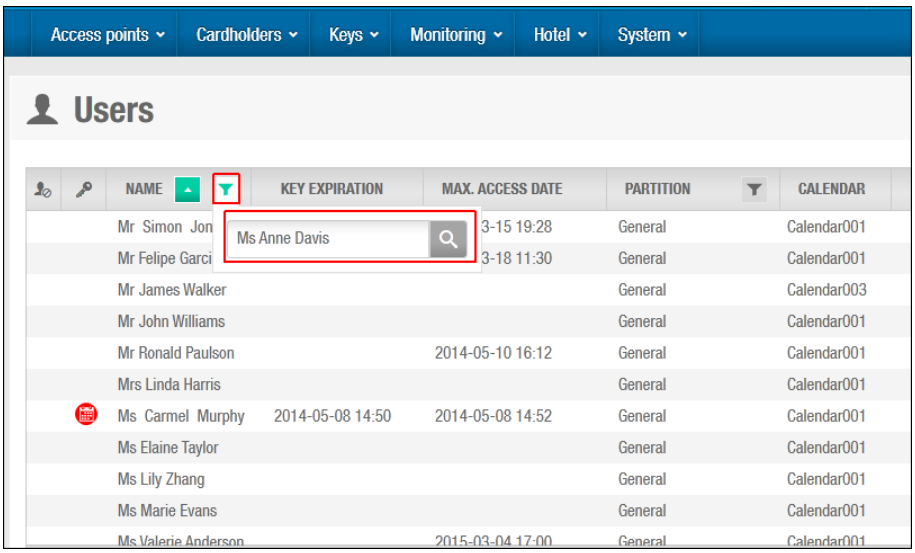


Figure 46: Filtering data using a search term

4. 4. 2. 5. Sorting Data Chronologically or Alphabetically

You can use the up/down arrow keys to display screen data alphabetically or chronologically as applicable.

The following figure shows an example of an **Operator groups** list screen with the up arrow highlighted. The operator group names are sorted and listed alphabetically.

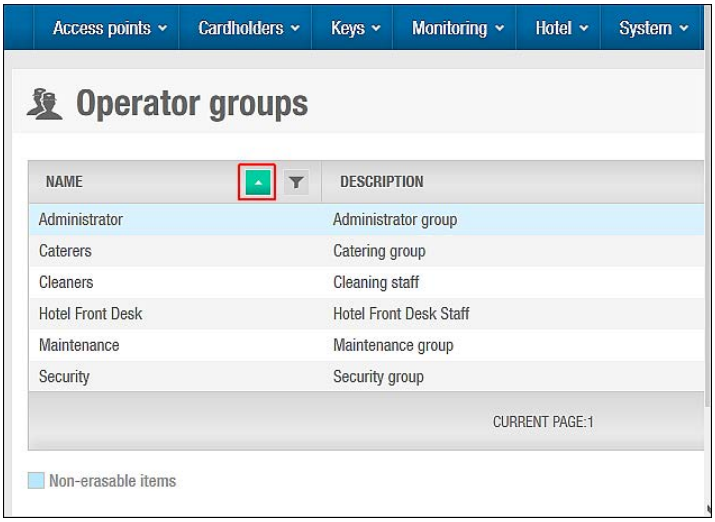


Figure 47: Sorting data alphabetically

NOTE: Data marked as non-erasable cannot be deleted from the system. Such entries are highlighted in blue on the list screens.

4. 4. 2. 6. Printing and Exporting Data in ProAccess SPACE

A **Print** button is displayed on various screens in ProAccess SPACE, for example, the **Users** screen, the **User** information screen, and the **Calendars** screen. You can use this button to print a hard copy of the data on the screen. For example, you can print the user list if you

want to keep a paper record of the users in your site. Alternatively, you can export the data to the following file formats:

- Acrobat (PDF) file
- CSV
- Excel 97-2003
- Rich text format
- TIFF file
- Web archive
- XPS document

The following example shows how to print a hard copy of the user list, or export it to a specific file format:

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

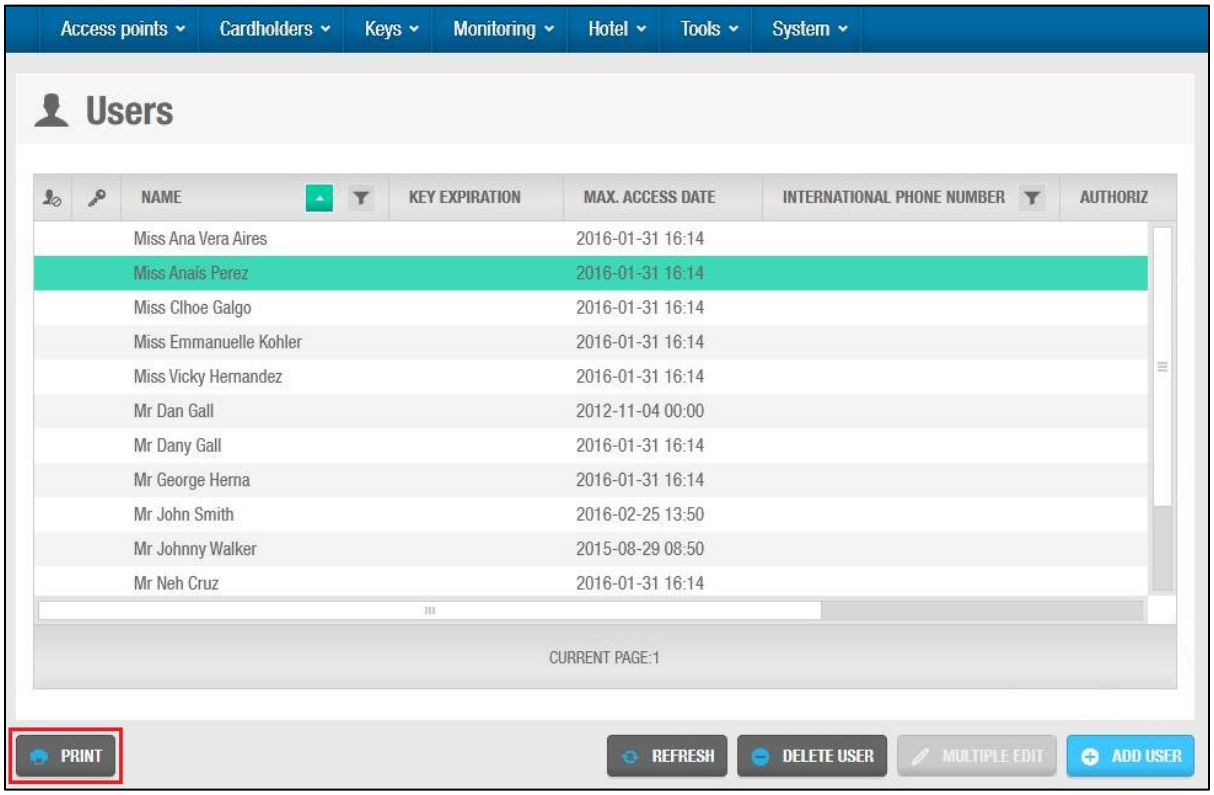


Figure 48: Users screen

2. Click **Print**. The **Users** dialog box, showing the user list, is displayed.

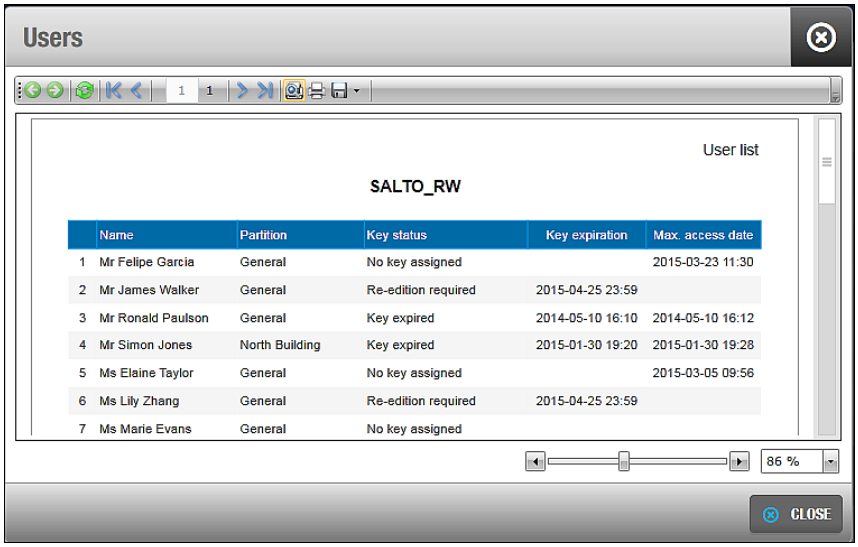


Figure 49: Users dialog box

The print preview view is displayed by default. You can click the **Switch to interactive view** icon to use the interactive view option. If you select a user before you click **Print**, the **Print** dialog box is displayed. This gives you the option to print either the complete user list or the user profile for the selected user.

3. Click the **Print report** icon. A pop-up is displayed confirming that the document is ready for printing.

   Alternatively, click the **Export** icon to select a file format and then click **Save** to download the file and save it to the appropriate file location.
4. Click **Print**. The **Print** dialog box is displayed.
5. Select your preferred printing options and click **Print** to print the user list.

4. 4. 2. 7. Users Multi edition

A **MULTIPLE EDIT** button is displayed. You can use this button to edit multiple user's files at the same time. For example, you can amend the key options or the key expiration.

To edit multiple user's file at the same time perform the following step:

1. Highlight the users you want to edit. A multi selection can be done by holding the **Ctrl** key and selecting the users with the curser.
2. Now that multiple users are selected, the **MULTIPLE EDIT** button turns blue. Click **MULTIPLE EDIT**

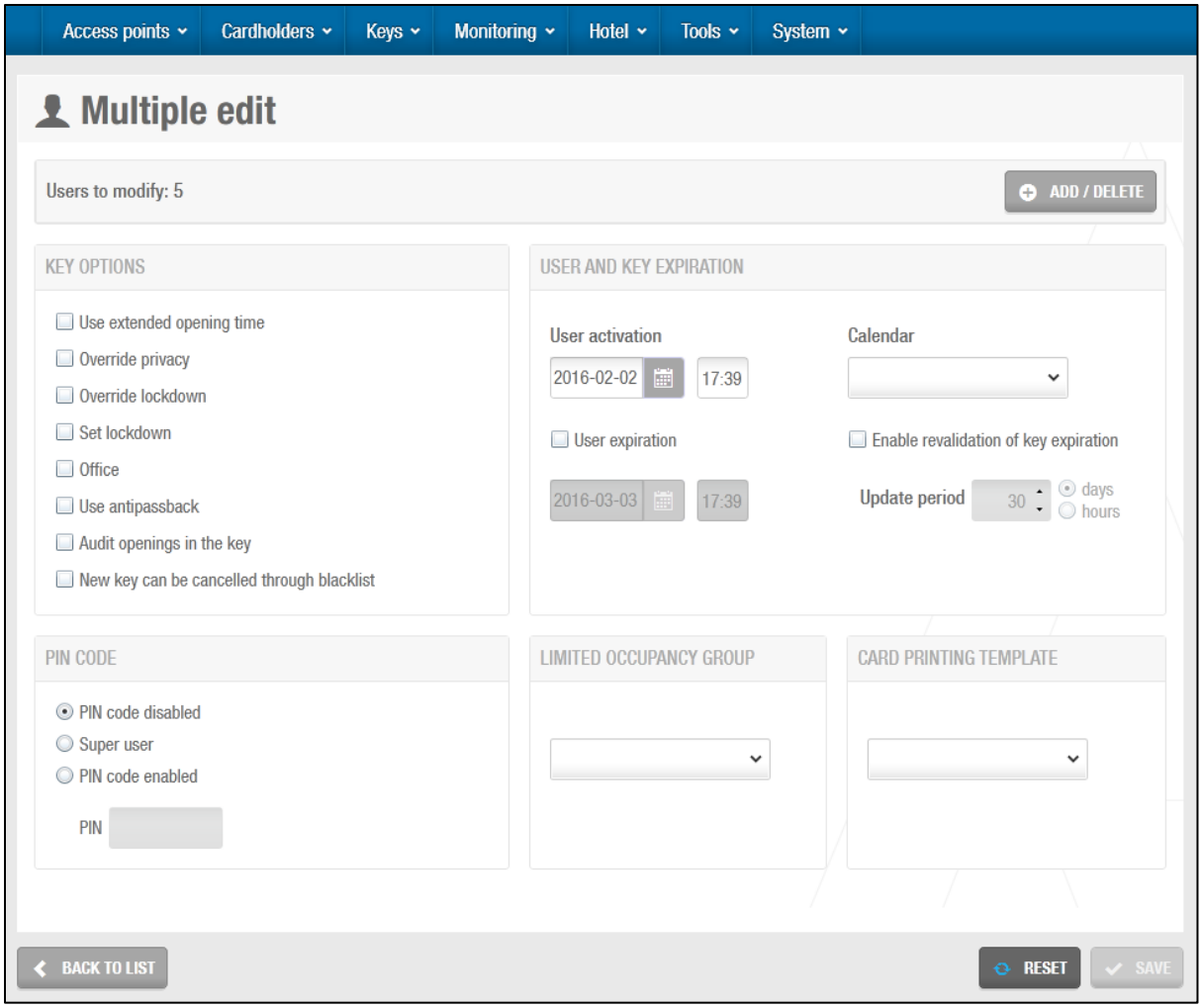


Figure 50: Users dialog box

4. 5. Logging Out of ProAccess SPACE

It is recommended that you manually log out of ProAccess SPACE at the end of your session to prevent other operators from making unauthorized changes. The system can also be configured to automatically log out operators after a specified period of inactivity.

NOTE: The system automatically logs you out of ProAccess SPACE after 120 seconds of inactivity. To change the automatic logout time, you must enable the AUTO_LOGOFF_TIMEOUT parameter in ProAccess SPACE General Options and set the value in numbers of seconds. For example, AUTO_LOGOFF_TIMEOUT=240 means that a session in ProAccess SPACE expires after four minutes of inactivity and operators will need to log back in. See ***Error! Reference source not found.*** for more information.

To manually log out of ProAccess SPACE, perform the following steps:

1. Click the **Logout** icon on the top right-hand side of the home screen. The **Confirmation** dialog box is displayed asking you to confirm that you want to log out.
2. Click **Yes**.

4. 6. Setup Checklist

This section provides a list of items that the admin operator (or an operator with admin rights) should create and configure in ProAccess SPACE so that the system can be used effectively.

NOTE: Additional configuration may be required in ProAccess SPACE General options before you can perform certain tasks in ProAccess SPACE that are associated with specialized functionality. You should consult with your SALTO technical support contact for assistance with this initial configuration.

Table 11: Setup checklist

Task	Mandatory for Non-Hotel Sites?	Mandatory for Hotel Sites?	Comments	Y/N
System				
1. Create and configure all required partitions.	Yes/No	Yes/No	Depends on whether the site uses partitions	
2. Create and configure all required operators.	Yes	Yes		
3. Create and configure all required operator groups.	Yes	Yes		
4. Create and configure all required calendars.	Yes	Yes		
5. Create and configure all required time zones.	Yes/No	Yes/No	Depends on whether the site uses the multiple time zones functionality	
6. Create and configure all required SALTO Network devices.	Yes	Yes		
7. Create and configure all required system jobs, for example, automatic database backups.	Yes	Yes		
Access Points				
1. Create and configure all required doors.	Yes	Yes		
2. Create and configure all required Energy Saving Devices (ESDs).	Yes	Yes		
3. Create and configure all required outputs.	Yes	Yes		
4. Create and configure all required lockers.	Yes/No	Yes/No	Depends on whether the site uses a locker system	
5. Create and configure all required zones.	Yes	Yes		
6. Create and configure all required locations.	Yes	Yes		
7. Create and configure all required functions.	Yes	Yes		
8. Create and configure all required roll-call areas.	Yes/No	Yes/No	Depends on whether the site uses roll-call areas	
9. Create and configure all required	Yes/No	Yes/No	Depends on whether the	

Task	Mandatory for Non-Hotel Sites?	Mandatory for Hotel Sites?	Comments	Y/N
lockdown areas.			site uses lockdown areas	
10. Create and configure all required limited occupancy areas.	Yes/No	Yes/No	Depends on whether the site uses this functionality (for example, for a parking area)	
11. Create and configure all required access point timed periods.	Yes	Yes		
12. Create and configure all required access point automatic changes.	Yes	Yes		
Peripherals				
Configure all required peripherals.	Yes	Yes		
Cardholders				
1. Create and configure all required user profiles.	Yes	Yes		
2. Create and configure all required user access levels.	Yes	Yes		
3. Create and configure all required limited occupancy groups.	Yes/No	Yes/No	Depends on whether the site uses limited occupancy area functionality	
4. Create and configure all required cardholder timetables.	Yes	Yes		
5. Assign all required user keys.	Yes	Yes		
Visitors				
Create and configure all required visitor access levels.	Yes	Yes		
Hotels				
1. Create and configure all required rooms. 2. Create and configure all required suites. 3. Create and configure all required keys for use by hotel staff and guests. 4. Create and configure all required guest access levels.	No	Yes		

5. ACCESS POINTS

This chapter contains the following sections:

5. 1. Access Points Process

Access points are generally created and managed by an operator with admin rights. Throughout this chapter, references are made to the admin operator. However, this can refer to any operator that has been granted admin rights.

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

1. **Doors created and configured**

   The admin operator creates doors and configures the door options.
2. **Doors associated**

   The admin operator associates users, access levels, zones, automatic outputs, and/or locations/functions with the specified doors.
3. **ESDs created and configured**

   The admin operator creates ESDs and configures the options.
4. **ESDs associated**

   The admin operator associates users and/or access levels with the specified ESDs and with the ESD_#1 and ESD_#2 outputs.
5. **Lockers created and configured**

   The admin operator creates lockers and configures the locker options.
6. **Lockers associated**

   The admin operator associates users, access levels, and/or zones with the specific locker. The admin operator can also create and define a free assignment zone for lockers. See *Creating Free Assignment Zones* for more information.
7. **Zones created and configured**

   The admin operator creates zones and configures the zone options.

8. **Zones associated**

   The admin operator associates access points, users, and/or access levels with the specified zones.

9. **Locations created and configured**

   The admin operator creates locations and configures the location options.

10. **Locations associated**

    The admin operator associates users and/or access points with the specified locations.

11. **Functions created and configured**

    The admin operator creates functions and configures the function options.

12. **Functions associated**

    The admin operator associates users and/or access points with the specified functions.

13. **Outputs created and configured**

    The admin operator creates outputs and configures the output options.

14. **Outputs associated**

    The admin operator associates users, access levels, and/or access points with the specified outputs.

15. **Roll-call areas created and configured**

    The admin operator creates roll-call areas and configures the roll-call options.

16. **Roll-call areas associated**

    The admin operator associates readers with the specified roll-call areas.

17. **Lockdown areas created and configured**

    The admin operator creates lockdown areas and configures the lockdown area options.

18. **Lockdown areas associated**

    The admin operator associates access points with the specified lockdown areas.

19. **Limited occupancy areas created and configured**

    The admin operator creates limited occupancy areas and configures the limited occupancy area options.

20. **Limited occupancy areas associated**

    The admin operator associates access points and/or limited occupancy groups with the specified limited occupancy areas.

21. **Access point timed periods created**

    The admin operator creates an access point timed period.

22. **Access point automatic changes created and configured**

    The admin operator creates an access point automatic change and configures the access point automatic change options.

5. 2. About Access Points

Access points is the term used within the SALTO system to describe doors, lockers, zones, locations, functions, and outputs. This chapter describes how to use access points to create

and control each of these. It also describes how to create roll-call areas, lockdown areas, limited occupancy areas, timed access periods to control access, and ESDs.

The information contained in this chapter applies to non-hotel sites only. See *About Hotel Access Points* for information about hotel access points.

5. 3. Doors

A door is an access point to an area, for example, a door to an office, a meeting room, or a leisure area. Each door is fitted with an electronic device that controls the lock. The lock can be mechanical, electrical, or magnetic. When a door is added to the system, data can then be transferred to the electronic device using a PPD. See *PPD* for more information.

The following sections describe how to create and configure a door within ProAccess SPACE.

5. 3. 1. Creating Doors

To create a door, perform the following steps:

1. Select **Access points** > **Doors**. The **Doors** screen is displayed.

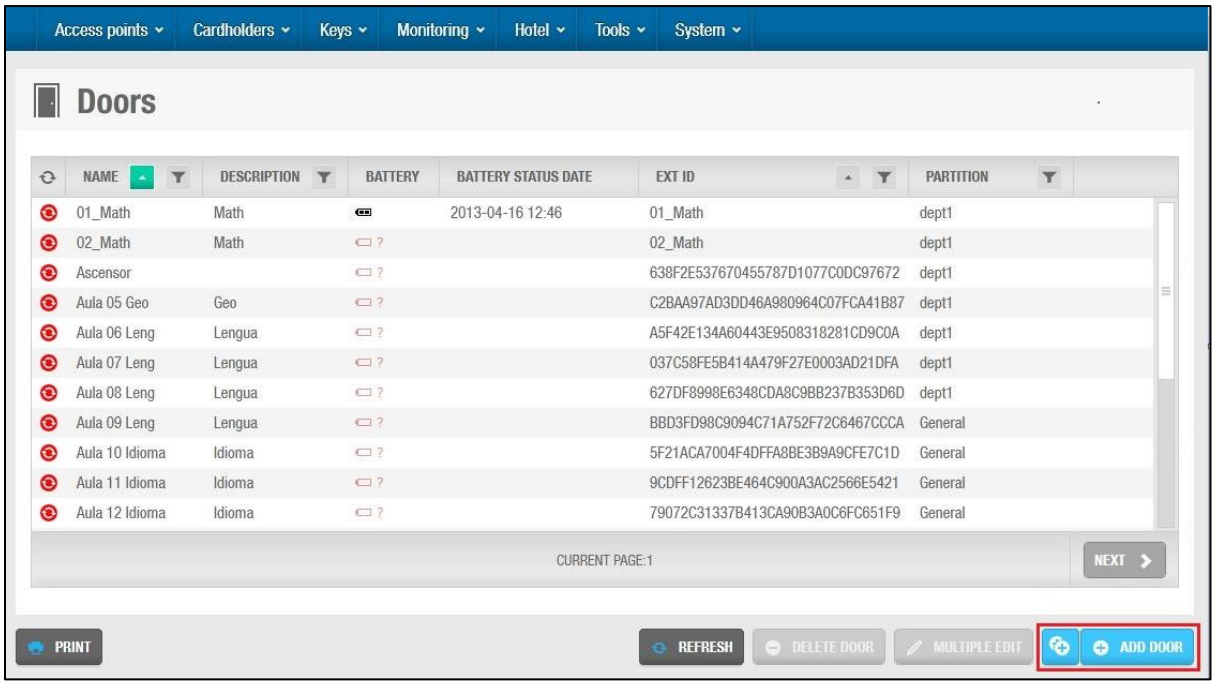


Figure 51: Doors screen

2. Click **Add Door**. The **Door** information screen is displayed.

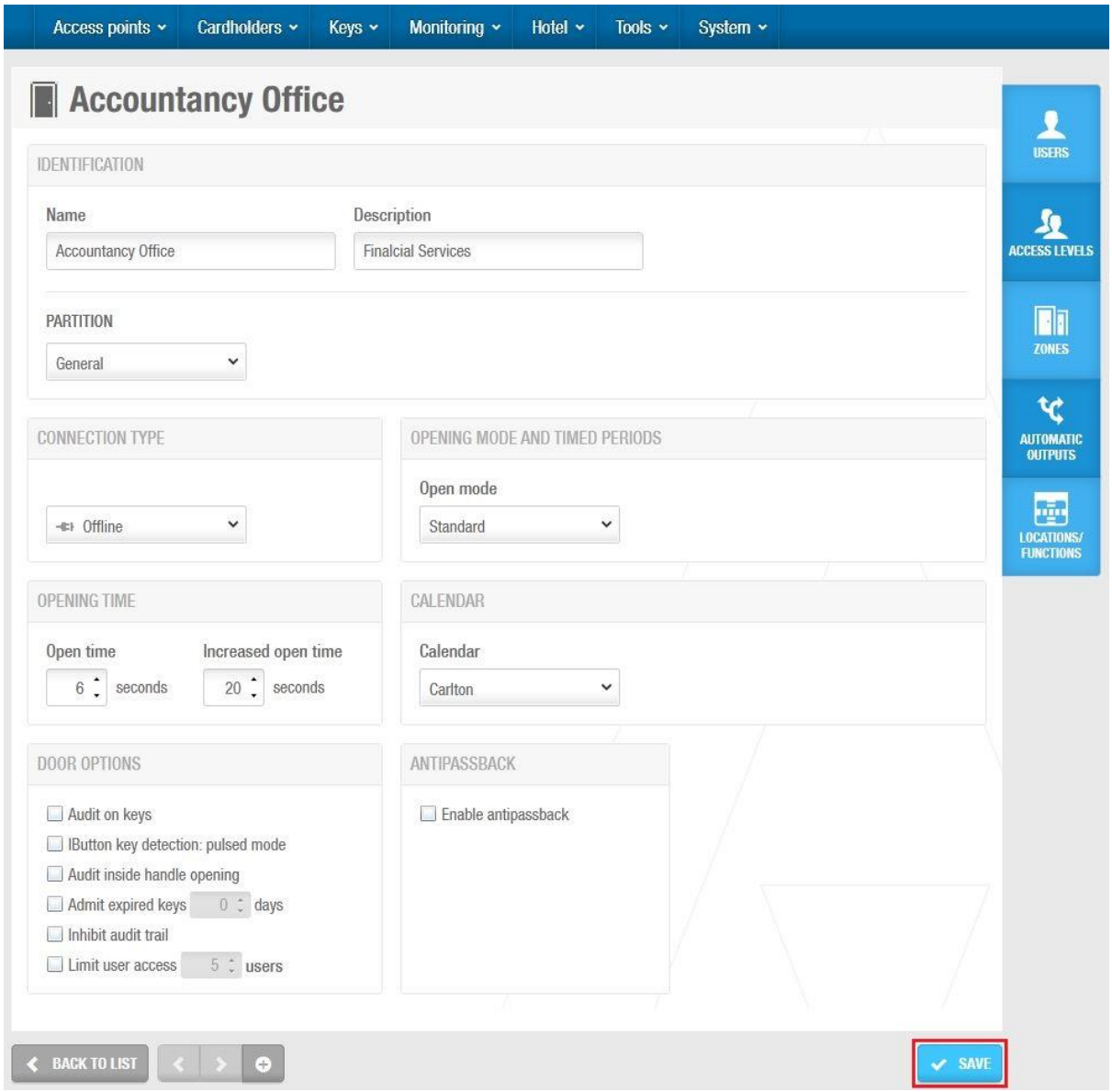


Figure 52: Door information screen

NOTE: A **Valid Until** information field is displayed on the information screens for access points if data relating to battery status and calendars, for example, is due to expire.

3. Type a name for the door in the **Name** field.
4. Type a description for the door in the **Description** field.
5. Select the relevant partition from the **Partition** drop-down list, if required.

   Partitions make it easier for different operators to manage the various sections of a site. For example, a partition could be the Humanities building in a university. Operators who have access to this partition can manage the items belonging to it (such as particular access points, users, access levels, etc.) depending on the partition permissions set by the admin operator. Operators who do not have access to a partition cannot manage the items belonging to it. See *System* Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

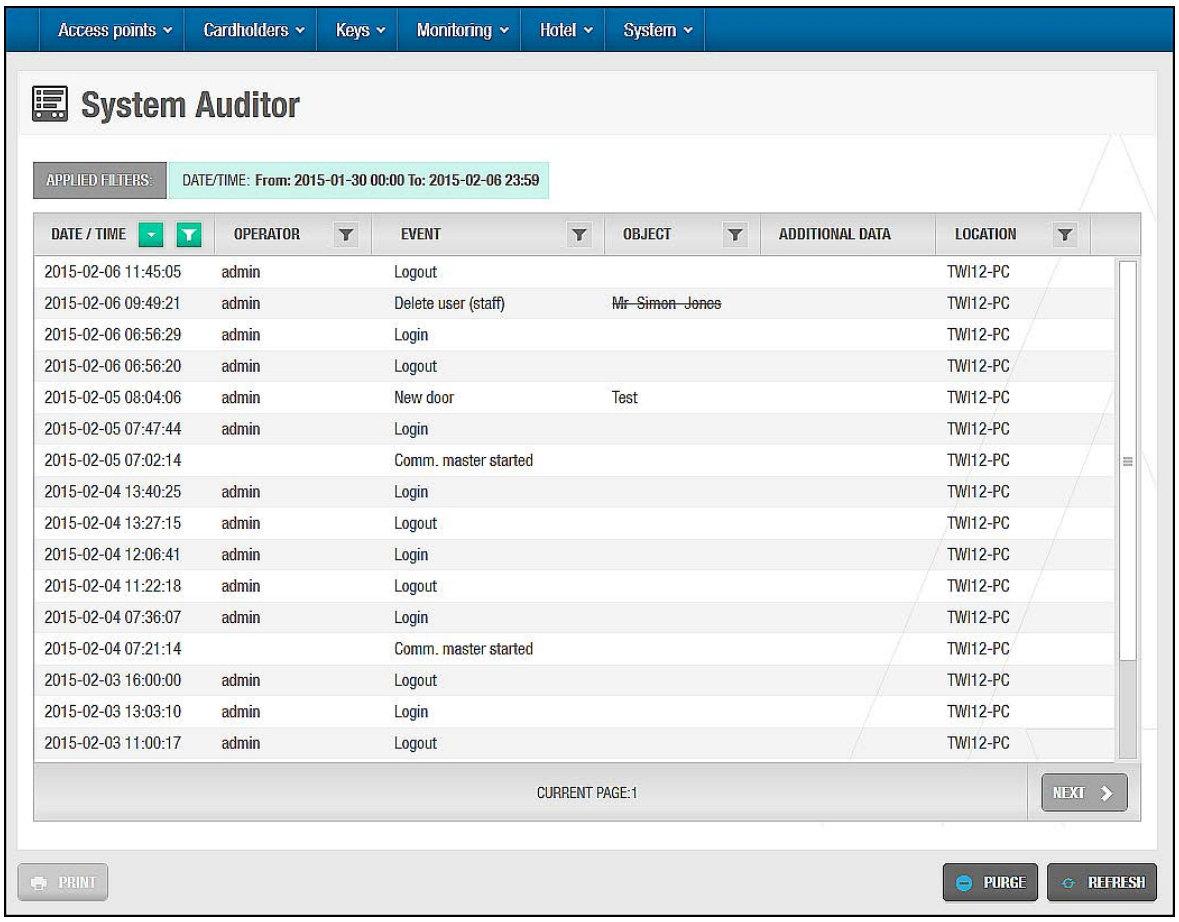


Figure 228: System Auditor information screen

5. 3. 2. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

5. 3. 3. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

1. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

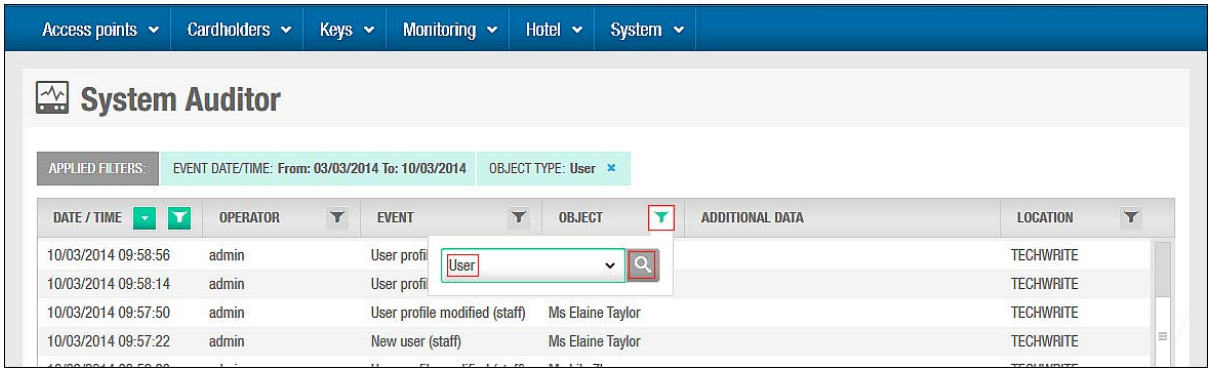


Figure 229: System Auditor information screen

2. Click the **Funnel** icon above the filter item. A search dialog box is displayed.

   For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.

   For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.

   For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.

3. Type your search term.

   Or

   Select a predefined search term from the drop-down list.

   Or

   Select a date range.

   You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.

   However, you cannot remove the **Date/Time** filter.

4. Click the **Search** icon. A filtered audit trail list is displayed.

5. 3. 3. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

5. 3. 4. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic*

System Auditor Purging for more information.

To purge the system auditor, perform the following steps:

1. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
2. Click **Purge**. The **Purge system auditor** dialog box is displayed.

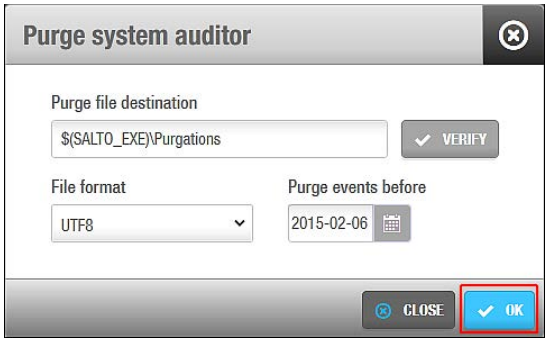


Figure 230: Purge system auditor dialog box

3. Type the appropriate destination folder name in the **Purge file destination** field.

   You can click **Verify** to verify the file directory exists and is correct.
4. Select a format from the **File format** drop-down list.

   This specifies the format of the file containing the purged events.
5. Select the required date by using the calendar in the **Purge events before** field.

   All events prior to the date you select are purged.
6. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
7. Click **OK**.

5. 4. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

5. 4. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

1. Select **System** > **Operators**. The **Operators** screen is displayed.

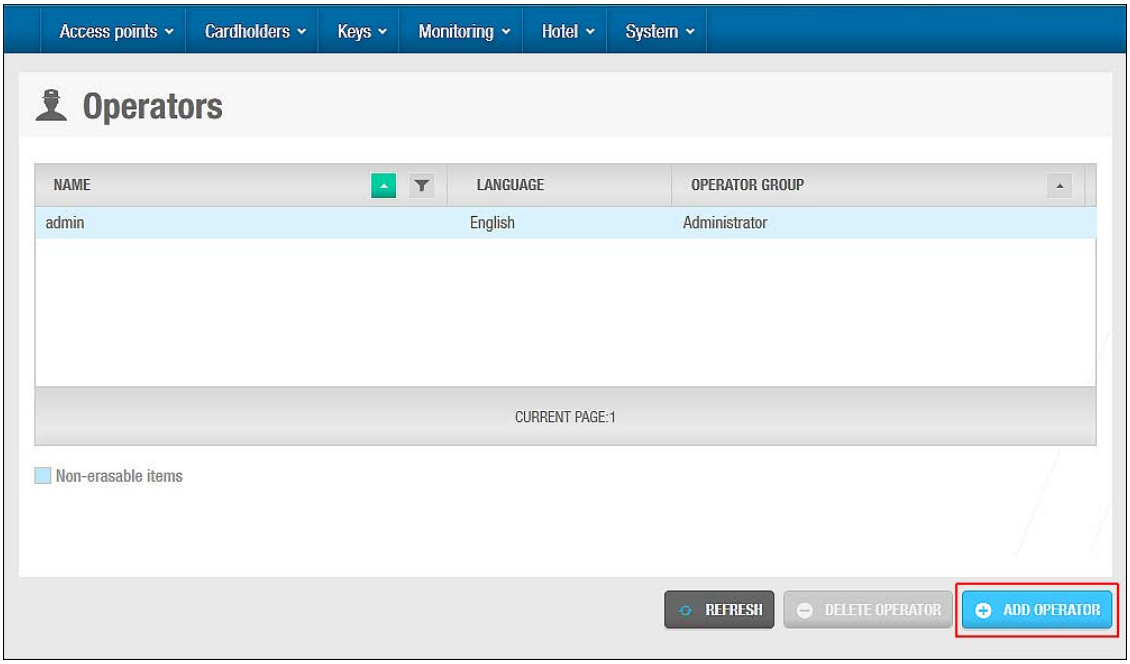


Figure 231: Operators screen

2. Click **Add Operator**. The **Operator** information screen is displayed.

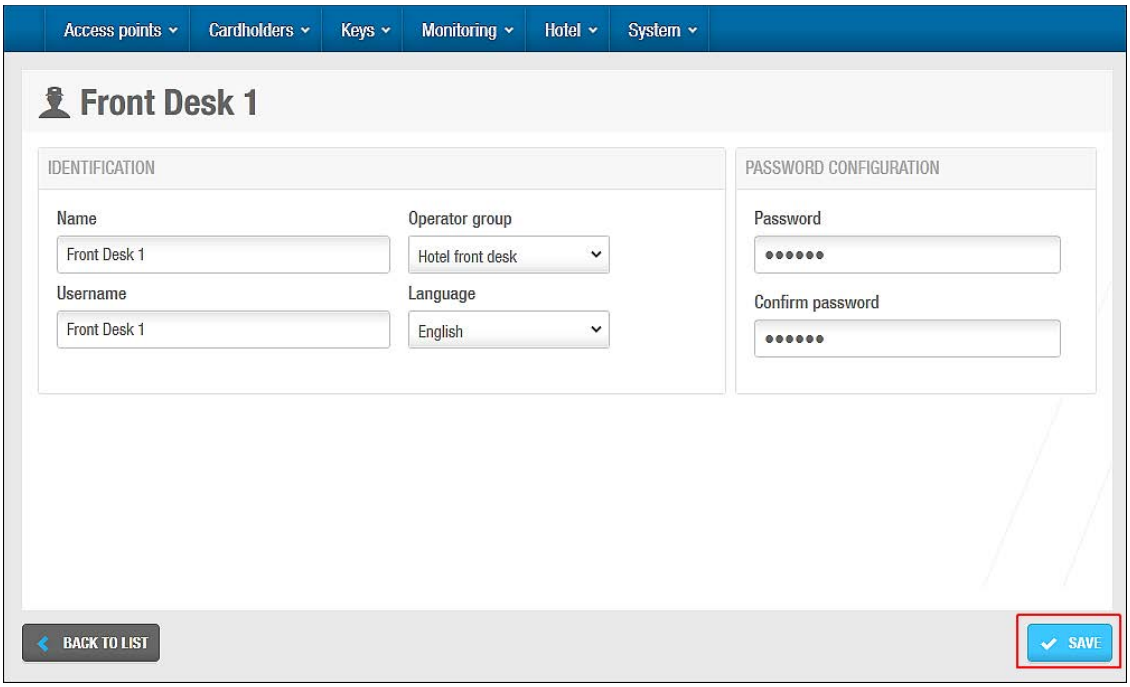


Figure 232: Operator information screen

3. Type the full name of the new operator in the **Name** field.

   A maximum of 56 characters can be entered. The name is not case sensitive.

4. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

   A maximum of 64 characters can be entered. The user name is not case sensitive.

5. Select the appropriate operator group from the **Operator group** drop-down list.
6. Select the display language for the operator in the **Language** drop-down list.

7. Type a password for the new operator in the **Password Configuration** panel.

   The password is case sensitive.
8. Confirm the password.
9. Click **Save**.

5. 5. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

5. 5. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

1. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

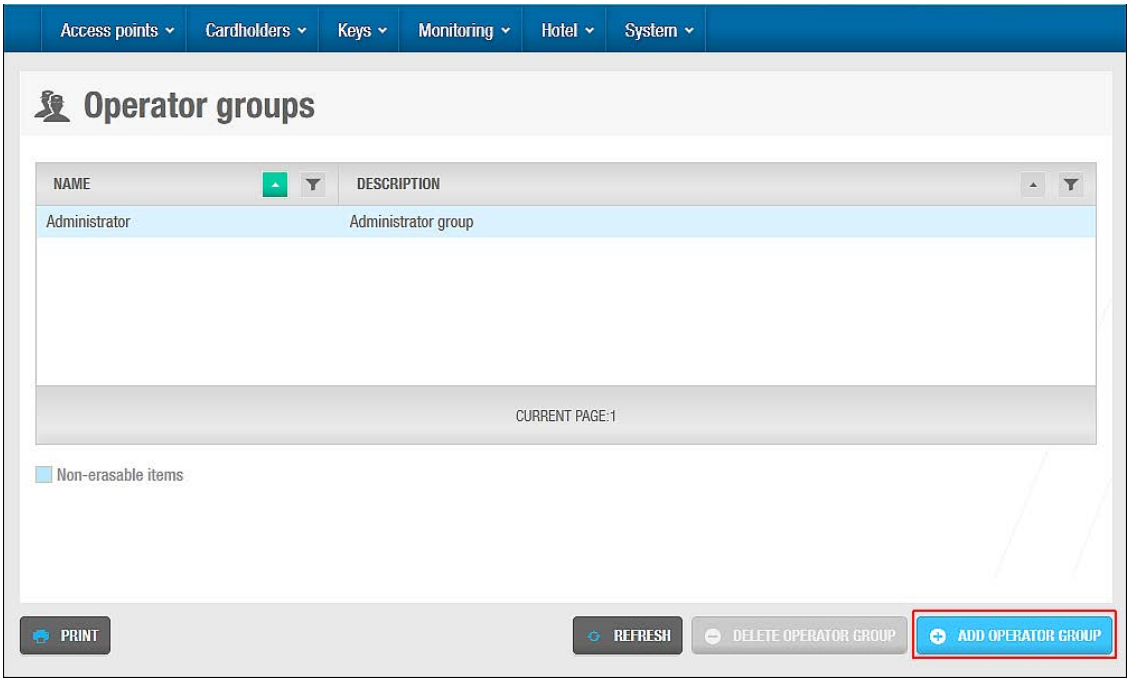


Figure 233: Operator groups screen

2. Click **Add Operator Group**. The **Operator group** information screen is displayed.

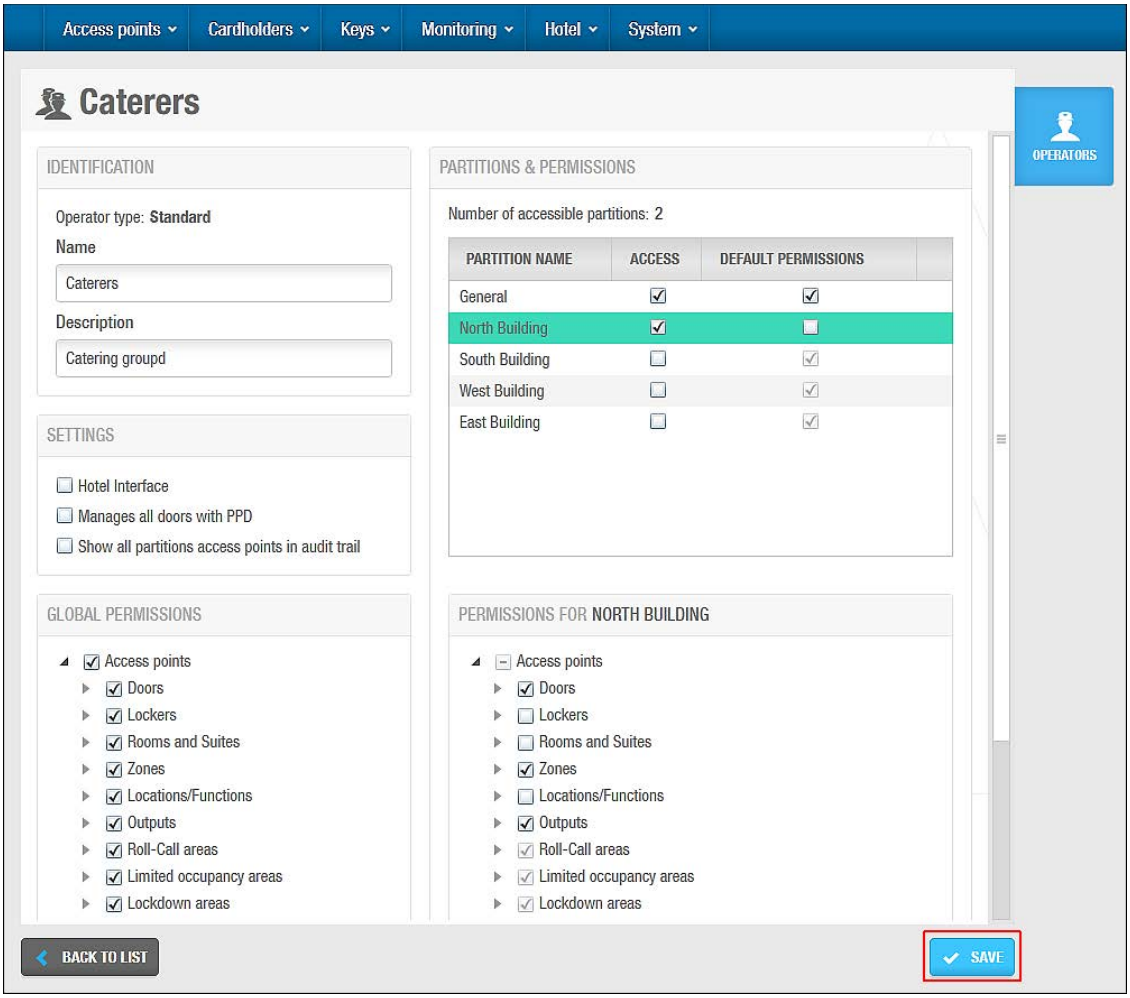


Figure 234: Operator group information screen

3. Type the name of the operator group in the **Name** field.
4. Type a description for the group in the **Description** field.
5. Select the appropriate options in the **Settings** panel.

   The options are described in *Operator Group Settings*.
6. Select the appropriate permissions in the **Global Permissions** panel.

   The options are described in *Operator Group Global Permissions*.
7. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

   You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes

in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.

8. Click **Save**.

5. 5. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

5. 5. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level **Monitoring** checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors

Permission	Description
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas

Permission	Description
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

5. 5. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

1. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
2. Double-click the operator group with the operator list you want to view.
3. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

   Partitions for more information. Note that the partitions functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.
4. Select the appropriate configuration and management options.

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

If required, you can activate additional fields on the **Door** information screen by using ProAccess SPACE General options. To activate the **Ext ID** field, the SHOW_EXT_ID parameter must be enabled. See ***Error! Reference source not found.*** for more information. The **Ext ID** field displays a unique identifier for the door, automatically generated by the system. You can amend this identifier if required.

You can also add and name a maximum of two general purpose fields using ProAccess SPACE General options. To activate a general purpose field, you must select the **Enable field** checkbox in **System** > **General options** > **Access points** tab in ProAccess SPACE. You can then name the field in accordance with the information that you want to capture.

NOTE: You can create multiple doors at once by using the **Multiple Add** option. In addition, you can edit multiple doors at once by using the **Multiple Edit** option. The **Multiple Edit** button is enabled when you select more than one entry on the **Doors** screen. This allows you to enter the appropriate identification and configuration details on the **Multiple edit** screen. The details are then applied to all of the selected entries. See *Configuring Doors* for more information about the configuration settings for doors.

5. 5. 3. Configuring Doors

The following sections describe the various fields used to configure doors.

5. 5. 3. 1. Connection Types

The **Connection Type** panel defines the connection type for the door. The default option is **Offline**. When you select any of the other (online) connection types from the **Connection Type** drop-down list, a **Configure** button is displayed on the **Door** information screen. See *Configuring Online Connection Types* for more information about configuring connection types.

Additional panels are also displayed on the **Door** information screen, depending on the connection type that you select.

The connection type options are described in the following table.

Table 12: Connection type options

Option	Description
Offline	Used for doors that are not connected to the SALTO network and need to be updated using a PPD. See *PPD* for more information about PPDs.
Online IP (CU5000)	Used for doors that are hardwired to the SALTO network and managed using Ethernet TCP/IP protocols. See *SALTO Network* for more information. When you select this option, a **Lockdown Area** panel and a **Limited Occupancy Area** panel are displayed on the **Door** information screen. For an online CU, you can add the door to a lockdown area and/or a limited occupancy area if required. See *Lockdown Areas* and *Limited Occupancy Areas* for more information. An **Extended expiration (offline)** checkbox is also displayed. If you select this, any keys that are presented are revalidated for a specific period, even if the CU is offline. See *User and Key Expiration* for more information.
Online IP (CU4200)	Used for doors that are hardwired to the SALTO network and managed using Ethernet TCP/IP protocols. See *SALTO Network* for more information. Data and power are transmitted using a Power over Ethernet (PoE) connection. When you select this option, a **Limited Occupancy Area** panel and a **Lockdown Area** panel are displayed on the **Door** information screen. An **Extended expiration (offline)** checkbox is also displayed. See above for more information about these options. The CU4200 functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.
Online RF (SALTO)	Used for doors that are connected to the SALTO network using RF technology. When you select this option, a **Lockdown Area** panel is displayed on the **Door** information screen. This means you can add the door to a lockdown area if required. See *Lockdown Areas* for more information. The RF functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.
Online RF (BAS)	Used for doors that are connected to a building automation system (BAS) that is integrated with the SALTO network. Before selecting this option, check that your BAS integration has been fully configured in ProAccess SPACE General options. See ***Error! Reference source not found.*** for more information. When you select this option, a **Lockdown Area** panel is displayed on the **Door** information screen. See *Lockdown Areas* for more information. The RF functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

5. 5. 3. 2. Opening Modes and Timed Periods

The **Open mode** drop-down list defines the lock's working mode.

NOTE: If you select certain opening modes, additional information fields and drop-down list options are displayed.

The options are described in the following table.

Table 13: Door open mode options

Option	Description
Standard	The lock only opens when an authorized key is used.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Office</td><td>The lock can be left open by any user who has the Office option selected in their user profile and has access to the door. See Mobile Phone Data
The Mobile Phone Data panel defines what mobile application the user will use.
Table 21: Mobile Phone Data options
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>International phone number</td><td>User mobile phone number. The Area code has to be entered first according to the country the mobile phone line is from.</td></tr>
<tr><td>Mobile app: JustIN mSVN</td><td>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.</td></tr>
<tr><td>Mobile app: JustIN Mobile</td><td>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.</td></tr>
</table>
Key Options for more information. To activate Office mode, present the key to the lock, while keeping the inner handle pressed down. To disable the Office mode, repeat the procedure.</td></tr>
</table>

Option	Description
Timed office	This is the same as the Office mode detailed above except that the Office mode is only allowed during defined time periods (for example from 08:00 to 15:00). The time periods must be previously defined. See *Roll-Call Areas* *A roll* call is used to list the individual users in a specified area at a particular time. For example, you can use a roll call to generate a report after a fire alarm goes off. This way, it is possible to check whether all the users in the area have been safely evacuated. The system generates the roll call by monitoring specific access points. By tracking when cardholders enter and exit using these access points, it is possible to see exactly who is inside or outside the roll-call area. The roll-call functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information. See *Roll-Call* for information about generating a list of individual user names in a roll-call area in ProAccess SPACE. You can also use ProAccess SPACE Roll-Call Monitoring to perform other roll-call tasks, such as searching all roll-call areas for a user and the time and date each user entered the roll-call area. See *Roll-Call* for more information.

5. 5. 4. Creating Roll-Call Areas

To create a roll-call area, perform the following steps:

1. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.

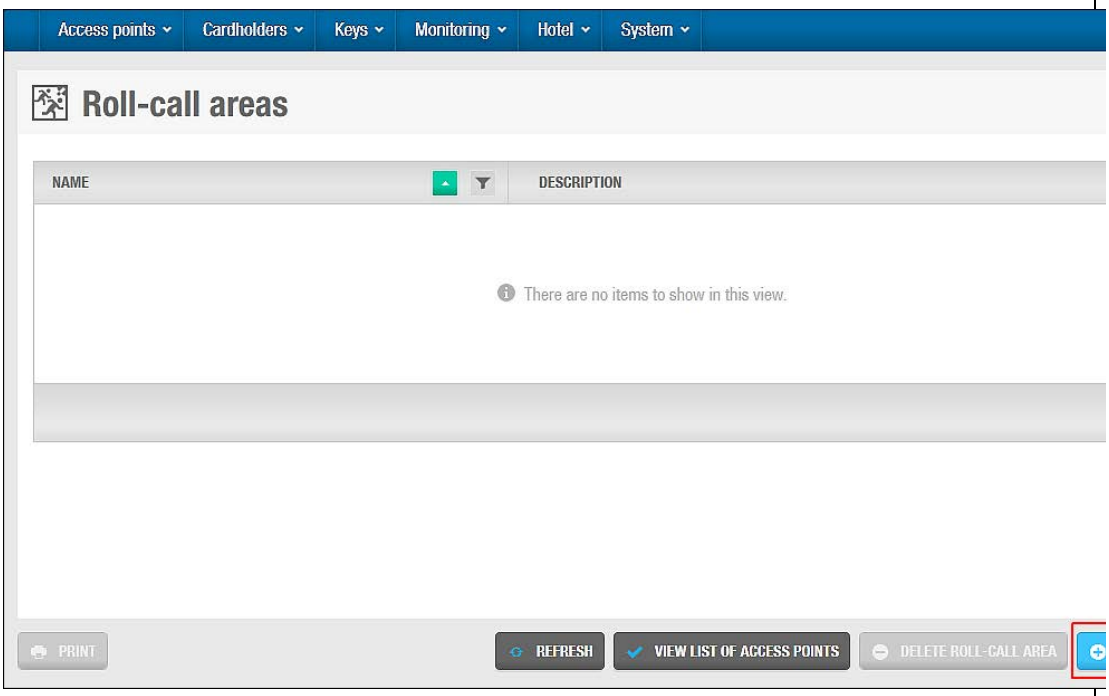
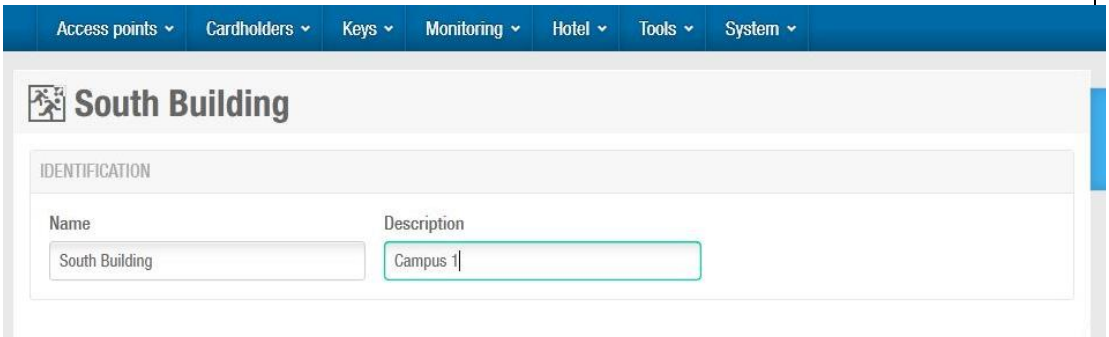


Figure 75: Roll-call areas screen

NOTE: The **View List of Access Points** button shows a list of access points associated with all roll-call areas.

2. Click **Add Roll-Call area**. The **Roll-call area** information screen is displayed.



Option	Description
Automatic opening	The lock opens automatically at specific times and remains open during a defined time period (for example from 08:00 to 18:00). At the end of each time period, the lock closes and reverts to Standard mode. It is essential to set an access point timed period for this mode.
Toggle	The lock can be left open by any authorized user that presents a valid key. You do not need to hold down the inner handle. The next authorized key presented then closes the door. This continues switching (toggling) on presentation of each valid key.
Timed toggle	This mode operates in the same way as the Toggle mode described above. However, you can only toggle the Office mode on and off within set access point timed periods.
Keypad only	The lock can be opened at any time by typing a valid code on a keypad. The keypad code must contain between one and eight digits and is the same for every user. When you select the **Keypad only** option from the **Open mode** drop-down list, a keypad code field is displayed in which you can define the code. The lock can also be opened with a valid key.
Timed keypad	This mode is the same as the Keypad only mode described above except that the Keypad only mode is only allowed during a defined timed period. The lock can be opened with a key at any time.
Key + PIN	The lock can only be opened using both a valid key and by typing a valid PIN on the keypad. This acts as a dual security control. If the PIN code is incorrect, access will not be granted. The PIN must be defined in the user profile. See *PIN Codes* for more information.
Timed key + PIN	This is the same as the Key + PIN mode above except that the Key + PIN mode is only allowed during specific time periods. Outside of these time periods, the lock operates in Standard mode.
Automatic opening + Office	This mode works in the same way as the Automatic opening mode. However, outside of the timed period, the lock reverts to Office mode rather than Standard mode.
Automatic opening + toggle	This mode is the same as Automatic + Office mode except that outside of the timed period the lock reverts to the Toggle mode.
Automatic changes	This 'mode' acts as an indication that the lock will work with a mixture of modes during certain time periods throughout the day. The combination of modes is defined in an automatic changes entry, for example, Automatic change#001. You can select an automatic changes entry using the drop-down list in the **Automatic changes** field. See *Access Point Automatic Changes* for more information.
Exit leaves open	The lock remains open when the inner handle is used until a valid key is presented. To activate this opening mode option, you must enable the EXIT_LEAVES_OPEN parameter in ProAccess SPACE General options. See ***Error! Reference source not found.*** for more information. This also activates the **Toggle + Exit leaves open** mode option in the **Open-mode** drop-down list.
Toggle + Exit leaves open	This mode is a combination of the Toggle mode and the Exit leaves open mode. The lock opens when an authorized key is presented and closes when the next authorized key is presented. The lock continues to switch back and forth on presentation of each valid key. However, when the inner handle is lowered, the lock remains open. To activate this opening mode option, you must enable the EXIT_LEAVES_OPEN parameter in ProAccess SPACE General options. See ***Error! Reference source not found.*** for more information.

5. 5. 5. 2. Opening Times

The **Opening Time** panel defines how long a door stays open after it has been unlocked.

The options are described in the following table.

Table 14: Door opening times

Option	Description
Open time	Defines how long the handle remains active. The door locks as soon as the handle is released, even if the time value is not reached. The default time value is six seconds. The value can be increased or decreased in the range 0 to 255 seconds.
Increased open time	Defines a longer opening time. This option is designed for disabled or 'hands full' users. The default time value is 20 seconds. The value can be increased or decreased in the range 0 to 255 seconds. You must enable this option in the user's profile. See *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. 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. Key Options for more information.

5. 5. 5. 3. Calendars and Time Zones

The **Calendar** drop-down list defines which calendar is applied to the door. See *PPD*

PPDs are connected to the operator's local PC through either a USB or COM port. See *PPD Settings* for more information. PPDs allow data to be transferred between the operator's PC and the locks. Data is downloaded from the PC to the PPD, and the PPD is used to perform tasks such as lock initialization and emergency openings. In the process, the PPD retrieves information (such as battery status) from the locks. This information is communicated to the system when the PPD is connected to the operator's PC.

See the *Portable Programming Device by SALTO* document for more information about PPDs and their configuration settings.

Table 56: PPD

 Portable Programming Device (PPD)	Used by admin operators to transfer configuration changes to a lock or by maintenance operators to check the battery status of the lock and collect the lock's audit trail

NOTE: It is important that the time is set correctly for the PC on which the SALTO software is running, as this controls the time and date settings for locks.

5. 5. 6. Peripheral Types

The functionality of the PPD is described in the following table.

Table 57: Peripheral types

Peripheral	Functionality
PPD	Communicates information to the locks such as door identification and configuration details. The operator downloads the information from their PC to the PPD and the PPD can then be connected to the lock. In this way, information is transferred to the lock. PPDs are used to: ▪ Update configuration changes to the lock (door profile, calendars etc.) ▪ Manually retrieve the audit trail stored on the lock for uploading to the server ▪ Perform a firmware diagnostic evaluation of the locking electronic components ▪ Upgrade the firmware of the locking components ▪ Open a door in the event of an emergency ▪ Read the battery status of the lock ▪ Perform a general diagnostic evaluation of the system

PPDs are configured in ProAccess SPACE General options. See *Devices Tab* for more information. The **PPD** information screen in ProAccess SPACE is used to download access point data to PPDs. This allows you to perform tasks with PPDs such as initializing and updating locks. You can also view the status of PPDs and update their firmware by using the **PPD** information screen.

5. 5. 7. PPD Menu Options

PPDs have seven menu options. Some of the menu options are available by default. Others are enabled when you select particular options on the **PPD** information screen in ProAccess SPACE, and download access point data to the PPD. See the *Portable Programming Device by SALTO* document for more information about using PPDs.

The options are described in the following table.

Table 58: PPD menu options

Option	Description
Update locks	Used to update a lock when the PPD is connected to it. To enable this menu option, you must download the appropriate access point data to the PPD by using the **PPD** information screen.
Firmware diagnostic	Used to perform a firmware diagnostic of the locking electronic components
Update firmware	Used to update the firmware of the locking electronic components
Collect audit trail	Used to collect audit trail data from offline doors and transfer it to the operator's local PC

Option	Description
Emergency opening	Used to perform an emergency opening if the lock battery dies or a reader error occurs. To enable this menu option, you must select the **Allow emergency opening** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. Alternatively, you can set this as a default option in ProAccess SPACE General options. You can also set a password for performing emergency openings using the PPD if required. See *Performing Emergency Door Openings* and *Devices Tab* for more information.
Initialize lock	Used to transfer access data to new locks or existing locks that have been fitted on a different access point and renamed. To enable this menu option, you must select the **Initialize locks** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. See *Initializing Locks* for more information.
Diagnostic	Used to retrieve information from the lock such as the battery status or serial number

5. 5. 8. Viewing PPD Status

You can view the status of a PPD you have connected to the PC by selecting **System** > **PPD**.

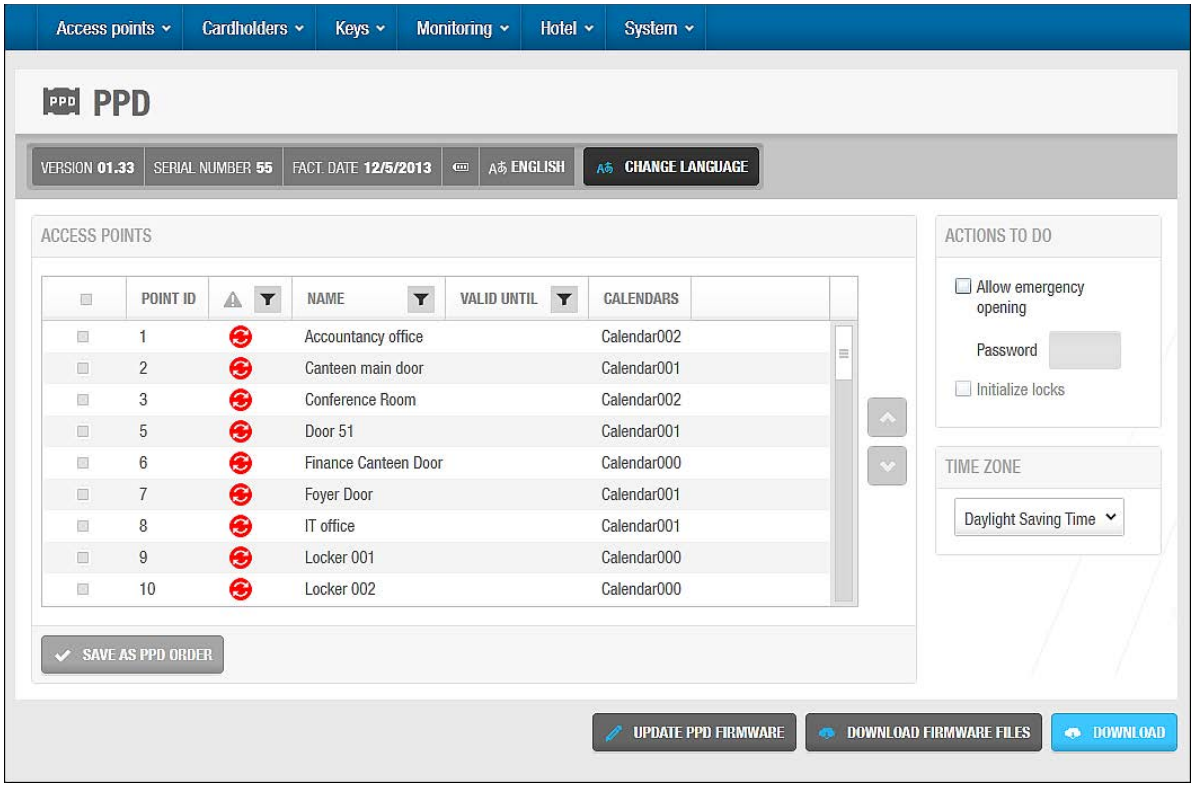


Figure 238: PPD information screen

The **PPD** information screen shows the following information about the PPD:

- Version
- Serial number
- Factory date (or date of manufacture)
- Battery status

- Language

5. 5. 9. Changing the PPD Language

You can change the language of the display messages in the PPDs if required.

To change the language displayed in a PPD, perform the following steps:

1. Connect the PPD to the PC.
2. Select **System** > **PPD**. The **PPD** information screen is displayed.
3. Click **Change Language**. The **Change language** dialog box is displayed.

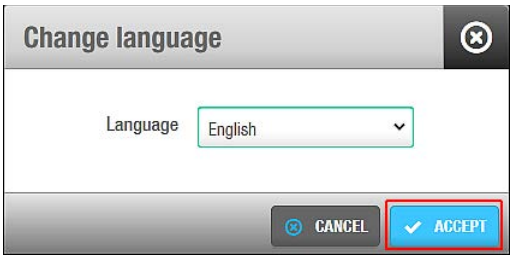


Figure 239: Change language dialog box

4. Select the required language from the **Language** drop-down list.
5. Click **Accept**. The **PPD** progress screen is displayed.
6. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
7. Click **OK**.

5. 5. 10. Using the PPD Information Screen

The **PPD** information screen displays a list of access points. This list varies depending on which time zone is selected in the **Time Zone** panel. It is important to remember that only access points for the selected time zone are displayed. Note that you must enable the multiple time zones functionality in ProAccess SPACE General options to display this panel in ProAccess SPACE. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Access points that need to be updated have a red **Update required** icon on the left-hand side of their name. You can download access point data to a PPD you have connected to the PC by selecting the required access points and clicking **Download**. You can then perform tasks such as updating locks with the PPD. See *Updating Locks* for more information. You must select additional options in the **Actions To Do** panel for certain tasks, for example, initializing locks. See *Initializing Locks* and *Performing Emergency Door Openings* for more information about this panel.

The following table describes some useful screen items.

Table 59: PPD information screen items

Item	Description
Access point checkboxes	Allow you to select individual access points
Checkbox column header	Allows you to select all of the displayed access points. To do so, select the checkbox in the column header.
Chevrons	Allow you to move entries up and down in the access point list

Item	Description
Save As PPD Order button	Allows you to save the access point list order. This specifies the order in which access point data is downloaded to the PPD and displayed in the PPD's menu.
Expand icon	Allows you to view the ESDs for rooms and suites. This icon is displayed on the left-hand side of the room and suite names.

5. 5. 11. Updating PPD Firmware

Firmware is software that is programmed on the read-only memory (ROM) of hardware devices. Firmware updates are available when a new version of the SALTO software is downloaded. Your SALTO technical support contact may also recommend specific firmware updates if required.

To update the firmware of a PPD, perform the following steps:

1. Connect the PPD to the PC.
2. Select **System** > **PPD**. The **PPD** information screen is displayed.

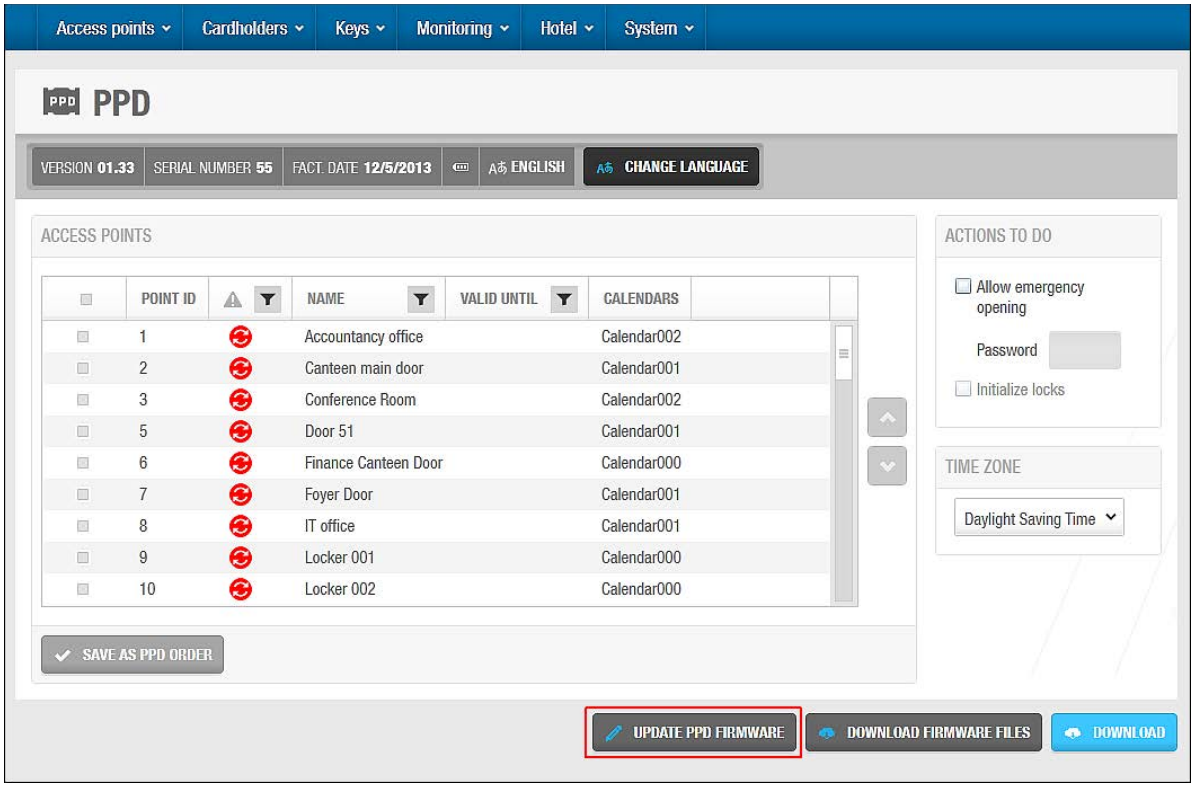


Figure 240: PPD information screen

3. Click **Update PPD Firmware**. The **Update PPD Firmware** dialog box, showing the available firmware files, is displayed.

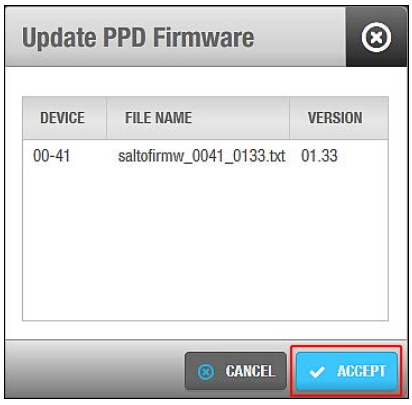


Figure 241: Update PPD Firmware dialog box

4. Select the required file.
5. Click **Accept**. The **PPD** progress screen is displayed.
6. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
7. Click **OK**.

5. 5. 12. Downloading Firmware Files

You can download firmware files to the PPD and use it to update the locking electronic components.

To download a firmware file to a PPD, perform the following steps:

1. Connect the PPD to the PC.
2. Select **System** > **PPD**. The **PPD** information screen is displayed.

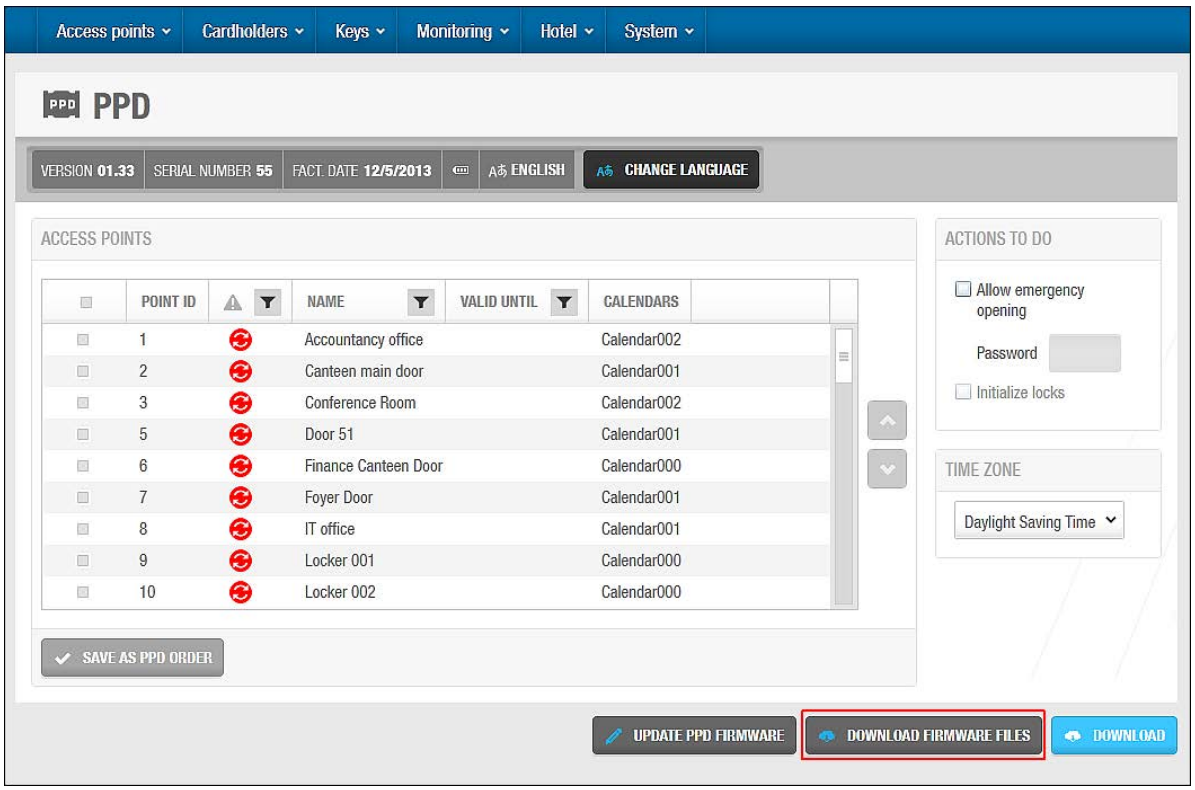


Figure 242: PPD information screen

3. Click **Download Firmware Files**. The **Download Firmware files** dialog box, showing the available firmware files, is displayed.

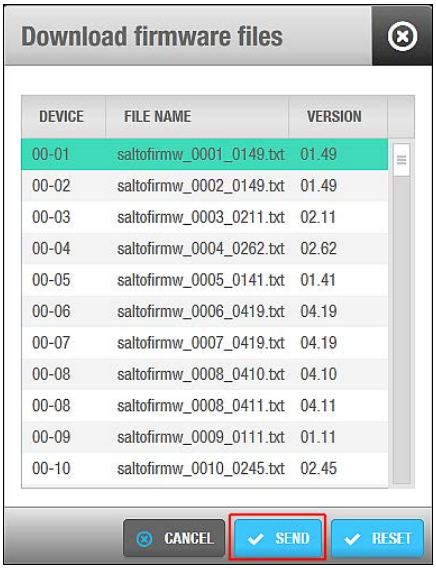


Figure 243: Download firmware files dialog box

4. Select the required file.

   You can hold down the Ctrl key while clicking the files to make multiple selections. Note that you can click **Reset** to delete any firmware files you have already downloaded.
5. Click **Send**. The **PPD** progress screen is displayed.
6. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
7. Click **OK**.

   You can now use the PPD to update the firmware of locking electronic components by selecting **Update Firmware** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

5. 5. 13. Initializing Locks

You must initialize each lock when it is installed. This programmes the lock, and transfers access point data relating to time zones and calendars, for example.

It is recommended that you connect the PPD to the PC after you initialize locks to communicate the most up-to-date information about the locks to the system.

NOTE: You can configure PPDs to assign IP addresses to online IP (CU5000) doors during initialization if required. You must enter each IP address on the system by using the **Access point: Online IP CU5000** information screen. Note that you must select **System** > **SALTO Network** and double-click the required online IP (CU5000) door on the **SALTO Network** screen to view the information screen. You must enable this option in ProAccess SPACE General options by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

PPDs can also be used to transfer SAM data to SALTO locks and wall readers during initialization (or when you perform updates). See *SAM and Issuing options General* options

See *General options* section.

SAM and Issuing Data for more information.

To initialize a lock, perform the following steps:

1. Connect the PPD to the PC.
2. Select **System** > **PPD**. The **PPD** information screen is displayed.

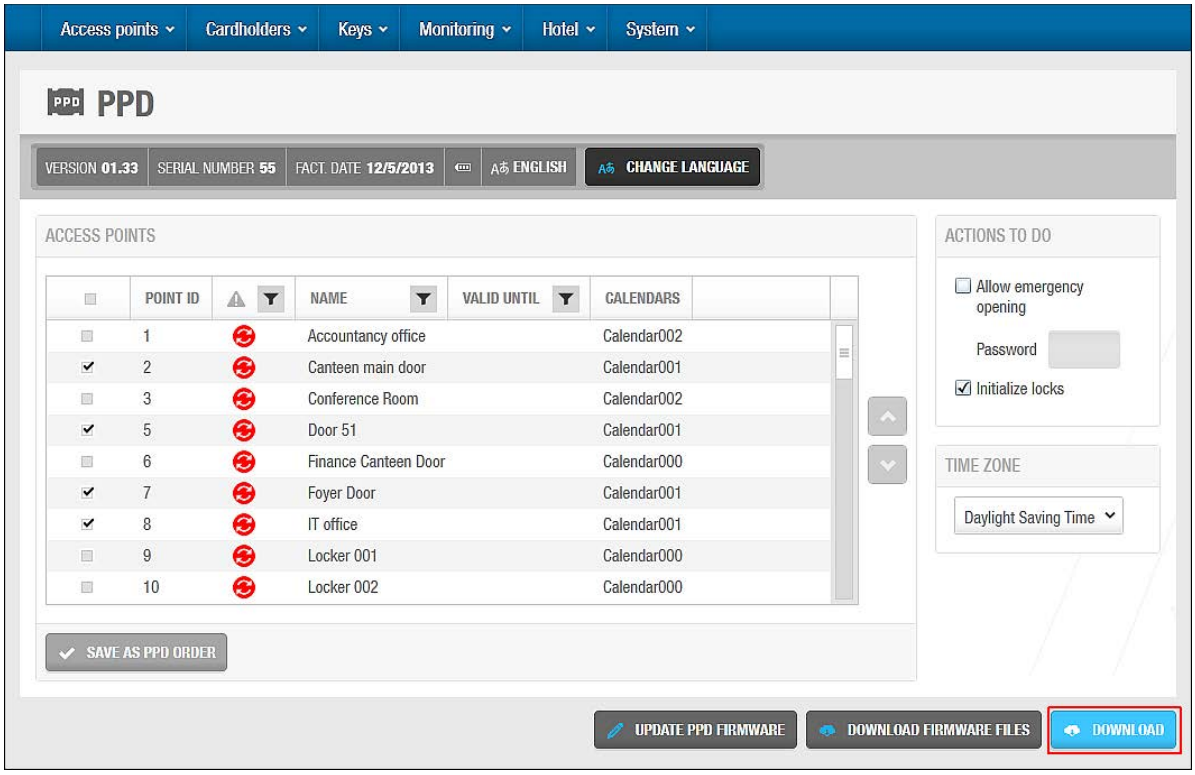


Figure 244: PPD information screen

3. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

   Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.
4. Select the checkbox of the access point for which you want to initialize the lock.

   You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.
5. Select the **Initialize locks** checkbox in the **Actions To Do** panel.
6. Click **Download**. The **PPD** progress screen is displayed.
7. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.

   You can now use the PPD to initialize the lock of the selected access point by selecting **Initialize Lock** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: If you initialize a lock that is already in use, its audit trail is deleted.

5. 5. 14. Initializing Rooms and ESDs

The procedure for initializing rooms and ESDs is the same as for initializing locks. See *Initializing Locks* for more information and a description of the steps you should follow.

NOTE: You can initialize rooms and their associated ESDs either together or separately. However, all of the rooms and ESDs that you select during the initialization process must have the same calendar.

5. 5. 15. Updating Locks

You must update offline locks when you make certain changes to access point data, such as enabling anti-passback or changing the opening mode of doors. You can view locks that need to be updated on the **PPD** information screen by selecting **System** > **PPD**. Note that you must connect a PPD to the PC before you can access the **PPD** information screen. Access points that need to be updated have a red **Update required** icon on the left-hand side of their name.

It is recommended to update offline locks at least every six months to ensure that the clock and calendars are up to date. You must also update locks after you replace their batteries. This is because access point data relating to time zones and calendars, for example, must be restored after a lock's battery dies.

You should connect the PPD to the PC after you update locks to communicate the most up-to-date information about the locks to the system.

To update a lock, perform the following steps:

1. Connect the PPD to the PC.
2. Select **System** > **PPD**. The **PPD** information screen is displayed.

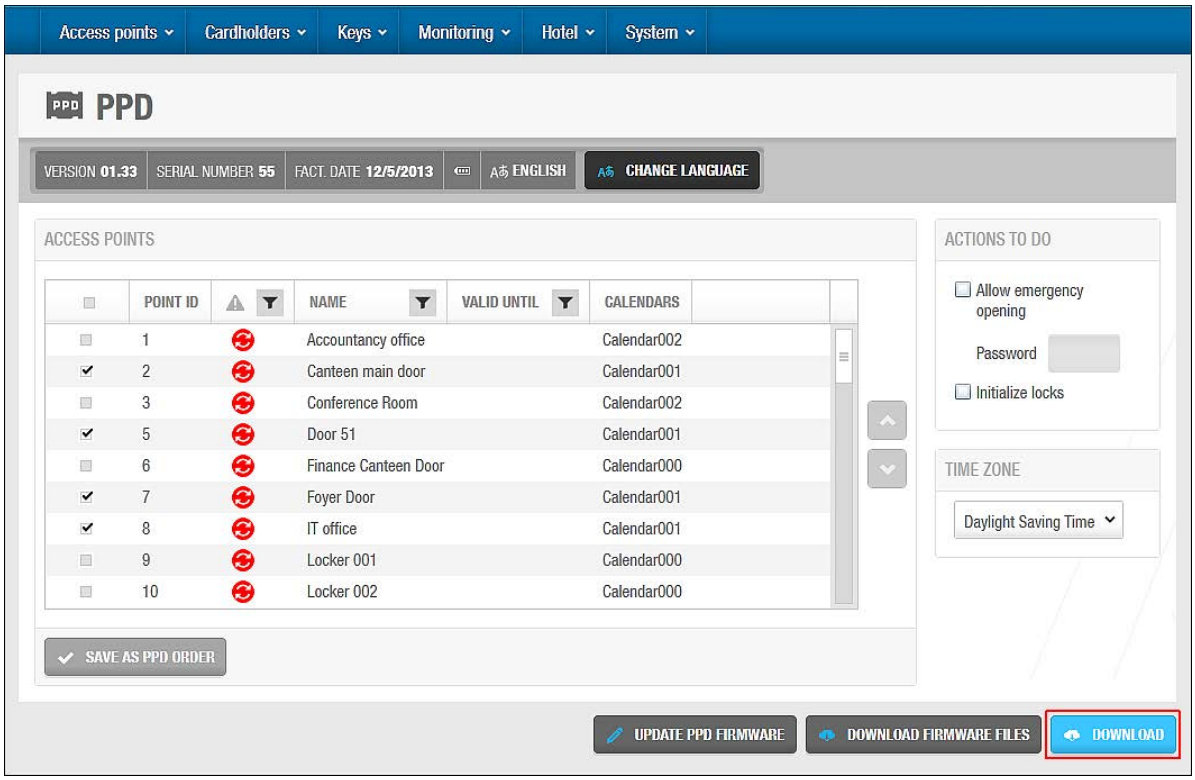


Figure 245: PPD information screen

3. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

   Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

4. Select the checkbox of the access point for which you want to update the lock.

   You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

5. Click **Download**. The **PPD** progress screen is displayed.
6. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
7. Click **OK**.

   You can now use the PPD to update the lock of the selected access point by selecting **Update Locks** in the PPD's menu and connecting the PPD to the lock. Alternatively, you can simply connect the PPD to the lock. In this case, it recognizes the lock and automatically displays the appropriate data. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: You can configure PPDs to automatically collect audit trail data when they are used to update locks. You must enable this option in ProAccess SPACE General options by selecting the **Collect audit trails automatically when updating locks** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

5. 5. 16. Performing Emergency Door Openings

You can use the PPD to perform an emergency opening if the lock battery dies or a reader error occurs, for example.

NOTE: You can perform emergency openings of online doors without using a PPD. See *Lockdown* for more information.

To perform an emergency opening, perform the following steps:

1. Connect the PPD to the PC.
2. Select **System** > **PPD**. The **PPD** information screen is displayed.

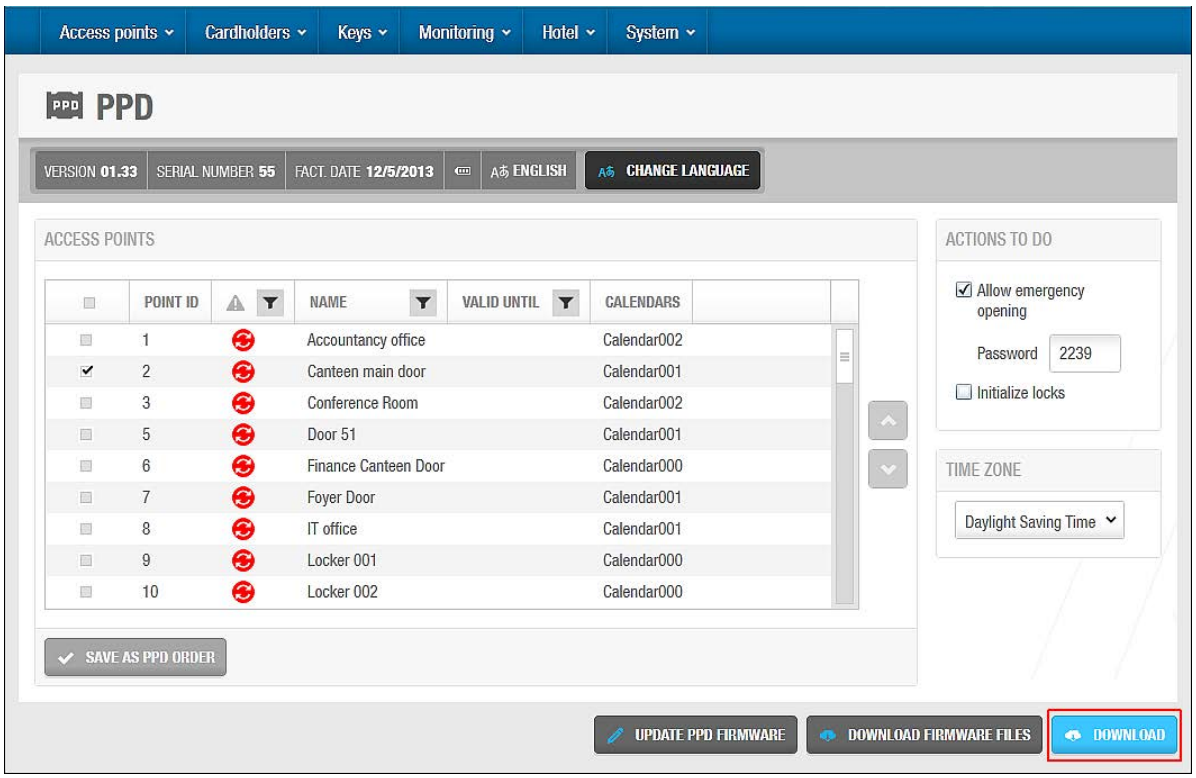


Figure 246: PPD information screen

3. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

   Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

4. Select the checkbox of the access point for which you want to perform the emergency opening.

   You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

5. Select the **Allow emergency opening** checkbox in the **Actions To Do** panel.

   The checkbox is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options. See *PPD Tab* for more information. Otherwise, you must select it each time you want to perform an emergency opening.

6. Type a password for the emergency opening in the **Password** field if required.

   The password can only contain digits. If you type a password, you must enter this password in the PPD before you can perform the emergency opening. Otherwise, the PPD does not require a password. The **Password** field is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options and entered a password there already for the option. See *Devices Tab* for more information. Your PPD firmware must be version 01.29 or higher to use this option.
7. Click **Download**. The **PPD** progress screen is displayed.
8. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
9. Click **OK**.

   You can now use the PPD to perform an emergency opening of the selected access point by selecting **Emergency Opening** in the PPD's menu and connecting the PPD to the lock. Note that you are required to enter a password in the PPD if you have enabled this option in either ProAccess SPACE PPD window or ProAccess SPACE Devices window. See the *Portable Programming Device by SALTO* document for more information about this process.

5. 5. 17. Collecting Audit Trail Data from Offline Doors

See *Audit Trails* for more information about audit trails. You must use a PPD to collect audit trail data from offline doors. See the *Portable Programming Device by SALTO* document for more information about this process. When you have collected the data, you can view it in ProAccess SPACE.

To view the audit trail data on the system, perform the following steps:

1. Connect the PPD to the PC.
2. Select **System** > **PPD**. The **PPD** information screen is displayed.

   The **Audit Trail** information screen is automatically updated with the information from the connected PPD when you display the **PPD** information screen.
3. Select **Monitoring** > **Audit Trail**. The **Audit trail** information screen, showing the new audit trail data, is displayed.

5. 6. SALTO Network

The SALTO network includes items like encoders, gateways, radio frequency (RF) nodes, CU4200 nodes, online doors, and CUs. These are added and managed in ProAccess SPACE. See *SALTO Virtual Network* for more information about the SALTO network.

The RF and CU4200 functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

NOTE: You can view the enabled channels for RF signals in ProAccess SPACE General options. To do so, select **System** > **General options** > **Devices**. There are 16 channels available and all of these are enabled by default. The frequency range of each channel is also displayed. You can disable a channel if required by clearing the checkbox for the channel and clicking **Save**.

RF mode 2 technology is compatible with ProAccess SPACE. However, RF mode

1 technology is not. If your site uses RF mode 1, an upgrade to ProAccess SPACE is not possible, which means that you must continue to use HAMS or ProAccess RW.

You can view the list of SALTO network items by selecting **System** > **SALTO Network**.

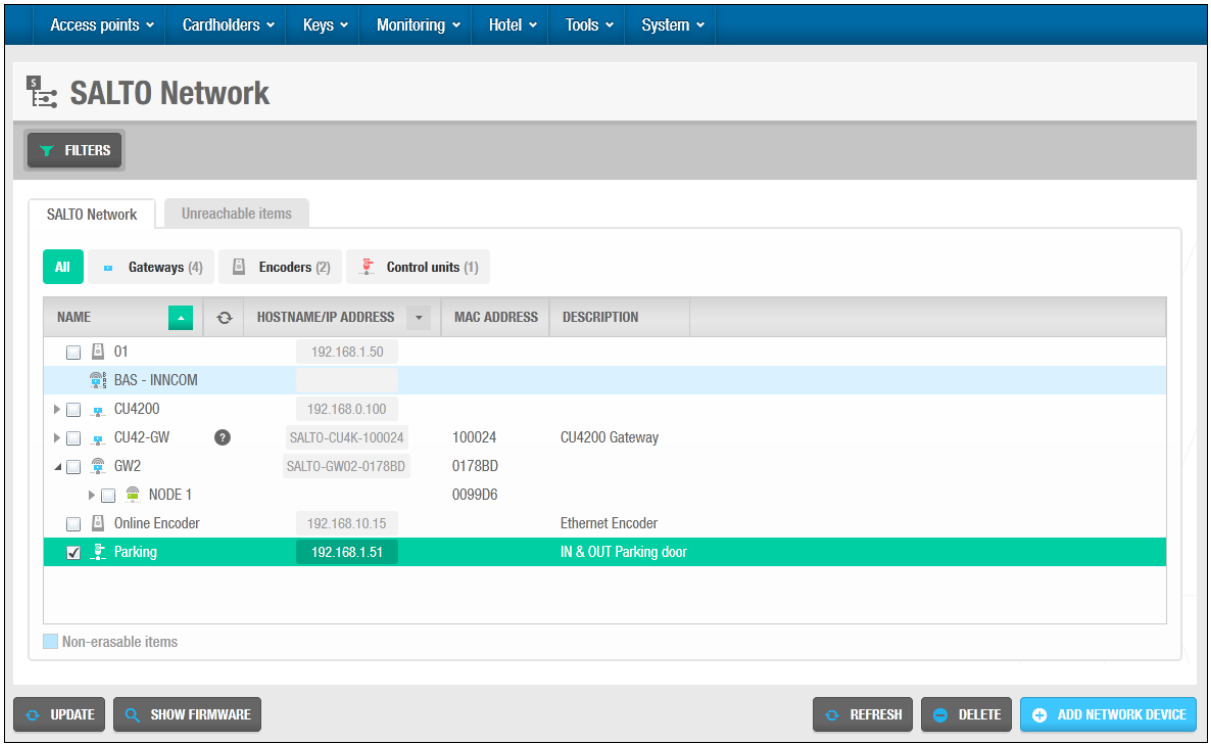


Figure 247: SALTO Network screen

The **SALTO Network** screen displays a list of all network items that have been added and are currently connected to the system.

The information is displayed in four different filtered views:

- **All**: This view shows all of the gateways, encoders, and CUs on the system.
- **Gateways**: This view shows RF gateways and CU4200 gateways. When you click the triangular **Expand** icon on the left-hand side of gateway names, all of the items to which they are connected are displayed. You can view all of the RF nodes and online RF (SALTO) access points connected to each RF gateway, and all of the CU4200 nodes and online IP (CU4200) access points connected to each CU4200 gateway. See *Configuring Online Connection Types* for more information.

NOTE: A BAS gateway may also be displayed on the **SALTO Network** screen. This gateway is created by default if you have fully configured your BAS integration in ProAccess SPACE General options. See *BAS Integration Tab* for more information.

- **Encoders**: This view shows the encoders on the system.
- **Control units**: This view shows online IP (CU5000) access points. See *Configuring Online Connection Types* for more information.

Click the appropriate tab to display each filtered view. The screen also includes an **Unreachable items** tab. Click on this tab to view and configure all items that require additional connection information.

The following table describes the buttons use on the SALTO network main screen.

Table 60: SALTO Network main screen buttons

Item	Description
Update	Allows you to update the selected access point.
Show firmware	Allows you to show the firmware of the selected access point and update it.
Refresh	Allows you to refresh the window with the most updated peripherals status.
Delete	Allows you to delete the selected peripheral.
Add Network device	Allows you to add a new online device.

5. 6. 1. Adding Network Devices

You can add the following network devices to the system:

- Ethernet encoders
- RF gateways
- RF nodes
- CU42E0 gateways
- CU4200 nodes

The following sections describe how to add these devices.

5. 6. 1. 1. Adding Ethernet Encoders

See *Encoders* for more information about encoders.

To add an Ethernet encoder, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Click **Add Network Device**. The **Add network device** dialog box is displayed.
3. Select **Encoder** from the drop-down list.
4. Click **OK**. The **Encoder** information screen is displayed.

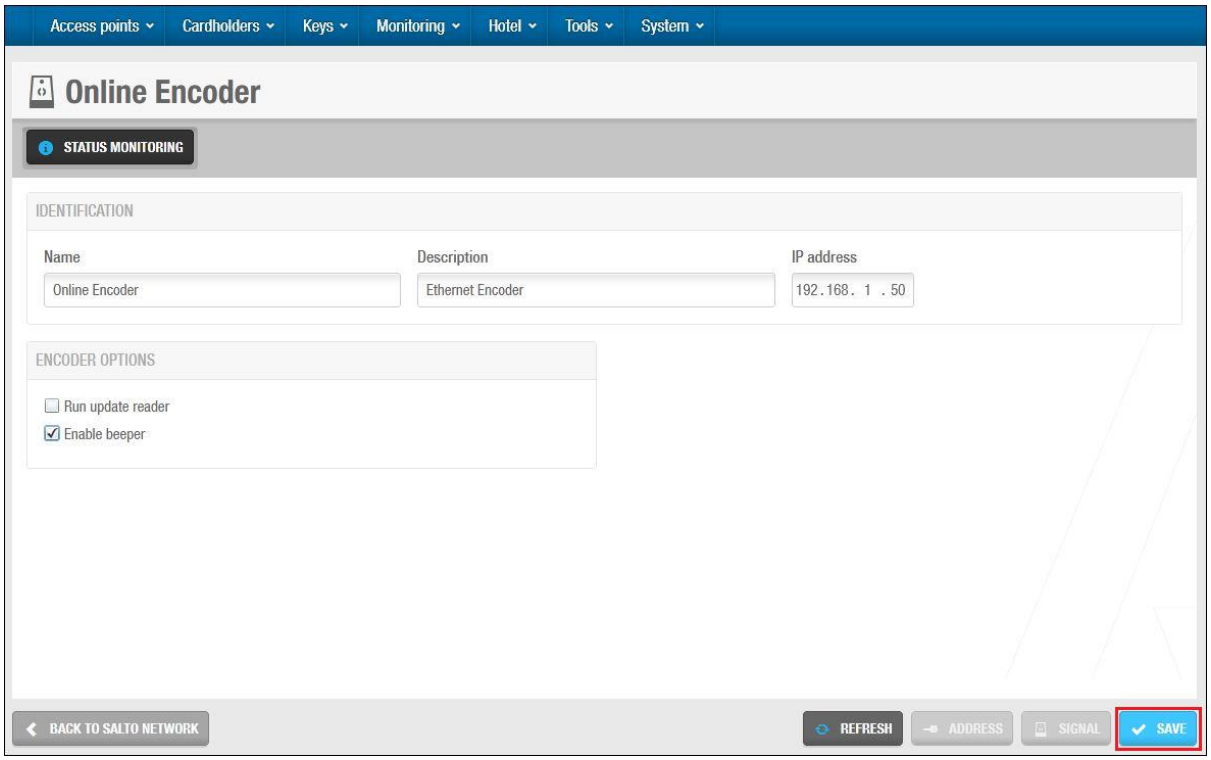


Figure 248: Encoder information screen

5. Type a name for the encoder in the **Name** field.
6. Type a description for the encoder in the **Description** field.
7. Type an IP address for the encoder in the **IP address** field.
8. Select the **Run update reader** checkbox if required.

   This option is used to configure an Ethernet encoder to update user keys automatically when users present their keys to it. If you select this option, the encoder runs continuously but it can only update keys. It cannot be used to encode keys with access data from the SALTO software. See *Updating Keys* for more information.
9. Select the **Enable beeper** checkbox if required.

   If you select this option, the encoder emits beeps when in use.
10. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Click **Save**.

5. 6. 1. 2. Adding RF Gateways

Gateways are hardware devices that provide a link between networks that use different base protocols. RF gateways allow data to be transmitted from the system to the SALTO RF locks, and from the RF locks to the system. RF gateways control RF nodes. See *Adding RF Nodes* for more information about RF nodes.

You must physically connect RF nodes to an RF gateway using an RS485 cable to establish communication between the RF nodes and the RF gateway. See the *SALTO Datasheet_Gatewayx2_xxx* document for more information about this process. You must

also connect RF nodes and RF gateways in ProAccess SPACE so the system can show which nodes and gateways are connected.

To add an RF gateway, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Click **Add Network Device**. The **Add network device** dialog box is displayed.
3. Select **RF gateway** from the drop-down list.
4. Click **OK**. The **RF gateway** information screen is displayed.

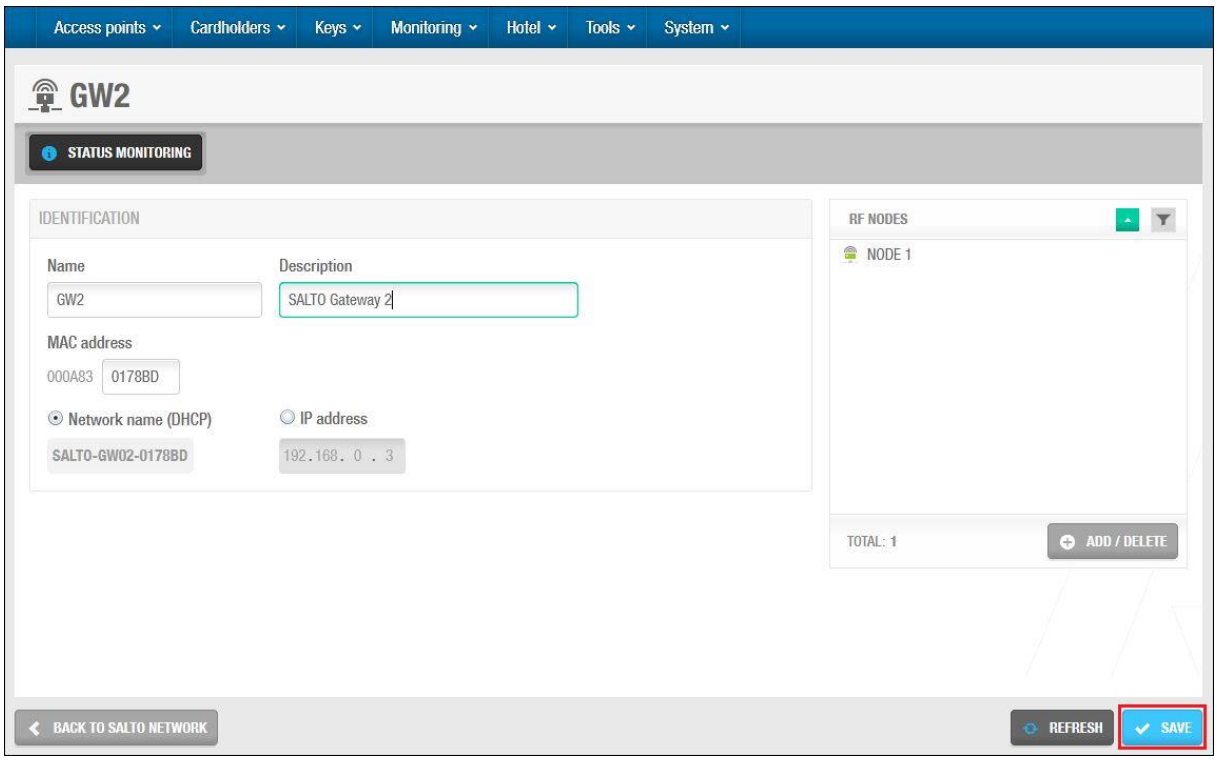


Figure 249: RF gateway information screen

5. Type a name for the RF gateway in the **Name** field.
6. Type a description for the RF gateway in the **Description** field.
7. Type the media access control (MAC) address in the **MAC address** field.

   This is usually displayed on the Ethernet board of the RF gateway.
8. Select either the **Network name (DHCP)** or **IP address** option.

   If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the RF gateway. A Dynamic Host Configuration Protocol (DHCP) server and a DNS are required for this option. If you select the **IP address** option, you must type a static IP address in the field.
9. Select the appropriate time zone from the **Time Zone** drop-down list.

   Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.
10. Click **Add/Delete** in the **RF Nodes** panel. The **Add/Delete** dialog box, showing a list of RF nodes, is displayed.

The **Add/Delete** dialog box only displays RF nodes if you have already added them to the system. You can also connect RF nodes to RF gateways when you add RF nodes to the system. See *Adding RF Nodes* for more information.

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

    You can hold down the Ctrl key while clicking the RF nodes to make multiple selections. You cannot add RF nodes that already belong to another gateway.

12. Click **Accept**. The selected RF node is displayed in the **RF Nodes** panel.
13. Click **Save**.

5. 6. 1. 3. Adding RF Nodes

RF nodes are network connection points that are physically connected to an RF gateway using an RS485 cable. See *Adding RF Gateways* for more information. This establishes communication between the RF nodes and the RF gateways. Also, in ProAccess SPACE you must connect RF nodes to RF gateways, and RF access points to RF nodes. This means that the system can show which items are connected.

NOTE: You must select **Online RF (SALTO)** in the **Connection Type** panel on the **Door** or **Room** information screen to define a door as an RF access point.

To add an RF node, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Click **Add Network Device**. The **Add network device** dialog box is displayed.
3. Select **RF node** from the drop-down list.
4. Click **OK**. The **RF node** information screen is displayed.

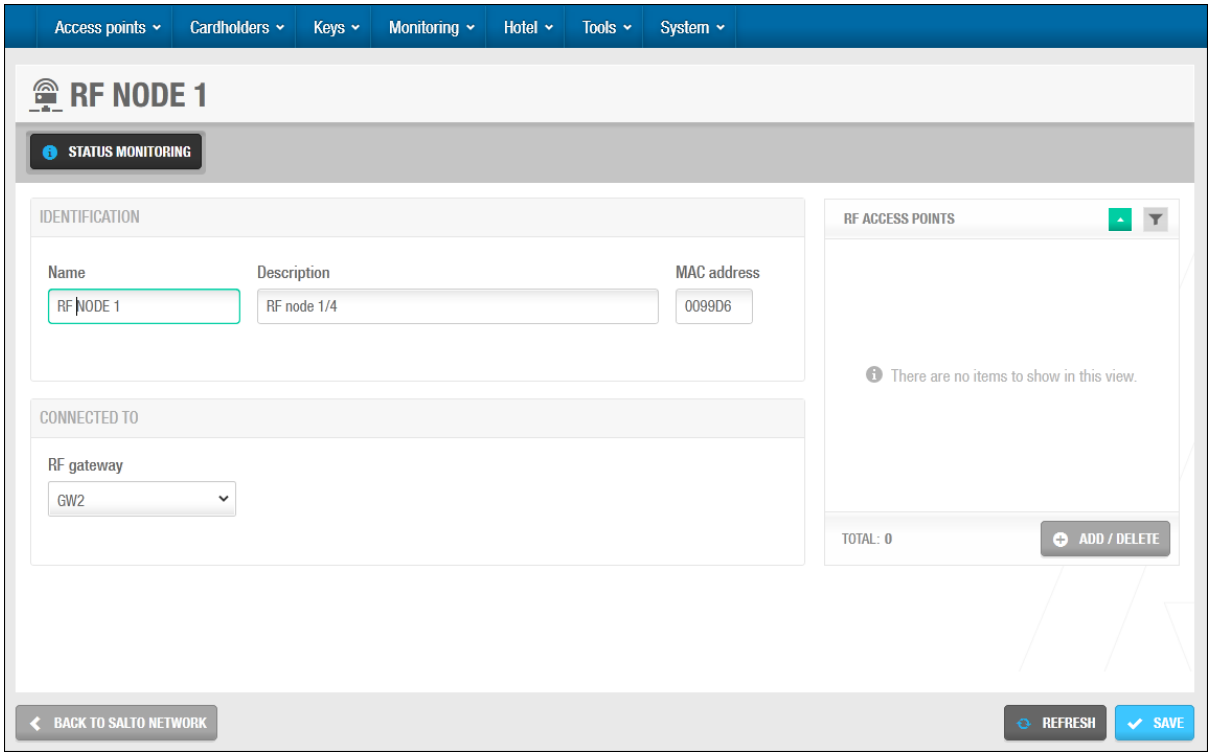


Figure 250: RF node information screen

5. Type a name for the RF node in the **Name** field.

6. Type a description for the RF node in the **Description** field.
7. Type the MAC address of the antenna in the **MAC address** field.
8. Select the RF gateway to which you want to connect the RF node from the **Connected to** drop-down list.

   The default option is **None**.
9. Click **Add/Delete** in the **RF Access Points** panel. The **Add/Delete** dialog box, showing a list of RF access points, is displayed.

   The **Add/Delete** dialog box only displays RF access points if you have already defined doors as RF access points by selecting **Online RF (SALTO)** in the **Connection Type** panel on the **Door** or **Room** information screens. You can also connect online RF (SALTO) doors to RF nodes by using the **Connected to** field on the **Online RF (SALTO)** information screen. See *Online RF (SALTO)* for more information.
10. Select the required RF access point in the left-hand panel and click the chevron. The selected RF access point is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the RF access points to make multiple selections. You cannot add RF access points that already belong to another RF node.
11. Click **Accept**. The selected RF access point is displayed in the **RF Access Points** panel.
12. Click **Save**.

NOTE: RF gateways have a mini node connected to them. You must add this node in ProAccess SPACE by following the procedure for adding RF nodes. Also, you must connect the mini node to the RF gateway in ProAccess SPACE.

5. 6. 1. 4. Adding CU42E0 Gateways

CU42E0 gateways are CUs that are connected to a local area network (LAN) using a network cable. They connect to the SALTO network using a TCP/IP connection. CU42E0 gateways can control CU4200 nodes. See *Adding CU4200 Nodes* section below for more information about CU4200 nodes.

The CU42E0 gateways provide a link between the CU4200 nodes and the SALTO system, and transmit data to the nodes. This means the CU4200 nodes do not require a TCP/IP connection. You must physically connect CU4200 nodes to a CU42E0 gateway using an RS485 cable. This establishes communication between the CU4200 nodes and the CU42E0 gateway. You must also link CU42E0 gateways and CU4200 nodes in ProAccess SPACE so the system can show which nodes and gateways are connected.

CU42E0 gateways control access to doors by activating their relays. Each CU42E0 gateway can control a maximum of two doors. They can also update user keys.

The CU42E0 supports up to 4 auxiliary CU4200 nodes, meaning this that up to 10 online doors can be controlled using a single IP address (1 CU42E0 gateways + 4 CU4200 nodes)

In stand-alone mode, dipswitches on the CU4200 node units must be set up to 0000, if online, each node should have its own configured address, using the suitable dipswitch combination in binary format. See the CU42X0 installation guide for more details. See image below for an example.

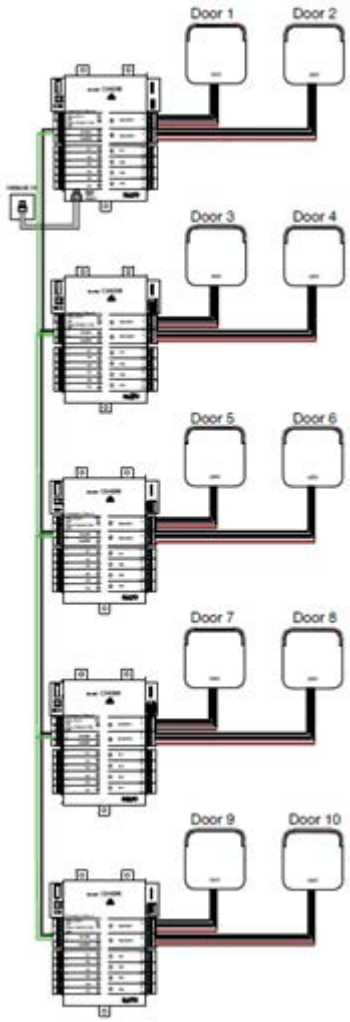


Figure 251: CU42E0 and CU4200 example

NOTE: The maximum distance between the gateway (CU42E0) and the last node (CU4200) in line cannot be over 300 meters.

To add a CU42E0 gateway, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Click **Add Network Device**. The **Add network device** dialog box is displayed.
3. Select **CU42E0 gateway** from the drop-down list.
4. Click **OK**. The **CU42E0 gateway** information screen is displayed.

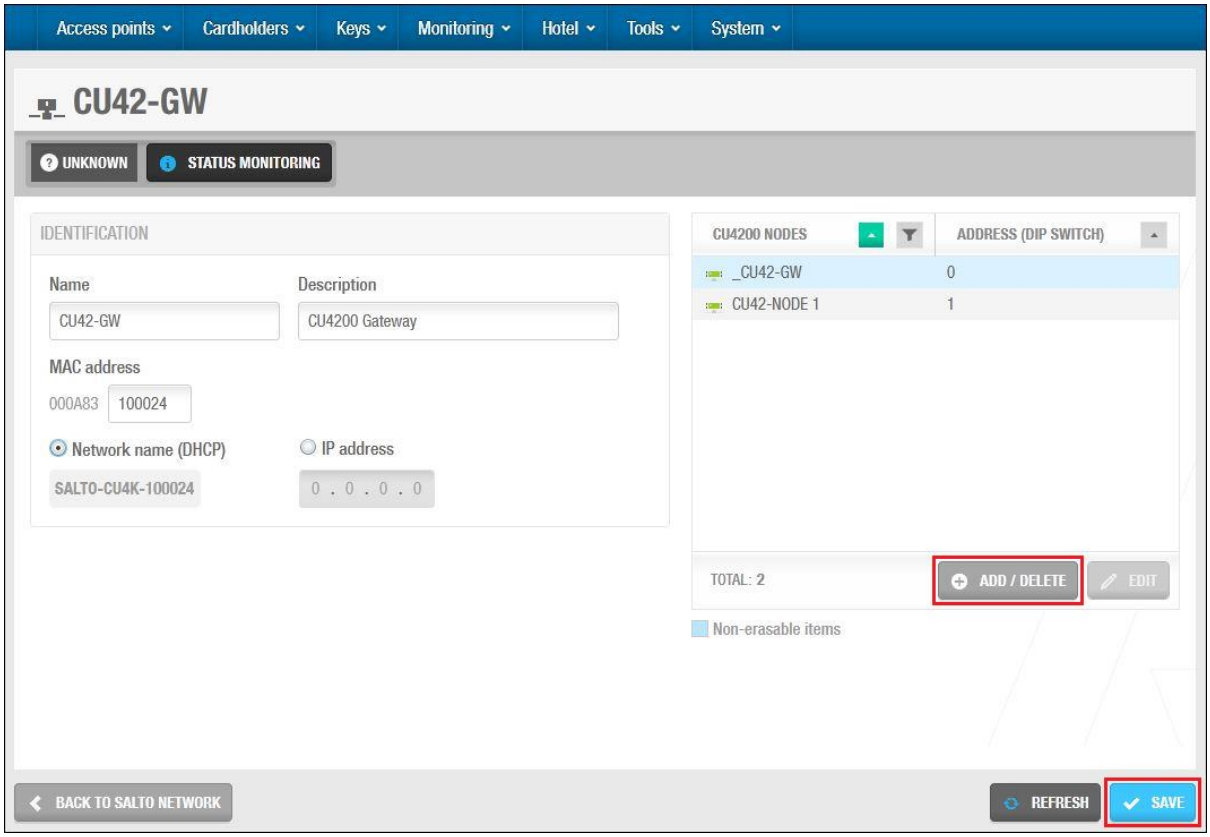


Figure 252: CU4200 gateway information screen

5. Type a name for the CU42E0 gateway in the **Name** field.
6. Type a description for the CU42E0 gateway in the **Description** field.
7. Type the MAC address in the **MAC address** field.

   The MAC address is displayed on a sticker on the CU.
8. Select either the **Network name (DHCP)** or **IP address** radio button.

   If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the CU42E0 gateway. A DHCP server and a DNS are required for this option. If you select the **IP address** option, you must type an IP address in the field.
9. Select the appropriate time zone from the **Time Zone** drop-down list.

   Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.
10. Click **Add/Delete** in the **CU4200 Node** panel. The **Add/Delete** dialog box, showing a list of CU4200 nodes, is displayed.

    The **Add/Delete** dialog box only displays CU4200 nodes if you have already added them to the system. You can also connect CU4200 nodes to CU42E0 gateways when you add CU4200 nodes to the system. See *Adding CU4200 Nodes* for more information.
11. Select the required CU4200 node in the left-hand panel and click the chevron. The selected CU4200 node is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the CU4200 nodes to make multiple selections. You cannot add CU4200 nodes that already belong to another CU4200 gateway.

NOTE: When you add a CU42E0 gateway, an embedded CU4200 node is automatically created. This cannot be deleted. Each CU42E0 gateway can support its embedded CU4200 node and a maximum of four other CU4200 nodes. The name of the embedded node will be always the same than the parent CU42E0 gateway preceeded by an underscore. For example: **_CU4200.**

12. Click **Accept**. The selected CU4200 node is displayed in the **CU4200 Node** panel.

    You can select the CU4200 node and click **Edit** to change the number in the **Address (dip switch)** column if required. See *Adding CU4200 Nodes* for more information about the **Address (dip switch)** field. Note that embedded CU4200 nodes have a fixed number (0). This cannot be changed.
13. Click **Save**.

5. 6. 1. 5. Adding CU4200 Nodes

CU4200 nodes are network connection points that are physically connected to a CU42E0 gateway using an RS485 cable. See *Adding CU42E0 Gateways* for more information about CU42E0 gateways. This establishes communication between the CU4200 nodes and the CU42E0 gateway.

The CU4200 nodes receive data from the CU42E0 gateway so they do not require a TCP/IP connection. Instead, they communicate with the SALTO network through the CU42E0 gateway to which they are connected.

You must connect CU4200 nodes to CU42E0 gateways in ProAccess SPACE. You must also connect CU4200 nodes to access points. This means that the system can show which items are connected. Each CU4200 node can control a maximum of two doors.

NOTE: You must select **Online IP (CU4200)** in the **Connection Type** panel on the **Door** and in **Room** information screen before you can connect an access point to a CU4200 node.

To add a CU4200 node, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Click **Add Network Device**. The **Add network device** dialog box is displayed.
3. Select **CU4200 node** from the drop-down list.
4. Click **OK**. The **CU4200 node** information screen is displayed.

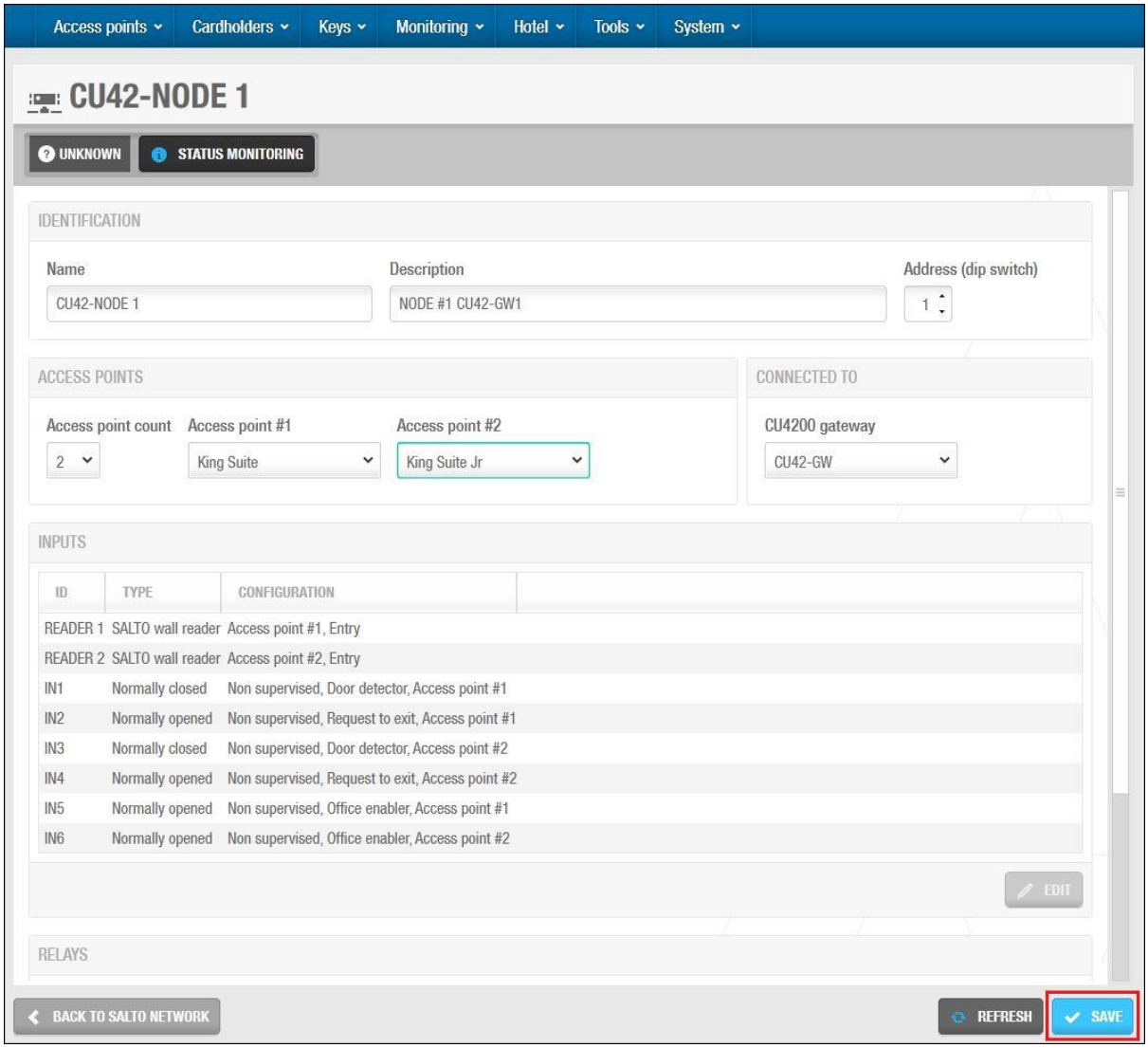


Figure 253: CU4200 node information screen

5. Type a name for the CU4200 node in the **Name** field.
6. Type a description for the CU4200 node in the **Description** field.
7. Select the required number by using the up and down arrows in the **Address (dip switch)** field.

   This number corresponds to the switches on the dip switch panel. The system allows you to select any number between 1 and 99. However, you must select a number between 1 and 15 due to hardware limitations. A CU42E0 gateway can support an embedded CU4200 node and a maximum of four other CU4200 nodes. Each CU4200 node that you connect to a specific CU42E0 gateway must have a unique number, for example, 1, 2, 3, until 15. Note that the value 0 is used for embedded CU4200 nodes. Bear in mind that addresses set up on the nodes should follow the physical dipswitches' configuration on each CU4200 unit.

Table 61: Dipswitch configuration

Dip switch	Address (dip switch)
0000	Address 0, only for embedded CU4200 nodes.
0001	Address 1

Dip switch	Address (dip switch)
0010	Address 2
0011	Address 3
0100	Address 4
0101	Address 5
0110	Address 6
0111	Address 7
1000	Address 8
1001	Address 9
1010	Address 10
1011	Address 11
1100	Address 12
1101	Address 13
1110	Address 14
1111	Address 15

See the following image as an example;

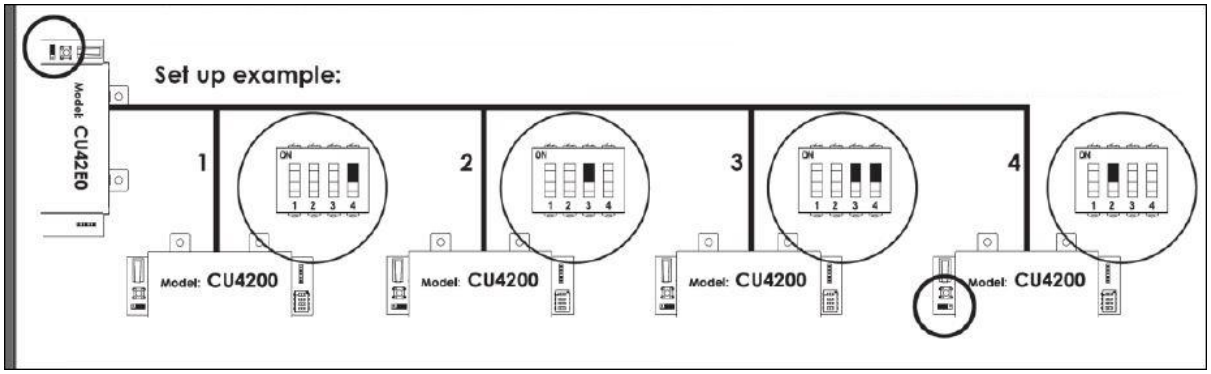


Figure 254: CU4200 dip switches set up

8. Select the required number from the **Access point count** drop-down list.

   You can select either **1** or **2.** This defines the number of doors you want the CU4200 node to control. Each CU4200 node can control two readers. This means it can control either one door that has two readers or two doors where each has one reader. If a door has two readers, one reader controls access from inside to outside, and the other reader controls access from outside to inside. You should select **1** if a door has two readers. If you select **2,** an **Access point #2** field is displayed on the right-hand side of the **Access point #1** field, and you can select an additional door from the drop-down list.

9. Select the required door from the **Access point #1** drop-down list.

   The **Access point** drop-down lists only display doors if you have already defined some as CU4200 access points. This is done by selecting **Online IP (CU4200)** in the **Connection Type** panel on the **Door** information screen. You can also connect online IP (CU4200) doors to CU4200 nodes in the **Connected to** field on the **Online IP (CU4200)** information screen. See *Online IP (CU4200)* for more information.

10. Select the CU42E0 gateway to which you want to connect the CU4200 node from the **Connected to** drop-down list.
11. Click **Save**.

5. 6. 1. 6. Using CU4200 Inputs

Inputs are the signals or data received by the CU4200. You can setup the inputs in ProAccess SPACE so the CU4200 can understand how to act. You can set Inputs for **Reader 1** and **Reader 2.** You can also set up to 6 inputs from third party devices.

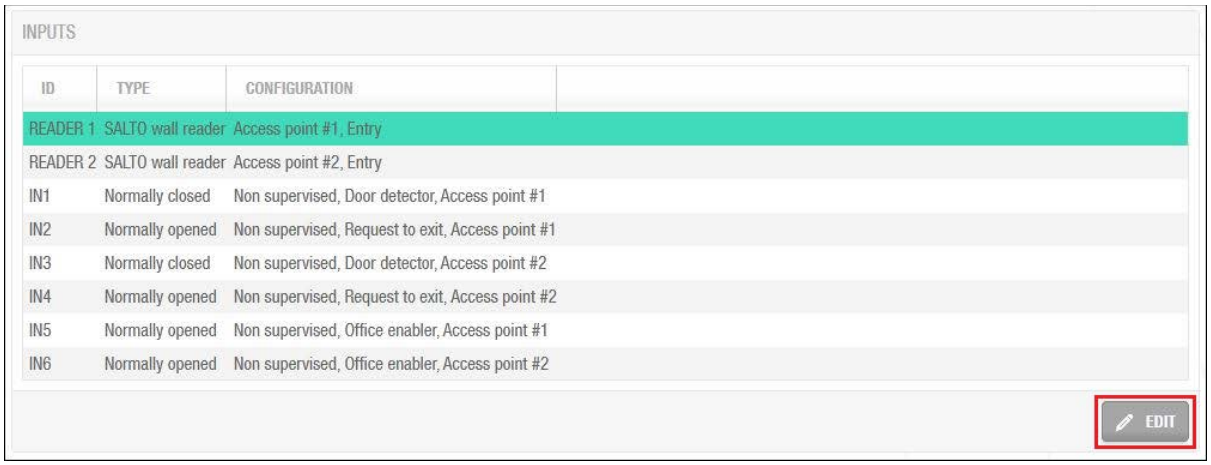


Figure 255: CU4200 node Inputs

You can set the CU4200 outputs according with the wall reader input. To manage the wall reader input, select the reader and click **Edit**.

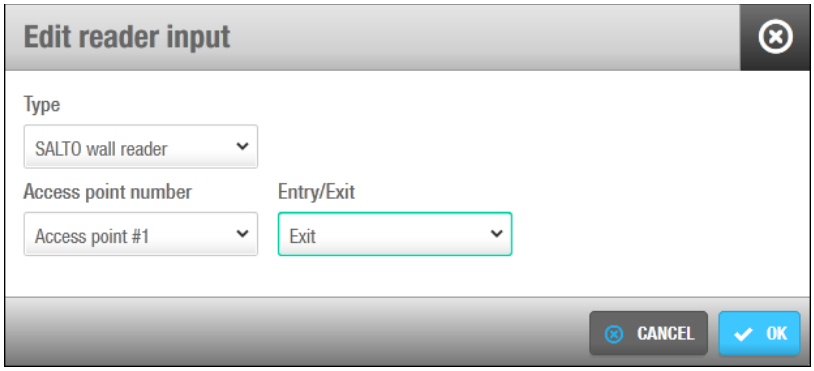


Figure 256: CU4200 node Reader Input

The **Reader input** fields are described in the following table.

Table 62: Reader Inputs fields

Field	Functionality
Type	You can select **None** if no SALTO wall reader is connected or **SALTO wall reader** if it is a SALTO wall reader. Other options may appear in the future. If **None** is selected, inputs 3, 4 and 5, 6 can be used with a third party wall reader.
Access point number	As the CU4200 can manage up to two different access points, you can decide whether the reader will trigger an opening in access point #1 or #2. See *Adding CU4200 Nodes* for more information.

Field	Functionality
Entry/Exit	Select whether the wall reader is an Entry or an Exit.

The CU4200 node can manage inputs from third party devices. Depending the signal or data arrived to the input the CU4200 Node can act accordingly. Select the **Input ID** and click **Edit**.

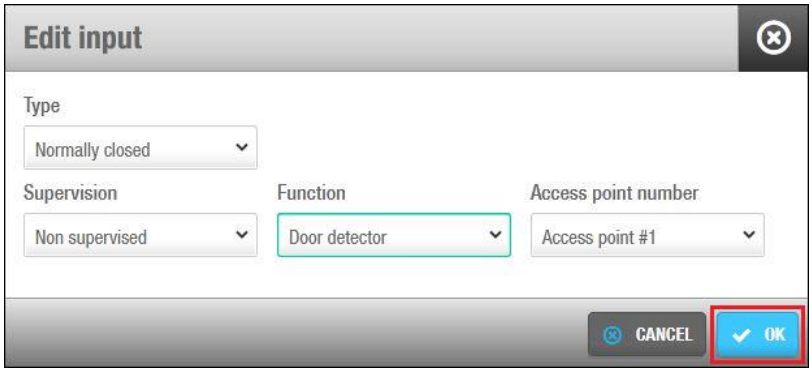


Figure 257: CU4200 node Reader Input

The **Inputs** fields are described in the table below,

Table 63: Inputs fields

Field	Functionality
Type	Status of the relay in normal position. The relay can be normally in closed position or opened position.
Supervision	Select the resistance as required for the supervision. A supervised input is protected against external attacks.
Function	Select the function you want for the relay. Options include doo Door detector, Office enabler, Intrusion inhibition, Request to open roller blind, Request to close roller blind, Request to Exit or Request to Open.

For example, according to the image below, a relay in normally opened position could send a request to open a roller blind when presenting a valid key in reader #1 from IN1 and request to close the roller blind from IN2.

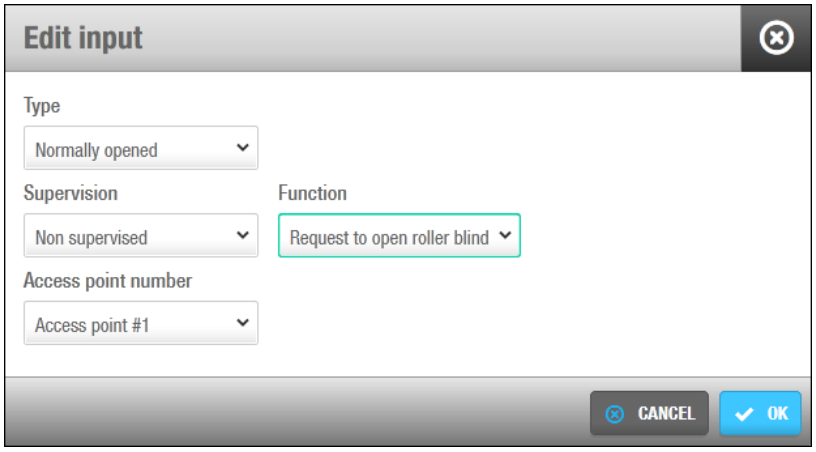


Figure 258: Roller blind example

A reader that is not from SALTO can also be used. **Edit Reader Input** Type must be set to **None**. **Type** field in **Edit Input** shows the **Third party reader** option in the dropdown menu. Only a **Wiegand** code is supported. See *Devices Tab* in General options for more information about how to configure the Wiegand format. An authorization code has to be entered for each user in the **Authorization code** field on the **User** profile. See *Users* in **Cardholders** menu for more information. Select the **Access point** from the **Access point number** dropdown menu and if it will be an **Entry** or an **Exit.**

5. 6. 1. 7. Managing CU4200 Relays

A relay is an electrically operated switch. It is used where it is necessary to control a circuit by a low-power signal. For example, you can control an electric or magnetic strike, trigger a camera recording or turn an alarm off.

The CU4200 node has 4 relays that can be configured independently. Select the relay ID and click **Edit**. The **Edit Relay** fields are described in the table below

Table 64: Edit Relay fields

Field	Functionality
Type	Select the appropriate type as needed.
Access point number	Select the access point in question. It can be **Access point #1, Access point #2** or both.
Output	The **Output** dropdown menu is shown when Output is selected in **Type** dropdown menu. Select the Output from the dropdown menu. The list of outputs have to be created first in **Outputs** list, in the **Access points** menu. See Access points *Outputs* for more information about how to create Outputs. The relay will be triggered when a key with a valid output is presented to the wall reader. See User *Outputs* for more information about how to add outputs in the user access.
Conditions	Select **Combined** in the **Type** dropdown menu to select a combination of conditions. According to the image below, the relay will be triggered if in Access point #1 the **Door is left opened**, if there is an **Intrusion** or if there is a **Card rejected**.

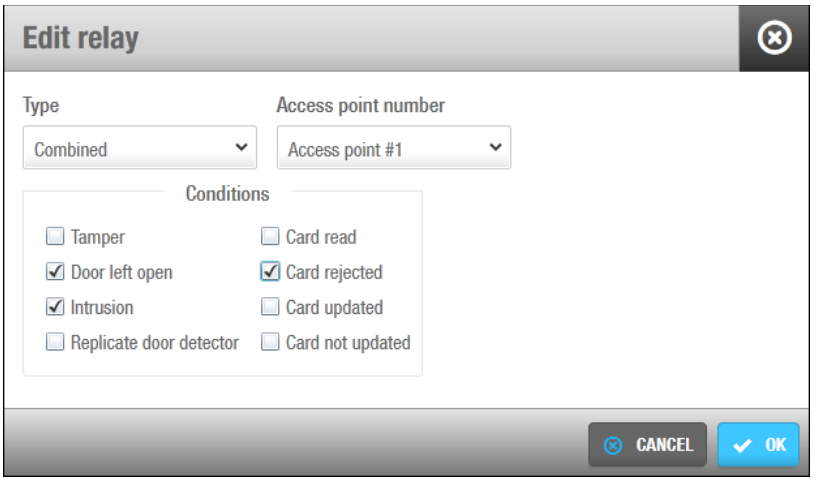


Figure 259: Combined relay type

5. 6. 1. 8. CU42X0 devices initialization and update

The CU42E0 gateways and CU4200 nodes are initialized and updated automatically. See table below for the frequency of each.

Table 65: CU42x0 Initialization and Update

Automatic process	Check Frequency	Notes
CU4K doors initialization	1 minute	Includes initialization + update
CU4K doors update	5 minutes	Can be executed on request
CU4K nodes initialization	1 minute	Includes initialization + update
CU4K nodes update	5 minutes	Can be executed on request

NOTE: Even if updates are performed automatically every 5 minutes for the CU42x0, a manual update can be performed immediately by selecting the device and clicking the **Update** button in **SALTO network**.

5. 6. 2. Filtering SALTO Network Data

You can filter SALTO network data by type, name, description, and/or IP address.

You can filter by the following item types:

- Online IP (CU5000)
- CU42E0 gateway
- CU4200 node
- Online IP (CU4200)
- Encoder
- RF gateway
- RF node
- Online RF (SALTO)
- BAS gateway
- Online RF (BAS integration)

To filter the SALTO network data, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Click **Filters**. The **Items filtering** dialog box is displayed.
3. Select a pre-defined search term from the **Type** drop-down list.
4. Type the name of the item you want to search for in the **Name** field.
5. Type the description of the item you want to search for in the **Description** field.
6. Type the IP address in the **IP address** field if appropriate.

   The **IP address** field is only displayed for relevant search term types.
7. Click **Apply Filter**. A filtered SALTO network list is displayed.

   When a filter has been applied, on the **SALTO Network** screen when you have applied a filter, the search type is displayed in light blue. You can click the search type to once again display all items on the list screen. You can click **Delete Filter** to delete the filter and to redefine the filter parameters.
8. Click the **Close** icon in the **Applied Filters** field when you have finished reviewing the filtered list or click **Filters** to apply another filter.

5. 6. 3. Configuring Online Connection Types

When adding a door or room to the system, you must specify the appropriate connection type – either online or offline. When you select an online connection type, the door or room is displayed on the **SALTO Network** screen, and you can double-click the entry to configure it.

There are four online connection types:

- Online IP (CU5000)
- Online IP (CU4200)
- Online RF (SALTO)
- Online RF (BAS integration)

NOTE: Your BAS integration must be fully configured in ProAccess SPACE General options before you can select this option. See *BAS Tab* for more information.

See *Connection Types* for more information about selecting the correct connection types in non-hotel sites. For information about connection types in non-hotel sites, see *Connection Types*.

5. 6. 3. 1. Online IP (CU5000)

To configure an online IP (CU5000) door, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Double-click the online IP (CU5000) door that you want to configure. The **Access point: Online IP (CU5000)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU5000) doors are online SVN points.

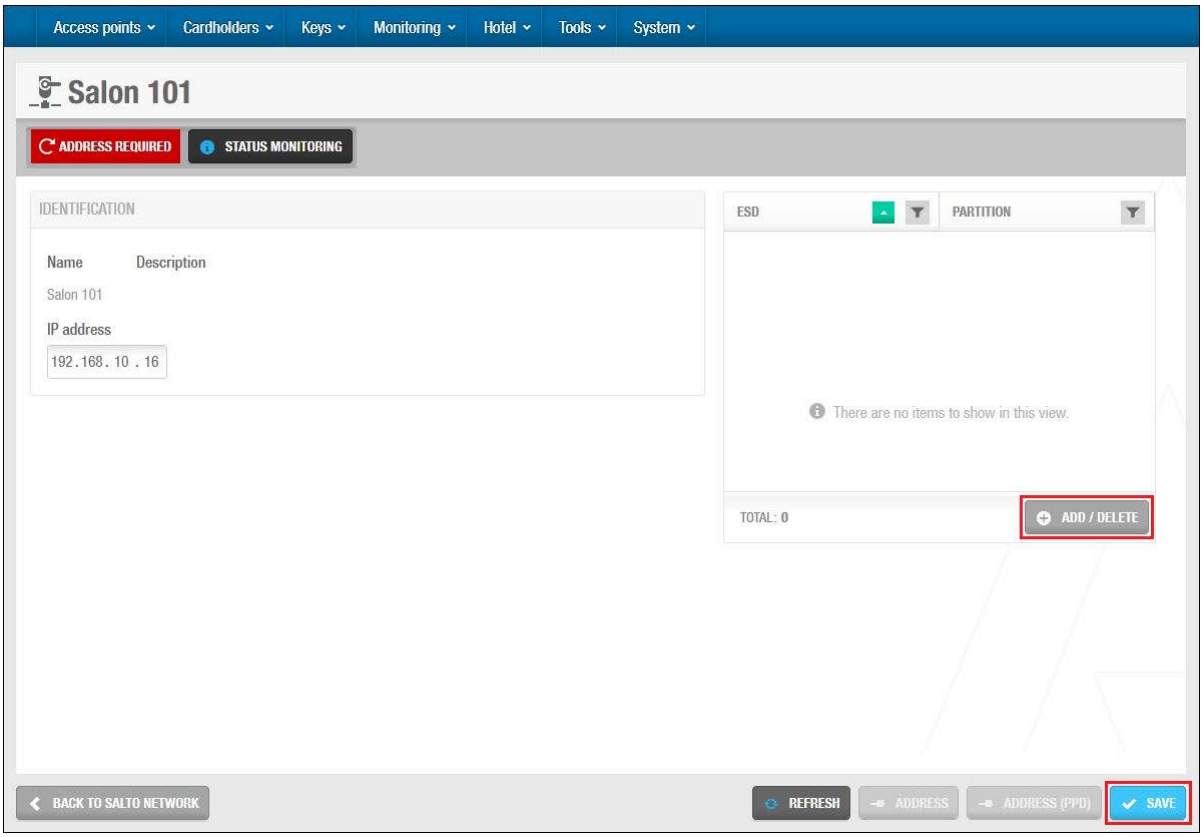


Figure 260: Access point: Online IP (CU5000) information screen

3. Type an IP address for the door in the **IP address** field.
4. Click **Add/Delete** in the **ESD** panel. The **Add/Delete** dialog box, showing a list of ESDs, is displayed. See *ESDs* for more information about ESDs.
5. Select the required ESD in the left-hand panel and click the chevron. The selected ESD is displayed in the right-hand panel.

   You can hold down the Ctrl key while clicking the ESDs to make multiple selections.
6. Click **Accept**. The selected ESD is displayed in the **ESD** panel.
7. Click **Save**.

5. 6. 3. 2. Online IP (CU4200)

To configure an online IP (CU4200) door, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Double-click the online IP (CU4200) door that you want to configure. The **Online IP (CU 4200)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU4200) doors that are not connected to CU4200 nodes are displayed in the **Unreachable items** tab. See *Adding CU4200 Nodes* for more information about CU4200 nodes.

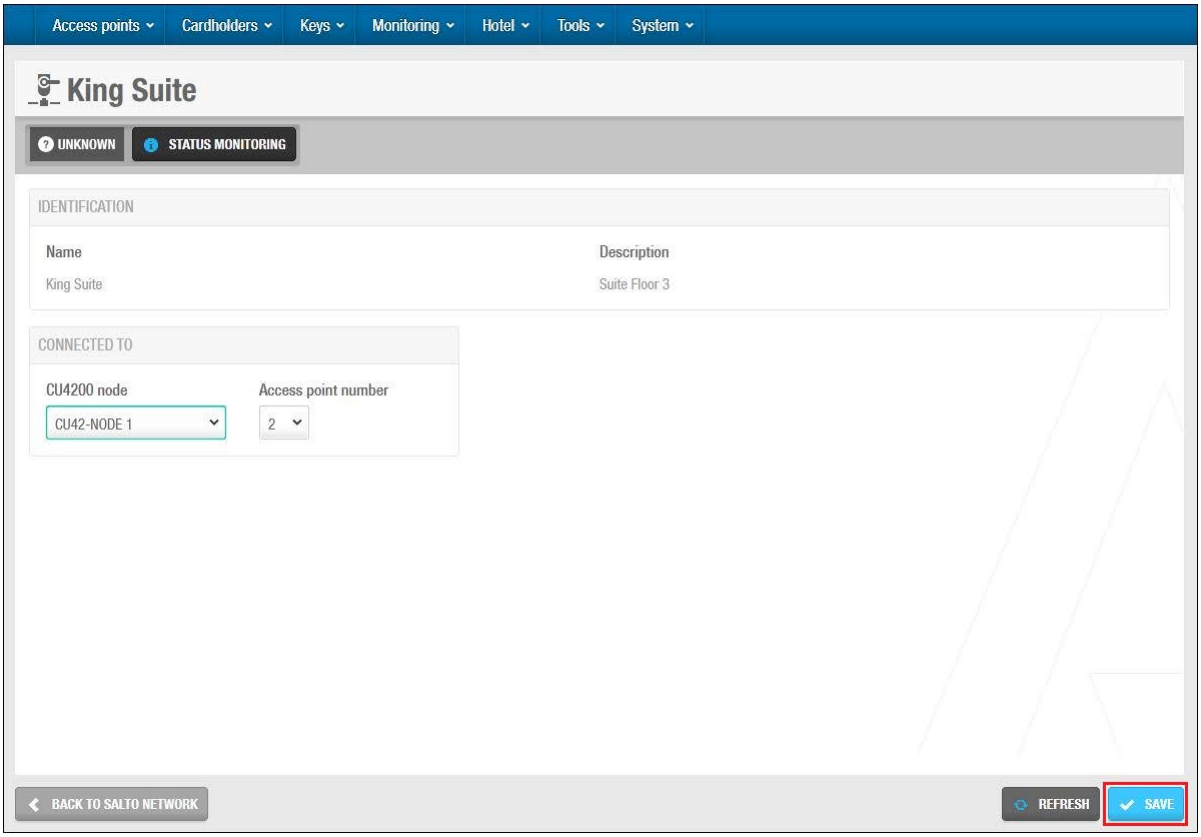


Figure 261: Online IP (CU4200) information screen

3. Select the CU4200 node to which you want to connect the door from the **Connected to** drop-down list.
4. Select either **1** or **2** from the **Door number** drop-down list.

   You cannot select **2** unless you have selected **2** in the **Access point count** drop-down list on the **CU4200 node** information screen. Otherwise, this exceeds the door number count for the node. See *Adding CU4200 Nodes* for more information.
5. Click **Save**.

5. 6. 3. 3. Online RF (SALTO)

To configure an online RF (SALTO) door, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Double-click the online RF (SALTO) door that you want to configure. The **Online RF (SALTO)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online RF (SALTO) doors that are not yet connected to RF nodes are displayed in the **Unreachable items** tab. See *Adding RF Nodes* for more information about RF nodes.

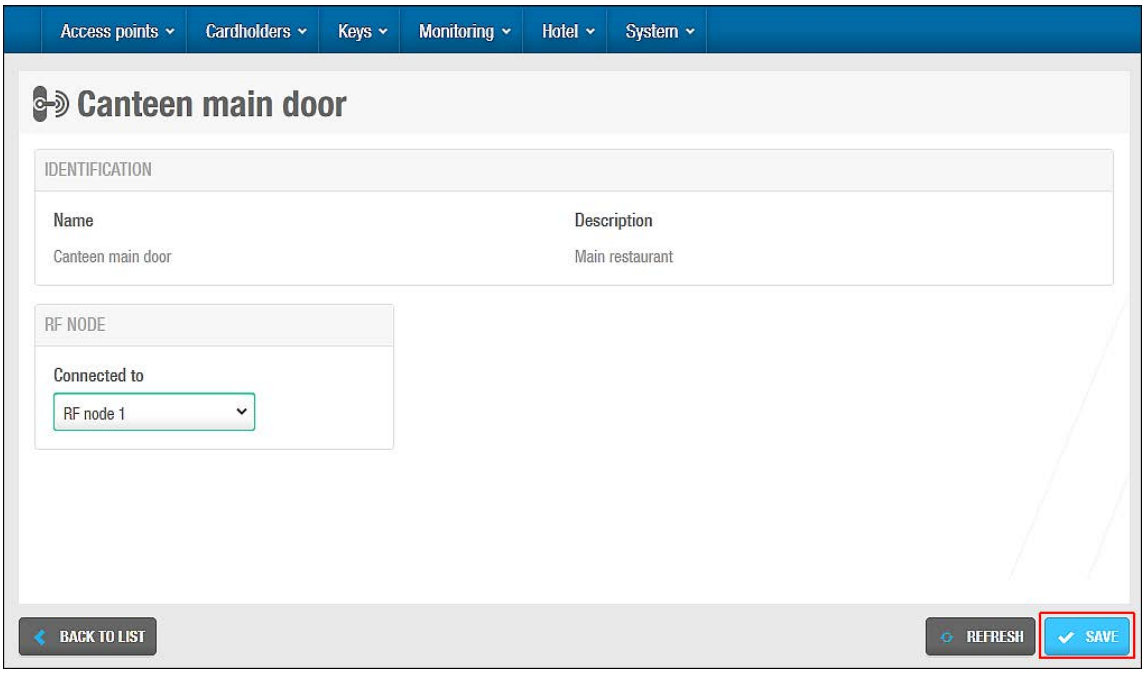


Figure 262: Online RF (SALTO) information screen

3. Select the RF node to which you want to connect the door from the **Connected to** drop-down list.
4. Click **Save**

5. 6. 4. Peripherals Addressing and Maintenance

SALTO network items like Control units, Ethernet encoders, gateways and RF nodes can be added and managed in ProAccess SPACE where you can also make changes such as updating online CUs or updating firmware.

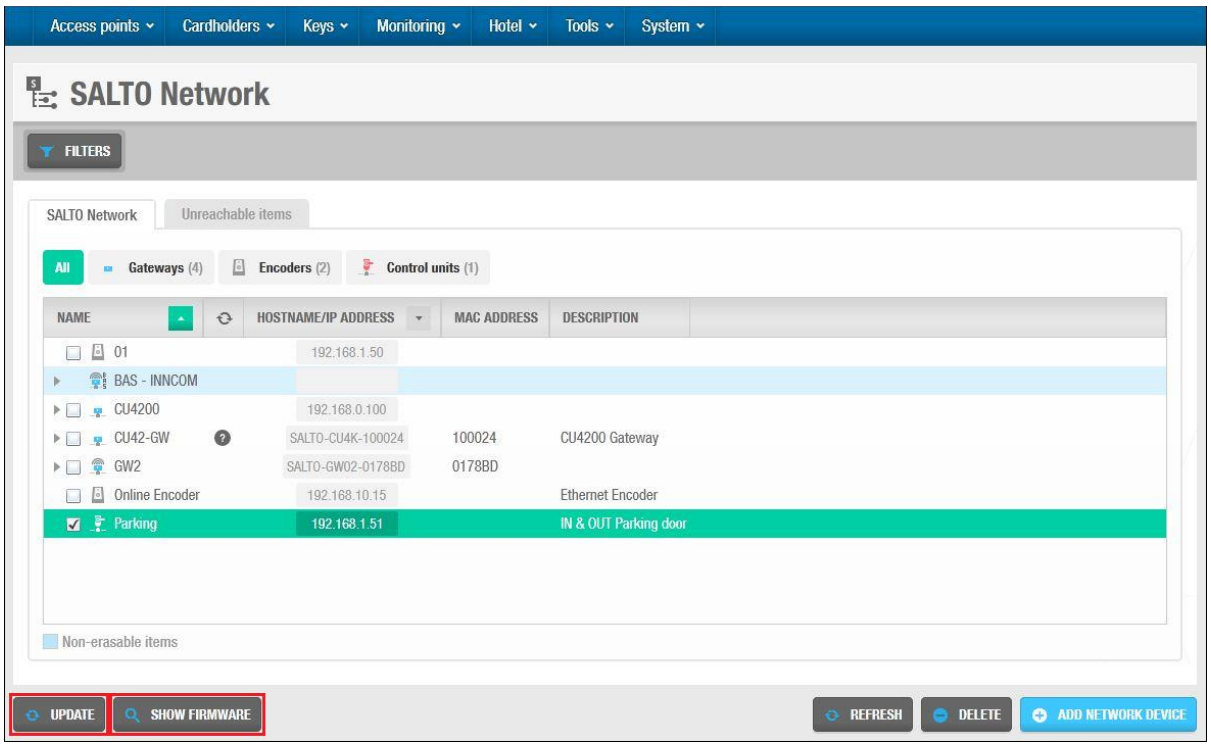


Figure 263: Address and Maintenance

The **Address** and **Maintenance** tab buttons are described in the following table.

Table 66: Maintenance buttons

Button	Functionality
Update	Allows updates to the SALTO database to be communicated to the selected network items. In addition, it allows blacklists to be transmitted automatically to doors without the need to visit each door with an updated key. SAM cards can also be used to transfer information to online doors and to update offline escutcheons and cylinders. See *SAM and Issuing Data* for more information. To SAM a local encoder, click **Supported Keys** on the **Settings** screen in ProAccess SPACE. See *Encoder Settings* for more information. You will find this button in all updatable devices such as control unit CU5000 and CU4200.
Show firmware	Displays the firmware version of the selected item. You can check the firmware version for any online device, CU, RF door, or Ethernet encoder. We recommended that you use the latest firmware version with the SALTO system. Online CUs consist of an Ethernet board and a CU board. This may require updating an individual or multiple online CUs to the most recent firmware version. See *Updating Firmware* for more information about updating multiple online CUs simultaneously. You will find this button in all firmware updatable devices such as control unit CU5000, CU4200 gateways and Ethernet encoders.
Address	Assigns an IP address that you have entered on the system for an Ethernet encoder or an online IP (CU5000) door if the peripheral is in the same network. When you click **CLR** on the online CU, for example, the device enters listening mode. When you click **Address** on the **Monitoring** tab, the software sends a broadcast to the online CU. When the broadcast reaches the online CU, it initializes it with the new IP and other door parameters. Note that you can only address one peripheral at a time when using this option. See *Adding Ethernet Encoders* and *Online IP (CU5000)* for more information about entering IP addresses for Ethernet encoders and online IP (CU5000) doors. You will find this button in all updatable devices such as control unit CU5000 and Ethernet encoders.
Address (PPD)	Assigns an IP address, using a PPD, to an online CU if the peripheral is in a different network. When the online CU is initialized by the PPD, click **Address (PPD)** on the **Monitoring** tab. This creates an authentication between the system and the peripheral. You must enable this option by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices** in ProAccess SPACE. See *Devices Tab* for more information. See also *PPD* for more information. You will find this button in all updatable devices such as control unit CU5000.
Signal	Used to help identify the physical Ethernet encoder that corresponds to the applicable IP/peripheral. After you select the peripheral in the list and click **Signal**, the LED of the applicable encoder starts flashing. At this point, the SAMing process can take place. See *SAM and Issuing Data* for more information.

The columns at the top of the **Maintenance** tab are described in the following table.

Table 67: Maintenance columns

Column	Functionality

Column	Functionality
Name	Specifies the name of the item (the icon immediately before the item name indicates the peripheral type)
Update Status	Shows the peripheral update status. If no update is required, no icon will be shown. The status could be **Update required**, **Address required** or **Unknown.** Note that this column does not have a title on the screen.
Hostname/ IP address	Specifies the network name that identifies the item
MAC Address	Specifies the MAC address of the device.
Description	Matches the details of the item entered in the **Description** field in ProAccess SPACE

5. 6. 4. 1. Updating Firmware

Firmware is software that is programmed on the ROM of hardware devices.

NOTE: SALTO provides firmware updates when new functionality is available or when a software bug is fixed. Each component has a unique file. Contact your SALTO technical support contact before updating any firmware file.

To update the firmware version of an item, perform the following steps:

1. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
2. Select the required item and click **Show firmware**. The **Firmware information** dialog box is displayed.

Figure 264: Peripheral firmware update dialog box

You can select multiple items on the **SALTO Network** peripheral list if required.

3. Select the checkbox next to the item that you want to update. The **Browse** button is enabled.

   If required, you can click **Check all** to update the firmware for multiple items simultaneously. You can only update multiples of the same item (for example, online CUs only or Ethernet encoders only) simultaneously.
4. Click **Browse** to select the required firmware file.
5. Click **Send firmware**. A confirmation screen is displayed when the firmware update is complete.

NOTE: You can update the firmware for local encoders by using the **Show Firmware** button on the **Settings** screen in ProAccess SPACE. See *Updating Encoder*

Firmware for more information.

Calendars for more information.

The **Time zone** panel defines which one of the system time zones is used for the door. You must enable the multiple time zones functionality in ProAccess SPACE System to display this panel in ProAccess SPACE. See ***Error! Reference source not found.*** and *Time Zones* for more information.

5. 6. 4. 2. Door Options

The **Door Options** panel defines how the door activity is audited.

The options are described in the following table.

Table 15: Door options

Option	Description
Audit on keys	Allows monitoring of when and where keys are used. You must enable this feature on both the access point and the user's key. When this option is selected, the door is enabled to write or stamp the audit on the key as long as the key's memory is not full. Also, **the Audit openings in the key** checkbox is enabled on the **User** information screen. If you select an online connection type in the **Connection Type** panel, the **Audit on keys** checkbox is greyed out. This is because online doors are connected to the system, and can send audit information directly to it.
IButton key detection: pulsed mode	Reduces the battery consumption and the risk of rust on the IButton reader contacts as the key detection is done in pulsed mode instead of continuous. To activate this option, you must enable the SHOW_KEY_DETECT_MODE parameter in ProAccess SPACE General options. See ***Error! Reference source not found.*** for more information. This option is only compatible with PPDs that have firmware version 1.02 or higher.
Audit inside handle opening	Allows monitoring of when a user exits a door. For RF doors, this data is automatically transferred and displayed in the audit trail.
Admit expired keys	Allows access to users holding expired keys for a specified number of days. The time range is 0 to 255 days. It can be applied to low security offline doors located before an SVN wall reader. It allows users to access the SVN wall reader to update their keys.
Inhibit audit trail	Ensures that the lock will not memorize openings in its audit trail. However, the lock can still write information on the key. To activate this option, you must select the **Allow audit trail inhibition** checkbox in **System** > **General options** > **Access point Tab** in ProAccess SPACE.
Limit user access	Limits access to the number of users shown in the **Limit user access** field. If you select **5** in the **Limit user access** field, for example, you cannot grant more than five individual users access to the door. This restriction does not apply to users in an access level associated with the door, or users that have access to a zone with which the door is associated. To activate this option, you must enable the LIMITED_USER_ACCESS parameter in ProAccess SPACE General options. See ***Error! Reference source not found.*** for more information.
Out of site	Allows keys to be invalidated (but not cancelled) when presented at SVN exit wall readers and sets a short default expiration period for revalidation of the keys upon re-entry. This option only applies to online IP (CU5000) and online IP (CU4200) doors that have two

Option	Description
	readers. To activate this option, you must select the **Enable "out of site" mode** checkbox in **System** > **General options** > **Access points** in ProAccess SPACE. When you select this checkbox, you can also enable Strict out of site mode in ProAccess SPACE General options. In this case, access permissions are also removed from keys when they are presented at SVN exit wall readers. See ***Error! Reference source not found.*** for more information.

5. 6. 4. 3. Enabling Anti-passback

Selecting the **Enable anti-passback** checkbox in the **Anti-passback** panel 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. The antipassback functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

If the door is a stand-alone unit, you must select the direction of the anti-passback control from the two options provided:

- Outside to inside
- Inside to outside

NOTE: You do not need to select the direction of the anti-passback control for a CU as they have two readers: reader 1 and reader 2. Reader 1 is always inside to outside and reader 2 is always outside to inside. Stand-alone doors only have one reader.

To fully enable the anti-passback functionality, you must select this option when creating and configuring a user in the **User** information screen. See *Creating Users* for more information.

You can also enable a 'strict' anti-passback functionality, if required. Use this where you want the system to prevent a user from exiting where there is no record of them previously entering. To enable this functionality, you must select the **Enable strict anti-passback** checkbox in **Systems** > **General options** > **Access points** in ProAccess SPACE. See ***Error! Reference source not found.*** for more information.

For this functionality to work with online doors, there must be an entrance wall reader and an exit wall reader. For offline doors, you must select the direction of the anti-passback control from the two options provided:

- Outside to inside
- Inside to outside

5. 6. 4. 4. Adding or Changing Door Opening Modes

To add or change a door opening mode, perform the following steps:

1. Select **Access points** > **Doors**. The **Doors** screen is displayed.
2. Double-click the required door. The **Door** information screen is displayed.

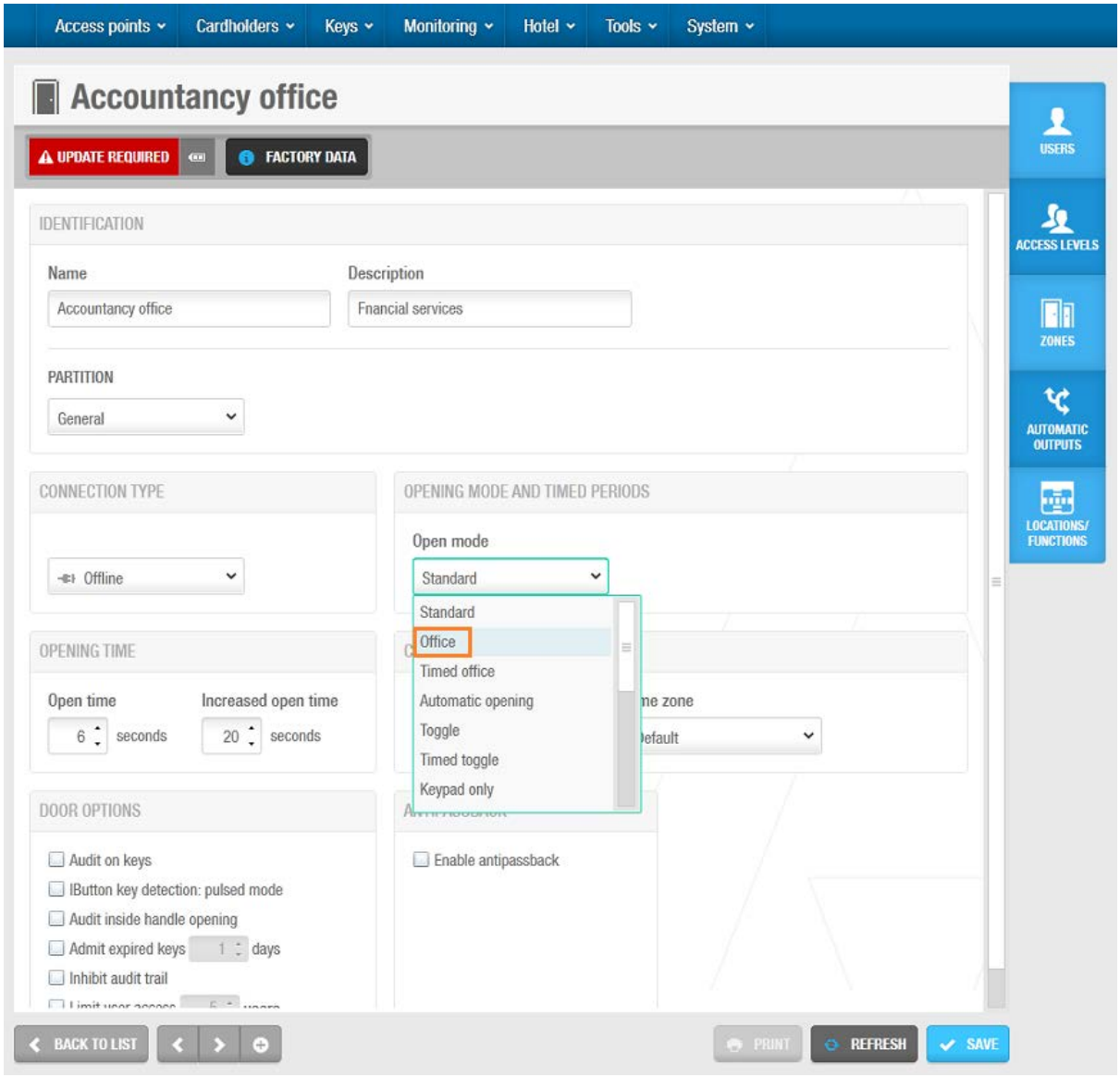


Figure 53: Door information screen

3. Select the required mode from the **Open mode** drop-down list.
4. Click **Save**.

NOTE: In the above example, the **Update Required** warning box is red because the offline door needs to be updated using a PPD. Online doors update automatically. See *PPD* for more information. The **Factory Data** button is displayed after you create and save a door entry. Factory data refers to manufacturing-specific information such as the manufacturing date and the firmware version. This button is only enabled when you connect a PPD to your PC after the PPD has been connected to a lock and information has been transferred.

5. 6. 5. Associating Doors

After you have created and configured a door, you must associate users, access levels, zones, automatic outputs, and/or locations/functions with that door. The following sections describe how to associate doors with the various entries.

NOTE: You must select a timetable and an access point timed period for each door. See *Cardholder Timetables* and *Roll-Call Areas*

A roll call is used to list the individual users in a specified area at a particular time. For example, you can use a roll call to generate a report after a fire alarm goes off. This way, it is possible to check whether all the users in the area have been safely evacuated. The system generates the roll call by monitoring specific access points. By tracking when cardholders enter and exit using these access points, it is possible to see exactly who is inside or outside the roll-call area.

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

See *Roll-Call* for information about generating a list of individual user names in a roll-call area in ProAccess SPACE. You can also use ProAccess SPACE Roll-Call Monitoring to perform other roll-call tasks, such as searching all roll-call areas for a user and the time and date each user entered the roll-call area. See *Roll-Call* for more information.

5. 6. 6. Creating Roll-Call Areas

To create a roll-call area, perform the following steps:

5. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.

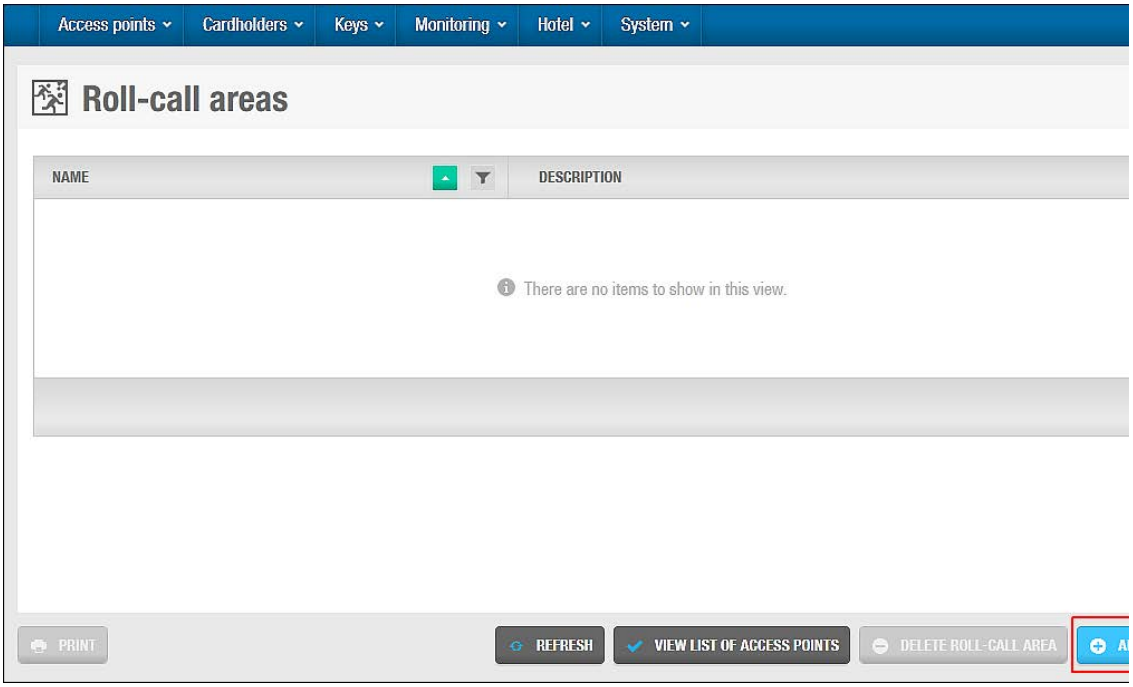


Figure 75: Roll-call areas screen

NOTE: The **View List of Access Points** button shows a list of access points associated with all roll-call areas.

6. Click **Add Roll-Call area**. The **Roll-call area** information screen is displayed.

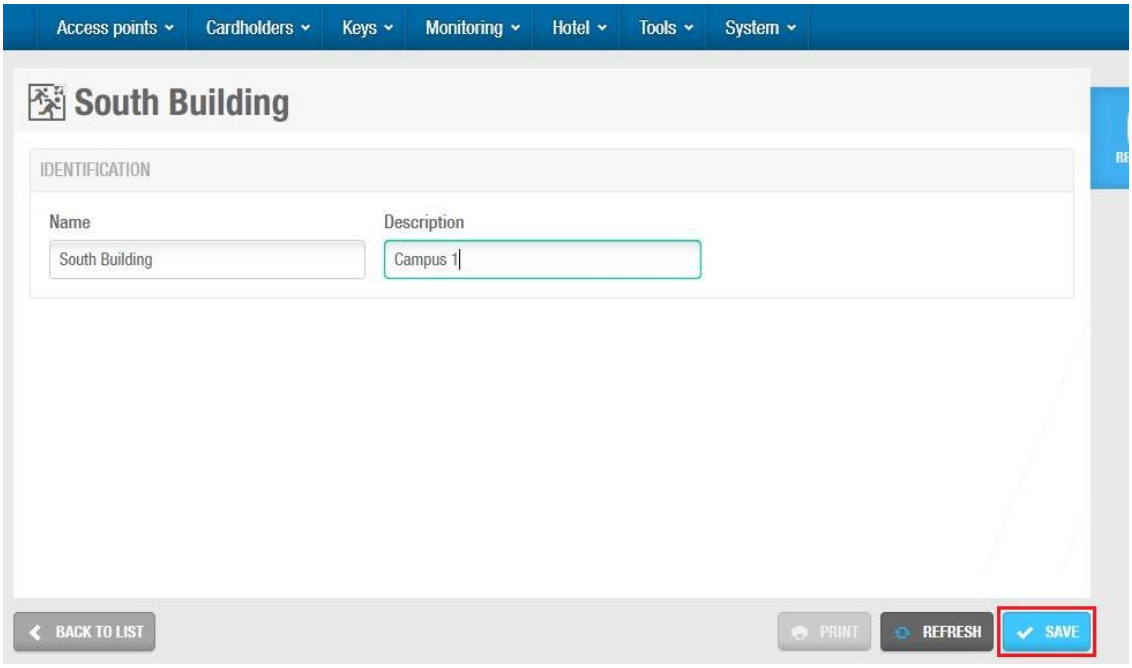


Figure 76: Roll-call area information screen

7. Type a name for the location in the **Name** field.
8. Type a description for the location in the **Description** field.
9. Click **Save**.

5. 6. 6. 1. Creating Roll-Call Exterior Areas

Roll-call areas list the individual users in a specified area at a particular time. To account for the individual users who are on a site but are not in any of the designated roll-call areas, you need to create a separate, exterior area, for example, an assembly area. This is an important concept to consider when creating roll-call areas.

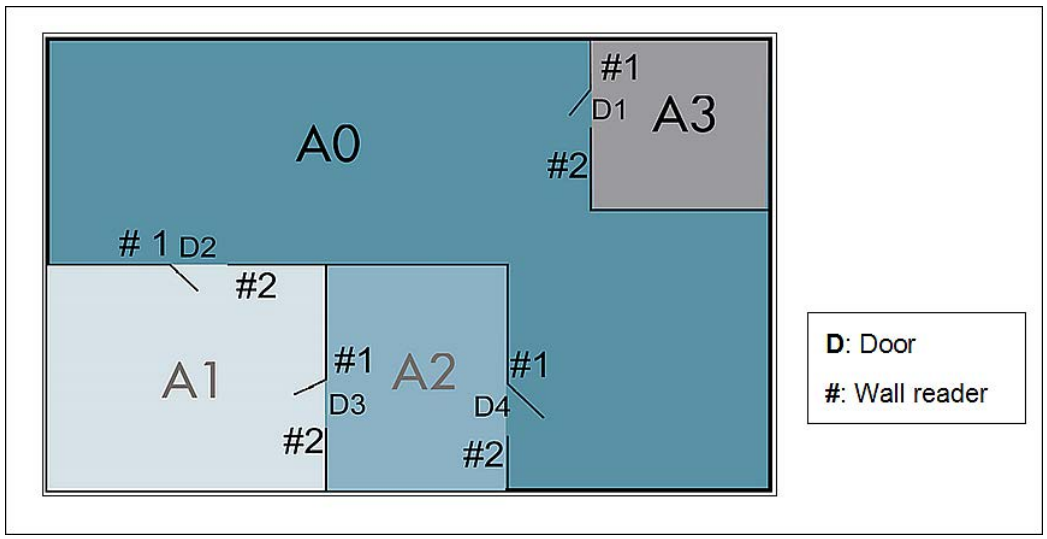


Figure 77: Designated roll-call areas and exterior area

In the above example, there are three standard roll-call areas: A1, A2, and A3. The exterior area is A0, which lists all users who are not in A1, A2, or A3.

A user in A1, A2, or A3 must present their key to a wall reader to exit that roll-call area. When a user presents their key, the system determines that the user has

exited the area and entered the exterior area A0. The exterior area allows the system to create accurate roll-call lists, accounting for all the people who are present.

5. 6. 7. Associating Roll-Call Areas

Once you have created a roll-call area, you must associate wall readers with that roll-call area. Each roll-call area must have two wall readers: one to track users entering the area and another to track users exiting the area. The following section describes how to associate roll-call areas with readers.

5. 6. 7. 1. Readers

To associate a reader with a roll-call area, perform the following steps:

10. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.
11. Double-click the roll-call area that you want to associate with a reader. The **Roll-call area** information screen is displayed.
12. Click **Readers** in the sidebar. The **Readers** dialog box is displayed.

    Note that the dialog box will be blank because you have not yet associated an access point with this particular roll-call area.
13. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.

    This list only applies to online CUs where there are two physical wall readers.
14. 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.
15. Click **Accept**. The roll-call area is now associated with the access point.

Access Point Timed Periods for more information.

5. 6. 7. 2. Users

To allow access to a door, you must associate the door with a user. See *Users* for a definition and information about how to create and configure a user.

To associate a user with a door, perform the following steps:

1. Select **Access points** > **Doors**. The **Doors** screen is displayed.
2. Double-click the door that you want to associate with a user. This means that you are assigning the user access permissions for that door. The **Door** information screen is displayed.
3. 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 door.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.
5. Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right-hand panel.
6. Click **Accept**. The selected user now has access permissions for that door.
7. Select the user in the **Users** dialog box if you want to select a cardholder timetable to be used. See *Cardholder Timetables* for more information.

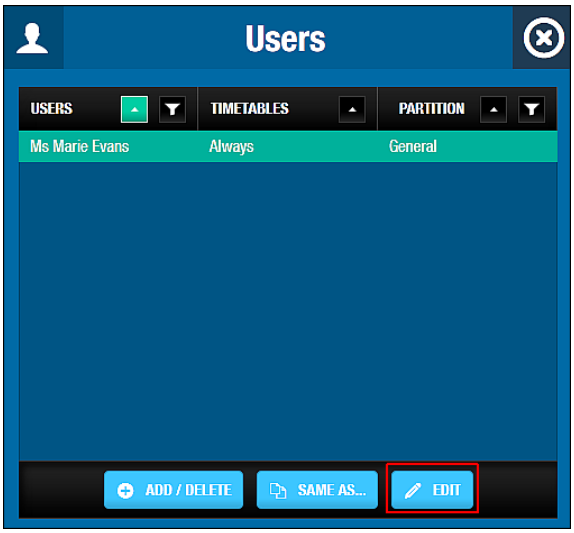


Figure 54: Users dialog box

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

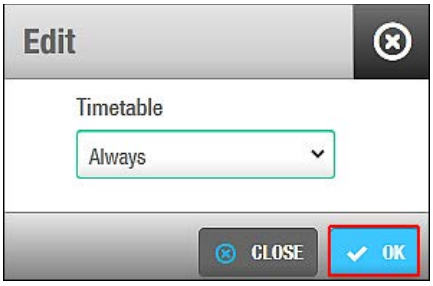


Figure 55: Edit dialog box

9. 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 users always have access to the door, 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 door at any time.
10. Click **OK**.

5. 6. 7. 3. Access Levels

See *User Access Levels*, *Visitor Access Levels*, and *Guest Access Levels* for information about how to create and configure access levels.

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

1. Select **Access points** > **Doors**. The **Doors** screen is displayed.
2. Double-click the door that you want to associate with an access level. The **Door** information screen is displayed.
3. Click **Access Levels** in the sidebar. The **Access levels** dialog box is displayed.

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

5. Select the required access level in the left-hand panel and click the chevron. The selected access level is displayed in the right-hand panel.
6. Click **Accept**. The door is now associated with the access level.

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

5. 6. 7. 4. Zones

See *Zones* for a definition and information about how to create and configure a zone.

To associate a door with a zone, perform the following steps:

1. Select **Access points** > **Doors**. The **Doors** screen is displayed.
2. Double-click the door that you want to associate with a zone. The **Door** information screen is displayed.
3. 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 door.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of zones, is displayed.
5. Select the required zone in the left-hand panel and click the chevron. The selected zone is displayed in the right-hand panel.
6. Click **Accept**. The door is now associated with the zone.

5. 6. 7. 5. Automatic Outputs

See *Automatic Outputs* for a definition and information about how to create and configure an automatic output.

To associate a door with an automatic output, perform the following steps:

1. Select **Access points** > **Doors**. The **Doors** screen is displayed.
2. Double-click the door that you want to associate with an automatic output. The **Door** information screen is displayed.
3. Click **Automatic Outputs** in the sidebar. The **Automatic Outputs** dialog box is displayed.

   Note that the dialog box will be blank because you have not yet associated an output with this particular door.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of automatic outputs, is displayed.
5. Select the required automatic outputs in the left-hand panel and click the chevron. The selected automatic output is displayed in the right-hand panel.
6. Click **Accept**. The selected door is now associated with the automatic output.
7. Select the output in the **Automatic Outputs** dialog box if you want to change the access point timed period. See *Roll-Call Areas*
8. *A roll* call is used to list the individual users in a specified area at a particular time. For example, you can use a roll call to generate a report after a fire alarm goes off. This way, it is possible to check whether all the users in the area have been safely evacuated. The system generates the roll call by monitoring specific access points. By tracking when cardholders enter and exit using these access points, it is possible to see exactly who is inside or outside the roll-call area.

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

See *Roll-Call* for information about generating a list of individual user names in a roll-call area in ProAccess SPACE. You can also use ProAccess SPACE Roll-Call Monitoring to perform other roll-call tasks, such as searching all roll-call areas for a user and the time and date each user entered the roll-call area. See *Roll-Call* for more information.

5. 6. 8. Creating Roll-Call Areas

To create a roll-call area, perform the following steps:

9. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.

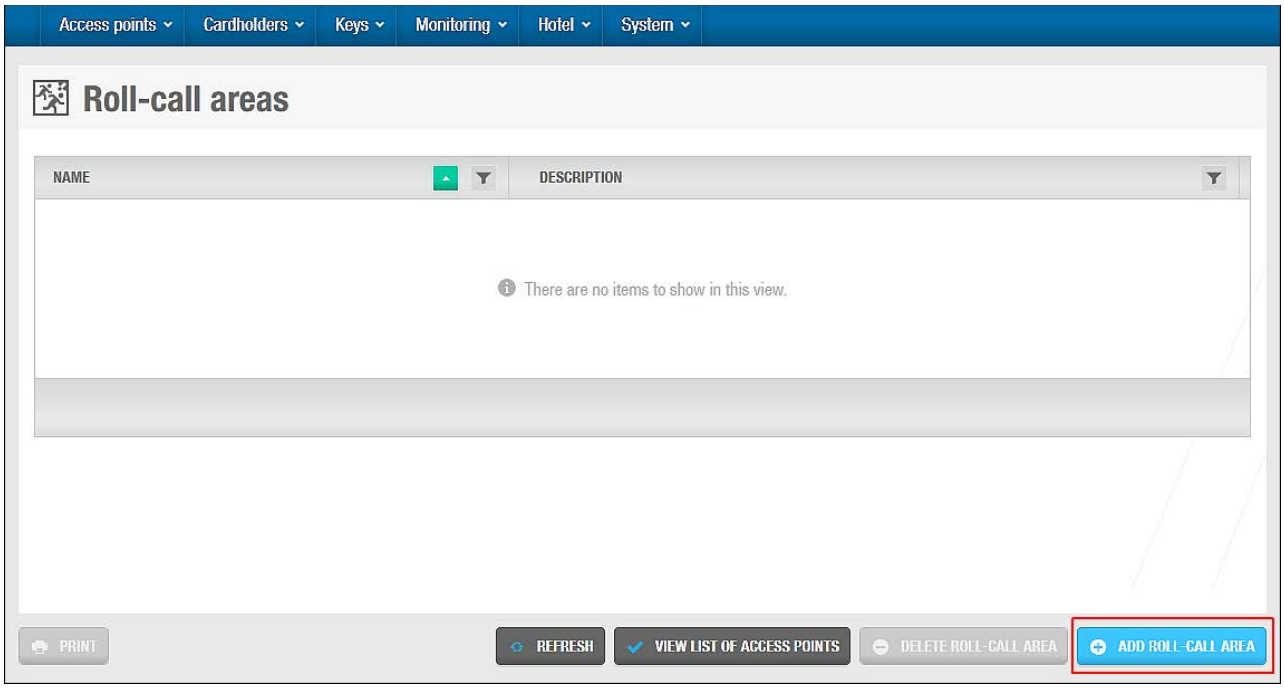


Figure 75: Roll-call areas screen

NOTE: The **View List of Access Points** button shows a list of access points associated with all roll-call areas.

10. Click **Add Roll-Call area**. The **Roll-call area** information screen is displayed.

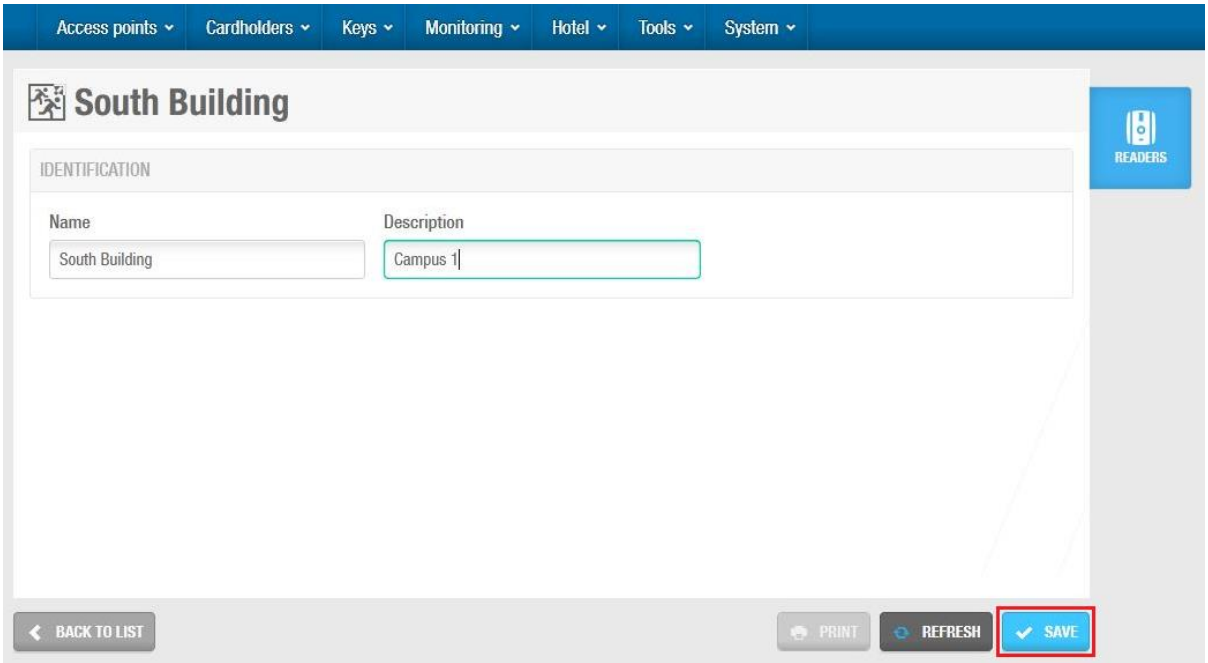


Figure 76: Roll-call area information screen

11. Type a name for the location in the **Name** field.
12. Type a description for the location in the **Description** field.
13. Click **Save**.

5. 6. 8. 1. Creating Roll-Call Exterior Areas

Roll-call areas list the individual users in a specified area at a particular time. To account for the individual users who are on a site but are not in any of the designated roll-call areas, you need to create a separate, exterior area, for example, an assembly area. This is an important concept to consider when creating roll-call areas.

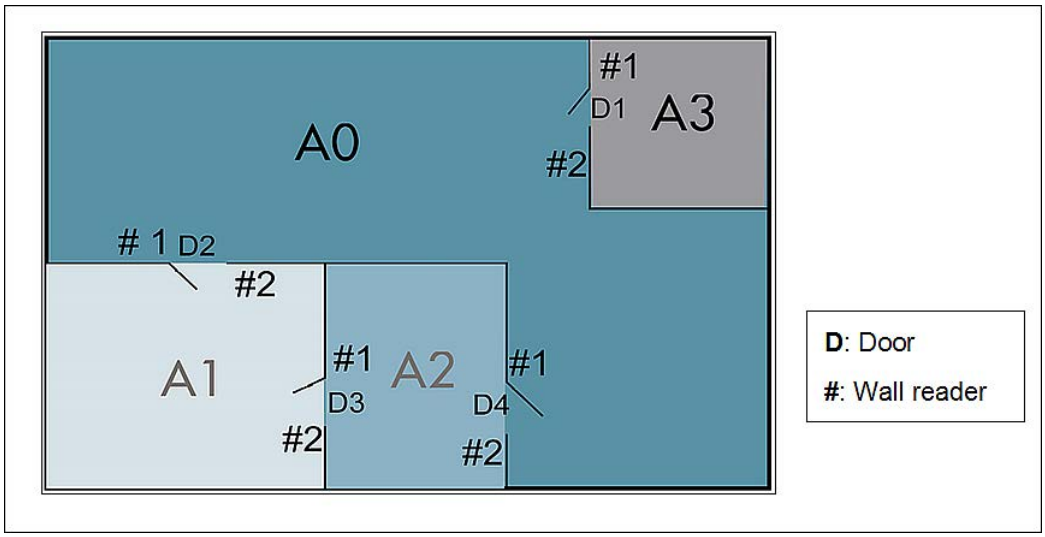


Figure 77: Designated roll-call areas and exterior area

In the above example, there are three standard roll-call areas: A1, A2, and A3. The exterior area is A0, which lists all users who are not in A1, A2, or A3.

A user in A1, A2, or A3 must present their key to a wall reader to exit that roll-call area. When a user presents their key, the system determines that the user has exited the area and entered the exterior area A0. The exterior area allows the system to create accurate roll-call lists, accounting for all the people who are present.

5. 6. 9. Associating Roll-Call Areas

Once you have created a roll-call area, you must associate wall readers with that roll-call area. Each roll-call area must have two wall readers: one to track users entering the area and another to track users exiting the area. The following section describes how to associate roll-call areas with readers.

5. 6. 9. 1. Readers

To associate a reader with a roll-call area, perform the following steps:

14. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.
15. Double-click the roll-call area that you want to associate with a reader. The **Roll-call area** information screen is displayed.
16. Click **Readers** in the sidebar. The **Readers** dialog box is displayed.

    Note that the dialog box will be blank because you have not yet associated an access point with this particular roll-call area.
17. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.

    This list only applies to online CUs where there are two physical wall readers.
18. 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.
19. Click **Accept**. The roll-call area is now associated with the access point.
20. Access Point Timed Periods for more information.

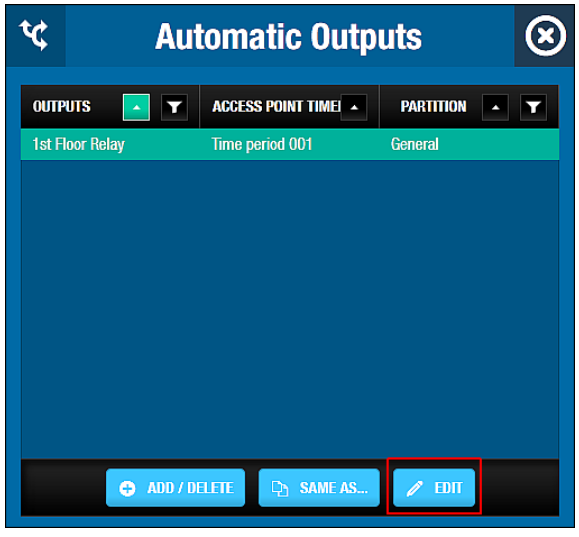


Figure 56: Automatic outputs dialog box

21. Click **Edit**. The **Edit** dialog box is displayed. **Time period 001** is selected by default.

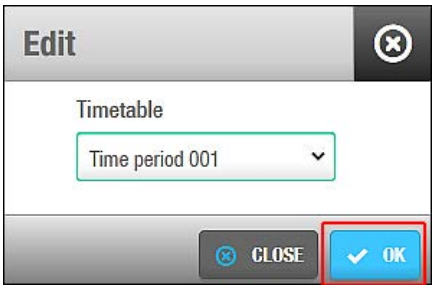


Figure 57: Edit dialog box

22. Select the appropriate access point timed period using the drop-down list.
23. Click **OK.**

5. 6. 9. 2. Locations/Functions

See *Locations* and *Functions* for a definition and information about how to create and associate a location and a function.

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

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

1. Select **Access points** > **Doors**. The **Doors** screen is displayed.
2. Double-click the door that you want to associate with a location/function. The **Door** information screen is displayed.
3. Click **Locations/Functions** in the sidebar. The **Locations/Functions** dialog box is displayed.

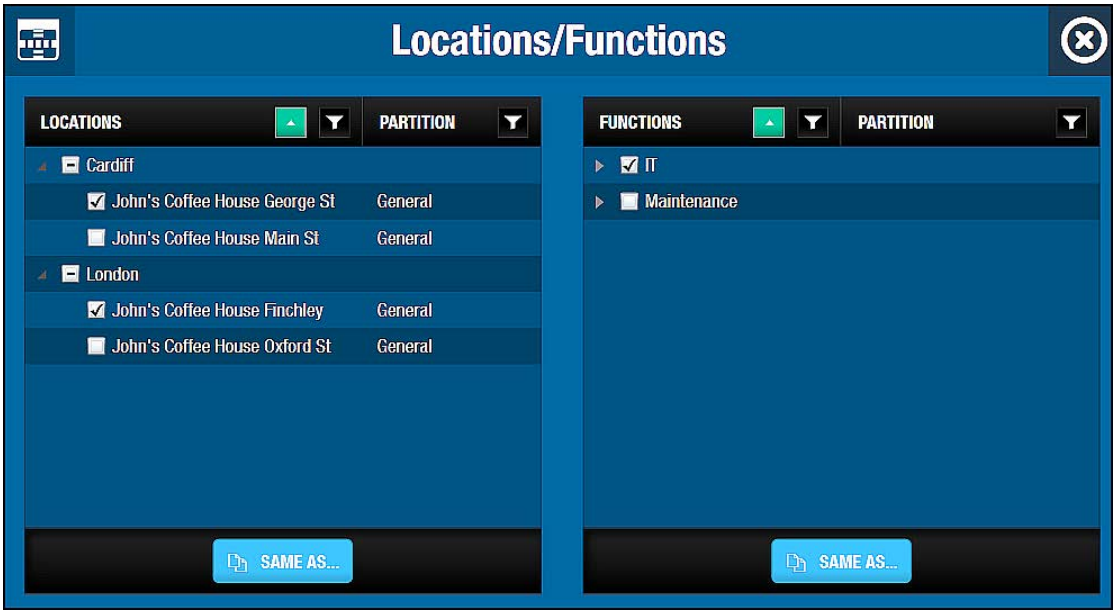


Figure 58: Locations/Functions dialog box

Note that the dialog box will be blank if you have not yet created a location or a function. See *Locations* and *Functions* for information about how to create and associate a location and a function. See ***Error! Reference source not found.*** for information about adding groupings for locations and functions.

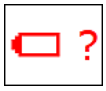
4. Select the required location in the **Locations** panel of the dialog box. The door is now associated with the location.
5. Select the required function in the **Functions** panel of the dialog box. The door is now associated with the function.

5. 6. 10. Door Icons

When you create doors, different icons are displayed on the **Doors** screen. These icons vary, depending on the battery status of doors and whether they need to be updated.

The icons are described in the following table.

Table 16: Door icons

Icon	Description
 Update required	Indicates that a door needs to be updated. This icon is displayed in the **Update required** column.
 Unknown	Indicates that the battery status of a door is unknown. This icon is displayed in the **Battery** column.
 Battery status	Indicates the battery status of a door. This can be normal, low, or run-out.

5. 7. Energy Saving Devices

Energy Saving Devices (ESDs) are used to control the activation of electrical equipment in a specific area. They are more commonly used in hotel sites (especially in hotel rooms). For hotel sites, they are created automatically when you enable ESDs by using the **Hotel** tab in ProAccess SPACE General options. For non-hotel sites, you can manually create ESDs within the system. This is done by creating them as door entries.

See *ESDs* for more general information about ESDs. See also *Associated Device Lists* for more information about using ESDs in hotel sites.

The following example shows a simple way of completing the ESD setup process:

1. **ESDs created and configured**

   The admin operator creates ESDs as door profiles in ProAccess SPACE and configures the options.

2. **ESDs associated**

   a) The admin operator associates users and/or access levels with the specified ESDs.
   b) The admin operator associates users and/or access levels with the ESD_#1 and the ESD_#2 outputs.

The ESD_#1 and the ESD_#2 outputs are automatically generated by the system. They cannot be deleted. These outputs activate the relays for ESDs. If required, they can be set up to control access to different electrical systems in your site. For example, the ESD_#1 output can be used to control access to electrical lights, and the ESD_#2 output can be used to control access to air conditioning (AC). Users must be associated with the ESD_#1 and the ESD_#2 outputs, as well as with the required ESD, in order to activate the ESD with their key.

NOTE: When you activate an ESD, you must initialize it using a PPD. See *Initializing Rooms and ESDs* for more information.

5. 7. 1. Creating ESDs

For non-hotel sites, the procedure for creating an ESD in the system is the same as for creating a door. However, only certain options on the **Door** information screen are applicable for ESDs. See *Creating Doors* for more information.

To create an ESD, perform the following steps:

1. Select **Access points** > **Doors**. The **Doors** screen is displayed.
2. Click **Add Door**. The **Door** information screen is displayed.
3. Type a name for the ESD in the **Name** field.
4. Type a description for the ESD in the **Description** field.
5. Select the relevant partition from the **Partition** drop-down list, if required.

See *System* Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

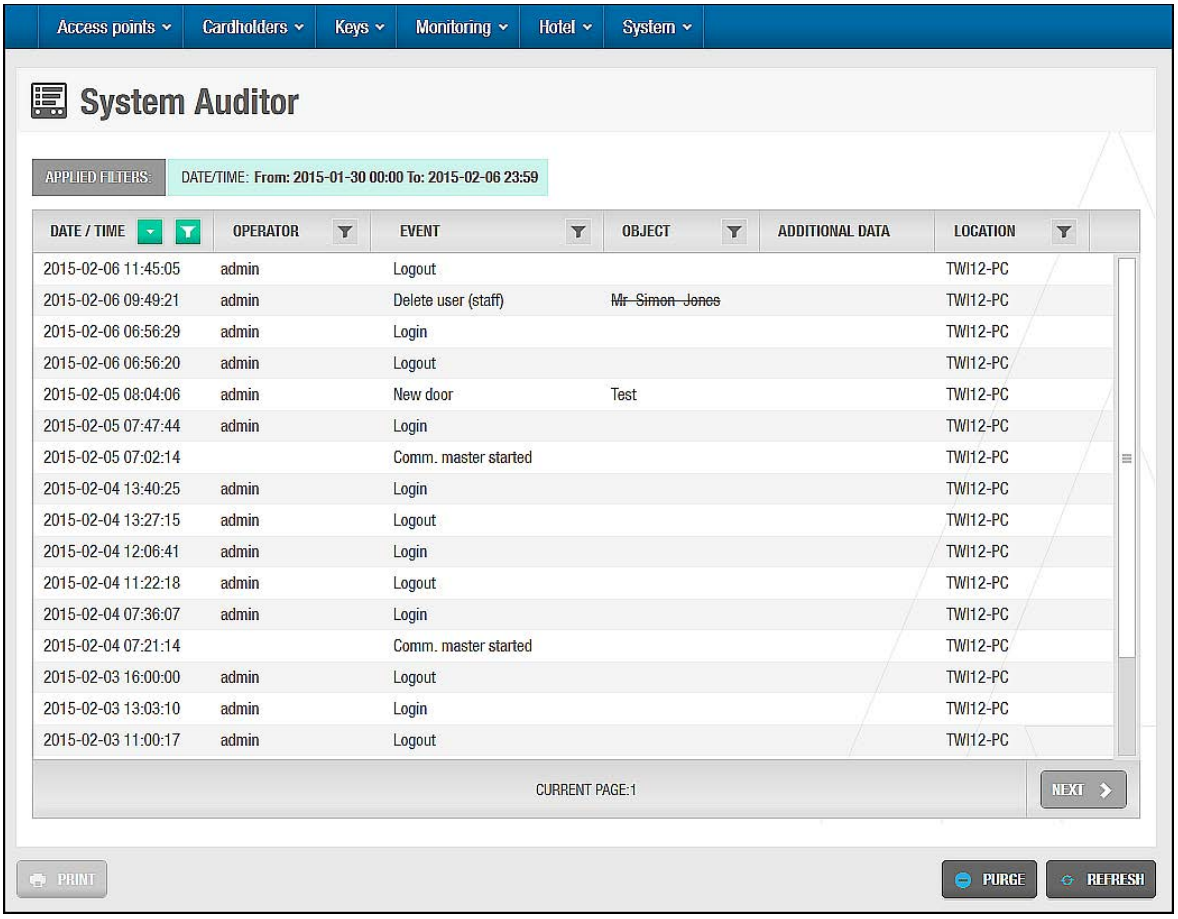


Figure 228: System Auditor information screen

5. 7. 2. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

5. 7. 3. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

6. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

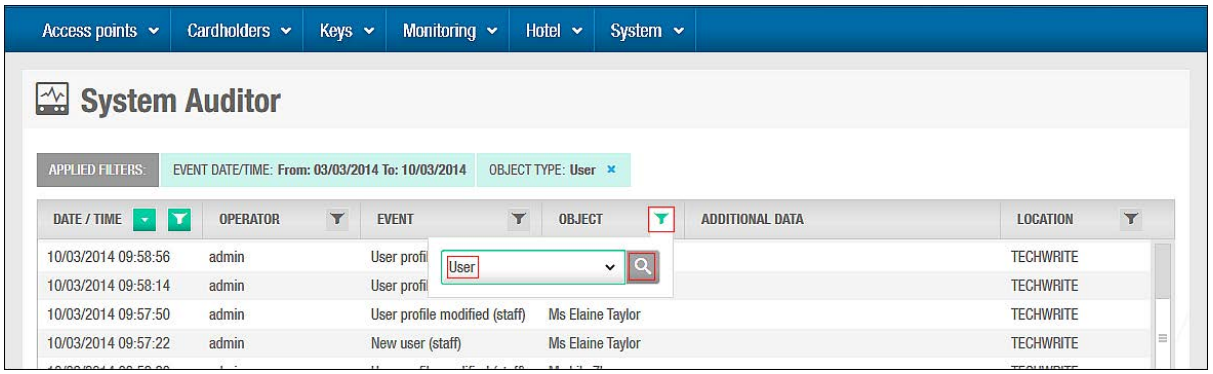


Figure 229: System Auditor information screen

7. Click the **Funnel** icon above the filter item. A search dialog box is displayed.
   For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.
   For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.
   For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.
8. Type your search term.
   Or
   Select a predefined search term from the drop-down list.
   Or
   Select a date range.
   You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.
   However, you cannot remove the **Date/Time** filter.
9. Click the **Search** icon. A filtered audit trail list is displayed.

5. 7. 3. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

5. 7. 4. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic System Auditor Purging* for more information.

To purge the system auditor, perform the following steps:

10. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
11. Click **Purge**. The **Purge system auditor** dialog box is displayed.

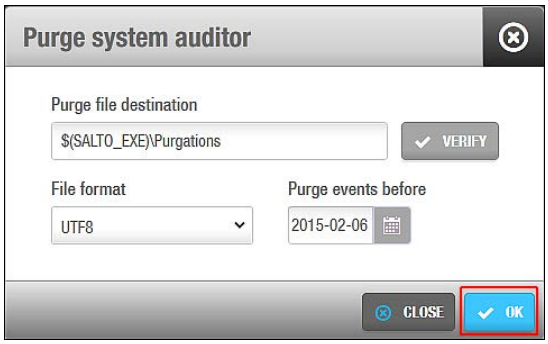


Figure 230: Purge system auditor dialog box

12. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
13. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
14. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
15. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
16. Click **OK**.

5. 8. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the

permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

5. 8. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

17. Select **System** > **Operators**. The **Operators** screen is displayed.

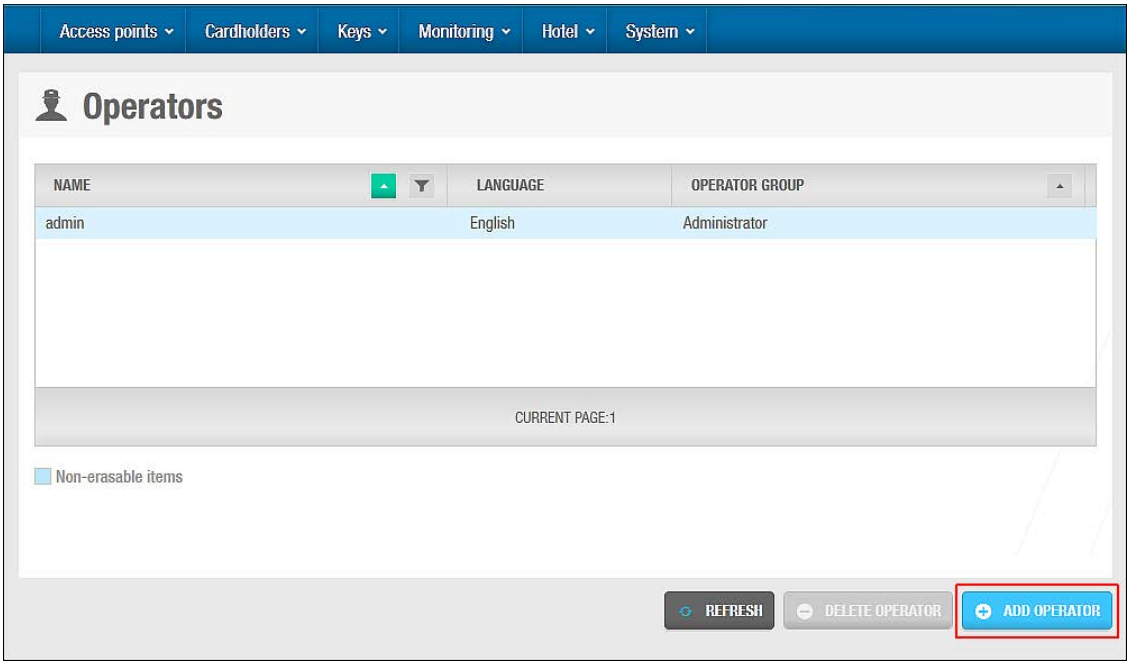


Figure 231: Operators screen

18. Click **Add Operator**. The **Operator** information screen is displayed.

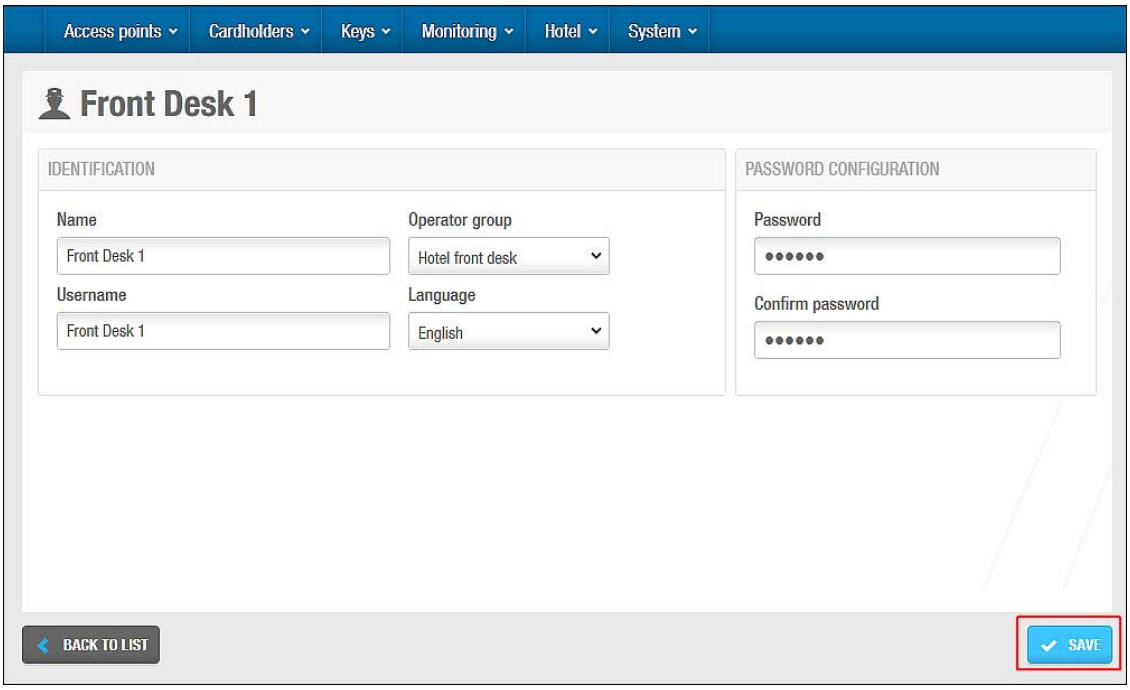


Figure 232: Operator information screen

19. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

20. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

    A maximum of 64 characters can be entered. The user name is not case sensitive.

21. Select the appropriate operator group from the **Operator group** drop-down list.
22. Select the display language for the operator in the **Language** drop-down list.
23. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.

24. Confirm the password.
25. Click **Save**.

5. 9. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.

- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

5. 9. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

26. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

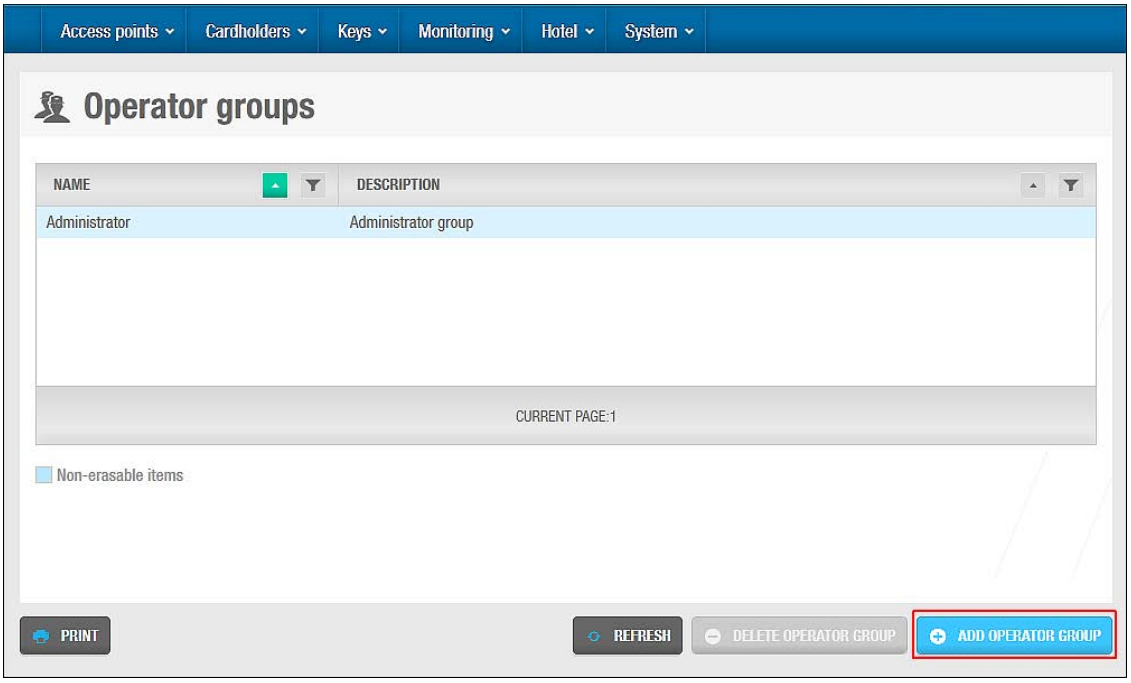


Figure 233: Operator groups screen

27. Click **Add Operator Group**. The **Operator group** information screen is displayed.

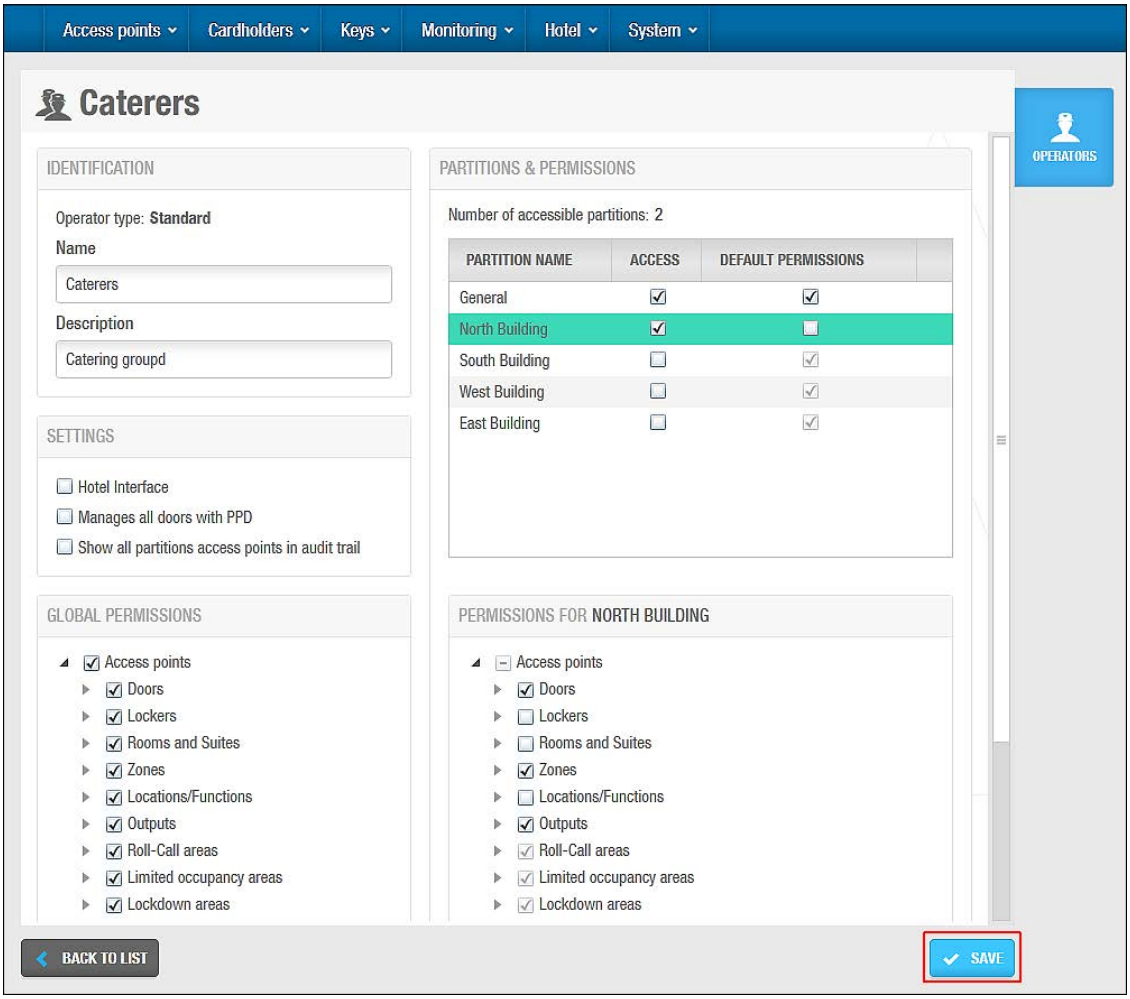


Figure 234: Operator group information screen

28. Type the name of the operator group in the **Name** field.
29. Type a description for the group in the **Description** field.
30. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.
31. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.
32. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.
33. Click **Save**.

5. 9. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

5. 9. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level **Monitoring** checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors

Permission	Description
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas

Permission	Description
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

5. 9. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

34. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
35. Double-click the operator group with the operator list you want to view.
36. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

    Partitions for more information.
37. Select the required values in the **Open time** and **Increased open time** fields in the **Opening Time** panel.

    See *Opening Times* for more information about these options.
38. Select the **Audit on keys** checkbox in the **Door Options** panel if required.

    See *Door Options* for more information about this option.
39. Click **Save**.

5. 9. 3. Associating ESDs with Users

You can associate ESDs with individual users or access levels. The procedure for associating an ESD with a user is the same as for associating a door with a user. See *Users* for more information and a description of the steps you should follow. Alternatively, you can associate an ESD with an access level.

5. 9. 4. Associating ESDs with Access Levels

The procedure for associating an ESD with an access level is the same as for associating a door with an access level. See *Access Levels* for more information and a description of the steps you should follow.

5. 9. 5. Associating Users with the ESD_#1 and ESD_#2 Outputs

You can associate the ESD_#1 and the ESD_#2 outputs with individual users or access levels. The procedure for associating a user with these outputs is the same as for other outputs. See *Outputs* or *Users* for more information and a description of the steps you should follow.

5. 9. 6. Associating User Access Levels with the ESD_#1 and ESD_#2 Outputs

The procedure for associating a user access level with the ESD_#1 and the ESD_#2 outputs is the same as for other outputs. See *Outputs* or *Access Levels* for more information and a description of the steps you should follow.

NOTE: If ESDs are in a room or office, for example, it is recommended that you associate them with the same zone as the room or office door. This makes them easier to manage in the system. See *Zones* for more information about zones.

5. 10. Lockers

The term 'locker' within the SALTO system can refer to a locker, cupboard, display cabinet, box, or case fitted with an electronic device that controls the lock. SALTO lockers are commonly used in corporate organizations, universities, and gyms. The lockers functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

You must initialize a locker with a PPD before it can be used. The procedure for initializing lockers is the same as for initializing locks. See *Initializing Locks* for more information and a description of the steps you should follow.

The following sections describe how to create and configure a locker.

5. 10. 1. Creating Lockers

To create a locker, perform the following steps:

1. Select **Access points** > **Lockers**. The **Lockers** screen is displayed.

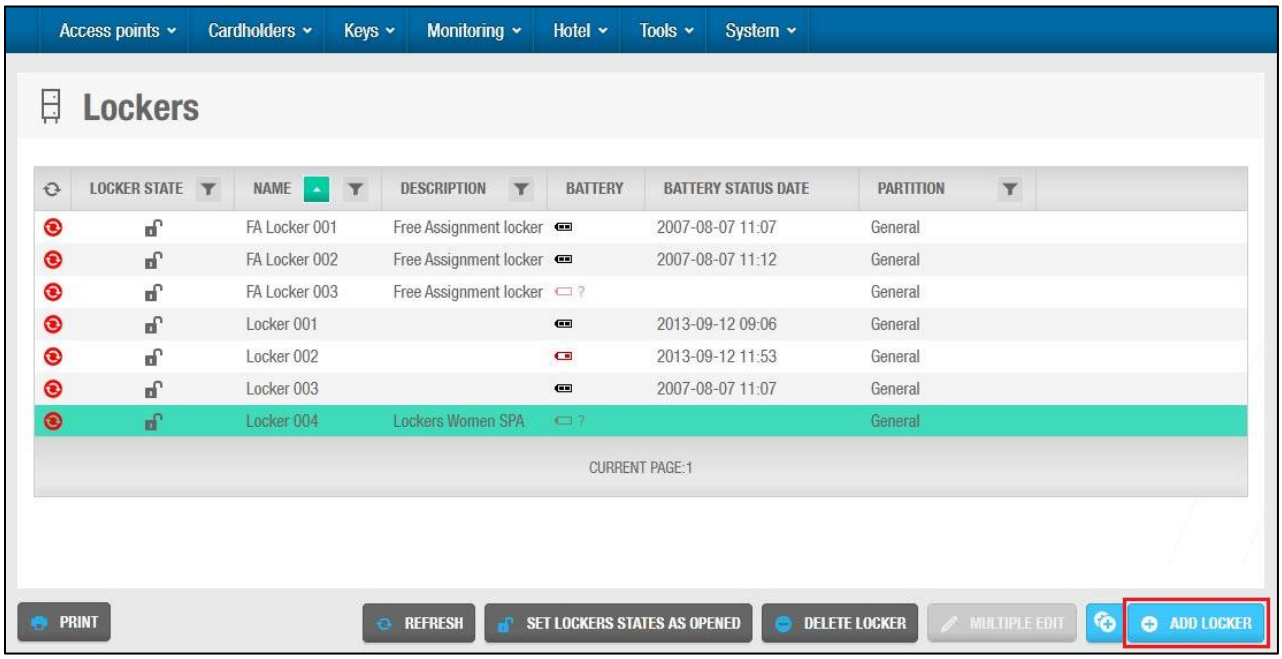


Figure 59: Lockers screen

NOTE: The **Set Lockers States As Opened** button gives you the option to reset the status of available lockers on the system. This option applies to all lockers in the system and changes the status of each locker to **Open** on its information screen. However, it does not affect the physical lockers. It is generally only used in sites such as gyms or spas where only free assignment lockers are in use. To activate this button, you must select the **Control of lockers left closed** checkbox in **System** > **General options** > **Access points** in ProAccess SPACE. See ***Error! Reference source not found.*** for more information.

2. Click **Add Locker**. The **Locker** information screen is displayed.

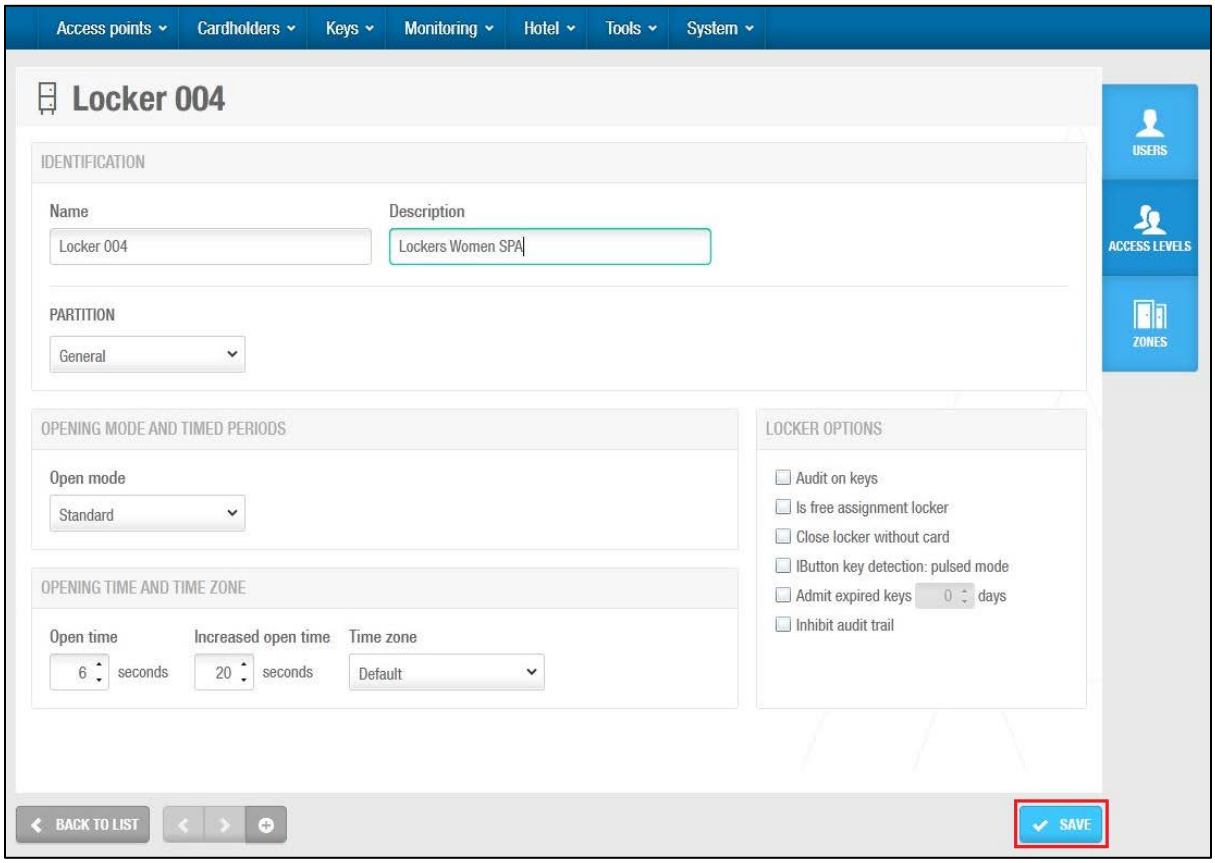


Figure 60: Locker information screen

3. Type a name for the locker in the **Name** field.
4. Type a description for the locker in the **Description** field.
5. Select the relevant partition from the **Partition** drop-down list, if required.

See *System* Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

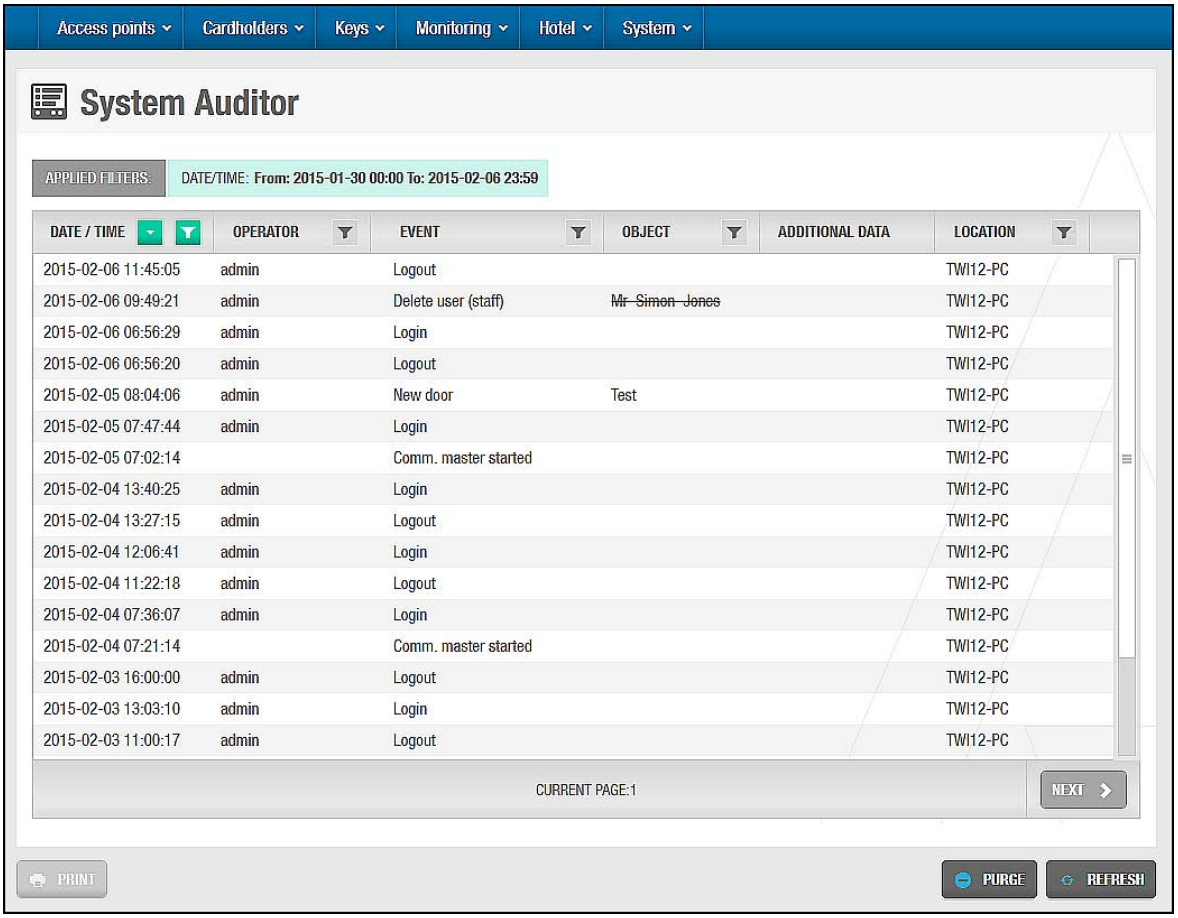


Figure 228: System Auditor information screen

5. 10. 2. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

5. 10. 3. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

6. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

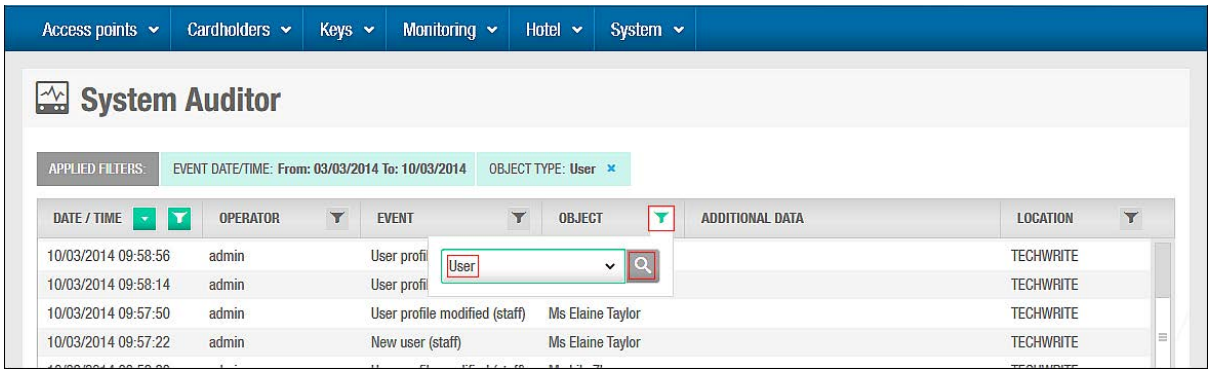


Figure 229: System Auditor information screen

7. Click the **Funnel** icon above the filter item. A search dialog box is displayed.

   For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.
   For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.
   For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.
8. Type your search term.

   Or
   Select a predefined search term from the drop-down list.
   Or
   Select a date range.
   You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.
   However, you cannot remove the **Date/Time** filter.
9. Click the **Search** icon. A filtered audit trail list is displayed.

5. 10. 3. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

5. 10. 4. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic System Auditor Purging* for more information.

To purge the system auditor, perform the following steps:

10. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
11. Click **Purge**. The **Purge system auditor** dialog box is displayed.

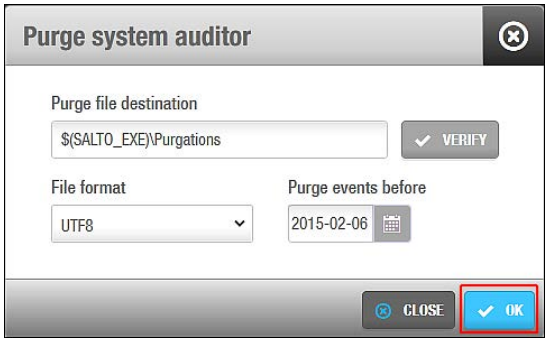


Figure 230: Purge system auditor dialog box

12. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
13. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
14. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
15. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
16. Click **OK**.

5. 11. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

5. 11. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

17. Select **System** > **Operators**. The **Operators** screen is displayed.

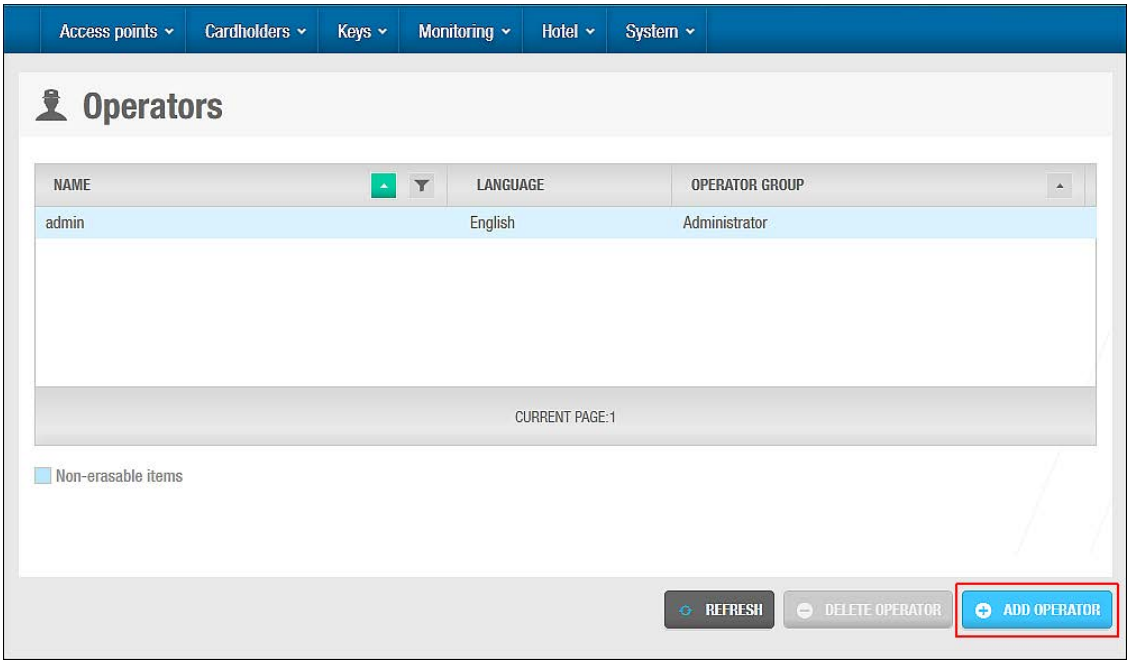


Figure 231: Operators screen

18. Click **Add Operator**. The **Operator** information screen is displayed.

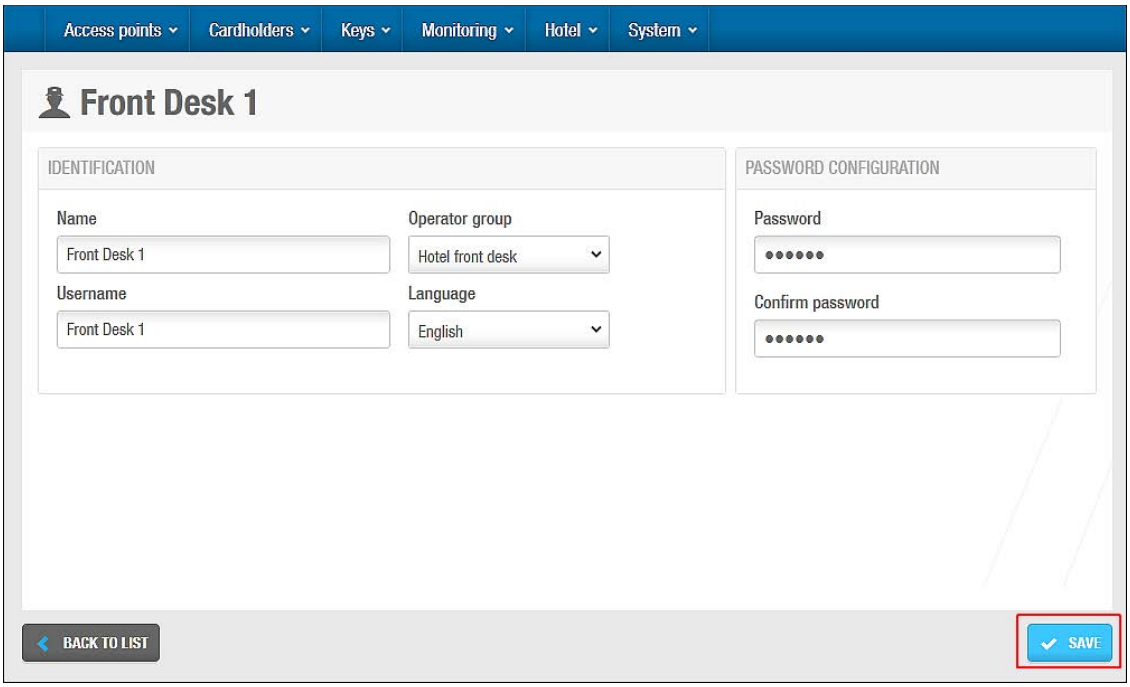


Figure 232: Operator information screen

19. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

20. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

    A maximum of 64 characters can be entered. The user name is not case sensitive.

21. Select the appropriate operator group from the **Operator group** drop-down list.
22. Select the display language for the operator in the **Language** drop-down list.

23. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.

24. Confirm the password.
25. Click **Save**.

5. 12. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

5. 12. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

26. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

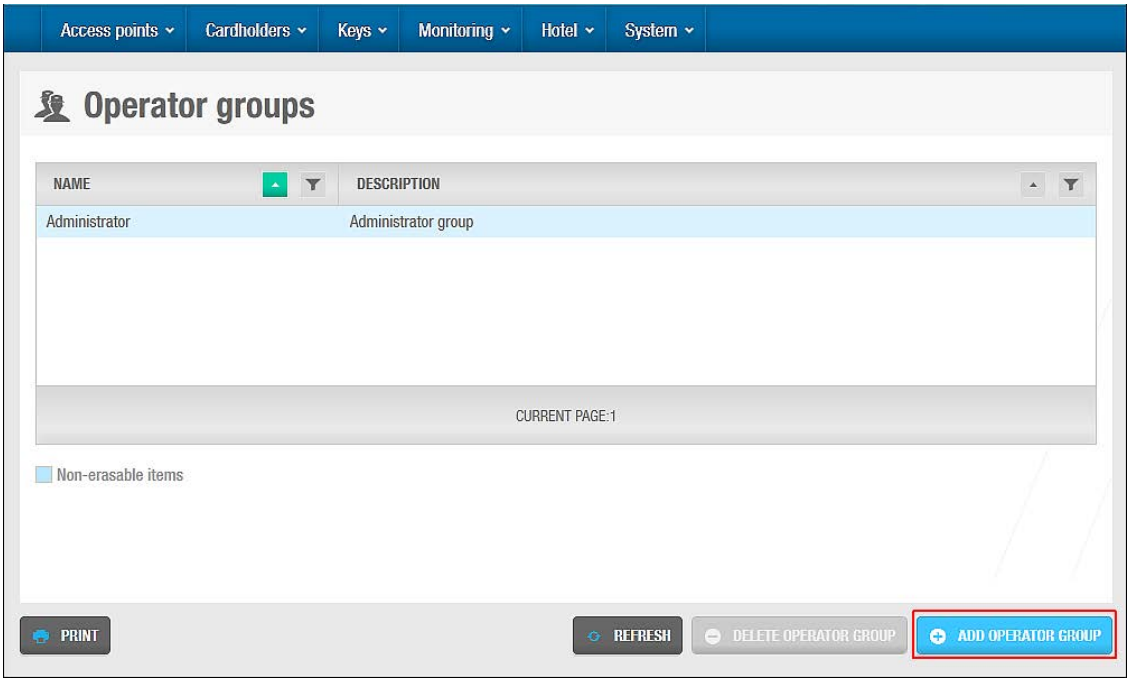


Figure 233: Operator groups screen

27. Click **Add Operator Group**. The **Operator group** information screen is displayed.

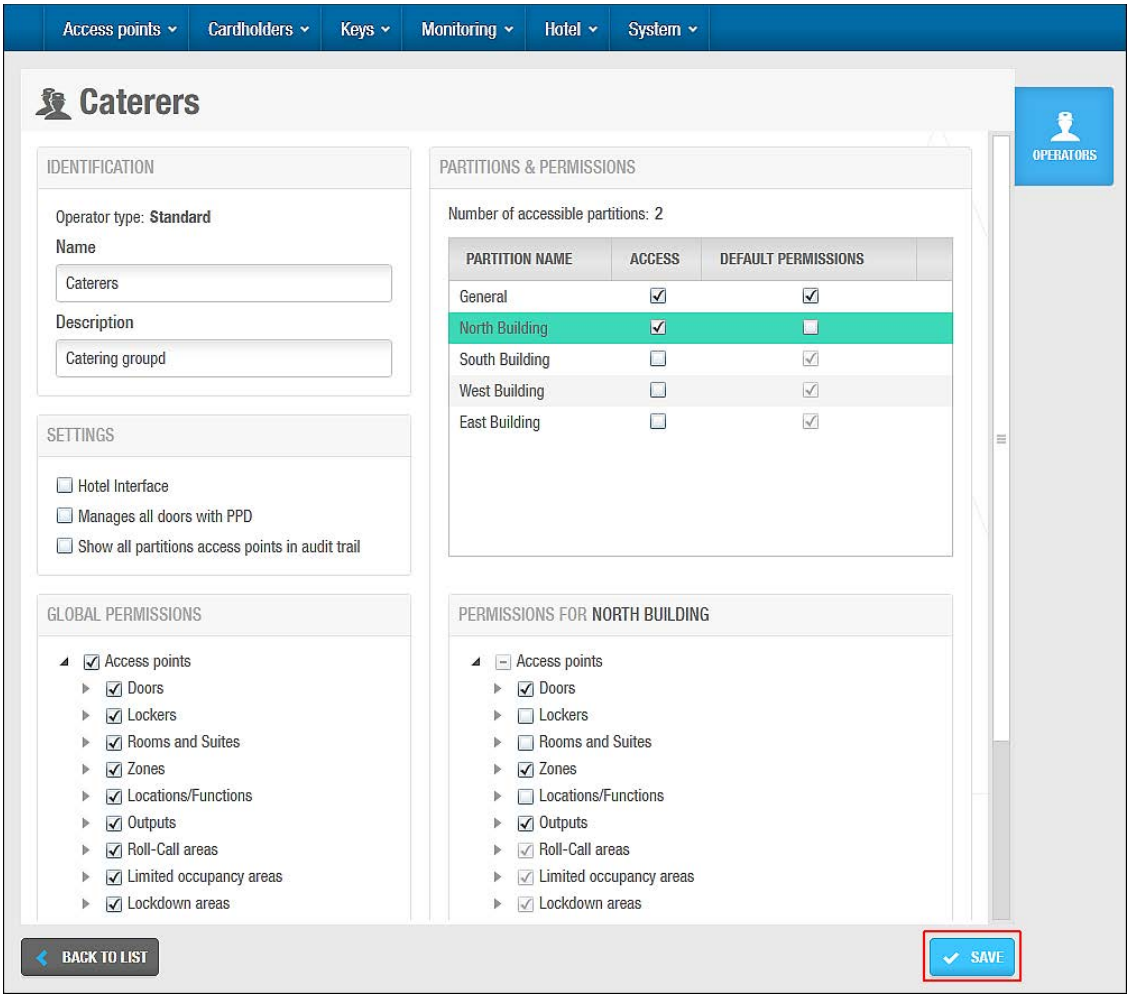


Figure 234: Operator group information screen

28. Type the name of the operator group in the **Name** field.
29. Type a description for the group in the **Description** field.
30. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.
31. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.
32. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes

in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.

33. Click **Save**.

5. 12. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

5. 12. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level **Monitoring** checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors

Permission	Description
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas

Permission	Description
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

5. 12. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

34. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
35. Double-click the operator group with the operator list you want to view.
36. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

    Partitions for more information.
37. Select the appropriate configuration and management options.

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

If required, you can activate additional fields on the **Locker** information screen using ProAccess SPACE General options. To activate the **Ext ID** field, the SHOW_EXT_ID parameter must be enabled. See ***Error! Reference source not found.*** for more information. The **Ext ID** field displays a unique identifier for the locker, automatically generated by the system. You can amend this identifier if required.

You can also add and name up to two general purpose fields. To activate a general purpose field, you must select an **Enable field** checkbox in **System** > **General options** > **Access point** in ProAccess SPACE. You can then name the field in accordance with the information that you want to capture.

NOTE: You can create multiple lockers at once by using the **Multiple Add** option. In addition, you can edit multiple lockers at once by using the **Multiple Edit** option. The **Multiple Edit** button is enabled when you select more than one entry on the **Lockers** screen. This allows you to enter the appropriate identification and configuration details on the **Multiple edit** screen. The details are then applied to all of the selected entries. See *Configuring Lockers* for more information about the configuration settings for lockers.

5. 12. 3. Configuring Lockers

The following sections describe the various fields used to configure lockers.

5. 12. 3. 1. Opening Modes and Timed Periods

The **Open mode** drop-down list defines the lock's working mode. There are two opening modes available for lockers.

The options are described in the following table.

Table 17: Locker open mode options

Option	Description
Standard	Can only be opened using an authorized key
Automatic opening	Can be opened without a key during the automatic opening time period. Outside of this, a key is required. You must select a timetable with this option.

5. 12. 3. 2. Opening Times and Time Zones

The **Opening Time** panel defines how long a locker thumbturn stays active after it is unlocked.

The options are described in the following table.

Table 18: Locker opening times

Option	Description
Open time	Defines how long a locker thumbturn stays active after it is unlocked The default time value is six seconds. The value can be increased or decreased in the range 0 to 255 seconds.
Increased open time	Defines a longer opening time. This option is designed for disabled or 'hands full' users. The default time value is 20 seconds. The value can be increased or decreased in the range 0 to 255 seconds. You must enable this option in the user's profile. See *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. 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. Key Options for more information.

The **Time zone** panel defines which one of the system time zones is used for the locker. You must enable the multiple time zones functionality in ProAccess SPACE General options to display this panel. See ***Error! Reference source not found.*** and *Time Zones* for more information.

5. 12. 3. 3. Locker Options

The **Locker Options** panel defines locker functionality, such as auditing locker activity, allowing users to secure a locker without a key, and reducing battery consumption.

The options are described in the following table.

Table 19: Locker options

Option	Description

Option	Description
Audit on keys	Allows monitoring of when and where keys are used. You must enable this feature on both the locker and the user's key.
Is free assignment locker	Defines whether a locker works as a free assignment locker within an area or has assigned access. To activate this option, you must enable the FREE_ASSIGNMENT_LOCKER parameter in ProAccess SPACE General options. See ***Error! Reference source not found.*** for more information.
Close locker without card	Allows a user or a group of users to secure the locker without a key. This is a useful feature for common lockers that are used by a small number of users, for example, medicine cabinets or store cupboards.
IButton key detection: pulsed mode	Reduces the battery consumption and the risk of rust on the IButton reader contacts as the key detection is done in pulsed mode instead of continuous. To activate this option, you must enable the SHOW_KEY_DETECT_MODE parameter in ProAccess SPACE General options. See ***Error! Reference source not found.*** for more information. This option is only compatible with PPDs that have firmware version 1.02 or higher.
Admit expired keys	Allows users holding expired keys to open a locker for a specified number of days. The range is 0 to 255 days. It also allows users to access an SVN wall reader to update their keys.
Inhibit audit trail	Ensures that the lock does not record openings in its audit trail. The lock can still write on the key. To activate this option, you must select the **Allow audit trail inhibition** checkbox in **System** > **General options** > **Access point** in ProAccess SPACE.

5. 12. 4. Associating Lockers

Once you have created a locker, you must associate users, access levels, and/or zones with the specific locker. The following sections describe how to associate lockers with the various entries.

5. 12. 4. 1. Users

To give access permissions for a locker, you must associate the locker with the user. See *Users* for a definition and information about how to create and configure a user.

To associate a user with a locker, perform the following steps:

1. Select **Access points** > **Lockers**. The **Lockers** screen is displayed.
2. Double-click the locker that you want to associate with a user. The **Locker** information screen is displayed.

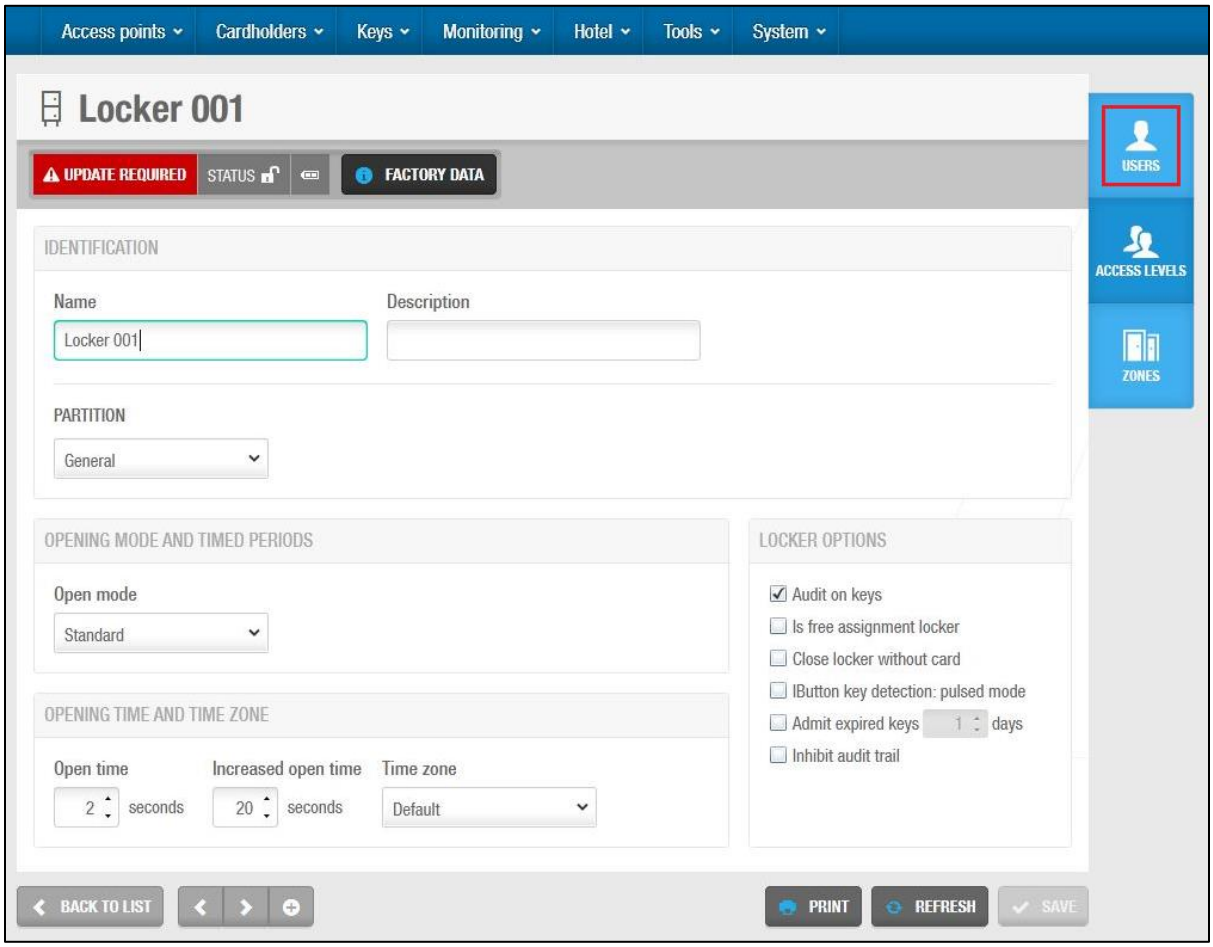


Figure 61: Locker information screen

NOTE: The **Status Open** information field is displayed on the **Locker** information screen if you have reset the status of available lockers to Open on the system by using the **Set Lockers States as Opened** button. This button is available on the **Lockers** list screen. See *Creating Lockers* for more information. The status of lockers is also updated when user keys are updated using an encoder.

3. 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 locker.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.
5. Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right-hand panel.
6. Click **Accept**. The selected user now has access permissions for the locker.

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

5. 12. 4. 2. Access Levels

See *User Access Levels*, *Visitor Access Levels*, and *Guest Access Levels* for information about how to create and configure access levels.

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

1. Select **Access points** > **Lockers**. The **Lockers** screen is displayed.
2. Double-click the locker that you want to associate with an access level. The **Locker** information screen is displayed.
3. Click **Access Levels** in the sidebar. The **Access levels** dialog box is displayed.

   Note that the dialog box will be blank because you have not yet associated an access level with this particular locker.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access levels, is displayed.
5. Select the required access level in the left-hand panel and click the chevron. The selected access level is displayed in the right-hand panel.
6. Click **Accept**. The locker is now associated with the selected access level.

   You can also select which cardholder timetable is used. See *Users* for more information and a description of the steps you should follow.

5. 12. 4. 3. Zones

See *Zones* for a definition and information about how to create and configure a zone.

To associate a locker with a zone, perform the following steps:

1. Select **Access points** > **Lockers**. The **Lockers** screen is displayed.
2. Double-click the locker that you want to associate with a zone. The **Locker** information screen is displayed.
3. 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 locker.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of zones, is displayed.
5. Click the required zone in the right panel.
6. Click the chevron that points to the right panel. The selected zone is displayed in the right panel.
7. Click **Accept**. The locker is now associated with the zone.

5. 12. 5. Locker Icons

When you create lockers, different icons are displayed on the **Lockers** screen. These icons are the same as those displayed for doors. See *Door Icons* for more information.

5. 12. 6. Lockers and Visitors

Visitors can only access lockers if their visitor entry has been associated with a zone containing lockers. They cannot be granted access to a single locker. See *Visitors* for more information.

You can opt to show if a visitor has left a locker opened or closed (preventing users accessing the locker) when the visitor checks out. To activate this option, select the **Control of lockers left closed** checkbox in **System** > **General options** > **Access point** in ProAccess SPACE. See ***Error! Reference source not found.*** for more information.

5. 13. Zones

A zone is a specified group of access points that are grouped together to make them easier to manage in the system. For example, a zone could be the doors on the first floor, all the lockers in the gym area, or all the doors in the financial services area.

When an offline access point is added to a zone, the access point must then be updated with the information using a PPD. See *PPD* for more information. A combination of 64K doors + high zones and 96 low zones can be created in the system (regardless of whether the doors are online or offline). For example, if the systems contains 50000 doors then we could create until 14000 zones.

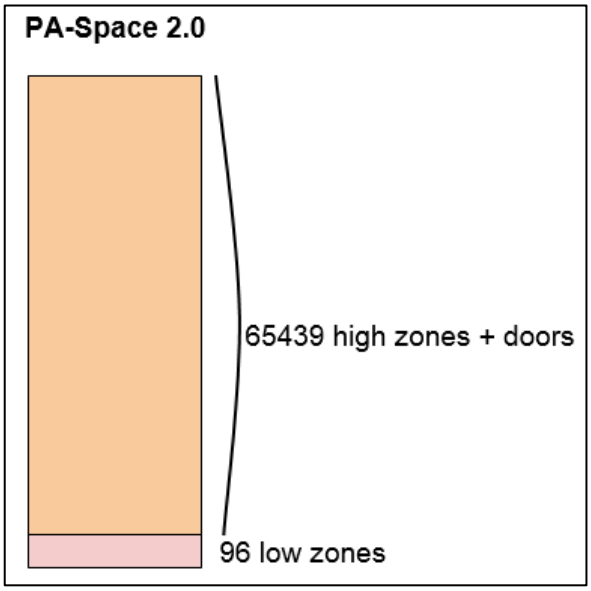


Figure 62: Locker information screen

NOTE: Creating a zone saves memory space on a key because it does not have to store large amounts of individual access point permission details. Instead, it just needs to store the permission information relating to one or more zone entries.

5. 13. 1. Creating Zones

To create a zone, perform the following steps:

1. Select **Access points** > **Zones**. The **Zones** screen is displayed.

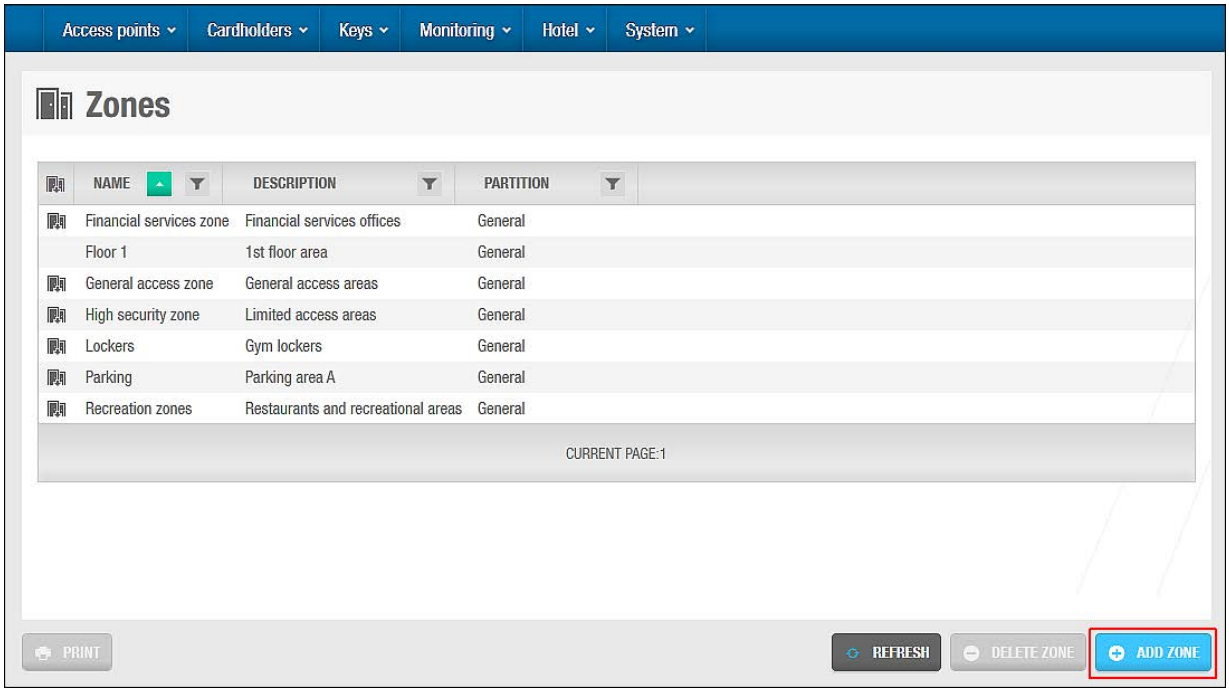


Figure 63: Zones screen

2. Click **Add Zone**. The **Zone** information screen is displayed.

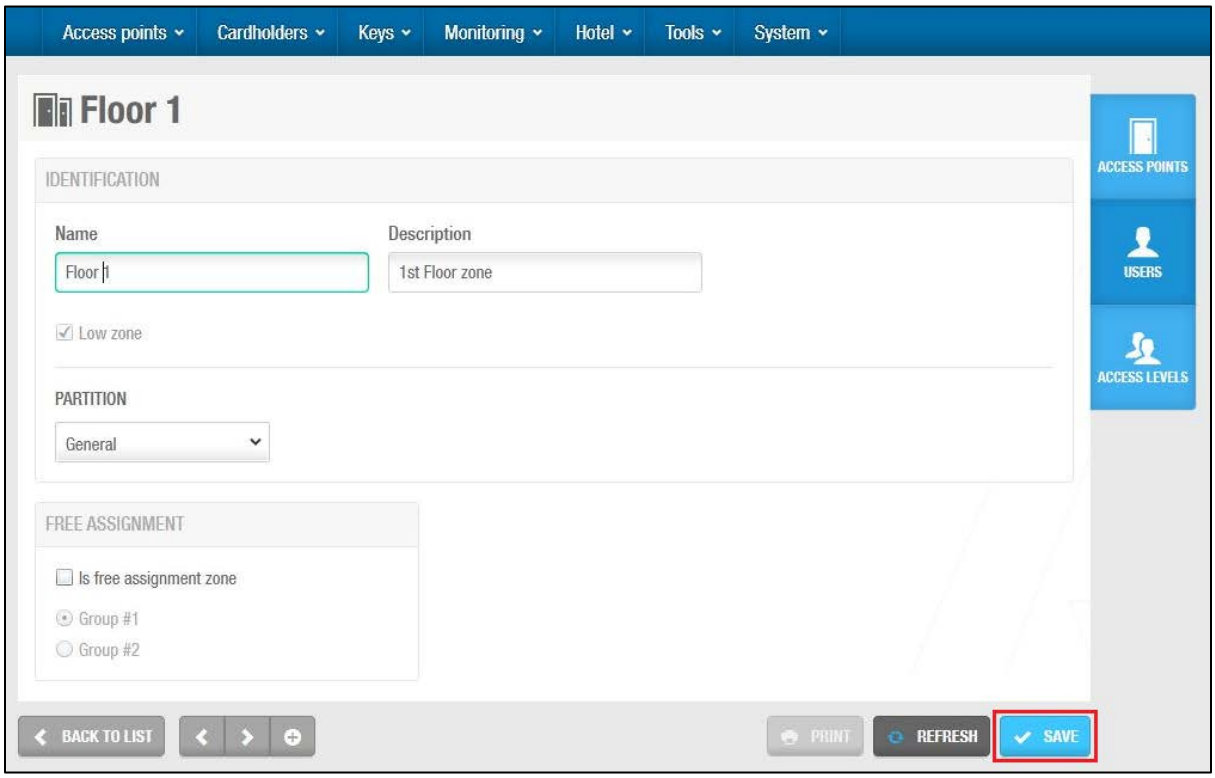


Figure 64: Zone information screen

3. Type a name for the zone in the **Name** field.
4. Type a description for the zone in the **Description** field.
5. Select the relevant partition from the **Partition** drop-down list, if required.

   See *System* Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

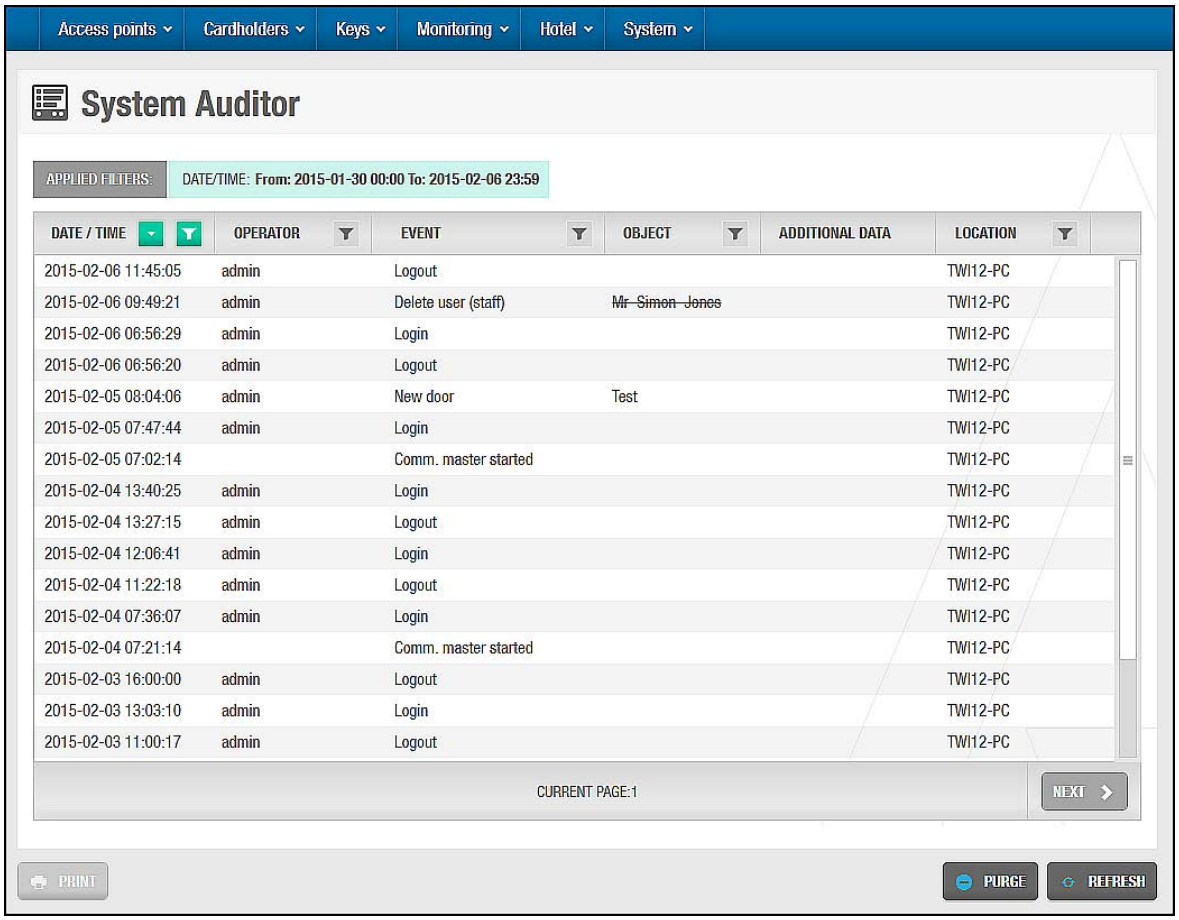


Figure 228: System Auditor information screen

5. 13. 2. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

5. 13. 3. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

6. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

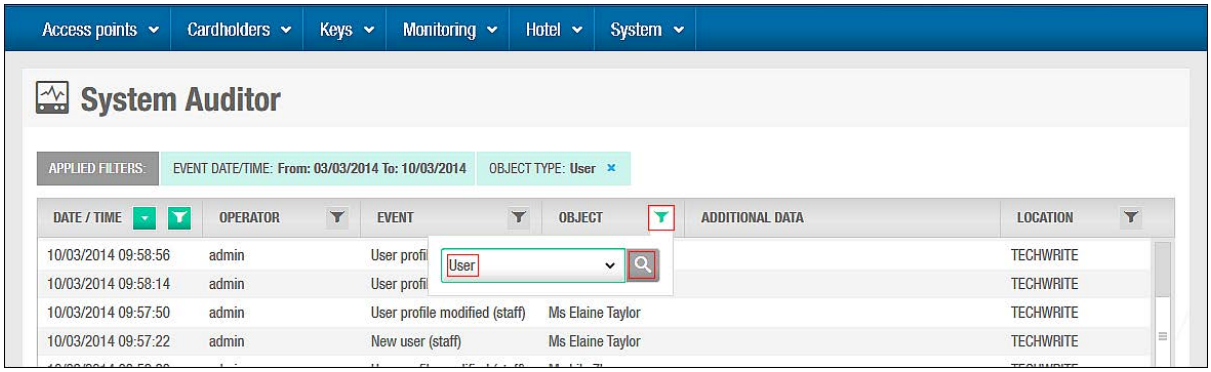


Figure 229: System Auditor information screen

7. Click the **Funnel** icon above the filter item. A search dialog box is displayed.

   For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.

   For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.

   For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.

8. Type your search term.

   Or

   Select a predefined search term from the drop-down list.

   Or

   Select a date range.

   You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.

   However, you cannot remove the **Date/Time** filter.

9. Click the **Search** icon. A filtered audit trail list is displayed.

5. 13. 3. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

5. 13. 4. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic*

System Auditor Purging for more information.

To purge the system auditor, perform the following steps:

10. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
11. Click **Purge**. The **Purge system auditor** dialog box is displayed.

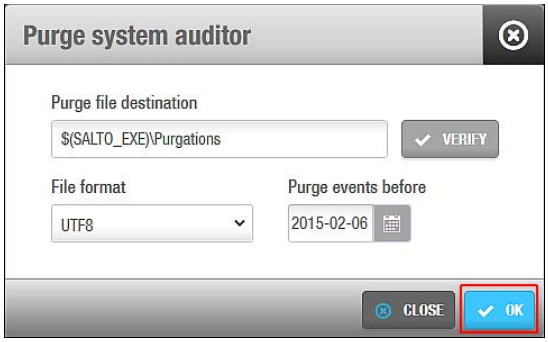


Figure 230: Purge system auditor dialog box

12. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
13. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
14. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
15. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
16. Click **OK**.

5. 14. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

5. 14. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

17. Select **System** > **Operators**. The **Operators** screen is displayed.

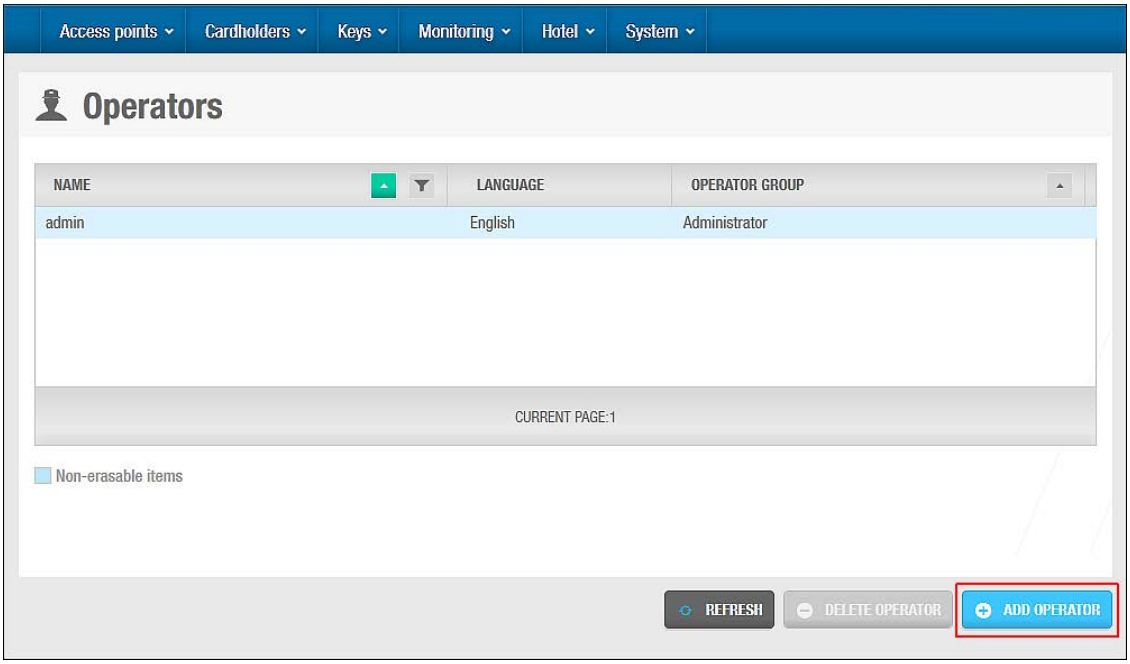


Figure 231: Operators screen

18. Click **Add Operator**. The **Operator** information screen is displayed.

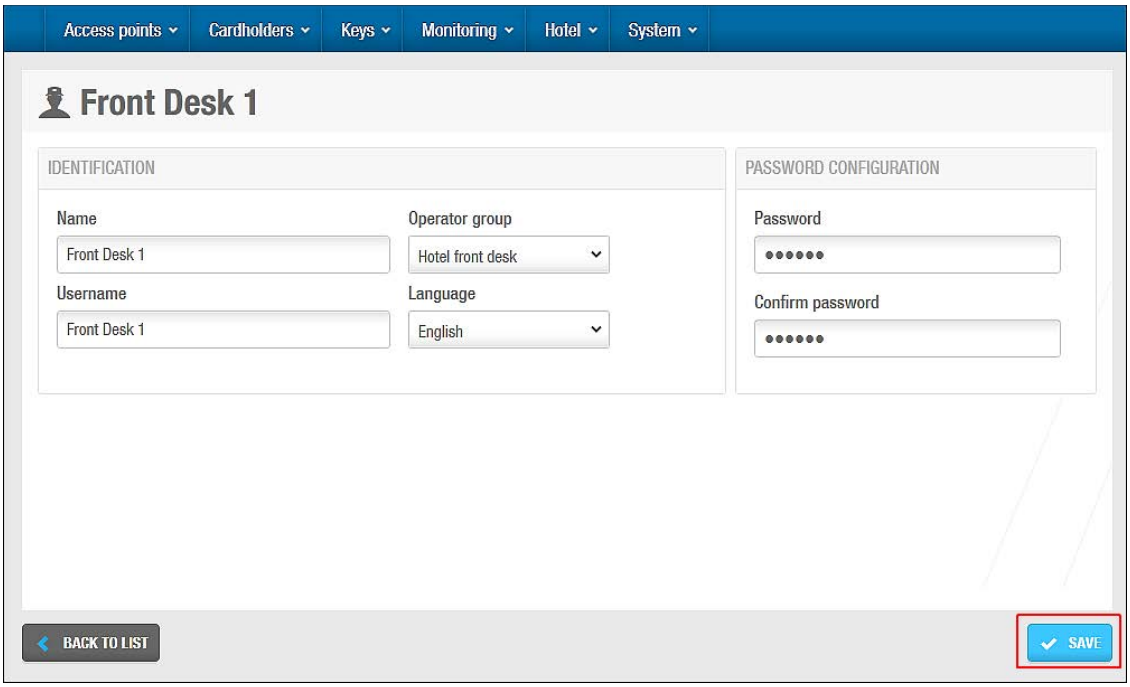


Figure 232: Operator information screen

19. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

20. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

    A maximum of 64 characters can be entered. The user name is not case sensitive.

21. Select the appropriate operator group from the **Operator group** drop-down list.
22. Select the display language for the operator in the **Language** drop-down list.

23. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.

24. Confirm the password.
25. Click **Save**.

5. 15. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

5. 15. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

26. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

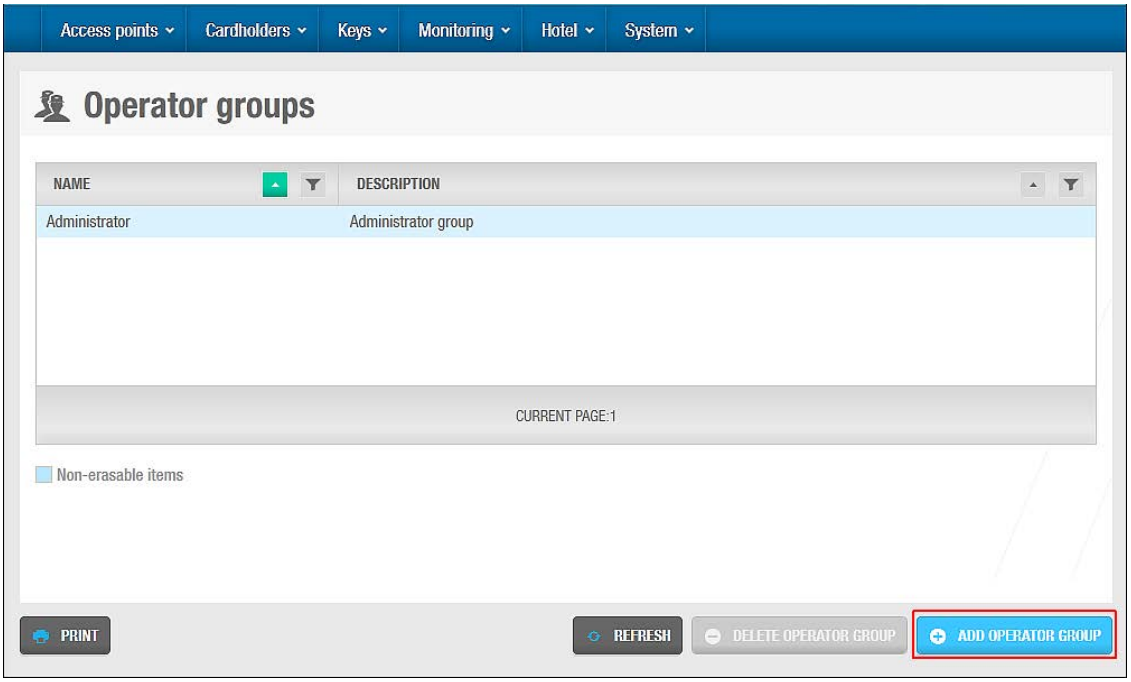


Figure 233: Operator groups screen

27. Click **Add Operator Group**. The **Operator group** information screen is displayed.

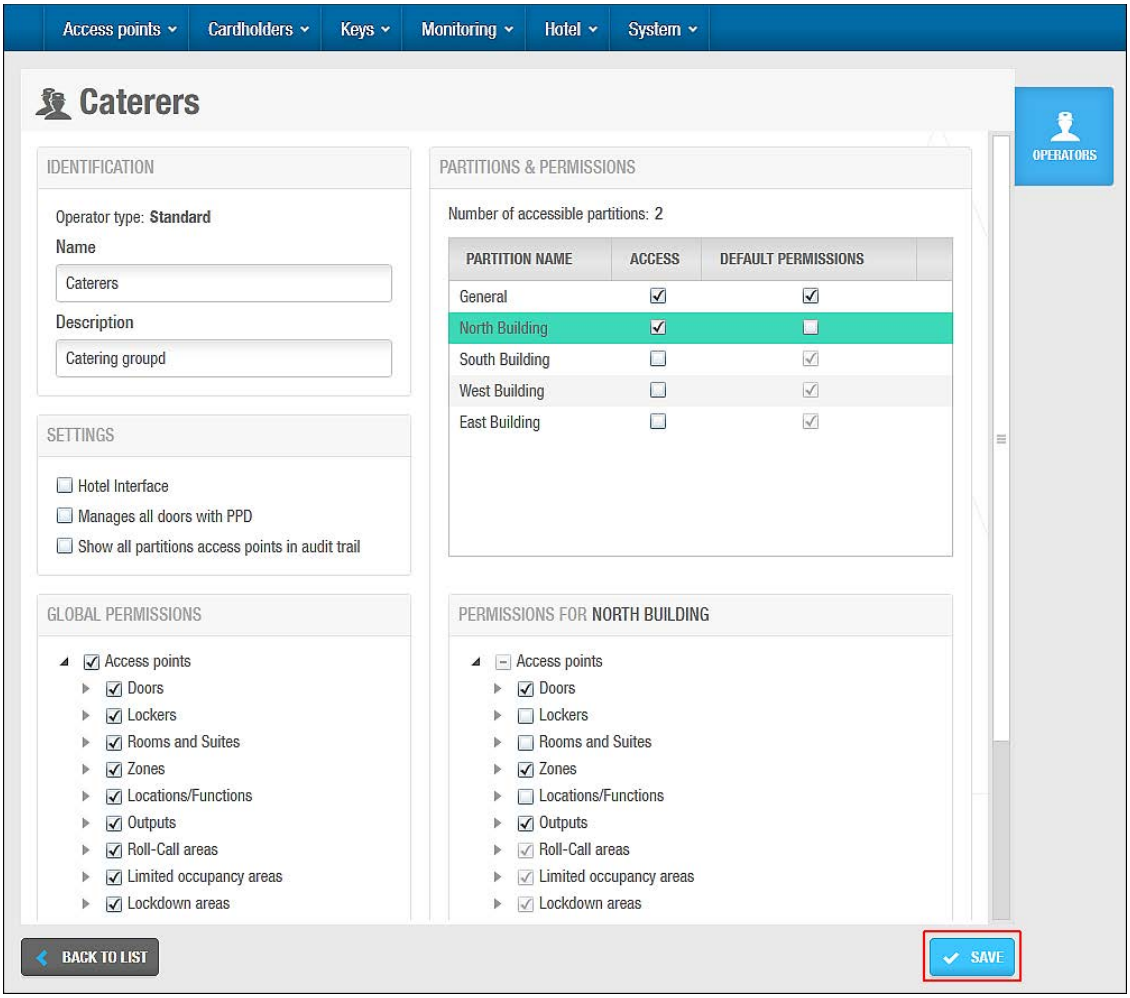


Figure 234: Operator group information screen

28. Type the name of the operator group in the **Name** field.
29. Type a description for the group in the **Description** field.
30. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.
31. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.
32. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes

in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.

33. Click **Save**.

5. 15. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

5. 15. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level **Monitoring** checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors

Permission	Description
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas

Permission	Description
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

5. 15. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

34. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
35. Double-click the operator group with the operator list you want to view.
36. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

    Partitions for more information.
37. Select **Low zone** if appropriate.

    See *Configuring Zones* for more information about this option.
38. Select **Is free assignment zone** if appropriate.

    The **Is free assignment zone** option only applies to lockers. See *Configuring Zones* and *Creating Free Assignment Zones* for more information about this option.
39. Click **Save**.

If required, you can activate the **Ext ID** field on the **Zone** information screen using ProAccess SPACE General options. To activate the **Ext ID** field, the SHOW_EXT_ID parameter must be enabled. See ***Error! Reference source not found.*** for more information.

5. 15. 3. Configuring Zones

The options for configuring zones are described in the following table.

Table 20: Zone options

Option	Description
Low zone	Zones are classified as high or low according to the way the zone information is stored on a lock. You can create up to 96 low zones and a combination of high zones and door, a total of 65439. A door can belong to a maximum of 116 zones, 96 of these being low zones and 20 being high zones for locks. When you have created 96 low zones, a message informs you that you must then create high zones. After you select the **Low zone** checkbox and save, you cannot change this value. If you need to create a high zone, you can delete the low zone and create a new high zone. High and low zones work in the same way so you generally create low zones until limits are reached.
Free assignment zone	Select this checkbox if you are creating a locker zone where users can choose any locker from a number of available lockers. To activate this option, you must enable the FREE_ASSIGNMENT_LOCKER advanced parameter in ProAccess SPACE General options. See *Creating Free Assignment Zones* for more information.

Option	Description
Group #1	To activate additional locker zone options, you must enable the FREE_ASSIGNMENT_LOCKER and FAL_MULTIPLE advanced parameters in ProAccess SPACE General options. When you enable the FAL_MULTIPLE parameter, the **Group#1** and **Group#2** options are displayed on the **Zone** information screen. You must select the **Is free assignment zone** checkbox before you can select a group option. See *Creating Free Assignment Zones* for more information.
Group #2	See above.

5. 15. 4. Associating Zones

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

5. 15. 4. 1. Access Points

See *About Access Points* for more information.

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

1. Select **Access points** > **Zones**. The **Zones** screen is displayed.
2. Double-click the zone that you want to associate with an access point. The **Zone** information screen is displayed.
3. 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 zone.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.
5. 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.
6. Click **Accept**. The zone is now associated with the access point.

5. 15. 4. 2. Users

You must associate a user with a zone to allow that user to access the access points within the zone.

To associate a user with a zone, perform the following steps:

1. Select **Access points** > **Zones**. The **Zones** screen is displayed.
2. Double-click the zone that you want to associate with a user. The **Zone** information screen is displayed.
3. 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 zone.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.
5. Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right-hand panel.
6. Click **Accept**. The selected user now has access to that zone.

You can also select which cardholder timetable is used. See *Users* for more information and a description of the steps you should follow.

5. 15. 4. 3. Access Levels

See *User Access Levels*, *Visitor Access Levels*, and *Guest Access Levels* for information about how to create and configure access levels.

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

1. Select **Access points** > **Zones**. The **Zones** screen is displayed.
2. Double-click the zone that you want to associate with an access level. The **Zone** information screen is displayed.
3. Click **Access Levels** in the sidebar. The **Access levels** dialog box is displayed.

   Note that the dialog box will be blank because you have not yet associated an access level with this particular zone.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access levels, is displayed.
5. Select the required access level in the left-hand panel and click the chevron. The selected access level is displayed in the right-hand panel.
6. Click **Accept**. The zone is now associated with the access level.

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

5. 15. 5. Creating Free Assignment Zones

A free assignment zone is an area where users are free to choose any locker. They do not have pre-assigned individual lockers.

Free assignment zones are generally created and configured in the following order:

1. **Free assignment zone parameters enabled and added**

   The admin operator enables the required parameters and options in ProAccess SPACE General options. See below for more information about this.
2. **New zone created and defined as a free assignment zone**

   The admin operator creates a zone in ProAccess SPACE and selects the **Is free assignment zone** checkbox. See *Creating Zones* for information about how to create zones.
3. **New lockers created and defined as free assignment lockers**

   The admin operator creates lockers and selects the **Is free assignment locker** checkbox.
4. **Lockers added to the zone**

   The admin operator adds the free assignment locker to the free assignment zone. See *Zones* for information about how to add lockers to zones.

Keys can be programmed in two ways for lockers. Static keys are used when users have permission to access a specific locker. Dynamic keys are used in free assignment zones where users can select any locker in the area. See ***Error! Reference source not found.*** for more information.

There are a number of General options configuration tasks associated with free assignment zones:

- To designate an area as a free assignment zone, you must enable the FREE_ASSIGNMENT_LOCKER parameter. See ***Error! Reference source not found.*** for more information.
- To activate additional locker zone options, you must enable the FAL_MULTIPLE advanced parameter. See ***Error! Reference source not found.*** for more information. This allows users to access lockers within two different free assignment zones using the same key.
- To limit the amount of time for which free assignment lockers can be used, select the **Time-limited occupancy** checkbox in **System** > **General options** > **Access points**. See ***Error! Reference source not found.*** for more information.

5. 16. Locations

In the SALTO system, a location is a large area of designated access points. For example, a company could create a location entry for each of its offices across Australia in Sydney, Melbourne, and Perth. You can assign access rights for each location.

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

1. **Location groupings added**

   The admin operator adds the location grouping in ProAccess SPACE General options. See ***Error! Reference source not found.*** for information about adding a location grouping.

2. **Locations created and configured**

   The admin operator creates locations and configures the location options in ProAccess SPACE.

3. **Locations associated**

   The admin operator associates users and/or access points with the specified locations in ProAccess SPACE.

5. 16. 1. Creating Locations

To create a location, perform the following steps:

1. Select **Access points** > **Locations**. The **Locations** screen is displayed.

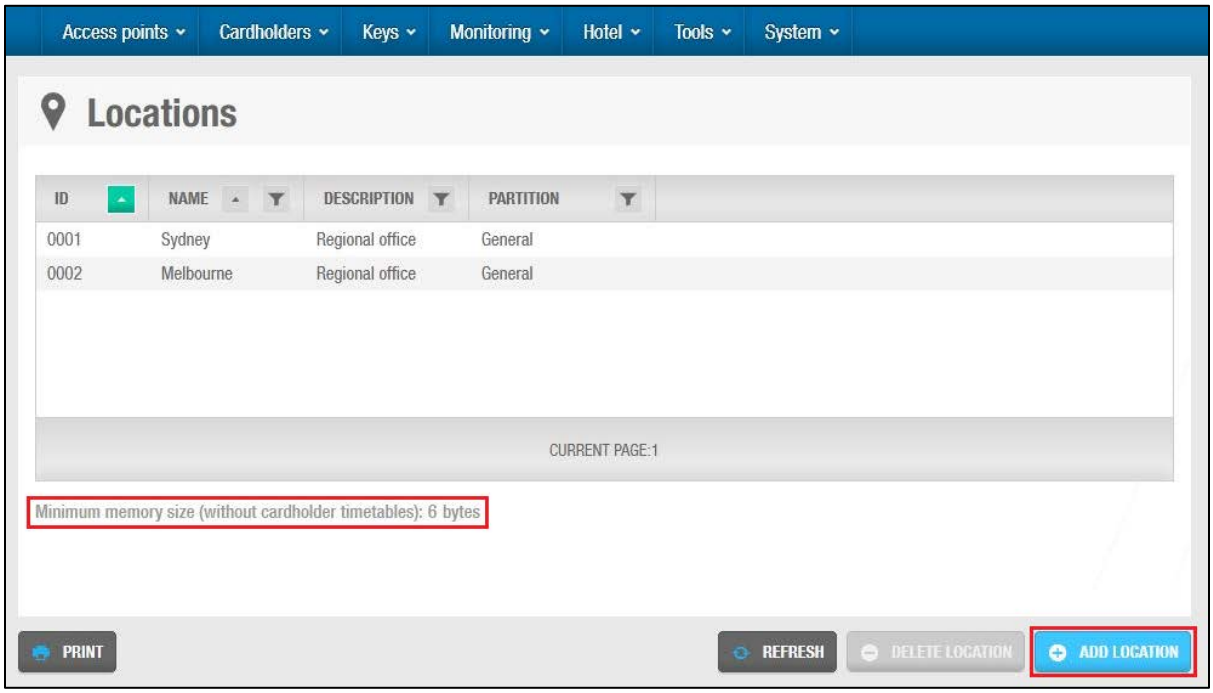


Figure 65: Locations screen

NOTE: The number of locations you create in ProAccess SPACE occupies a fixed amount of memory on keys. The text **Minimum memory size (without cardholder timetables):** indicates the size of the fixed space allocated.

2. Click **Add Location**. The **Location** information screen is displayed.

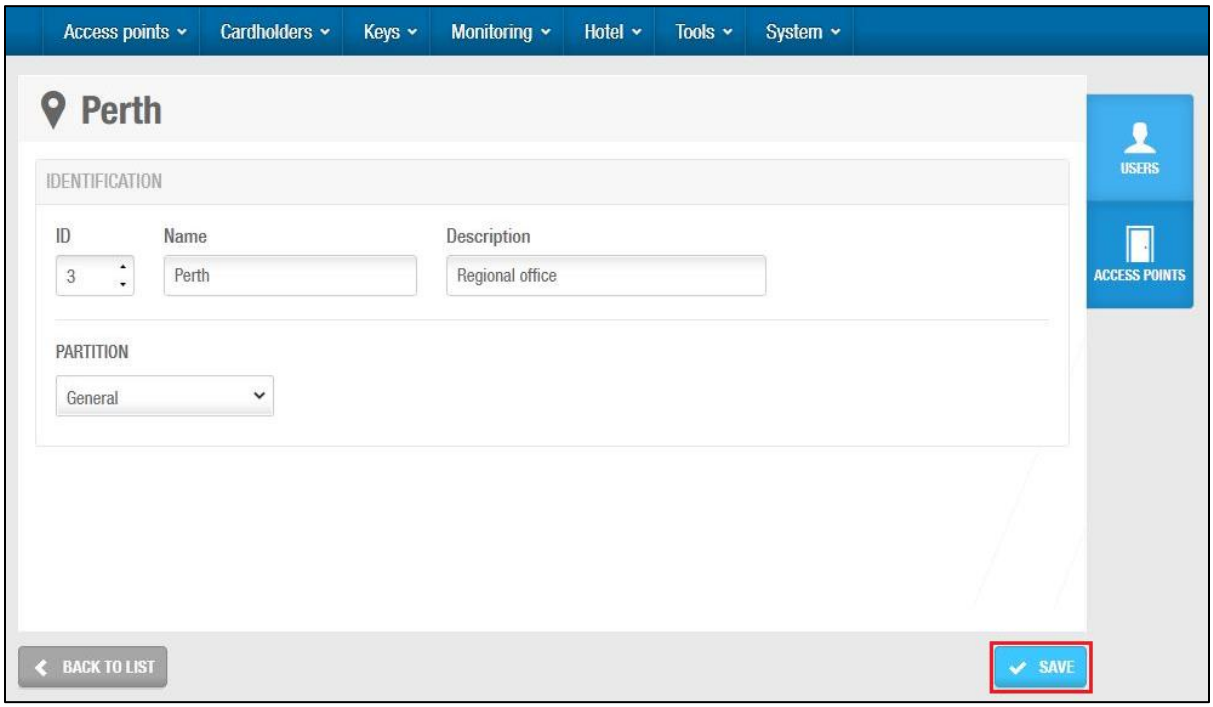


Figure 66: Location information screen

3. Type a name for the location in the **Name** field.
4. Type a description for the location in the **Description** field.
5. Select the relevant partition from the **Partition** drop-down list, if required.

   See *System* Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

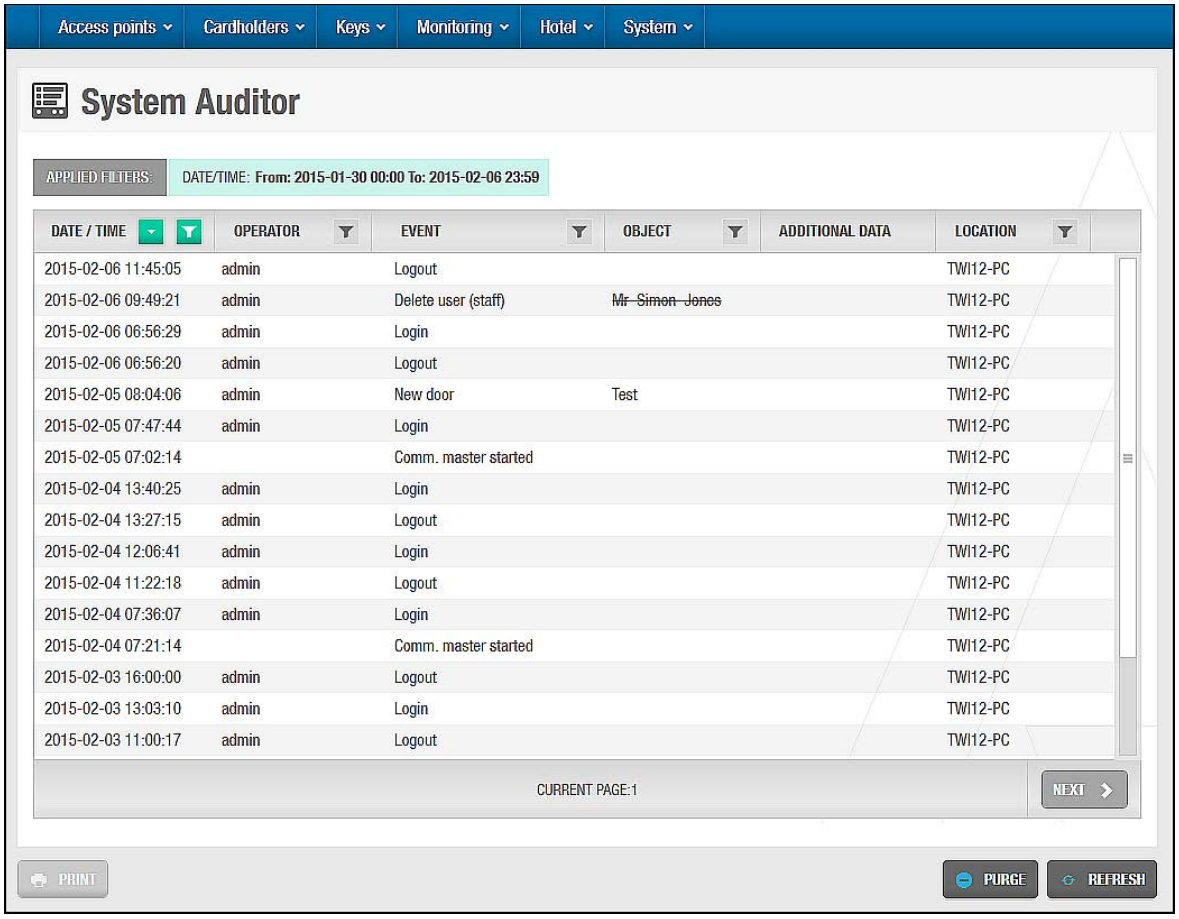


Figure 228: System Auditor information screen

5. 16. 2. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

5. 16. 3. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

6. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

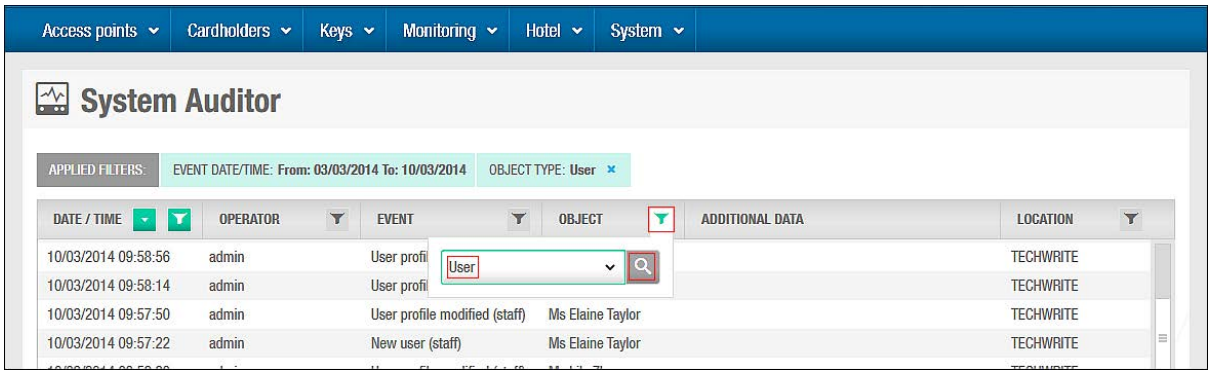


Figure 229: System Auditor information screen

7. Click the **Funnel** icon above the filter item. A search dialog box is displayed.
   For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.
   For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.
   For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.
8. Type your search term.
   Or
   Select a predefined search term from the drop-down list.
   Or
   Select a date range.
   You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it. However, you cannot remove the **Date/Time** filter.
9. Click the **Search** icon. A filtered audit trail list is displayed.

5. 16. 3. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

5. 16. 4. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic System Auditor Purging* for more information.

To purge the system auditor, perform the following steps:

10. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
11. Click **Purge**. The **Purge system auditor** dialog box is displayed.

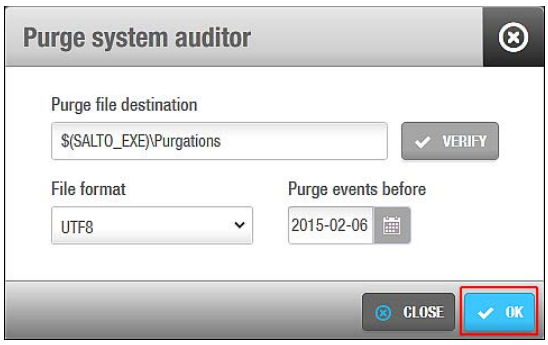


Figure 230: Purge system auditor dialog box

12. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
13. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
14. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
15. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
16. Click **OK**.

5. 17. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

5. 17. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

17. Select **System** > **Operators**. The **Operators** screen is displayed.

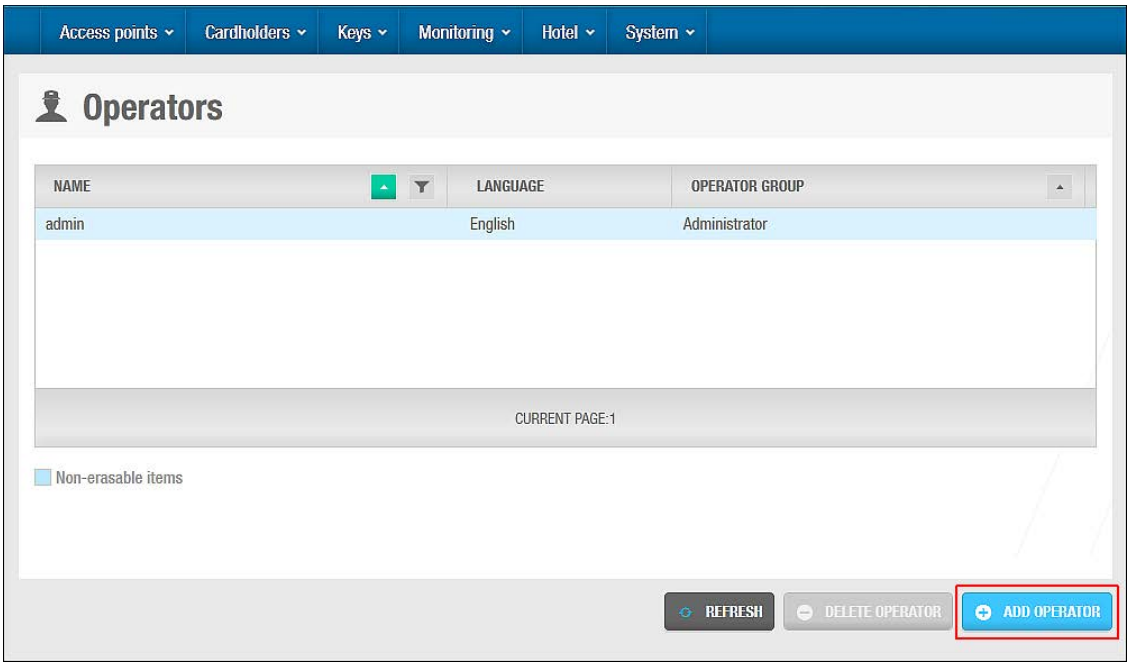


Figure 231: Operators screen

18. Click **Add Operator**. The **Operator** information screen is displayed.

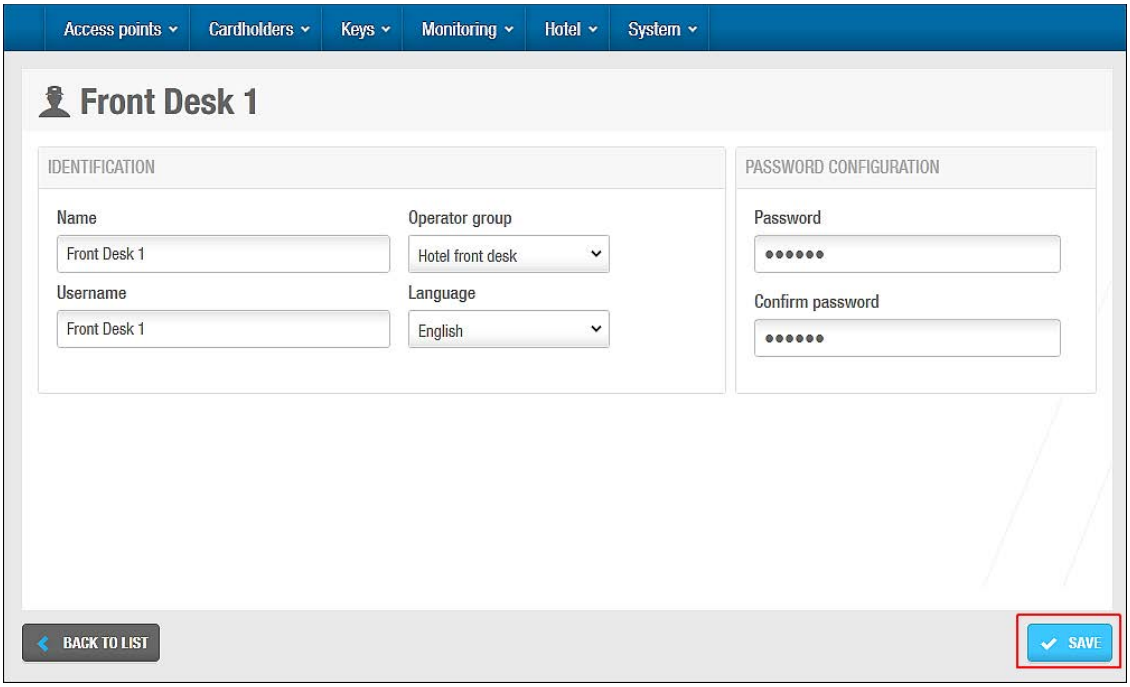


Figure 232: Operator information screen

19. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

20. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

A maximum of 64 characters can be entered. The user name is not case sensitive.

21. Select the appropriate operator group from the **Operator group** drop-down list.
22. Select the display language for the operator in the **Language** drop-down list.
23. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.
24. Confirm the password.
25. Click **Save**.

5. 18. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

5. 18. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

26. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

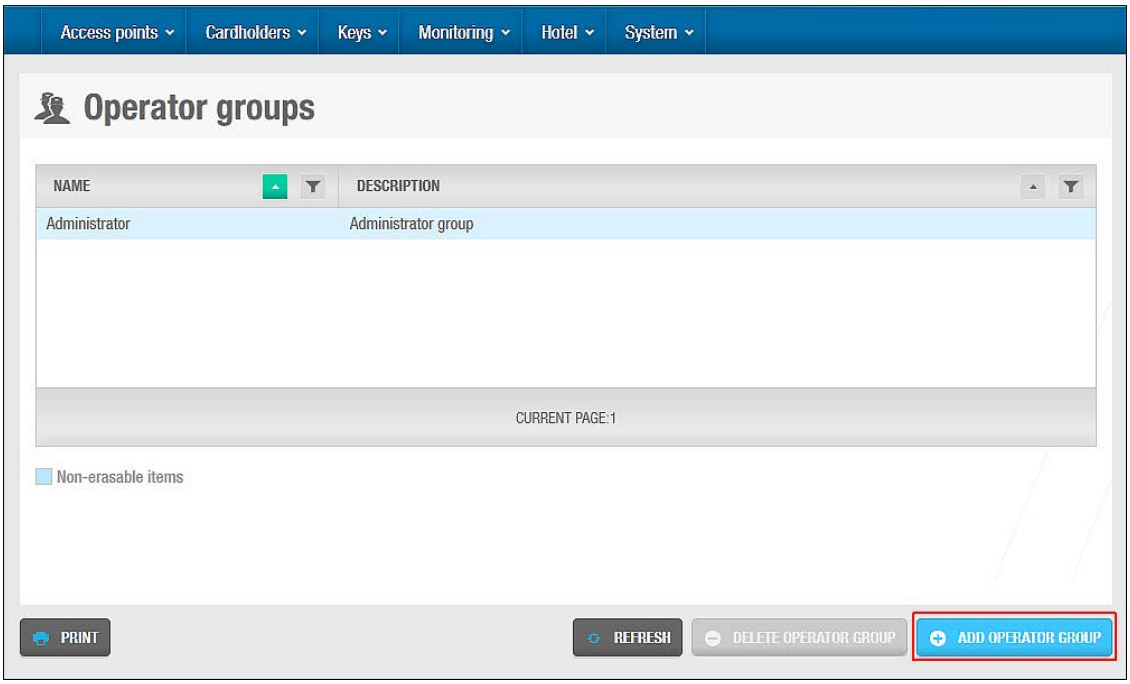


Figure 233: Operator groups screen

27. Click **Add Operator Group**. The **Operator group** information screen is displayed.

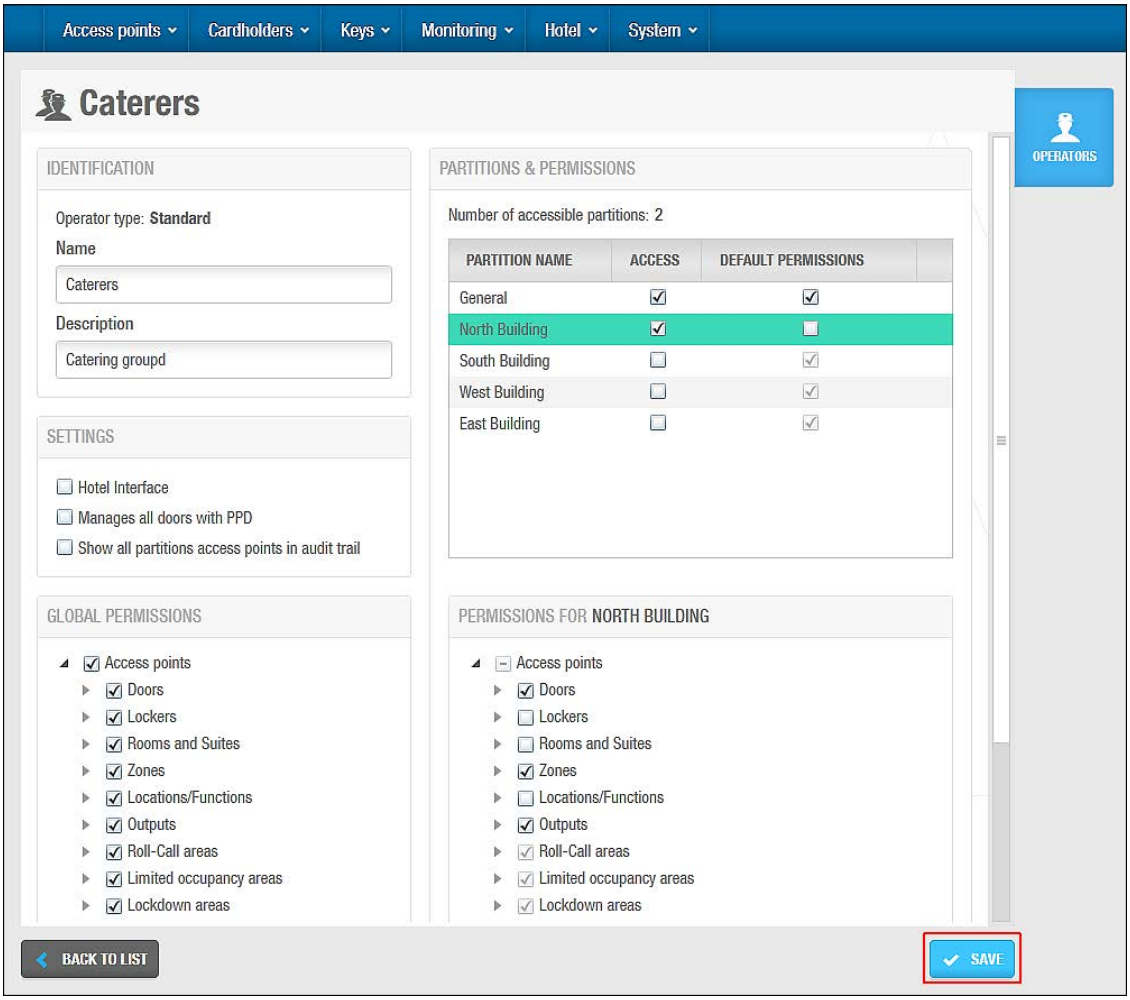


Figure 234: Operator group information screen

28. Type the name of the operator group in the **Name** field.
29. Type a description for the group in the **Description** field.
30. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.
31. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.
32. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.
33. Click **Save**.

5. 18. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

5. 18. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level

Monitoring checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs

Permission	Description
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels

Permission	Description
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.

Permission	Description
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars

Permission	Description
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

5. 18. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

34. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
35. Double-click the operator group with the operator list you want to view.
36. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

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

NOTE: The **ID** field is automatically populated, but numbers from 1 to 1024 can be edited if required. By default, if you skip **ID** numbers, for example from 5 to 125, SALTO reserves the memory space between these numbers, even if no **ID** numbers are created. SALTO recommends using this default setting. ProAccess SPACE generates an error if you enter a value higher than 1024.

5. 18. 3. Associating Locations

Once you have created a location, you must associate users and access points with that location. An example of a user would be a staff member who always works at that location. For example, for a Sydney location, you could provide an IT manager with access to all IT areas in that location. The following sections describe how to associate locations with the various entries.

5. 18. 3. 1. Users

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

1. Select **Access points** > **Locations**. The **Locations** screen is displayed.
2. Double-click the location that you want to associate with a user. The **Location** information screen is displayed.
3. 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 location.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.
5. Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right-hand panel.
6. Click **Accept**. The selected user now has access permissions for that location.

5. 18. 3. 2. Access Points

See *About Access Points* for more information.

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

1. Select **Access points** > **Locations**. The **Locations** screen is displayed.
2. Double-click the location that you want to associate with an access point. The **Location** information screen is displayed.
3. 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 location.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.
5. 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.
6. Click **Accept**. The location is now associated with that access point.

5. 19. Functions

A function is a category of permissions within a SALTO location. For example, if a company creates a location for each of its offices across the country, it can assign functions such as entrances and maintenance, to each location. For the company location Melbourne, for example, the company can assign the entrances function to all building entrances at that location.

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

1. **Function groupings added**

   The admin operator adds the function grouping in ProAccess SPACE General options. See ***Error! Reference source not found.*** for information about adding a function grouping.
2. **Functions created and configured**

   The admin operator creates functions and configures the function options in ProAccess SPACE.
3. **Functions associated**

The admin operator associates users and/or access points with the specified functions in ProAccess SPACE.

5. 19. 1. Creating Functions

To create a function, perform the following steps:

1. Select **Access points** > **Functions**. The **Functions** screen is displayed.

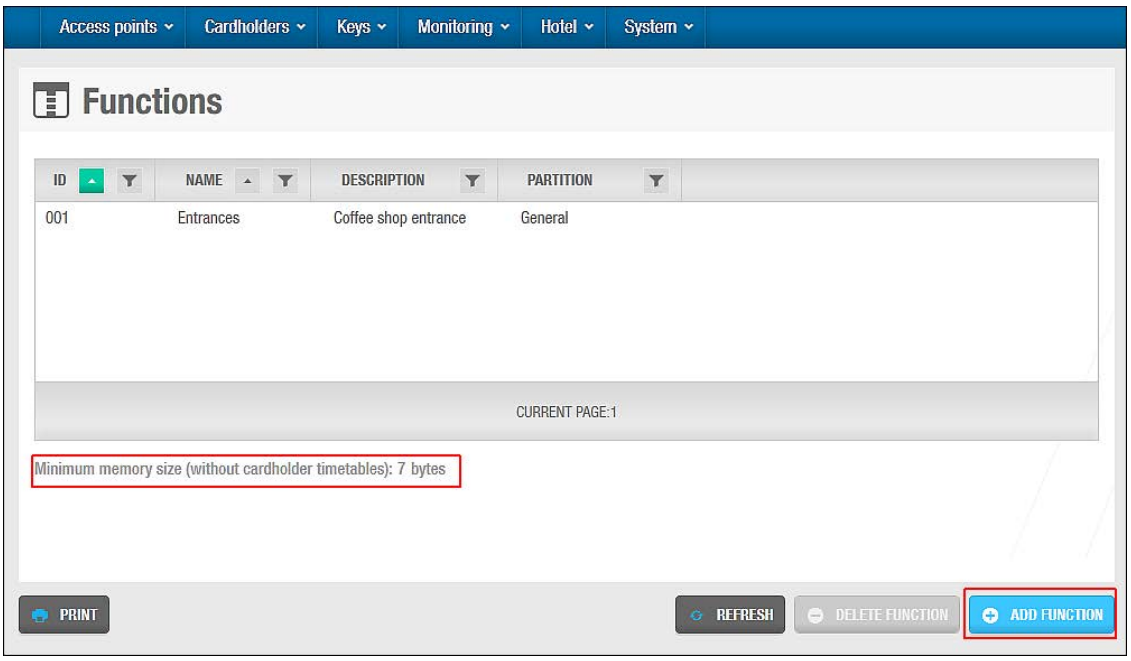


Figure 67: Functions screen

NOTE: The number of functions you create in ProAccess SPACE occupies a fixed amount of memory on keys. The text **Minimum memory size (without cardholder timetables):** indicates the size of the fixed space allocated.

2. Click **Add Function**. The **Function** information screen is displayed.

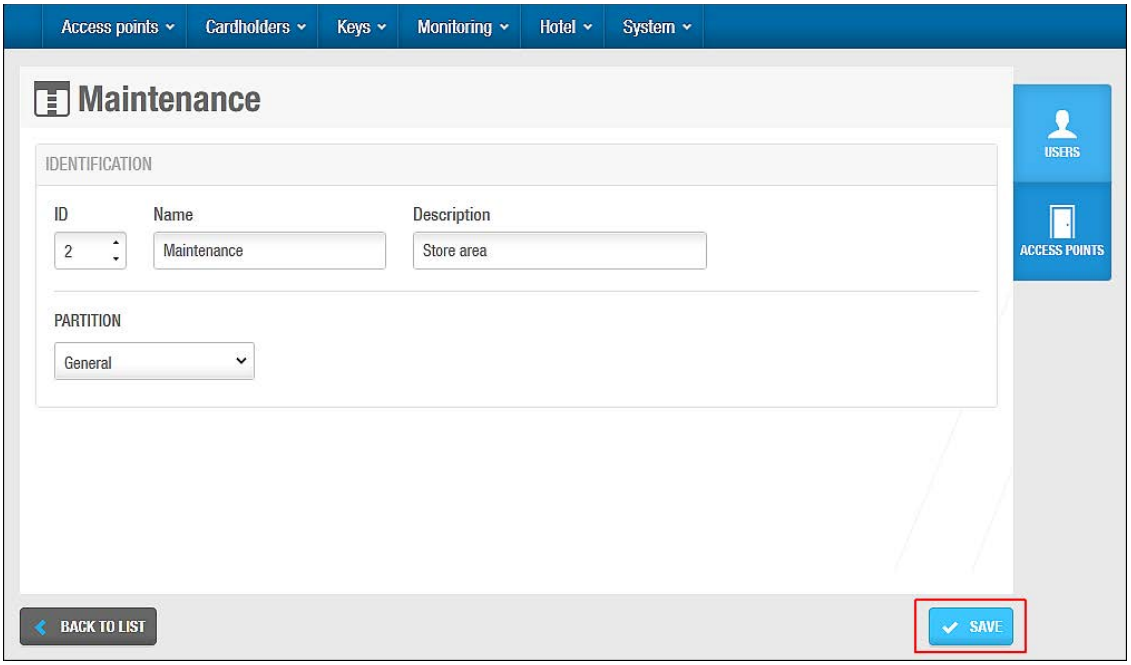


Figure 68: Function information screen

3. Type a name for the function in the **Name** field.
4. Type a description for the function in the **Description** field.
5. Select the relevant partition from the **Partition** drop-down list, if required.

See *System* Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

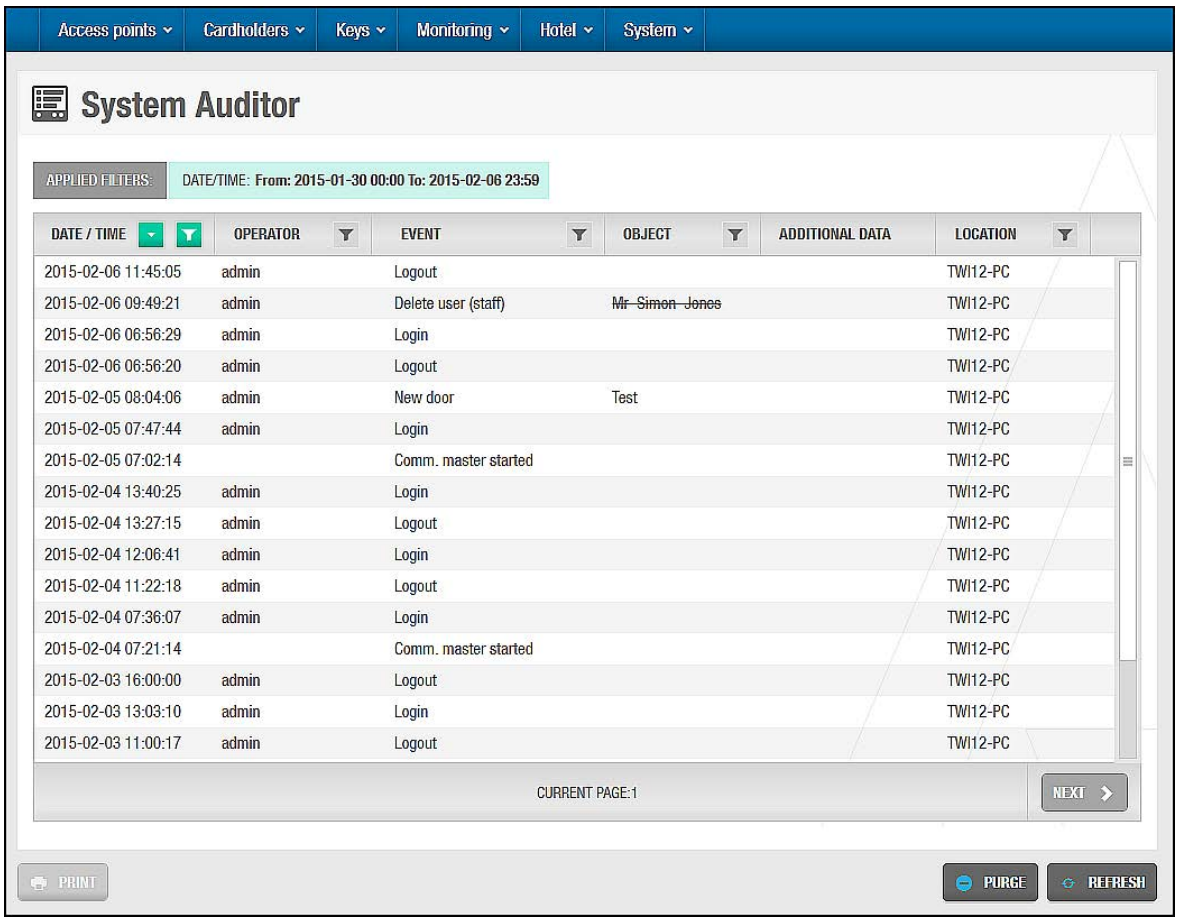


Figure 228: System Auditor information screen

5. 19. 2. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

5. 19. 3. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

6. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

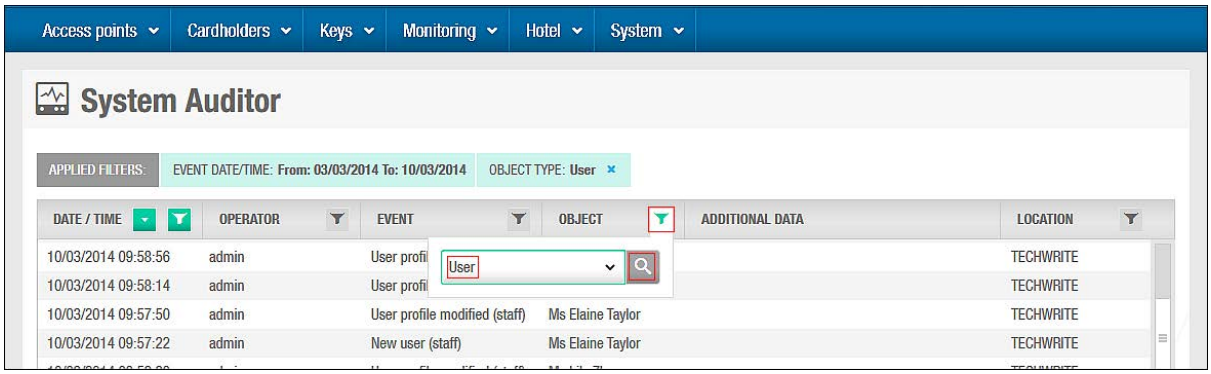


Figure 229: System Auditor information screen

7. Click the **Funnel** icon above the filter item. A search dialog box is displayed.
   For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.
   For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.
   For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.
8. Type your search term.
   Or
   Select a predefined search term from the drop-down list.
   Or
   Select a date range.
   You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it. However, you cannot remove the **Date/Time** filter.
9. Click the **Search** icon. A filtered audit trail list is displayed.

5. 19. 3. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

5. 19. 4. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic System Auditor Purging* for more information.

To purge the system auditor, perform the following steps:

10. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
11. Click **Purge**. The **Purge system auditor** dialog box is displayed.

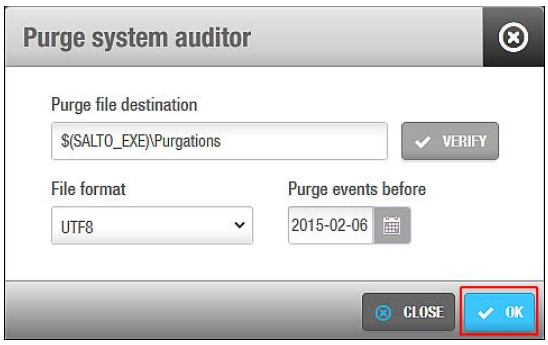


Figure 230: Purge system auditor dialog box

12. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
13. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
14. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
15. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
16. Click **OK**.

5. 20. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

5. 20. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

17. Select **System** > **Operators**. The **Operators** screen is displayed.

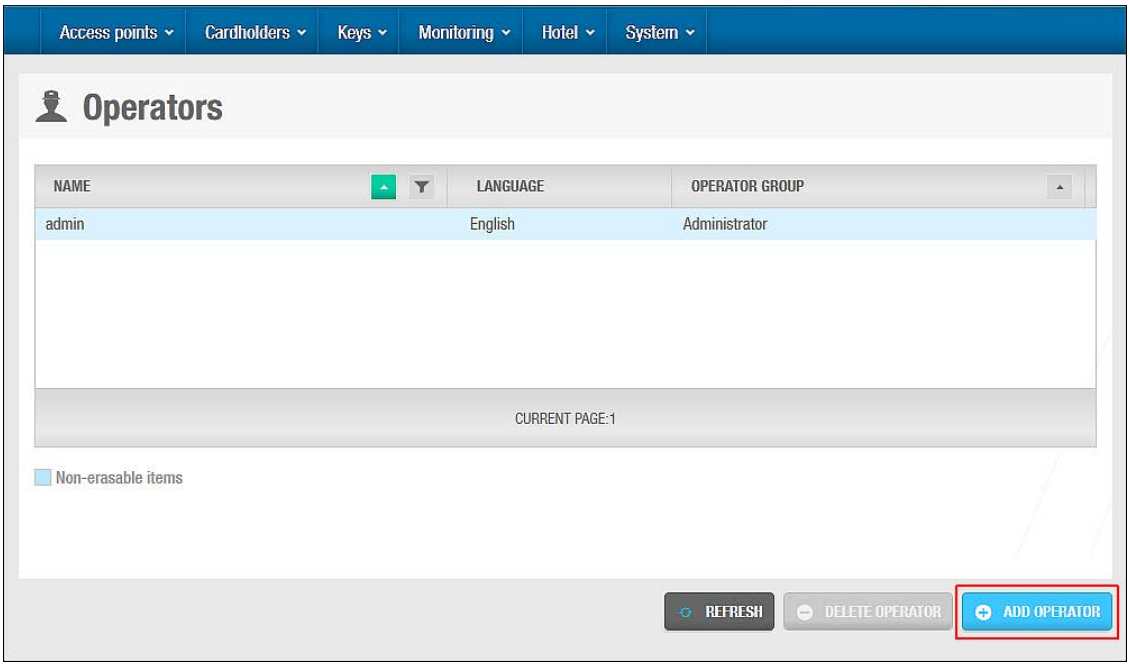


Figure 231: Operators screen

18. Click **Add Operator**. The **Operator** information screen is displayed.

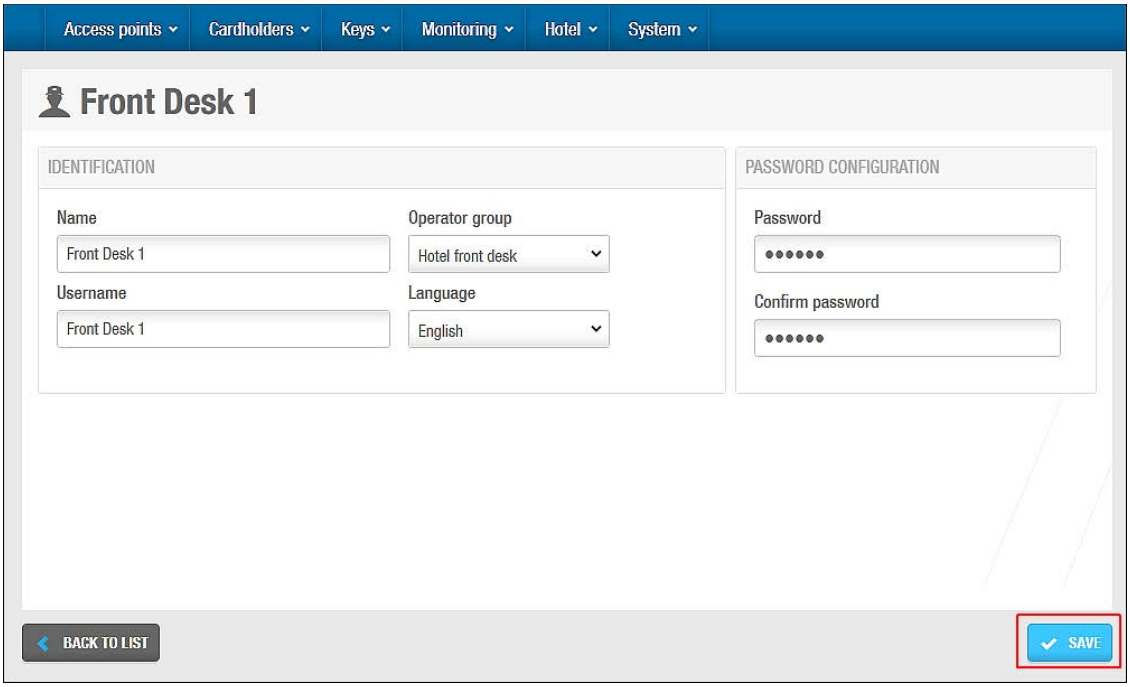


Figure 232: Operator information screen

19. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

20. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

A maximum of 64 characters can be entered. The user name is not case sensitive.

21. Select the appropriate operator group from the **Operator group** drop-down list.
22. Select the display language for the operator in the **Language** drop-down list.
23. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.
24. Confirm the password.
25. Click **Save**.

5. 21. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

5. 21. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

26. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

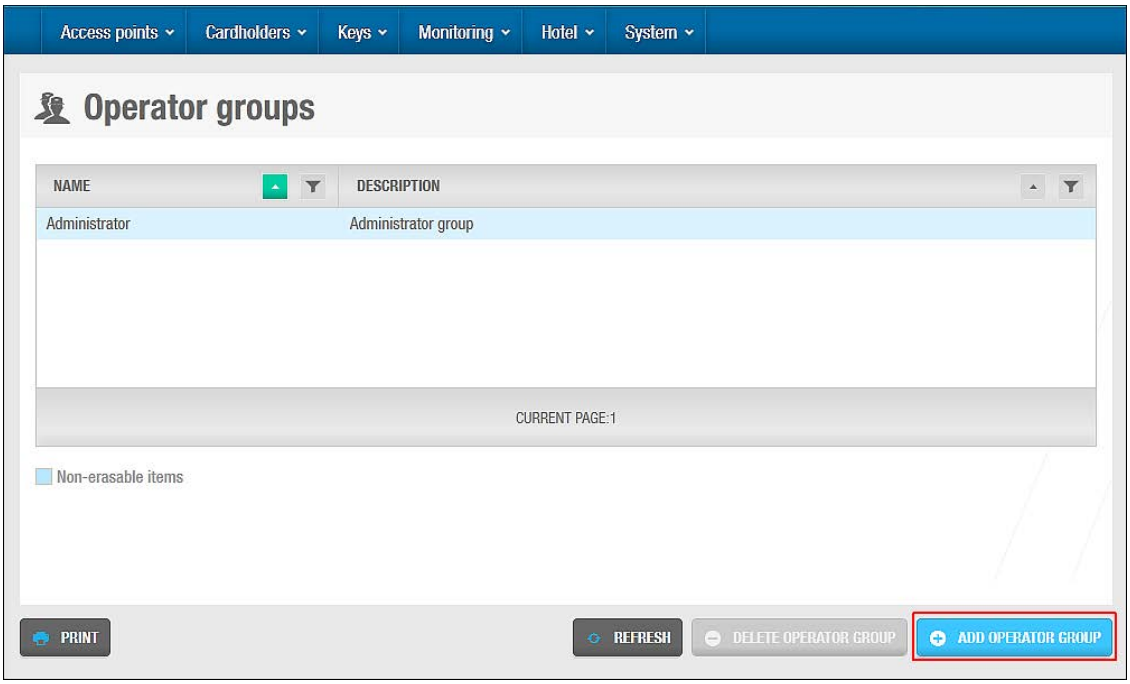


Figure 233: Operator groups screen

27. Click **Add Operator Group**. The **Operator group** information screen is displayed.

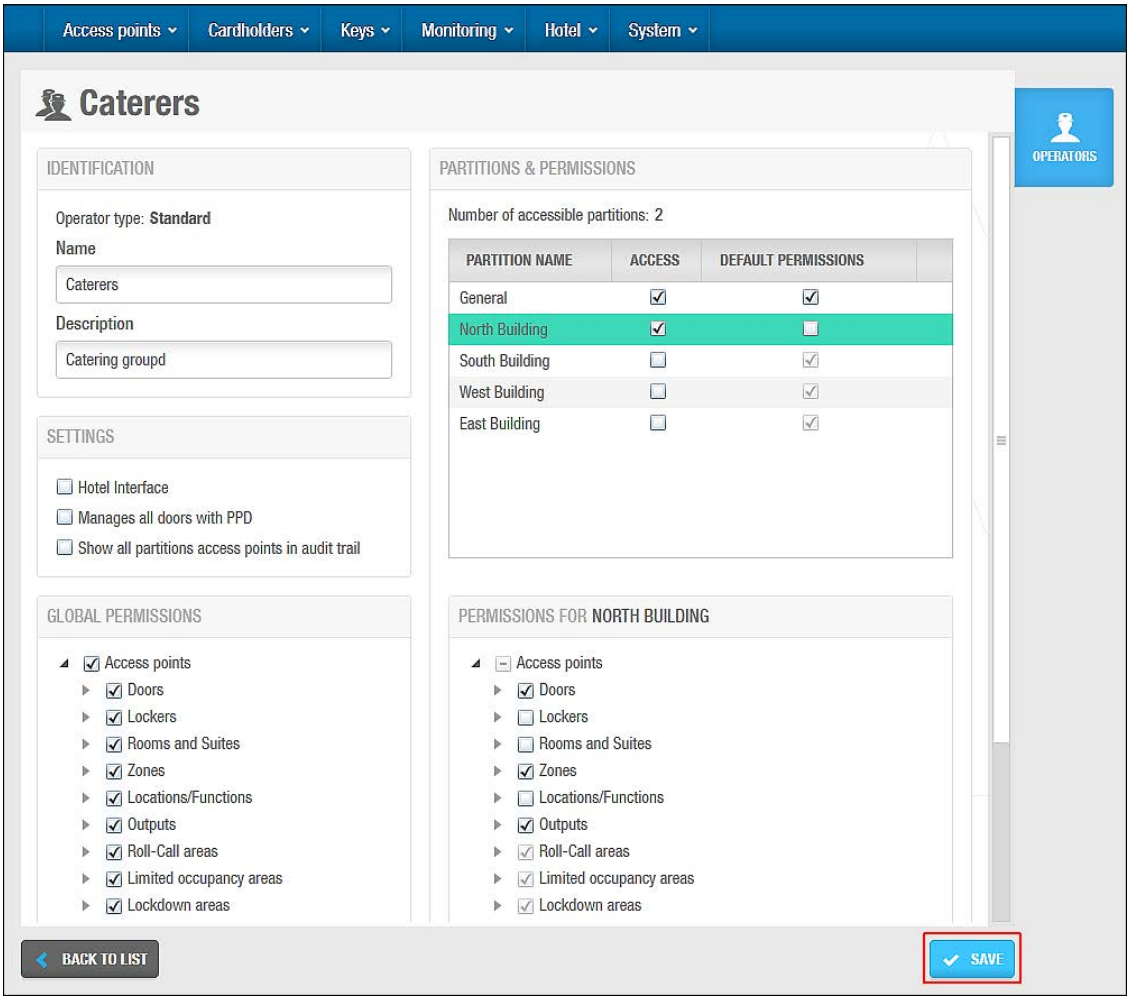


Figure 234: Operator group information screen

28. Type the name of the operator group in the **Name** field.
29. Type a description for the group in the **Description** field.
30. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.
31. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.
32. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.
33. Click **Save**.

5. 21. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

5. 21. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level

Monitoring checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs

Permission	Description
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels

Permission	Description
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.

Permission	Description
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars

Permission	Description
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

5. 21. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

34. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
35. Double-click the operator group with the operator list you want to view.
36. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

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

5. 21. 3. Associating Functions

Once you have created a function, you must associate users and access points with that function. For example, you could associate electrician users with a maintenance function. The following sections describe how to associate functions with the various entries.

5. 21. 3. 1. Users

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

1. Select **Access points** > **Functions**. The **Functions** screen is displayed.
2. Double-click the function that you want to associate with a user. The **Function** information screen is displayed.
3. 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 function.

4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.
5. Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right-hand panel.
6. Click **Accept**. The selected user now has access permissions for that function.

5. 21. 3. 2. Access Points

See *About Access Points* for more information.

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

1. Select **Access points** > **Functions**. The **Functions** screen is displayed.
2. Double-click the function that you want to associate with an access point. The **Function** information screen is displayed.
3. 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 function.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.
5. 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.
6. Click **Accept**. The function is now associated with the access point.

5. 22. Outputs

In the SALTO system, an output is a type of electrical permission or authorization used to activate devices like ESDs or elevators.

For example, you can control elevator access to specific floors by creating outputs. If a CU is connected to a relay extension board, you can use outputs to specify that only a designated user can activate one or multiple relays in an elevator. If you enable Floor 1 and Floor 3 in their access permissions, the user can only access those specific floors and not Floor 2.

Similarly, you can control the energy usage in a room or a floor by creating an output. For example, if you enable an ESD for Room 101, only an authorized key will allow the electrical devices in that room to be switched on.

The information for creating outputs in the following sections applies to non-hotel sites only. See *ESDs* for more general information about ESDs. See *Associated Device Lists* for more information about using ESDs in hotel sites.

5. 22. 1. Creating Outputs

To create an output, perform the following steps:

1. Select **Access points** > **Outputs**. The **Outputs** screen is displayed.

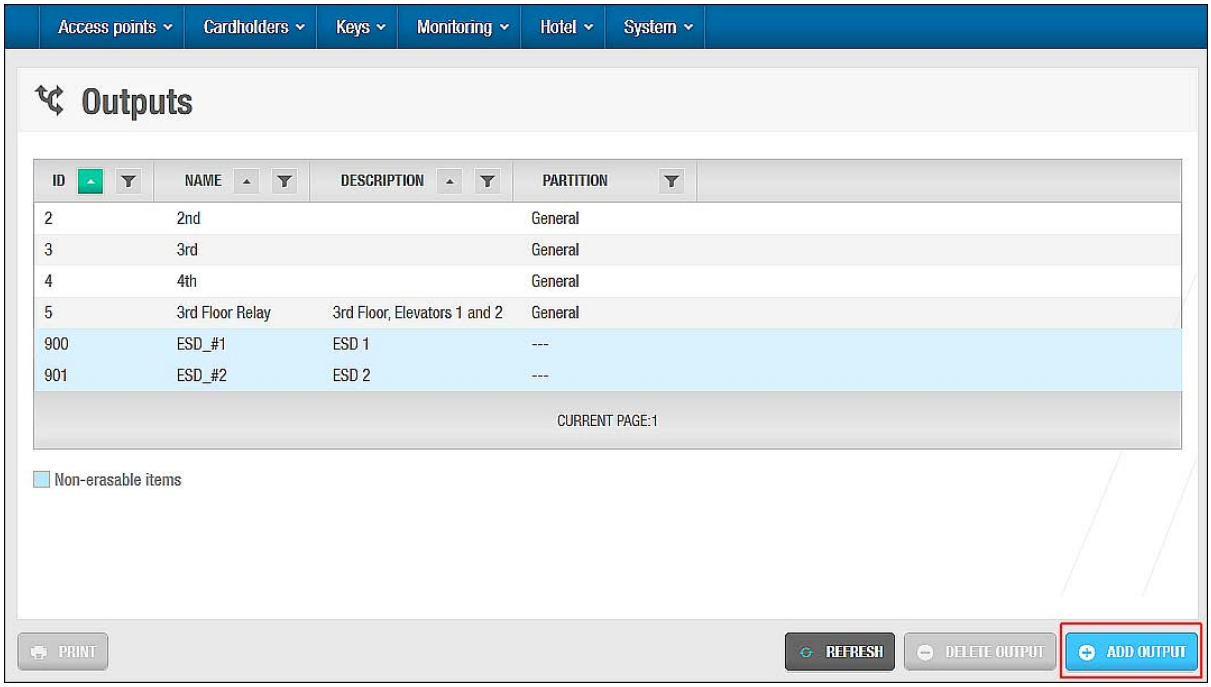


Figure 69: Outputs screen

2. Click **Add Output**. The **Output** information screen is displayed.

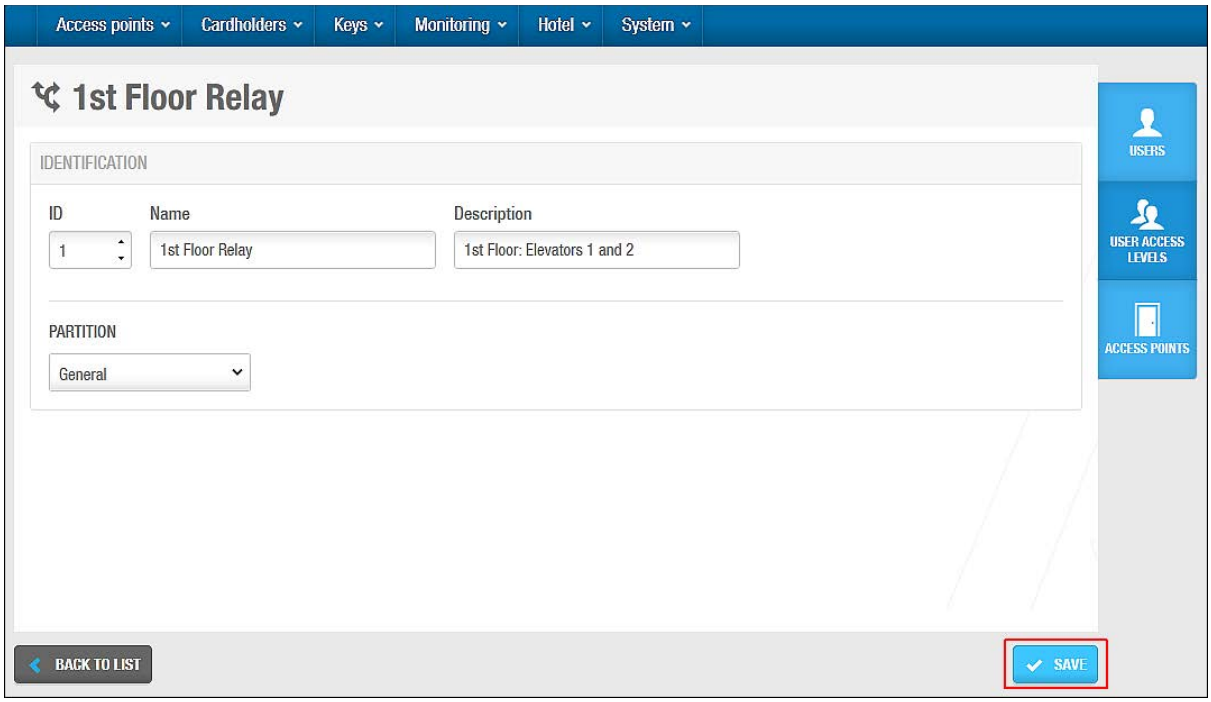


Figure 70: Output information screen

3. Type a name for the output in the **Name** field.
4. Type a description for the output in the **Description** field.
5. Select the relevant partition from the **Partition** drop-down list, if required.

See *System* Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows

events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

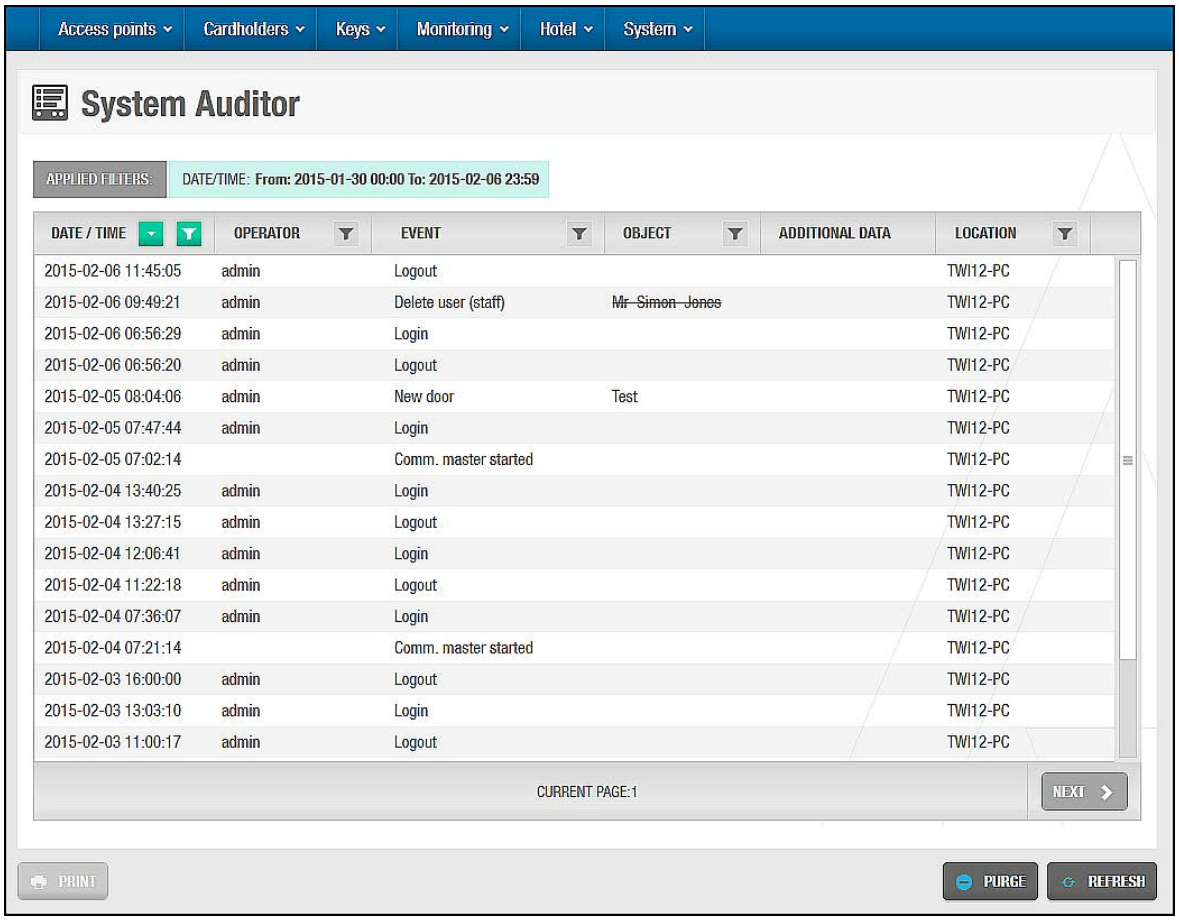


Figure 228: System Auditor information screen

5. 22. 2. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

5. 22. 3. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

6. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

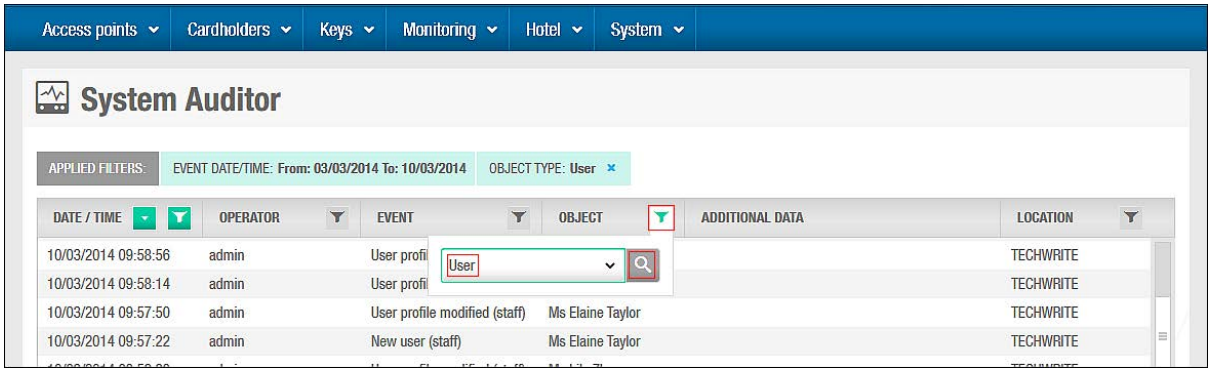


Figure 229: System Auditor information screen

7. Click the **Funnel** icon above the filter item. A search dialog box is displayed.

   For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.

   For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.

   For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.

8. Type your search term.

   Or

   Select a predefined search term from the drop-down list.

   Or

   Select a date range.

   You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.

   However, you cannot remove the **Date/Time** filter.

9. Click the **Search** icon. A filtered audit trail list is displayed.

5. 22. 3. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

5. 22. 4. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic*

System Auditor Purging for more information.

To purge the system auditor, perform the following steps:

10. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
11. Click **Purge**. The **Purge system auditor** dialog box is displayed.

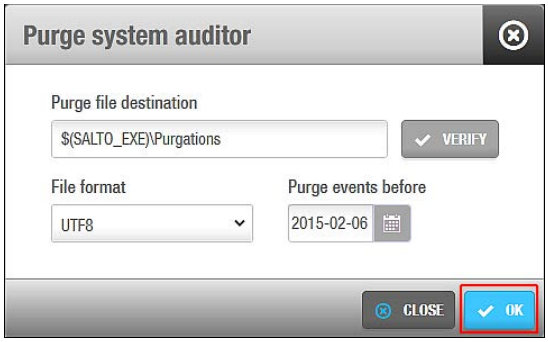


Figure 230: Purge system auditor dialog box

12. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
13. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
14. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
15. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
16. Click **OK**.

5. 23. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

5. 23. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

17. Select **System** > **Operators**. The **Operators** screen is displayed.

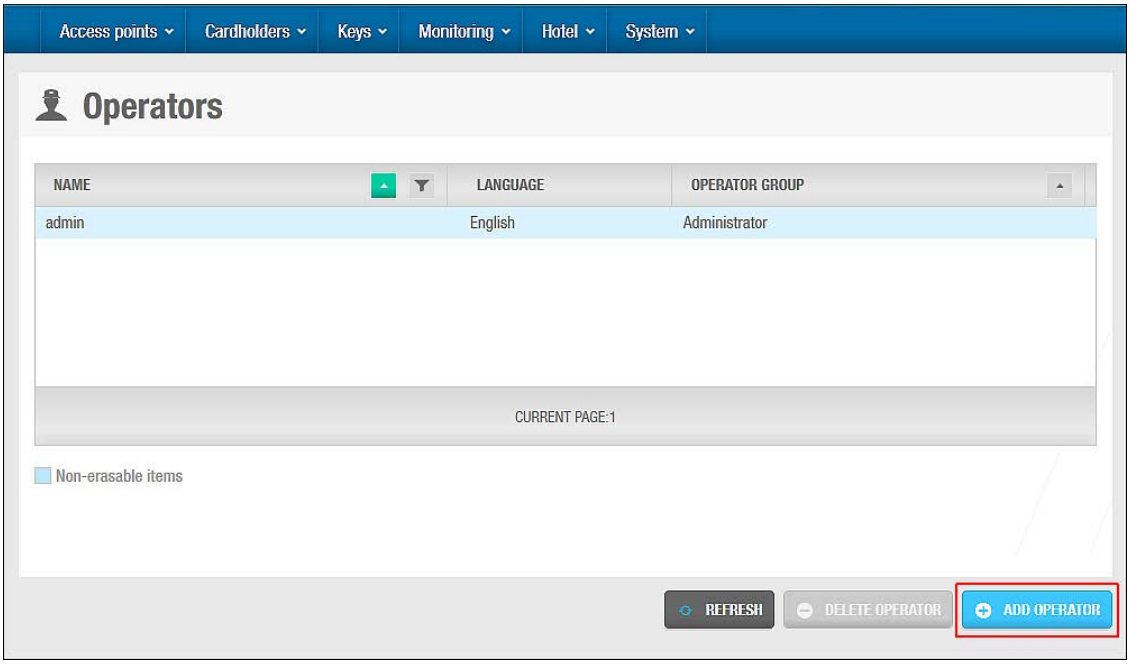


Figure 231: Operators screen

18. Click **Add Operator**. The **Operator** information screen is displayed.

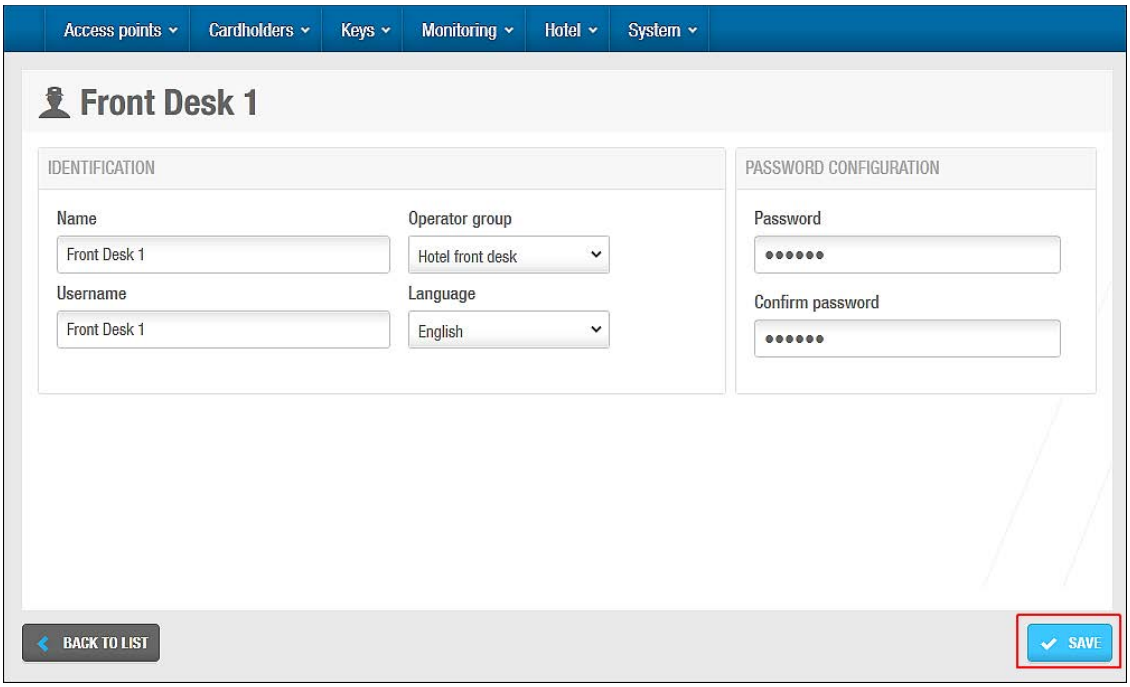


Figure 232: Operator information screen

19. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

20. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

    A maximum of 64 characters can be entered. The user name is not case sensitive.

21. Select the appropriate operator group from the **Operator group** drop-down list.
22. Select the display language for the operator in the **Language** drop-down list.

23. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.

24. Confirm the password.
25. Click **Save**.

5. 24. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

5. 24. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

26. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

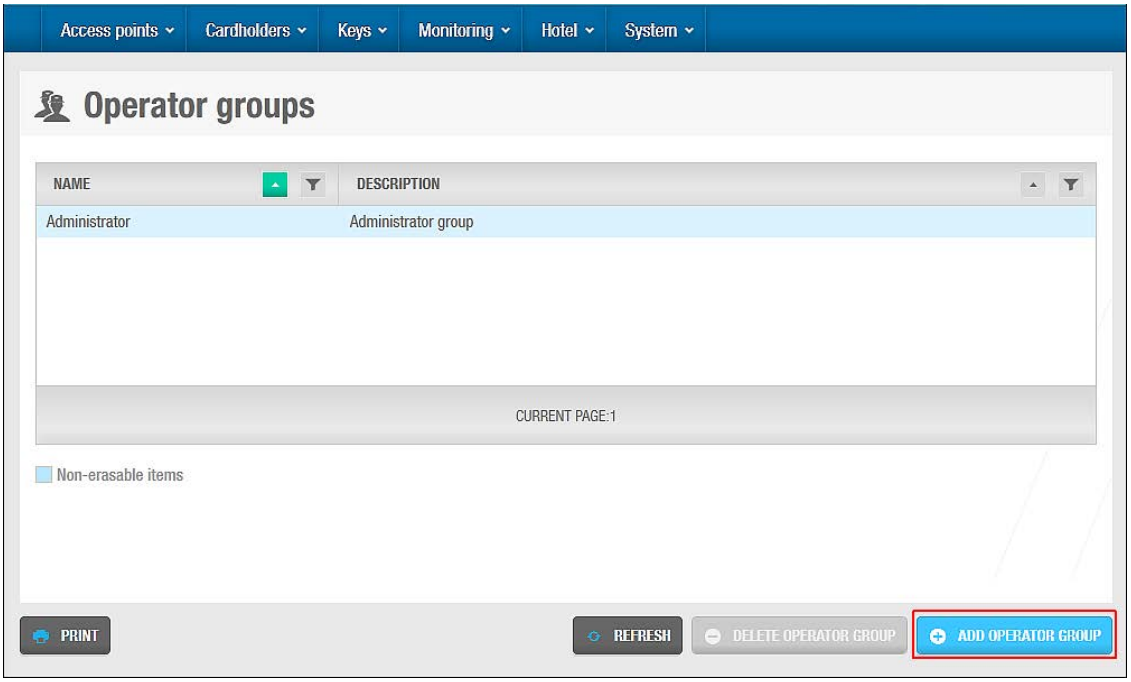


Figure 233: Operator groups screen

27. Click **Add Operator Group**. The **Operator group** information screen is displayed.

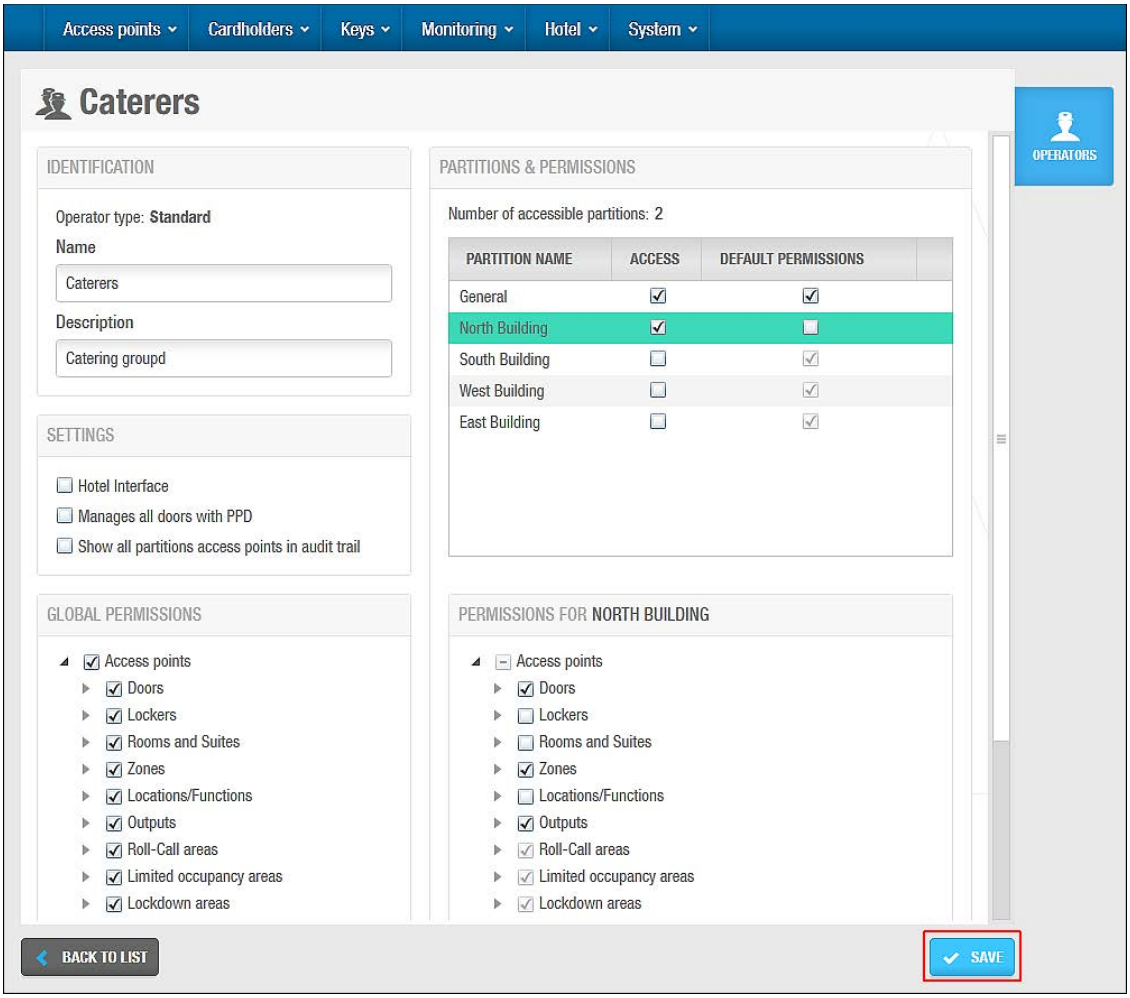


Figure 234: Operator group information screen

28. Type the name of the operator group in the **Name** field.
29. Type a description for the group in the **Description** field.
30. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.
31. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.
32. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes

in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.

33. Click **Save**.

5. 24. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

5. 24. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level **Monitoring** checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors

Permission	Description
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas

Permission	Description
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

5. 24. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

34. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
35. Double-click the operator group with the operator list you want to view.
36. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

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

NOTE: The **ID** field is automatically populated but numbers from 1 to 128 can be edited if required. Each output ID number corresponds to one relay. For example, output 1 is relay 1.

5. 24. 3. Associating Outputs

Once you have created an output, you must associate users, access levels, and/or access points with the specified output. The following sections describe how to associate outputs with the various entries.

5. 24. 3. 1. Users

To assign an output to a user, perform the following steps:

1. Select **Access points** > **Outputs**. The **Outputs** screen is displayed.
2. Double-click the output that you want to assign to a user. The **Output** information screen is displayed.
3. 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 output.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.
5. Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right-hand panel.
6. Click **Accept**. The output is now associated with the user.

5. 24. 3. 2. Access Levels

See *User Access Levels*, *Visitor Access Levels*, and *Guest Access Levels* for information about how to create and configure access levels.

To associate an output with an access level, perform the following steps:

1. Select **Access points** > **Outputs**. The **Outputs** screen is displayed.
2. Double-click the output that you want to associate with an access level. The **Output** information screen is displayed.
3. Click **Access Levels** in the sidebar. The **Access levels** dialog box is displayed.

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

4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access levels, is displayed.
5. Select the required access level in the left-hand panel and click the chevron. The selected access level is displayed in the right-hand panel.
6. Click **Accept**. The output is now associated with the access level.

5. 24. 3. 3. Access Points

See *About Access Points* for information about access points.

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

1. Select **Access points** > **Outputs**. The **Outputs** screen is displayed.
2. Double-click the output that you want to associate with an access point. The **Output** information screen is displayed.
3. 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 output.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.
5. 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.
6. Click **Accept**. The output is now associated with the access point.

   You can change which access point timed period is used. See *Automatic Outputs* for more information and a description of the steps you should follow.

5. 24. 4. Automatic Outputs

If you want outputs associated with a door to operate in Automatic opening mode for a specific time period, you must assign an access point timed period to the output. You can do this when associating an automatic output with a door. The maximum number of automatic outputs that you can associate with a door is four. See *Automatic Outputs* for more information about this. See also *Roll-Call Areas*

A roll call is used to list the individual users in a specified area at a particular time. For example, you can use a roll call to generate a report after a fire alarm goes off. This way, it is possible to check whether all the users in the area have been safely evacuated. The system generates the roll call by monitoring specific access points. By tracking when cardholders enter and exit using these access points, it is possible to see exactly who is inside or outside the roll-call area.

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

See *Roll-Call* for information about generating a list of individual user names in a roll-call area in ProAccess SPACE. You can also use ProAccess SPACE Roll-Call Monitoring to perform other roll-call tasks, such as searching all roll-call areas for a user and the time and date each user entered the roll-call area. See *Roll-Call* for more information.

5. 24. 5. Creating Roll-Call Areas

To create a roll-call area, perform the following steps:

7. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.

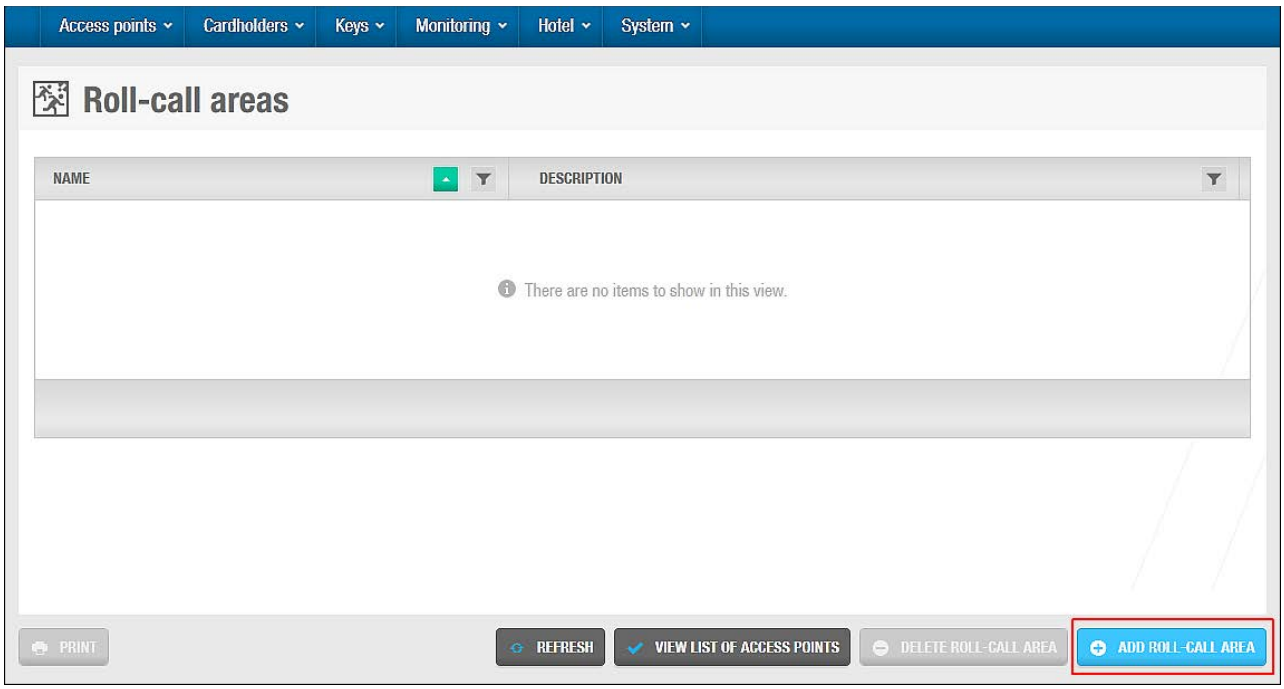


Figure 75: Roll-call areas screen

NOTE: The **View List of Access Points** button shows a list of access points associated with all roll-call areas.

8. Click **Add Roll-Call area**. The **Roll-call area** information screen is displayed.

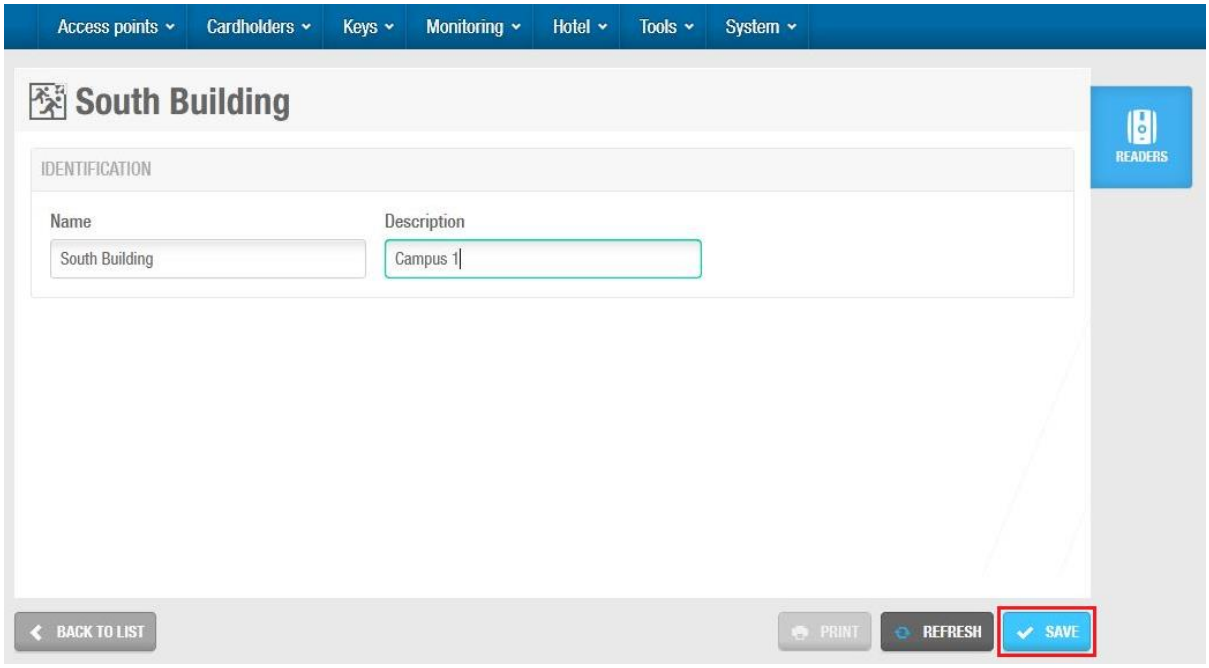


Figure 76: Roll-call area information screen

9. Type a name for the location in the **Name** field.
10. Type a description for the location in the **Description** field.
11. Click **Save**.

5. 24. 5. 1. Creating Roll-Call Exterior Areas

Roll-call areas list the individual users in a specified area at a particular time. To account for the individual users who are on a site but are not in any of the designated roll-call areas, you need to create a separate, exterior area, for example, an assembly area. This is an important concept to consider when creating roll-call areas.

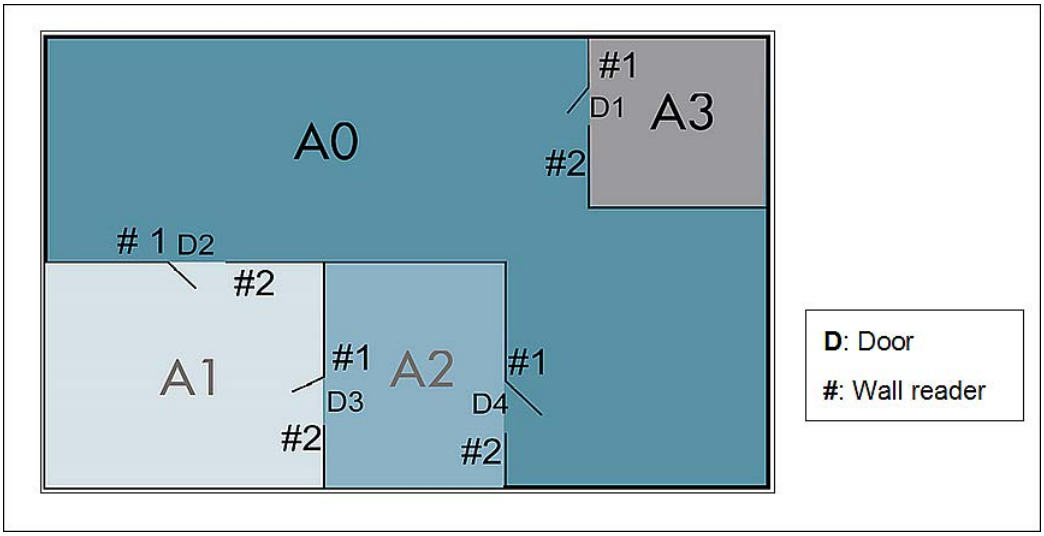


Figure 77: Designated roll-call areas and exterior area

In the above example, there are three standard roll-call areas: A1, A2, and A3. The exterior area is A0, which lists all users who are not in A1, A2, or A3.

A user in A1, A2, or A3 must present their key to a wall reader to exit that roll-call area. When a user presents their key, the system determines that the user has exited the area and entered the exterior area A0. The exterior area allows the system to create accurate roll-call lists, accounting for all the people who are present.

5. 24. 6. Associating Roll-Call Areas

Once you have created a roll-call area, you must associate wall readers with that roll-call area. Each roll-call area must have two wall readers: one to track users entering the area and another to track users exiting the area. The following section describes how to associate roll-call areas with readers.

5. 24. 6. 1. Readers

To associate a reader with a roll-call area, perform the following steps:

12. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.
13. Double-click the roll-call area that you want to associate with a reader. The **Roll-call area** information screen is displayed.
14. Click **Readers** in the sidebar. The **Readers** dialog box is displayed.

    Note that the dialog box will be blank because you have not yet associated an access point with this particular roll-call area.
15. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.

    This list only applies to online CUs where there are two physical wall readers.

16. 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.
17. Click **Accept**. The roll-call area is now associated with the access point.

Access Point Timed Periods for more information.

5. 25. Lockdown Areas

A lockdown area is a defined area where all access points can be closed or opened in an emergency situation. For example, a lockdown area in a university campus could be all access points in the Physics building. If there is ever a security threat (or other type of emergency situation) within that building, you can choose to close or open all the doors as appropriate.

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

See *Lockdown* for information about opening and closing lockdown areas.

NOTE: You cannot use **Lockdown monitoring** in ProAccess SPACE to open and close offline doors in an emergency situation. However, if offline doors are fitted with AMOK locks, which have two readers, you can give users permissions to perform a manual lockdown. To do this, you must select the **Set lockdown** option on the **User** information screen. This means that users can enable and disable lockdown mode for the doors by presenting their key to the door's inside reader. You can also give users permissions to open both online and offline doors when they are in lockdown by selecting the **Override lockdown** checkbox on the **User** information screen in ProAccess SPACE. See *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.
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.

Key Options for more information.

5. 25. 1. Creating Lockdown Areas

To create a lockdown area, perform the following steps:

1. Select **Access points** > **Lockdown areas**. The **Lockdown areas** screen is displayed.

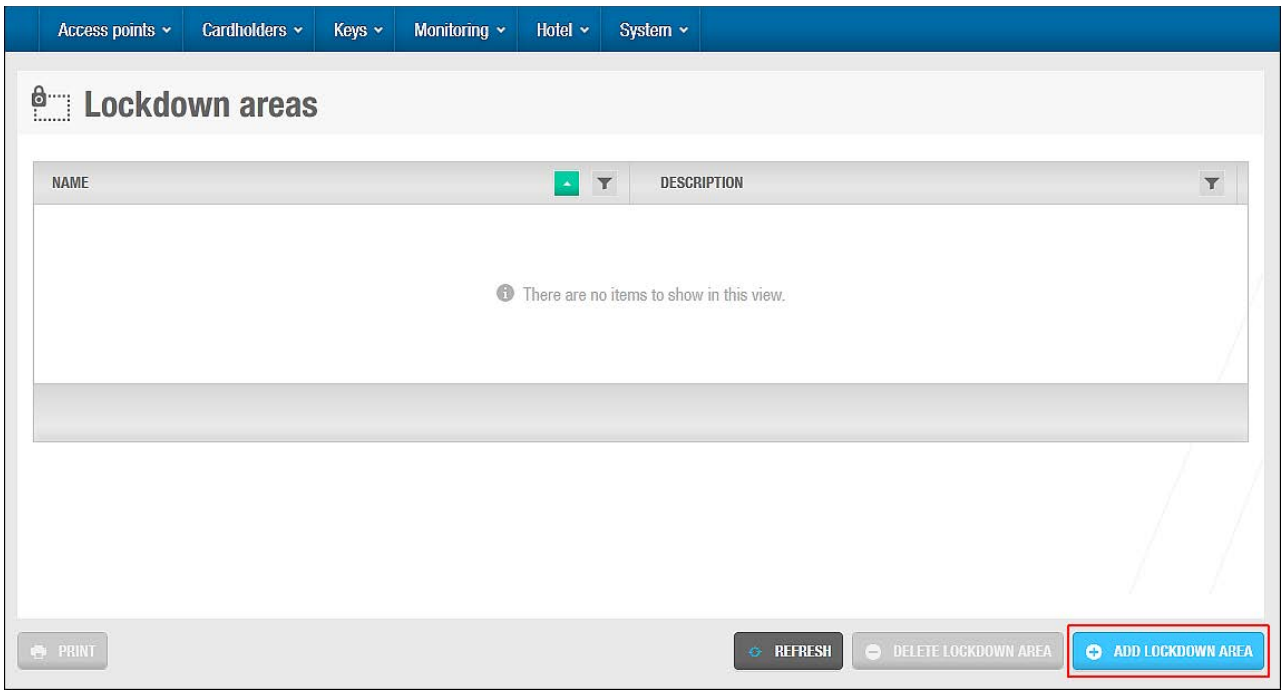


Figure 71: Lockdown areas screen

2. Click **Add Lockdown Area**. The **Lockdown area** information screen is displayed.

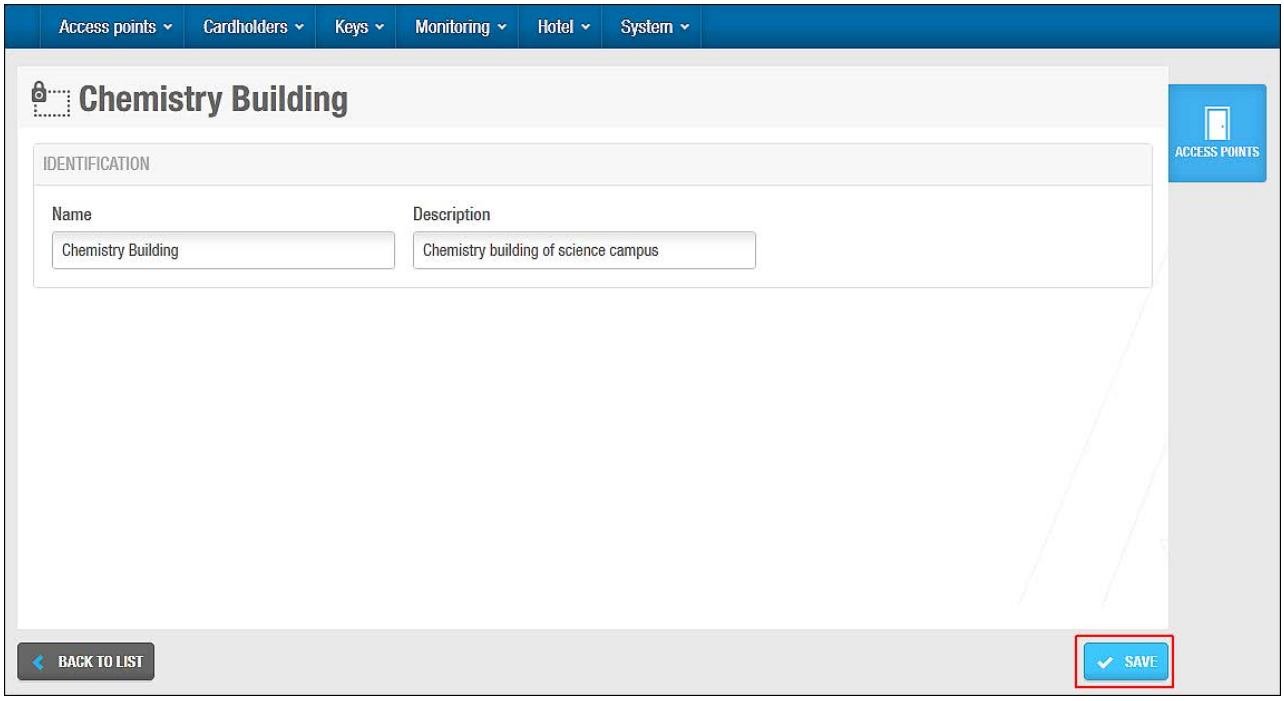


Figure 72: Lockdown area information screen

3. Type a name for the location in the **Name** field.
4. Type a description for the location in the **Description** field.
5. Click **Save**.

5. 25. 2. Associating Lockdown Areas

Once you have created a lockdown area, you must associate access points with that lockdown area. The following section describes how to associate lockdown areas with access points.

5. 25. 2. 1. Access Points

To associate an online access point with a lockdown area, perform the following steps:

1. Select **Access points** > **Lockdown areas**. The **Lockdown areas** screen is displayed.
2. Double-click the lockdown area that you want to associate with an access point. The **Lockdown area** information screen is displayed.
3. 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 lockdown area.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.
5. 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.
6. Click **Accept**. The lockdown area is now associated with the access point.

5. 26. Limited Occupancy Areas

In the SALTO system, a limited occupancy area is an area with a specified maximum number of permitted users. For example, if a parking area contains 20 spaces, the system counts how many spaces are occupied. When 20 users have occupied a space, the next user will be denied access, even if they have a valid key.

Use the limited occupancy areas functionality in ProAccess SPACE to designate the applicable area and to specify the number of permitted users. You can then use the Limited occupancy monitoring option in ProAccess SPACE to generate a list of individual user names within each limited occupancy area. See *Limited Occupancy* for more information.

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

5. 26. 1. Creating Limited Occupancy Areas

To create a lockdown area, perform the following steps:

1. Select **Access points** > **Limited occupancy areas**. The **Limited occupancy areas** screen is displayed.

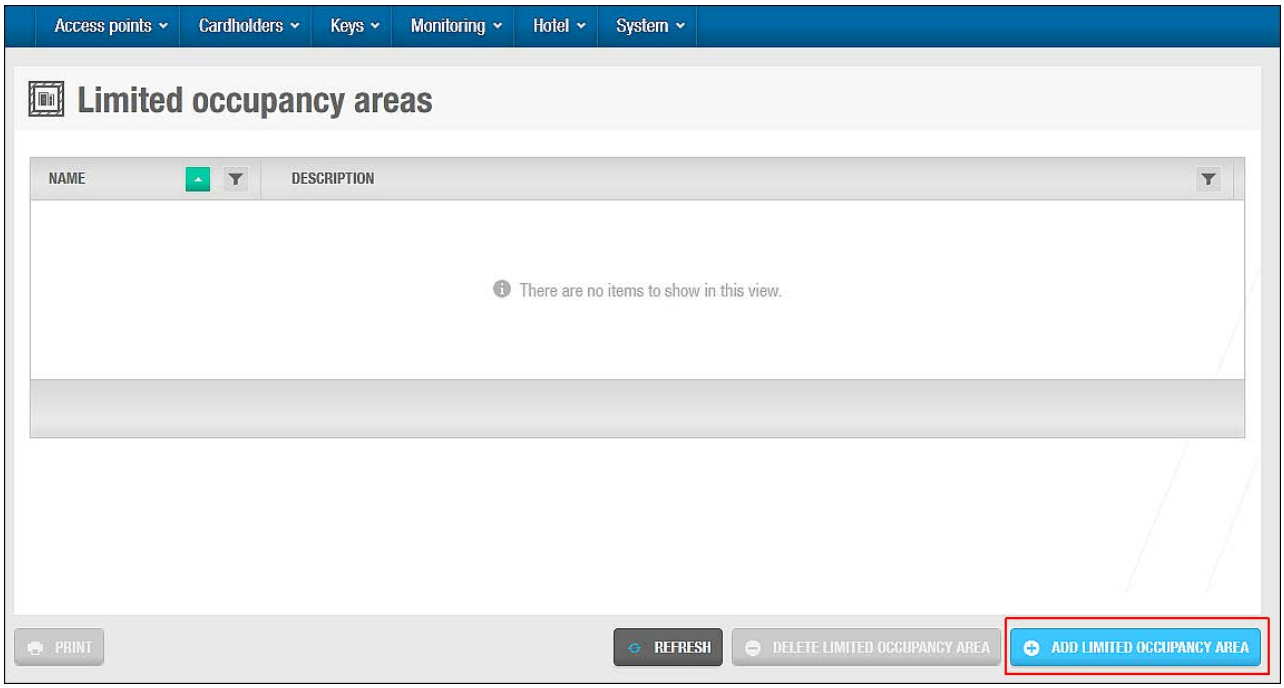


Figure 73: Limited occupancy areas screen

2. Click **Add Limited Occupancy Area**. The **Limited occupancy area** information screen is displayed.

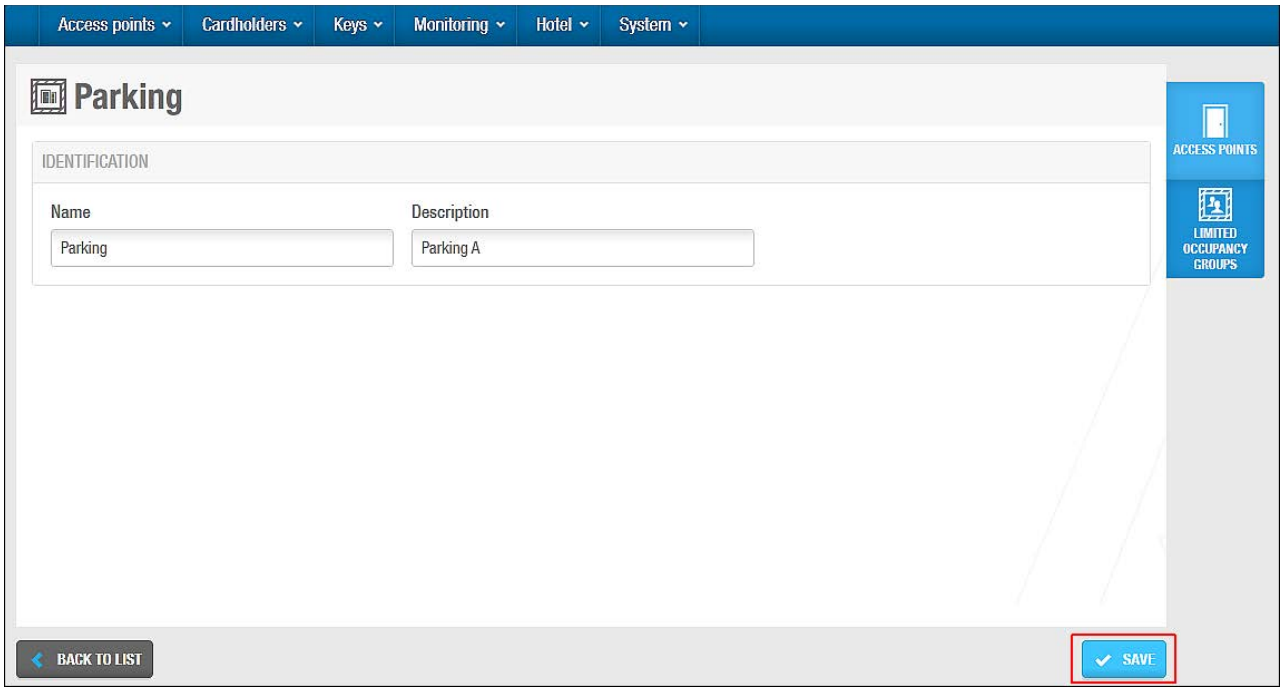


Figure 74: Limited occupancy area information screen

3. Type a name for the limited occupancy area in the **Name** field.
4. Type a description for the limited occupancy area in the **Description** field.
5. Click **Save**.

5. 26. 2. Associating Limited Occupancy Areas

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

5. 26. 2. 1. Access Points

To associate an access point with a limited occupancy area, perform the following steps:

1. Select **Access points** > **Limited occupancy areas**. The **Limited occupancy areas** screen is displayed.
2. Double-click the limited occupancy area that you want to associate with an access point. The **Limited occupancy area** information screen is displayed.
3. 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 limited occupancy area.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.
5. 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.
6. Click **Accept**. The limited occupancy area is now associated with the access point.

5. 26. 2. 2. Limited Occupancy Groups

A limited occupancy group is a grouping of users who require access to a specified limited occupancy area. A user can only belong to one group and this group can have access to multiple limited occupancy areas. See *Limited Occupancy Groups* for more information.

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

1. Select **Access points** > **Limited occupancy areas**. The **Limited occupancy areas** screen is displayed.
2. Double-click the limited occupancy area that you want to associate with a limited occupancy group. The **Limited occupancy area** information screen is displayed.
3. Click **Limited Occupancy Groups** in the sidebar. The **Limited occupancy groups** dialog box is displayed.

   Note that the dialog box will be blank because you have not yet associated a limited occupancy group with this particular limited occupancy area.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of limited occupancy groups, is displayed.
5. Select the required limited occupancy group in the left-hand panel and click the chevron. The selected limited occupancy group is displayed in the right-hand panel.
6. Click **Accept**. The limited occupancy area is now associated with the limited occupancy group.

5. 27. Roll-Call Areas

A roll call is used to list the individual users in a specified area at a particular time. For example, you can use a roll call to generate a report after a fire alarm goes off. This way, it is

possible to check whether all the users in the area have been safely evacuated. The system generates the roll call by monitoring specific access points. By tracking when cardholders enter and exit using these access points, it is possible to see exactly who is inside or outside the roll-call area.

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

See *Roll-Call* for information about generating a list of individual user names in a roll-call area in ProAccess SPACE. You can also use ProAccess SPACE Roll-Call Monitoring to perform other roll-call tasks, such as searching all roll-call areas for a user and the time and date each user entered the roll-call area. See *Roll-Call* for more information.

5. 27. 1. Creating Roll-Call Areas

To create a roll-call area, perform the following steps:

7. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.

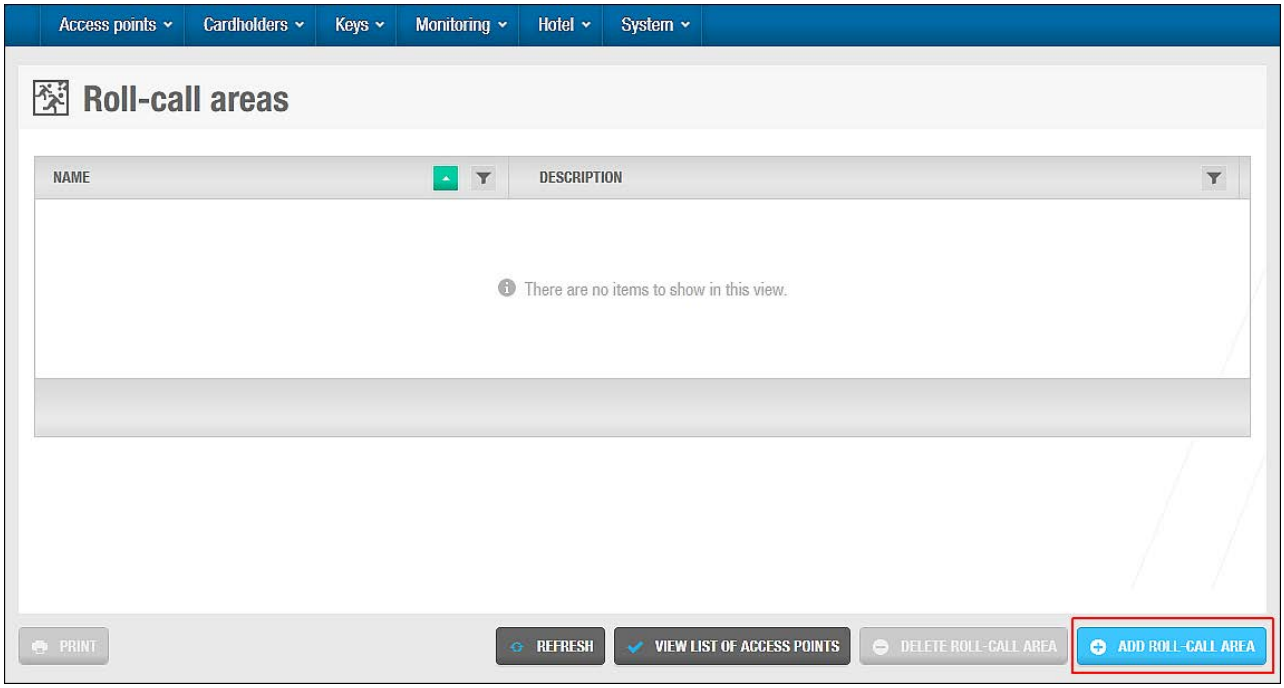


Figure 75: Roll-call areas screen

NOTE: The **View List of Access Points** button shows a list of access points associated with all roll-call areas.

8. Click **Add Roll-Call area**. The **Roll-call area** information screen is displayed.

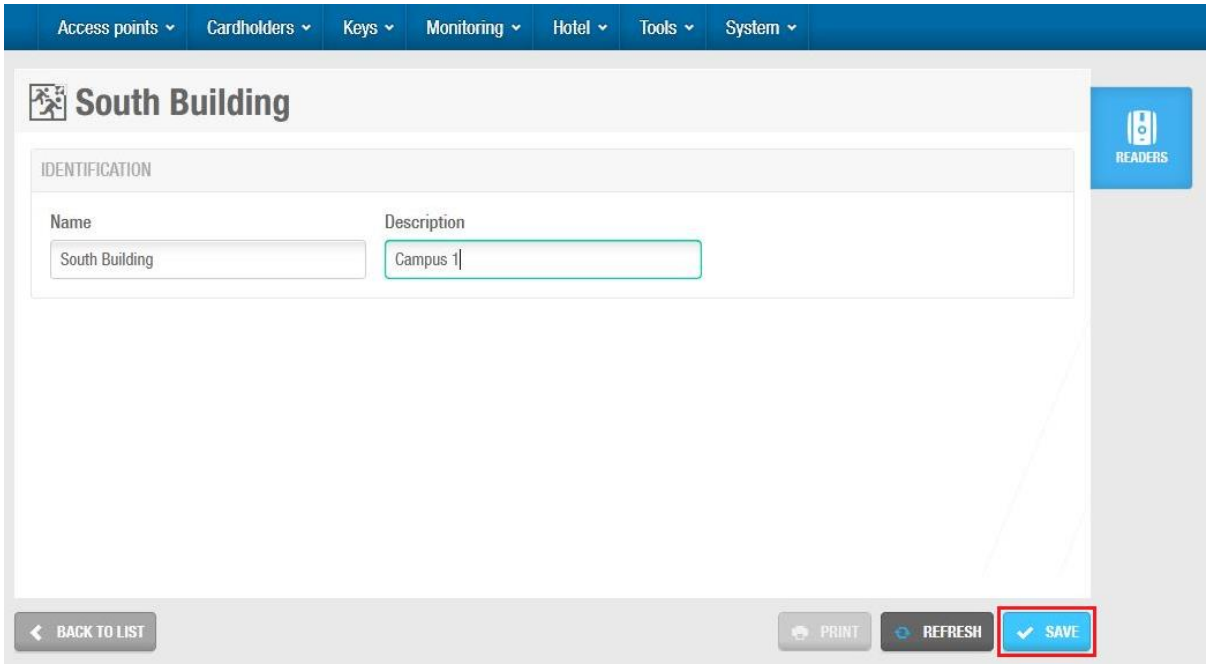


Figure 76: Roll-call area information screen

9. Type a name for the location in the **Name** field.
10. Type a description for the location in the **Description** field.
11. Click **Save**.

5. 27. 1. 1. Creating Roll-Call Exterior Areas

Roll-call areas list the individual users in a specified area at a particular time. To account for the individual users who are on a site but are not in any of the designated roll-call areas, you need to create a separate, exterior area, for example, an assembly area. This is an important concept to consider when creating roll-call areas.

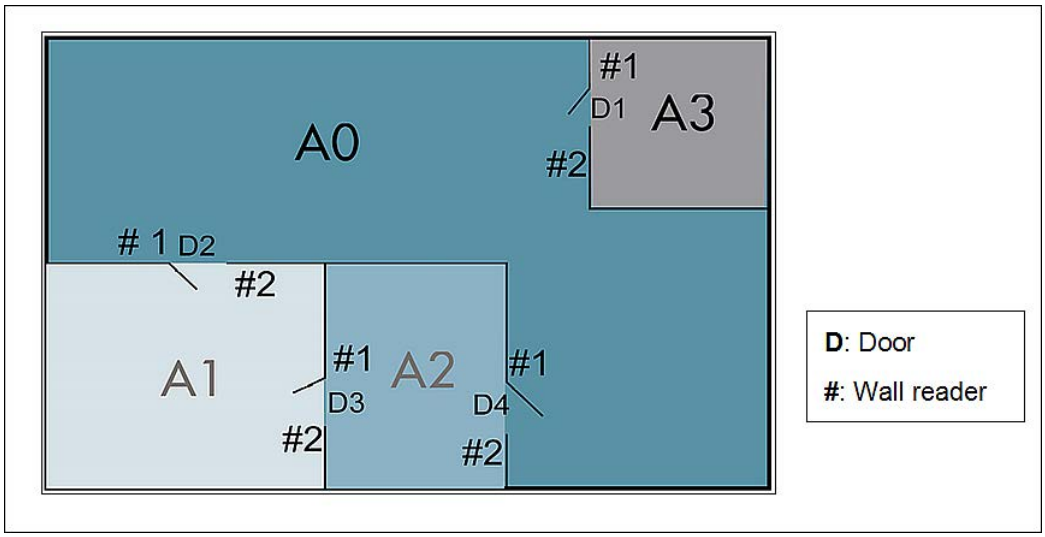


Figure 77: Designated roll-call areas and exterior area

In the above example, there are three standard roll-call areas: A1, A2, and A3. The exterior area is A0, which lists all users who are not in A1, A2, or A3.

A user in A1, A2, or A3 must present their key to a wall reader to exit that roll-call area. When a user presents their key, the system determines that the user has exited the area and entered the exterior area A0. The exterior area allows the system to create accurate roll-call lists, accounting for all the people who are present.

5. 27. 2. Associating Roll-Call Areas

Once you have created a roll-call area, you must associate wall readers with that roll-call area. Each roll-call area must have two wall readers: one to track users entering the area and another to track users exiting the area. The following section describes how to associate roll-call areas with readers.

5. 27. 2. 1. Readers

To associate a reader with a roll-call area, perform the following steps:

12. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.
13. Double-click the roll-call area that you want to associate with a reader. The **Roll-call area** information screen is displayed.
14. Click **Readers** in the sidebar. The **Readers** dialog box is displayed.

    Note that the dialog box will be blank because you have not yet associated an access point with this particular roll-call area.
15. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.

    This list only applies to online CUs where there are two physical wall readers.
16. 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.
17. Click **Accept**. The roll-call area is now associated with the access point.

5. 28. Access Point Timed Periods

An access point timed period defines a time interval during which an access point uses a specified opening mode. For example, you can define a canteen door to automatically open at 12.00 and close at 14.00. Outside of this time period, the lock reverts to Standard mode and a key is required to open it.

Opening modes are defined when you set up doors and/or lockers. See *Configuring Doors* and *Configuring Lockers* for more information. When you select an opening mode for an access point, you must define the relevant time period using the **Access point timed periods** screen as described in *Creating Access Point Timed Periods*.

Three parameters define an access point timed period:

- Start time
- End time
- Day of the week

There are four day types:

- Monday to Sunday
- Holiday
- Special 1

- Special 2

NOTE: You must configure the system calendar before you create access point timed periods. See *PPD*

PPDs are connected to the operator's local PC through either a USB or COM port. See *PPD Settings* for more information. PPDs allow data to be transferred between the operator's PC and the locks. Data is downloaded from the PC to the PPD, and the PPD is used to perform tasks such as lock initialization and emergency openings. In the process, the PPD retrieves information (such as battery status) from the locks. This information is communicated to the system when the PPD is connected to the operator's PC.

See the *Portable Programming Device by SALTO* document for more information about PPDs and their configuration settings.

Table 56: PPD

 Portable Programming Device (PPD)	Used by admin operators to transfer configuration changes to a lock or by maintenance operators to check the battery status of the lock and collect the lock's audit trail

NOTE: It is important that the time is set correctly for the PC on which the SALTO software is running, as this controls the time and date settings for locks.

5. 28. 1. Peripheral Types

The functionality of the PPD is described in the following table.

Table 57: Peripheral types

Peripheral	Functionality
PPD	Communicates information to the locks such as door identification and configuration details. The operator downloads the information from their PC to the PPD and the PPD can then be connected to the lock. In this way, information is transferred to the lock. PPDs are used to: ▪ Update configuration changes to the lock (door profile, calendars etc.) ▪ Manually retrieve the audit trail stored on the lock for uploading to the server ▪ Perform a firmware diagnostic evaluation of the locking electronic components ▪ Upgrade the firmware of the locking components ▪ Open a door in the event of an emergency ▪ Read the battery status of the lock ▪ Perform a general diagnostic evaluation of the system

PPDs are configured in ProAccess SPACE General options. See *Devices Tab* for more information. The **PPD** information screen in ProAccess SPACE is used to download access point data to PPDs. This allows you to perform tasks with PPDs such as initializing and updating locks. You can also view the status of PPDs and

update their firmware by using the **PPD** information screen.

5. 28. 2. PPD Menu Options

PPDs have seven menu options. Some of the menu options are available by default. Others are enabled when you select particular options on the **PPD** information screen in ProAccess SPACE, and download access point data to the PPD. See the *Portable Programming Device by SALTO* document for more information about using PPDs.

The options are described in the following table.

Table 58: PPD menu options

Option	Description
Update locks	Used to update a lock when the PPD is connected to it. To enable this menu option, you must download the appropriate access point data to the PPD by using the **PPD** information screen.
Firmware diagnostic	Used to perform a firmware diagnostic of the locking electronic components
Update firmware	Used to update the firmware of the locking electronic components
Collect audit trail	Used to collect audit trail data from offline doors and transfer it to the operator's local PC
Emergency opening	Used to perform an emergency opening if the lock battery dies or a reader error occurs. To enable this menu option, you must select the **Allow emergency opening** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. Alternatively, you can set this as a default option in ProAccess SPACE General options. You can also set a password for performing emergency openings using the PPD if required. See *Performing Emergency Door Openings* and *Devices Tab* for more information.
Initialize lock	Used to transfer access data to new locks or existing locks that have been fitted on a different access point and renamed. To enable this menu option, you must select the **Initialize locks** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. See *Initializing Locks* for more information.
Diagnostic	Used to retrieve information from the lock such as the battery status or serial number

5. 28. 3. Viewing PPD Status

You can view the status of a PPD you have connected to the PC by selecting **System** > **PPD**.

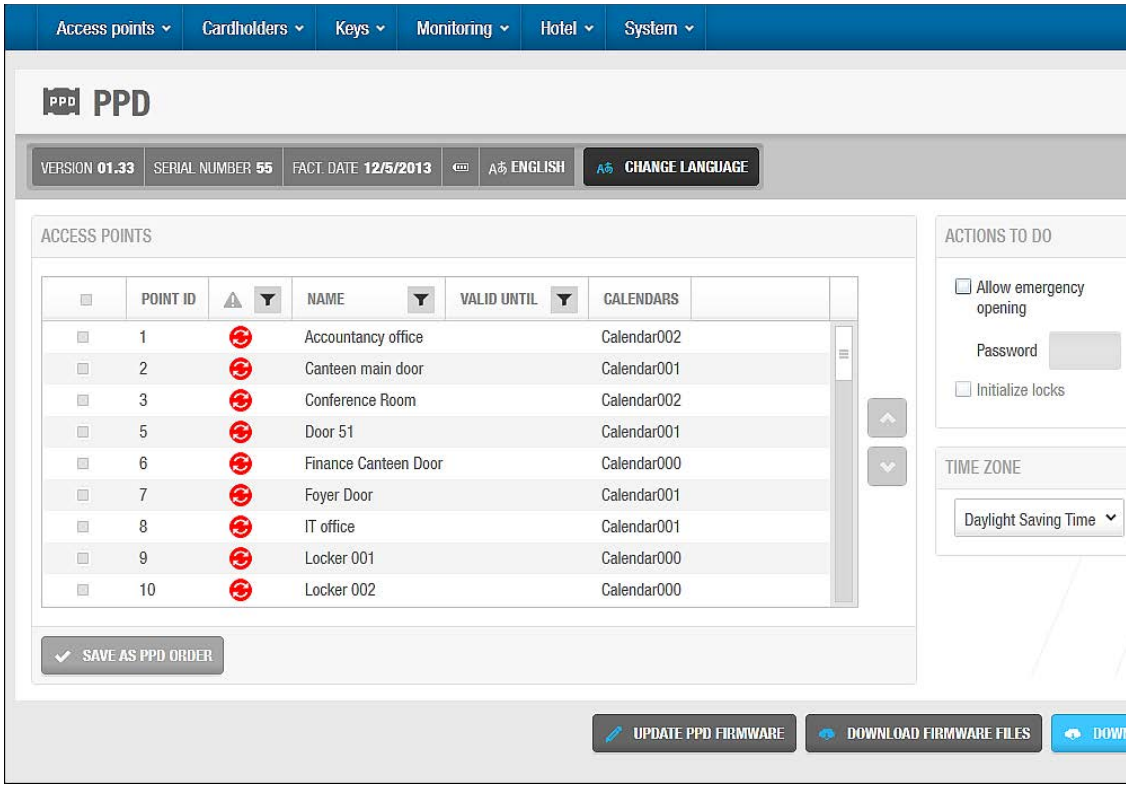


Figure 238: PPD information screen

The **PPD** information screen shows the following information about the PPD:

- Version
- Serial number
- Factory date (or date of manufacture)
- Battery status
- Language

5. 28. 4. Changing the PPD Language

You can change the language of the display messages in the PPDs if required.

To change the language displayed in a PPD, perform the following steps:

18. Connect the PPD to the PC.
19. Select **System** > **PPD**. The **PPD** information screen is displayed.
20. Click **Change Language**. The **Change language** dialog box is displayed.

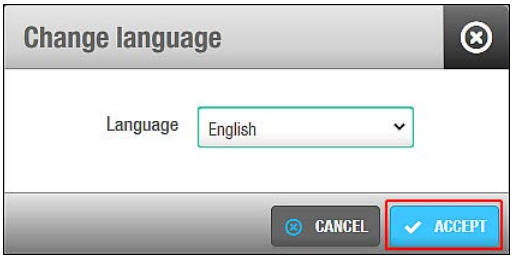


Figure 239: Change language dialog box

21. Select the required language from the **Language** drop-down list.
22. Click **Accept**. The **PPD** progress screen is displayed.
23. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
24. Click **OK**.

5. 28. 5. Using the PPD Information Screen

The **PPD** information screen displays a list of access points. This list varies depending on which time zone is selected in the **Time Zone** panel. It is important to remember that only access points for the selected time zone are displayed. Note that you must enable the multiple time zones functionality in ProAccess SPACE General options to display this panel in ProAccess SPACE. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Access points that need to be updated have a red **Update required** icon on the left-hand side of their name. You can download access point data to a PPD you have connected to the PC by selecting the required access points and clicking **Download**. You can then perform tasks such as updating locks with the PPD. See *Updating Locks* for more information. You must select additional options in the **Actions To Do** panel for certain tasks, for example, initializing locks. See *Initializing Locks* and *Performing Emergency Door Openings* for more information about this panel.

The following table describes some useful screen items.

Table 59: PPD information screen items

Item	Description
Access point checkboxes	Allow you to select individual access points
Checkbox column header	Allows you to select all of the displayed access points. To do so, select the checkbox in the column header.
Chevrons	Allow you to move entries up and down in the access point list
Save As PPD Order button	Allows you to save the access point list order. This specifies the order in which access point data is downloaded to the PPD and displayed in the PPD's menu.
Expand icon	Allows you to view the ESDs for rooms and suites. This icon is displayed on the left-hand side of the room and suite names.

5. 28. 6. Updating PPD Firmware

Firmware is software that is programmed on the read-only memory (ROM) of hardware devices. Firmware updates are available when a new version of the SALTO software is downloaded. Your SALTO technical support contact may also recommend specific firmware updates if required.

To update the firmware of a PPD, perform the following steps:

25. Connect the PPD to the PC.
26. Select **System** > **PPD**. The **PPD** information screen is displayed.

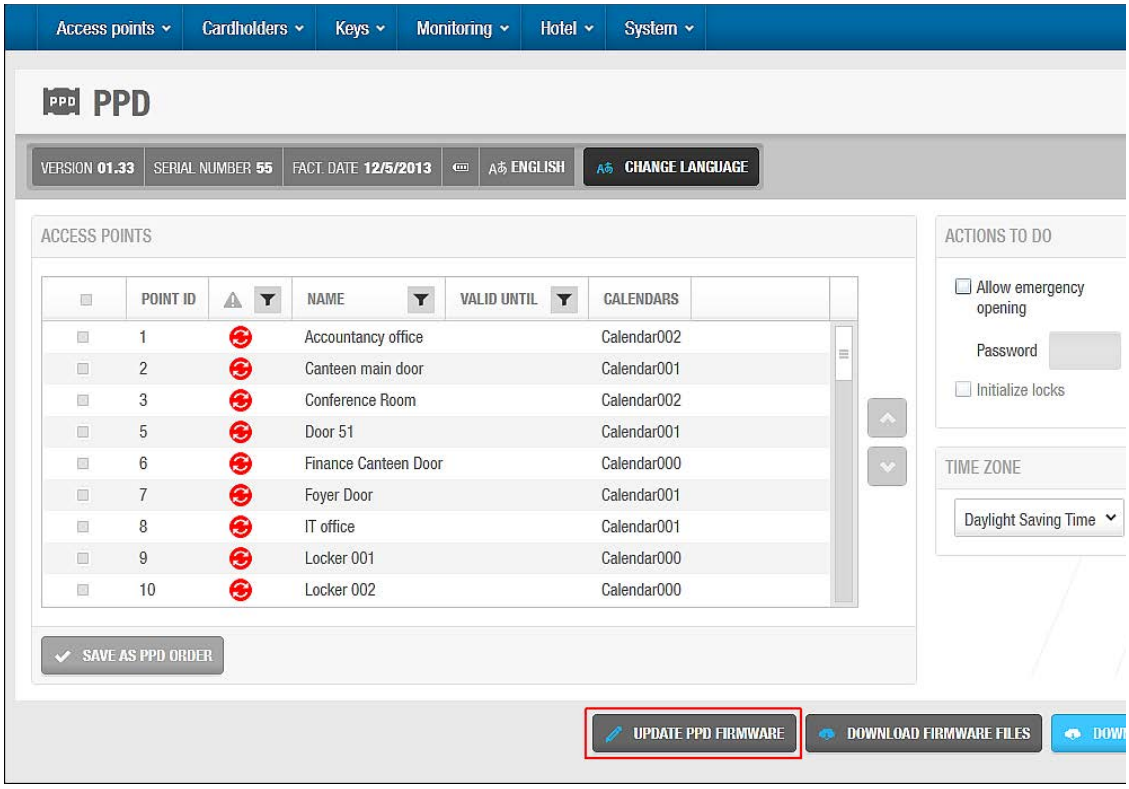


Figure 240: PPD information screen

27. Click **Update PPD Firmware**. The **Update PPD Firmware** dialog box, showing the available firmware files, is displayed.

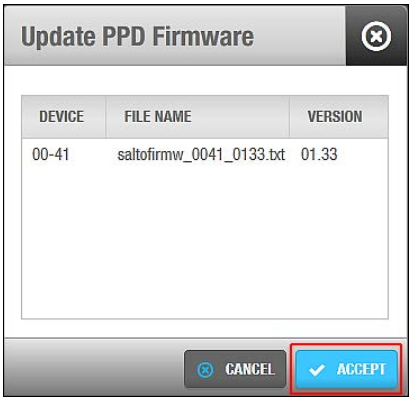


Figure 241: Update PPD Firmware dialog box

28. Select the required file.
29. Click **Accept**. The **PPD** progress screen is displayed.
30. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
31. Click **OK**.

5. 28. 7. Downloading Firmware Files

You can download firmware files to the PPD and use it to update the locking electronic components.

To download a firmware file to a PPD, perform the following steps:

32. Connect the PPD to the PC.
33. Select **System** > **PPD**. The **PPD** information screen is displayed.

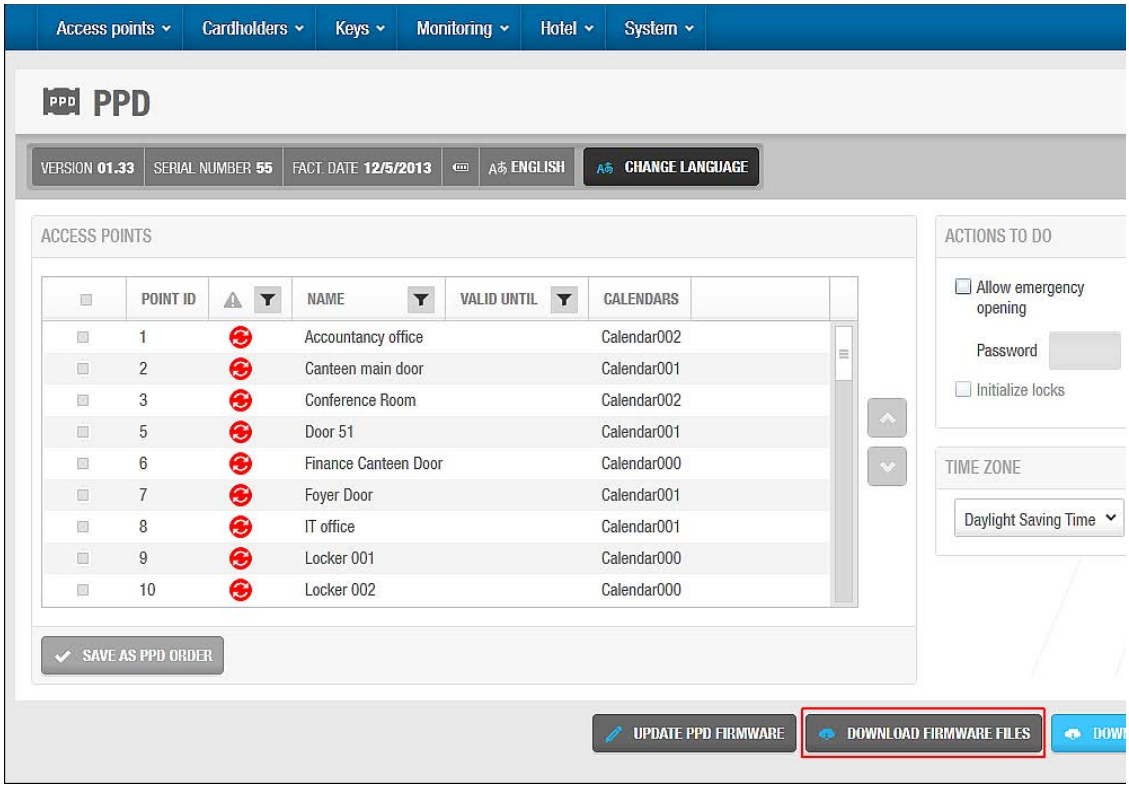


Figure 242: PPD information screen

34. Click **Download Firmware Files**. The **Download Firmware files** dialog box, showing the available firmware files, is displayed.

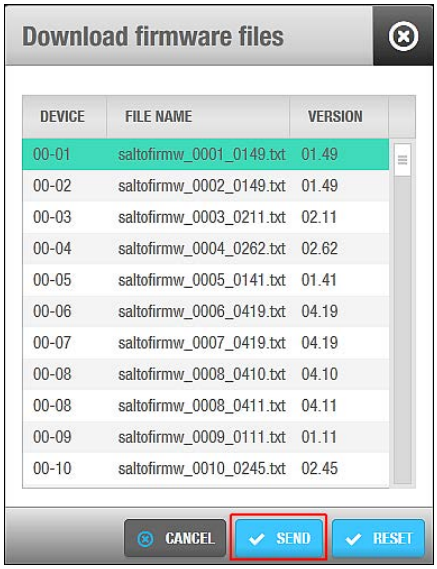


Figure 243: Download firmware files dialog box

35. Select the required file.

    You can hold down the Ctrl key while clicking the files to make multiple selections. Note that you can click **Reset** to delete any firmware files you have already downloaded.
36. Click **Send**. The **PPD** progress screen is displayed.
37. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
38. Click **OK**.

You can now use the PPD to update the firmware of locking electronic components by selecting **Update Firmware** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

5. 28. 8. Initializing Locks

You must initialize each lock when it is installed. This programmes the lock, and transfers access point data relating to time zones and calendars, for example.

It is recommended that you connect the PPD to the PC after you initialize locks to communicate the most up-to-date information about the locks to the system.

NOTE: You can configure PPDs to assign IP addresses to online IP (CU5000) doors during initialization if required. You must enter each IP address on the system by using the **Access point: Online IP CU5000** information screen. Note that you must select **System** > **SALTO Network** and double-click the required online IP (CU5000) door on the **SALTO Network** screen to view the information screen. You must enable this option in ProAccess SPACE General options by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

PPDs can also be used to transfer SAM data to SALTO locks and wall readers during initialization (or when you perform updates). See *SAM and Issuing options General* options

See *General options* section.

SAM and Issuing Data for more information.

To initialize a lock, perform the following steps:

39. Connect the PPD to the PC.
40. Select **System** > **PPD**. The **PPD** information screen is displayed.

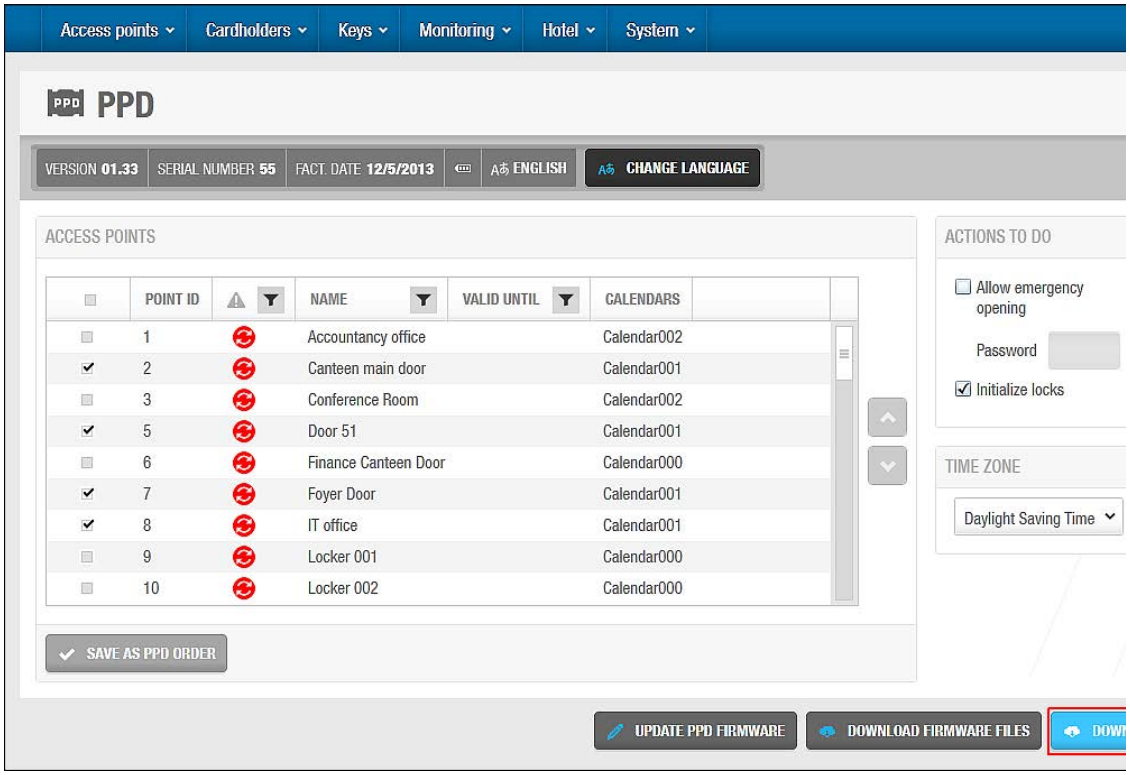


Figure 244: PPD information screen

41. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.
42. Select the checkbox of the access point for which you want to initialize the lock.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.
43. Select the **Initialize locks** checkbox in the **Actions To Do** panel.
44. Click **Download**. The **PPD** progress screen is displayed.
45. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.

    You can now use the PPD to initialize the lock of the selected access point by selecting **Initialize Lock** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: If you initialize a lock that is already in use, its audit trail is deleted.

5. 28. 9. Initializing Rooms and ESDs

The procedure for initializing rooms and ESDs is the same as for initializing locks. See *Initializing Locks* for more information and a description of the steps you should follow.

NOTE: You can initialize rooms and their associated ESDs either together or separately. However, all of the rooms and ESDs that you select during the initialization process must have the same calendar.

5. 28. 10. Updating Locks

You must update offline locks when you make certain changes to access point data, such as enabling anti-passback or changing the opening mode of doors. You can view locks that need to be updated on the **PPD** information screen by selecting **System** > **PPD**. Note that you must connect a PPD to the PC before you can access the **PPD** information screen. Access points that need to be updated have a red **Update required** icon on the left-hand side of their name.

It is recommended to update offline locks at least every six months to ensure that the clock and calendars are up to date. You must also update locks after you replace their batteries. This is because access point data relating to time zones and calendars, for example, must be restored after a lock's battery dies.

You should connect the PPD to the PC after you update locks to communicate the most up-to-date information about the locks to the system.

To update a lock, perform the following steps:

46. Connect the PPD to the PC.
47. Select **System** > **PPD**. The **PPD** information screen is displayed.

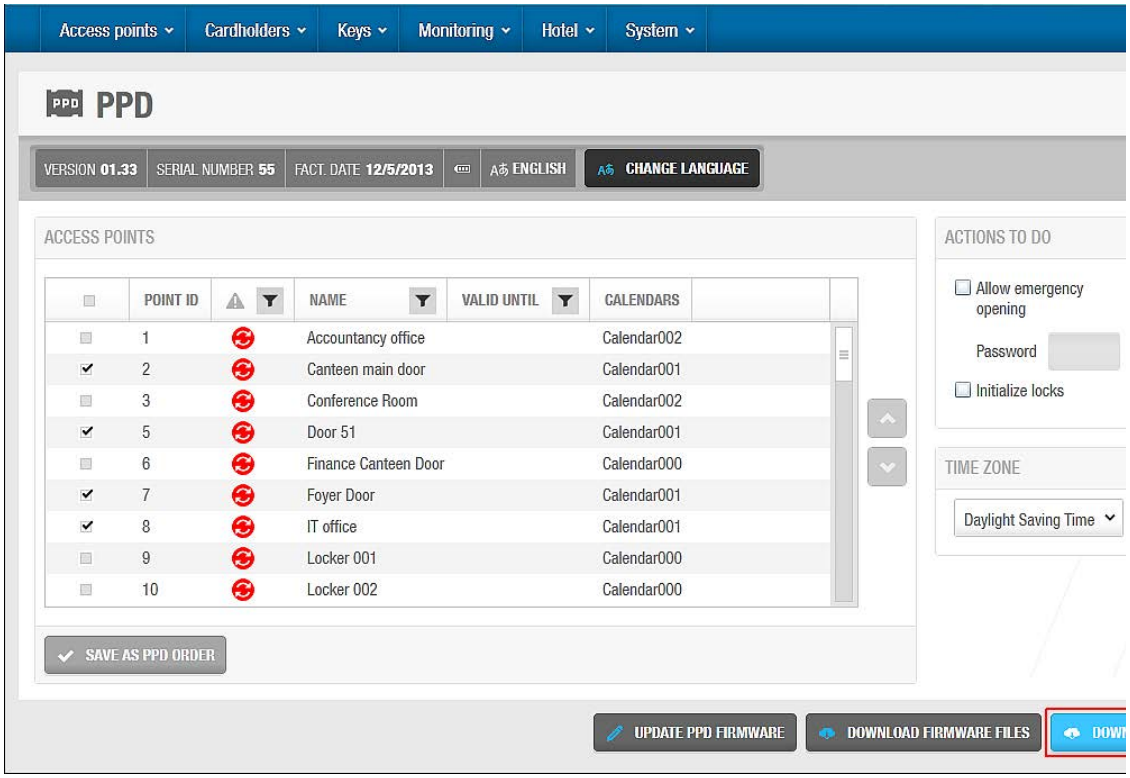


Figure 245: PPD information screen

48. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

49. Select the checkbox of the access point for which you want to update the lock.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

50. Click **Download**. The **PPD** progress screen is displayed.
51. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
52. Click **OK**.

    You can now use the PPD to update the lock of the selected access point by selecting **Update Locks** in the PPD's menu and connecting the PPD to the lock. Alternatively, you can simply connect the PPD to the lock. In this case, it recognizes the lock and automatically displays the appropriate data. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: You can configure PPDs to automatically collect audit trail data when they are used to update locks. You must enable this option in ProAccess SPACE General options by selecting the **Collect audit trails automatically when updating locks** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

5. 28. 11. Performing Emergency Door Openings

You can use the PPD to perform an emergency opening if the lock battery dies or a reader error occurs, for example.

NOTE: You can perform emergency openings of online doors without using a PPD. See *Lockdown* for more information.

To perform an emergency opening, perform the following steps:

53. Connect the PPD to the PC.
54. Select **System** > **PPD**. The **PPD** information screen is displayed.

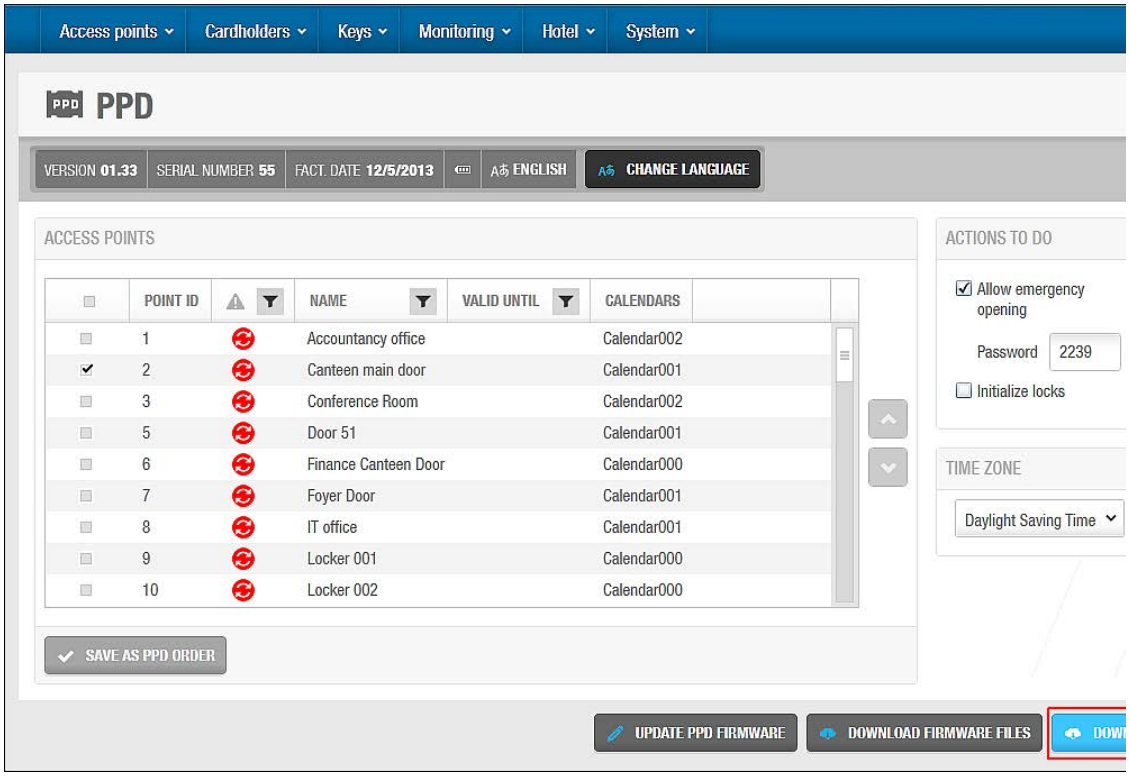


Figure 246: PPD information screen

55. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

56. Select the checkbox of the access point for which you want to perform the emergency opening.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

57. Select the **Allow emergency opening** checkbox in the **Actions To Do** panel.

    The checkbox is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options. See *PPD Tab* for more

information. Otherwise, you must select it each time you want to perform an emergency opening.

58. Type a password for the emergency opening in the **Password** field if required.

    The password can only contain digits. If you type a password, you must enter this password in the PPD before you can perform the emergency opening. Otherwise, the PPD does not require a password. The **Password** field is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options and entered a password there already for the option. See *Devices Tab* for more information. Your PPD firmware must be version 01.29 or higher to use this option.

59. Click **Download**. The **PPD** progress screen is displayed.
60. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
61. Click **OK**.

    You can now use the PPD to perform an emergency opening of the selected access point by selecting **Emergency Opening** in the PPD's menu and connecting the PPD to the lock. Note that you are required to enter a password in the PPD if you have enabled this option in either ProAccess SPACE PPD window or ProAccess SPACE Devices window. See the *Portable Programming Device by SALTO* document for more information about this process.

5. 28. 12. Collecting Audit Trail Data from Offline Doors

See *Audit Trails* for more information about audit trails. You must use a PPD to collect audit trail data from offline doors. See the *Portable Programming Device by SALTO* document for more information about this process. When you have collected the data, you can view it in ProAccess SPACE.

To view the audit trail data on the system, perform the following steps:

62. Connect the PPD to the PC.
63. Select **System** > **PPD**. The **PPD** information screen is displayed.

    The **Audit Trail** information screen is automatically updated with the information from the connected PPD when you display the **PPD** information screen.

64. Select **Monitoring** > **Audit Trail**. The **Audit trail** information screen, showing the new audit trail data, is displayed.

5. 29. SALTO Network

The SALTO network includes items like encoders, gateways, radio frequency (RF) nodes, CU4200 nodes, online doors, and CUs. These are added and managed in ProAccess SPACE. See *SALTO Virtual Network* for more information about the SALTO network.

The RF and CU4200 functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

NOTE: You can view the enabled channels for RF signals in ProAccess SPACE General options. To do so, select **System** > **General options** > **Devices**. There are 16 channels available and all of these are enabled by default. The frequency range of each channel is also displayed. You can disable a channel if required by clearing the checkbox for the channel and clicking **Save**.

RF mode 2 technology is compatible with ProAccess SPACE. However,

RF mode 1 technology is not. If your site uses RF mode 1, an upgrade to ProAccess SPACE is not possible, which means that you must continue to use HAMS or ProAccess RW.

You can view the list of SALTO network items by selecting **System** > **SALTO Network**.

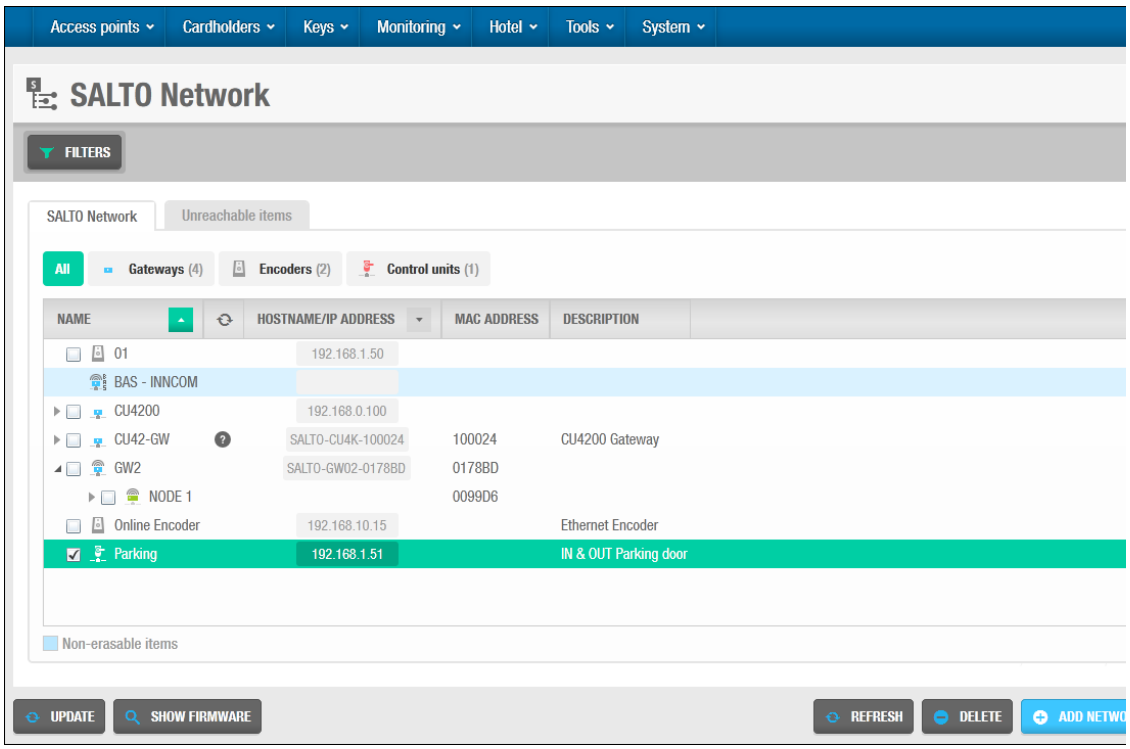


Figure 247: SALTO Network screen

The **SALTO Network** screen displays a list of all network items that have been added and are currently connected to the system.

The information is displayed in four different filtered views:

- **All**: This view shows all of the gateways, encoders, and CUs on the system.
- **Gateways**: This view shows RF gateways and CU4200 gateways. When you click the triangular **Expand** icon on the left-hand side of gateway names, all of the items to which they are connected are displayed. You can view all of the RF nodes and online RF (SALTO) access points connected to each RF gateway, and all of the CU4200 nodes and online IP (CU4200) access points connected to each CU4200 gateway. See *Configuring Online Connection Types* for more information.

NOTE: A BAS gateway may also be displayed on the **SALTO Network** screen. This gateway is created by default if you have fully configured your BAS integration in ProAccess SPACE General options. See *BAS Integration Tab* for more information.

- **Encoders**: This view shows the encoders on the system.
- **Control units**: This view shows online IP (CU5000) access points. See *Configuring Online Connection Types* for more information.

Click the appropriate tab to display each filtered view. The screen also includes an **Unreachable items** tab. Click on this tab to view and configure all items that require additional connection information.

The following table describes the buttons use on the SALTO network main screen.

Table 60: SALTO Network main screen buttons

Item	Description
Update	Allows you to update the selected access point.
Show firmware	Allows you to show the firmware of the selected access point and update it.
Refresh	Allows you to refresh the window with the most updated peripherals status.
Delete	Allows you to delete the selected peripheral.
Add Network device	Allows you to add a new online device.

5. 29. 1. Adding Network Devices

You can add the following network devices to the system:

- Ethernet encoders
- RF gateways
- RF nodes
- CU42E0 gateways
- CU4200 nodes

The following sections describe how to add these devices.

5. 29. 1. 1. Adding Ethernet Encoders

See *Encoders* for more information about encoders.

To add an Ethernet encoder, perform the following steps:

65. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
66. Click **Add Network Device**. The **Add network device** dialog box is displayed.
67. Select **Encoder** from the drop-down list.
68. Click **OK**. The **Encoder** information screen is displayed.

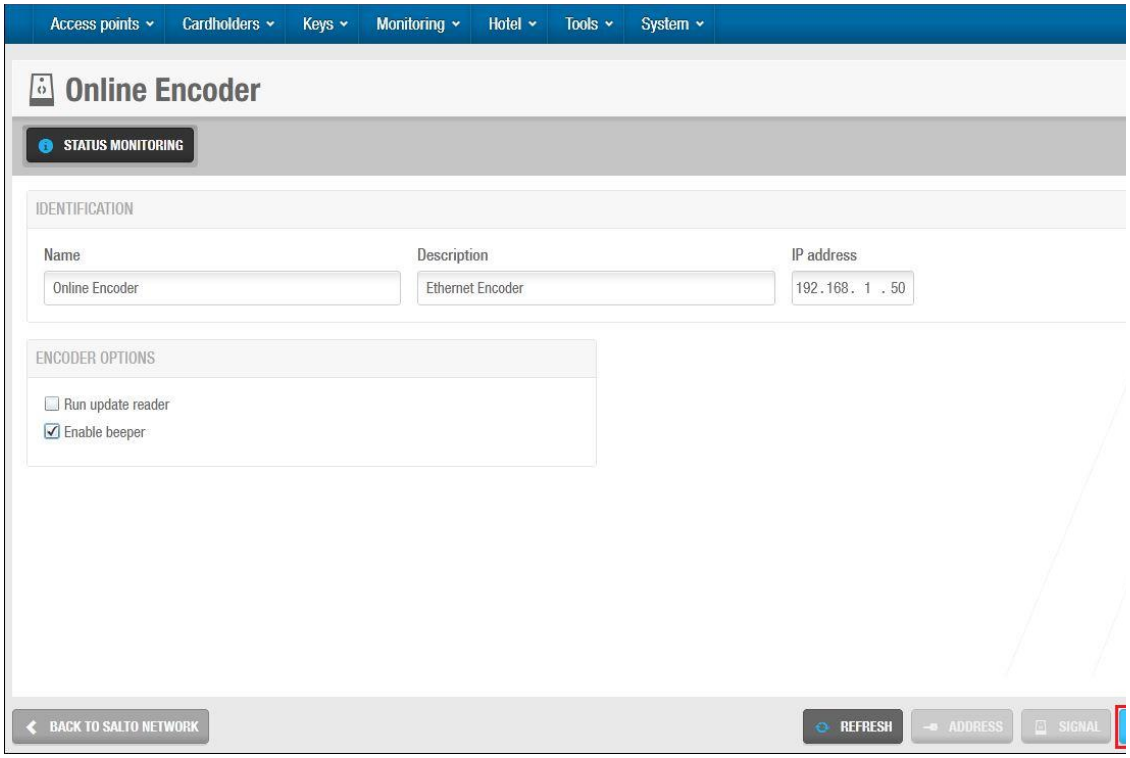


Figure 248: Encoder information screen

69. Type a name for the encoder in the **Name** field.
70. Type a description for the encoder in the **Description** field.
71. Type an IP address for the encoder in the **IP address** field.
72. Select the **Run update reader** checkbox if required.

    This option is used to configure an Ethernet encoder to update user keys automatically when users present their keys to it. If you select this option, the encoder runs continuously but it can only update keys. It cannot be used to encode keys with access data from the SALTO software. See *Updating Keys* for more information.
73. Select the **Enable beeper** checkbox if required.

    If you select this option, the encoder emits beeps when in use.
74. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Click **Save**.

5. 29. 1. 2. Adding RF Gateways

Gateways are hardware devices that provide a link between networks that use different base protocols. RF gateways allow data to be transmitted from the system to the SALTO RF locks, and from the RF locks to the system. RF gateways control RF nodes. See *Adding RF Nodes* for more information about RF nodes.

You must physically connect RF nodes to an RF gateway using an RS485 cable to establish communication between the RF nodes and the RF gateway. See the *SALTO Datasheet_Gatewayx2_xxx* document for more information about this process. You must also connect RF nodes and RF gateways in ProAccess SPACE so the system can show which nodes and gateways are connected.

To add an RF gateway, perform the following steps:

75. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
76. Click **Add Network Device**. The **Add network device** dialog box is displayed.
77. Select **RF gateway** from the drop-down list.
78. Click **OK**. The **RF gateway** information screen is displayed.

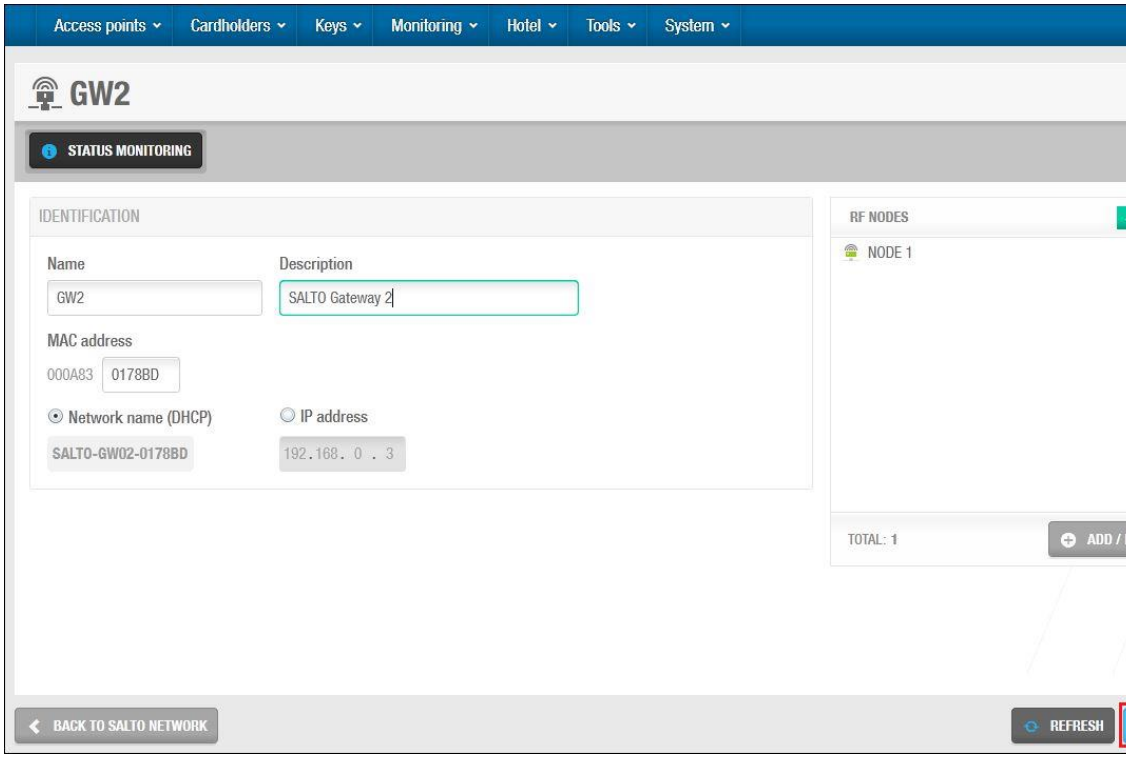


Figure 249: RF gateway information screen

79. Type a name for the RF gateway in the **Name** field.
80. Type a description for the RF gateway in the **Description** field.
81. Type the media access control (MAC) address in the **MAC address** field.

    This is usually displayed on the Ethernet board of the RF gateway.
82. Select either the **Network name (DHCP)** or **IP address** option.

    If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the RF gateway. A Dynamic Host Configuration Protocol (DHCP) server and a DNS are required for this option. If you select the **IP address** option, you must type a static IP address in the field.
83. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.
84. Click **Add/Delete** in the **RF Nodes** panel. The **Add/Delete** dialog box, showing a list of RF nodes, is displayed.

    The **Add/Delete** dialog box only displays RF nodes if you have already added them to the system. You can also connect RF nodes to RF gateways when you add RF nodes to the system. See *Adding RF Nodes* for more information.
85. Select the required RF node in the left-hand panel and click the chevron. The selected RF node is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the RF nodes to make multiple selections. You cannot add RF nodes that already belong to another gateway.
86. Click **Accept**. The selected RF node is displayed in the **RF Nodes** panel.

87. Click **Save**.

5. 29. 1. 3. Adding RF Nodes

RF nodes are network connection points that are physically connected to an RF gateway using an RS485 cable. See *Adding RF Gateways* for more information. This establishes communication between the RF nodes and the RF gateways. Also, in ProAccess SPACE you must connect RF nodes to RF gateways, and RF access points to RF nodes. This means that the system can show which items are connected.

NOTE: You must select **Online RF (SALTO)** in the **Connection Type** panel on the **Door** or **Room** information screen to define a door as an RF access point.

To add an RF node, perform the following steps:

88. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
89. Click **Add Network Device**. The **Add network device** dialog box is displayed.
90. Select **RF node** from the drop-down list.
91. Click **OK**. The **RF node** information screen is displayed.

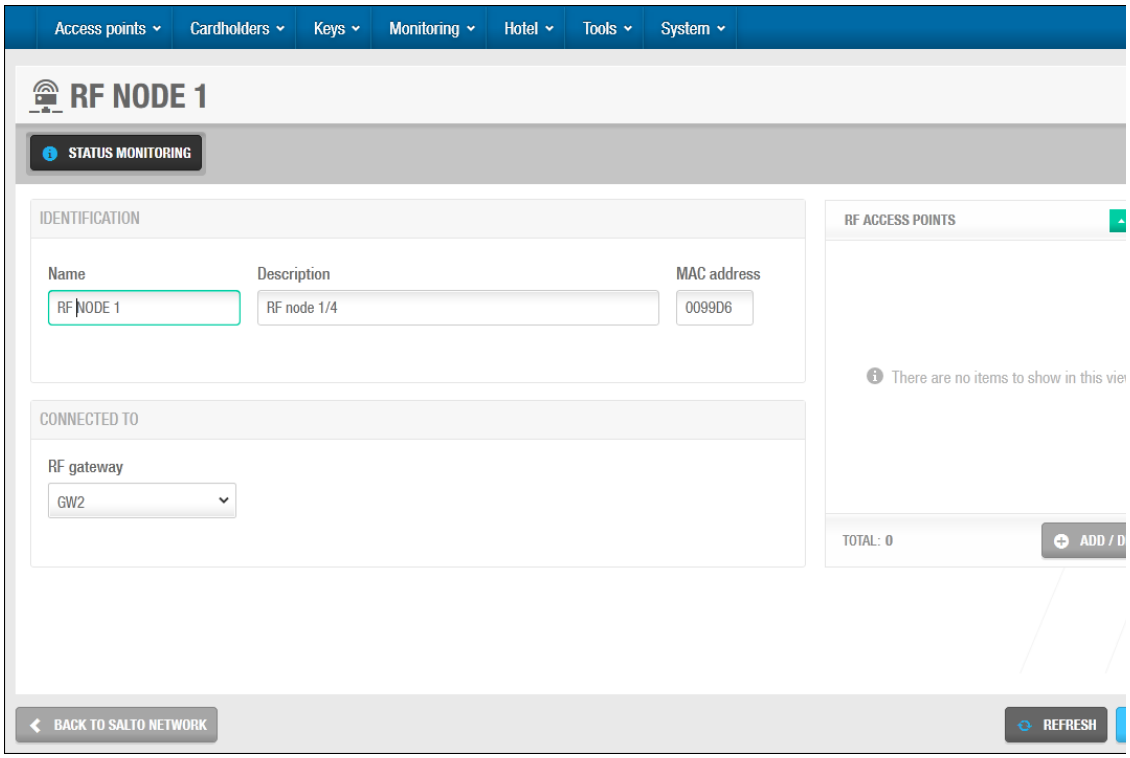


Figure 250: RF node information screen

92. Type a name for the RF node in the **Name** field.
93. Type a description for the RF node in the **Description** field.
94. Type the MAC address of the antenna in the **MAC address** field.
95. Select the RF gateway to which you want to connect the RF node from the **Connected to** drop-down list.

    The default option is **None**.
96. Click **Add/Delete** in the **RF Access Points** panel. The **Add/Delete** dialog box, showing a list of RF access points, is displayed.

    The **Add/Delete** dialog box only displays RF access points if you have already defined doors as RF access points by selecting **Online RF (SALTO)** in the

Connection Type panel on the **Door** or **Room** information screens. You can also connect online RF (SALTO) doors to RF nodes by using the **Connected to** field on the **Online RF (SALTO)** information screen. See *Online RF (SALTO)* for more information.

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

    You can hold down the Ctrl key while clicking the RF access points to make multiple selections. You cannot add RF access points that already belong to another RF node.
98. Click **Accept**. The selected RF access point is displayed in the **RF Access Points** panel.
99. Click **Save**.

NOTE: RF gateways have a mini node connected to them. You must add this node in ProAccess SPACE by following the procedure for adding RF nodes. Also, you must connect the mini node to the RF gateway in ProAccess SPACE.

5. 29. 1. 4. Adding CU42E0 Gateways

CU42E0 gateways are CUs that are connected to a local area network (LAN) using a network cable. They connect to the SALTO network using a TCP/IP connection. CU42E0 gateways can control CU4200 nodes. See *Adding CU4200 Nodes* section below for more information about CU4200 nodes.

The CU42E0 gateways provide a link between the CU4200 nodes and the SALTO system, and transmit data to the nodes. This means the CU4200 nodes do not require a TCP/IP connection. You must physically connect CU4200 nodes to a CU42E0 gateway using an RS485 cable. This establishes communication between the CU4200 nodes and the CU42E0 gateway. You must also link CU42E0 gateways and CU4200 nodes in ProAccess SPACE so the system can show which nodes and gateways are connected.

CU42E0 gateways control access to doors by activating their relays. Each CU42E0 gateway can control a maximum of two doors. They can also update user keys.

The CU42E0 supports up to 4 auxiliary CU4200 nodes, meaning this that up to 10 online doors can be controlled using a single IP address (1 CU42E0 gateways + 4 CU4200 nodes)

In stand-alone mode, dipswitches on the CU4200 node units must be set up to 0000, if online, each node should have its own configured address, using the suitable dipswitch combination in binary format. See the CU42X0 installation guide for more details. See image below for an example.

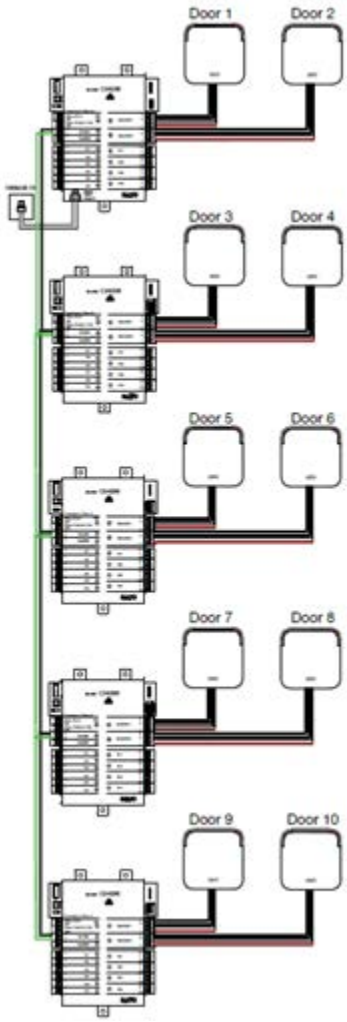


Figure 251: CU42E0 and CU4200 example

NOTE: The maximum distance between the gateway (CU42E0) and the last node (CU4200) in line cannot be over 300 meters.

To add a CU42E0 gateway, perform the following steps:

100. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
101. Click **Add Network Device**. The **Add network device** dialog box is displayed.
102. Select **CU42E0 gateway** from the drop-down list.
103. Click **OK**. The **CU42E0 gateway** information screen is displayed.

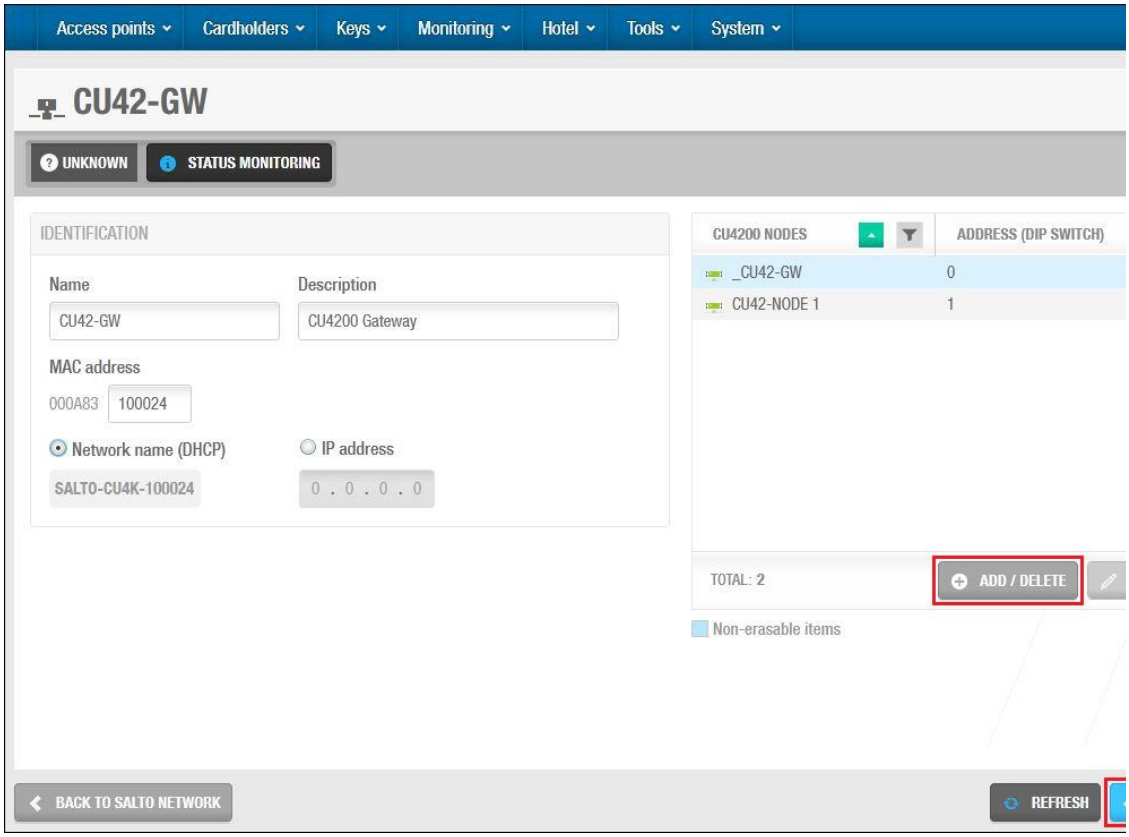


Figure 252: CU4200 gateway information screen

104. Type a name for the CU42E0 gateway in the **Name** field.
105. Type a description for the CU42E0 gateway in the **Description** field.
106. Type the MAC address in the **MAC address** field.

    The MAC address is displayed on a sticker on the CU.

107. Select either the **Network name (DHCP)** or **IP address** radio button.

    If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the CU42E0 gateway. A DHCP server and a DNS are required for this option. If you select the **IP address** option, you must type an IP address in the field.

108. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

109. Click **Add/Delete** in the **CU4200 Node** panel. The **Add/Delete** dialog box, showing a list of CU4200 nodes, is displayed.

    The **Add/Delete** dialog box only displays CU4200 nodes if you have already added them to the system. You can also connect CU4200 nodes to CU42E0 gateways when you add CU4200 nodes to the system. See *Adding CU4200 Nodes* for more information.

110. Select the required CU4200 node in the left-hand panel and click the chevron. The selected CU4200 node is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the CU4200 nodes to make multiple selections. You cannot add CU4200 nodes that already belong to another CU4200 gateway.

NOTE: When you add a CU42E0 gateway, an embedded CU4200 node is automatically created. This cannot be deleted. Each CU42E0 gateway

can support its embedded CU4200 node and a maximum of four other CU4200 nodes. The name of the embedded node will be always the same than the parent CU42E0 gateway preceeded by an underscore. For example: **_CU4200.**

111. Click **Accept**. The selected CU4200 node is displayed in the **CU4200 Node** panel.

    You can select the CU4200 node and click **Edit** to change the number in the **Address (dip switch)** column if required. See *Adding CU4200 Nodes* for more information about the **Address (dip switch)** field. Note that embedded CU4200 nodes have a fixed number (0). This cannot be changed.

112. Click **Save**.

5. 29. 1. 5. Adding CU4200 Nodes

CU4200 nodes are network connection points that are physically connected to a CU42E0 gateway using an RS485 cable. See *Adding CU42E0 Gateways* for more information about CU42E0 gateways. This establishes communication between the CU4200 nodes and the CU42E0 gateway.

The CU4200 nodes receive data from the CU42E0 gateway so they do not require a TCP/IP connection. Instead, they communicate with the SALTO network through the CU42E0 gateway to which they are connected.

You must connect CU4200 nodes to CU42E0 gateways in ProAccess SPACE. You must also connect CU4200 nodes to access points. This means that the system can show which items are connected. Each CU4200 node can control a maximum of two doors.

NOTE: You must select **Online IP (CU4200)** in the **Connection Type** panel on the **Door** and in **Room** information screen before you can connect an access point to a CU4200 node.

To add a CU4200 node, perform the following steps:

113. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
114. Click **Add Network Device**. The **Add network device** dialog box is displayed.
115. Select **CU4200 node** from the drop-down list.
116. Click **OK**. The **CU4200 node** information screen is displayed.

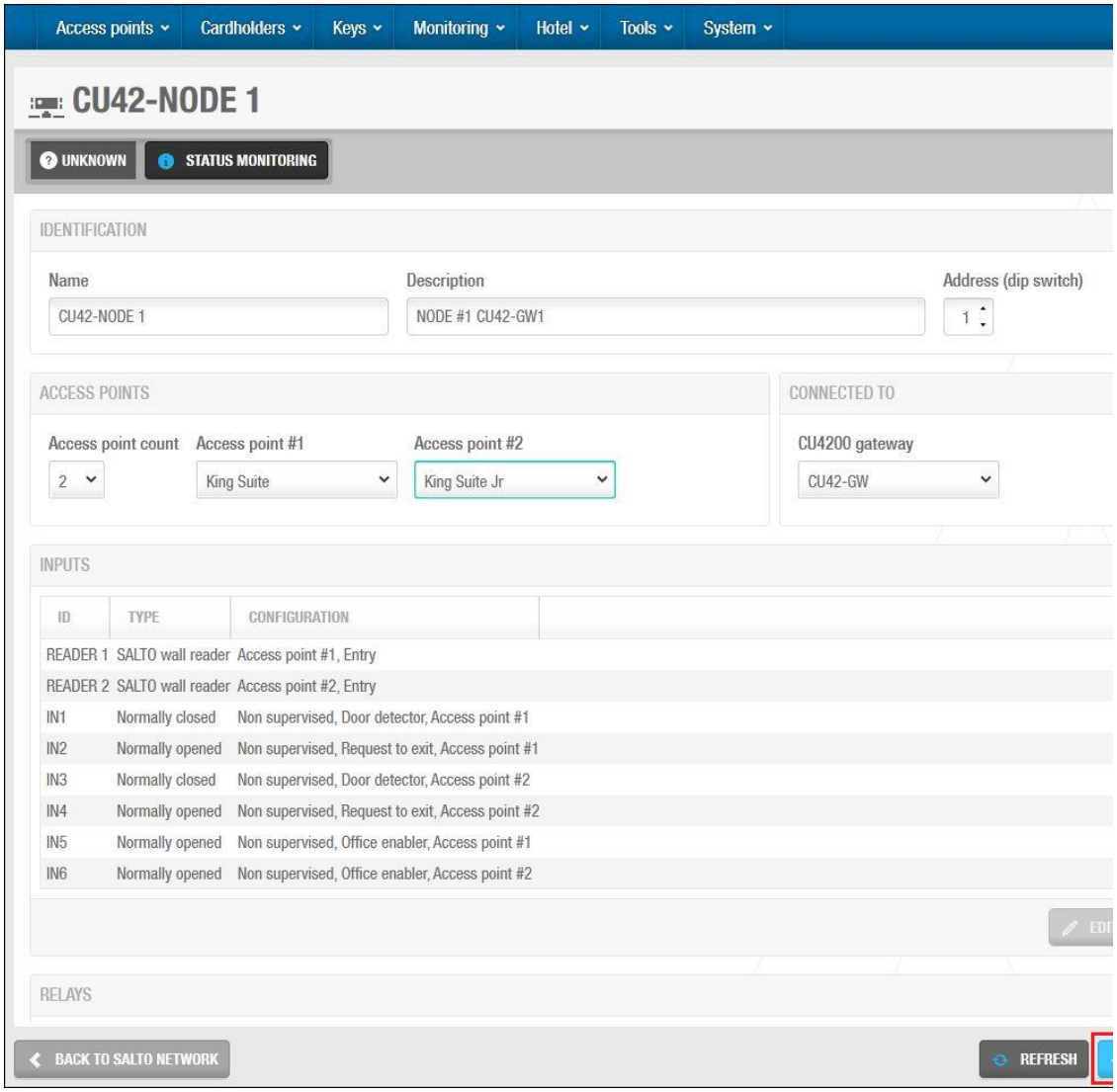


Figure 253: CU4200 node information screen

117. Type a name for the CU4200 node in the **Name** field.
118. Type a description for the CU4200 node in the **Description** field.
119. Select the required number by using the up and down arrows in the **Address (dip switch)** field.

    This number corresponds to the switches on the dip switch panel. The system allows you to select any number between 1 and 99. However, you must select a number between 1 and 15 due to hardware limitations. A CU42E0 gateway can support an embedded CU4200 node and a maximum of four other CU4200 nodes. Each CU4200 node that you connect to a specific CU42E0 gateway must have a unique number, for example, 1, 2, 3, until 15. Note that the value 0 is used for embedded CU4200 nodes. Bear in mind that addresses set up on the nodes should follow the physical dipswitches' configuration on each CU4200 unit.

Table 61: Dipswitch configuration

Dip switch	Address (dip switch)
0000	Address 0, only for embedded CU4200 nodes.
0001	Address 1
0010	Address 2

0011	Address 3
0100	Address 4
0101	Address 5
0110	Address 6
0111	Address 7
1000	Address 8
1001	Address 9
1010	Address 10
1011	Address 11
1100	Address 12
1101	Address 13
1110	Address 14
1111	Address 15

See the following image as an example;

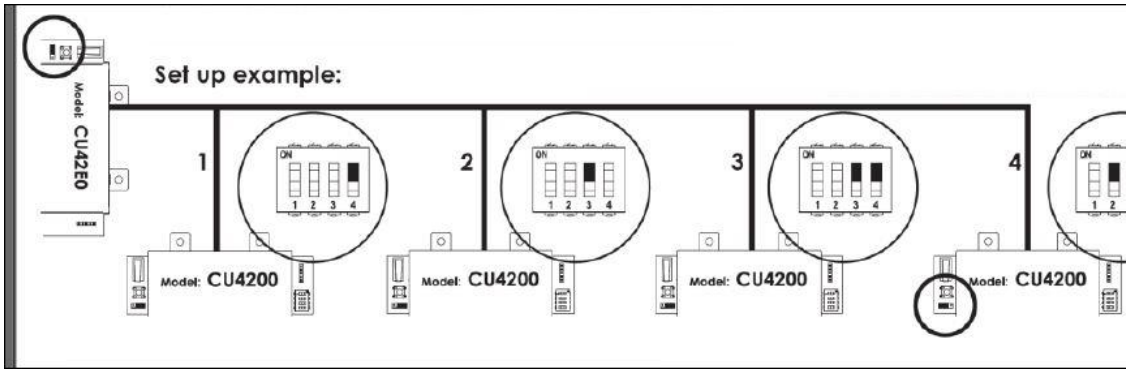


Figure 254: CU4200 dip switches set up

120. Select the required number from the **Access point count** drop-down list.

You can select either **1** or **2.** This defines the number of doors you want the CU4200 node to control. Each CU4200 node can control two readers. This means it can control either one door that has two readers or two doors where each has one reader. If a door has two readers, one reader controls access from inside to outside, and the other reader controls access from outside to inside. You should select **1** if a door has two readers. If you select **2,** an **Access point #2** field is displayed on the right-hand side of the **Access point #1** field, and you can select an additional door from the drop-down list.

121. Select the required door from the **Access point #1** drop-down list.

The **Access point** drop-down lists only display doors if you have already defined some as CU4200 access points. This is done by selecting **Online IP (CU4200)** in the **Connection Type** panel on the **Door** information screen. You can also connect online IP (CU4200) doors to CU4200 nodes in the **Connected to** field on the **Online IP (CU4200)** information screen. See *Online IP (CU4200)* for more information.

122. Select the CU42E0 gateway to which you want to connect the CU4200 node from the **Connected to** drop-down list.

123. Click **Save**.

5. 29. 1. 6. Using CU4200 Inputs

Inputs are the signals or data received by the CU4200. You can setup the inputs in ProAccess SPACE so the CU4200 can understand how to act. You can set Inputs for **Reader 1** and **Reader 2.** You can also set up to 6 inputs from third party devices.

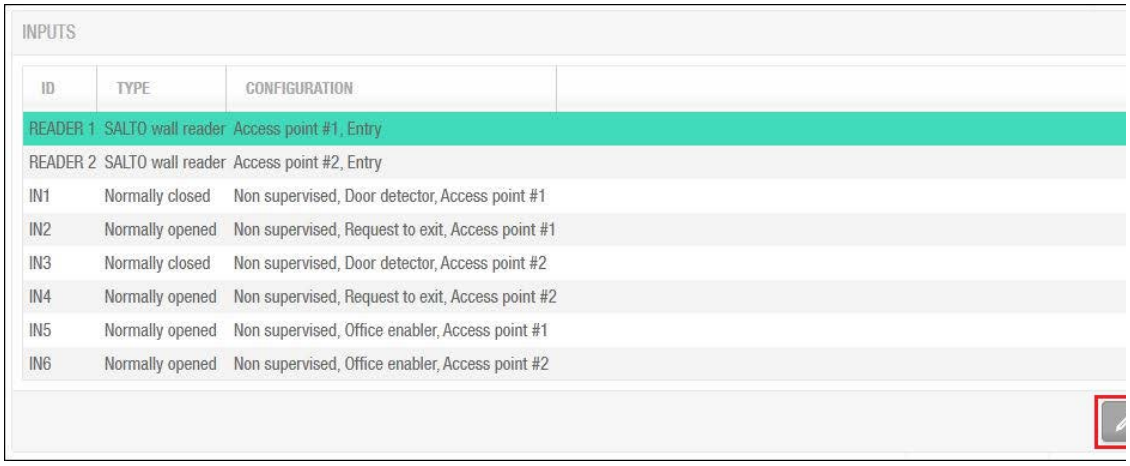


Figure 255: CU4200 node Inputs

You can set the CU4200 outputs according with the wall reader input. To manage the wall reader input, select the reader and click **Edit**.

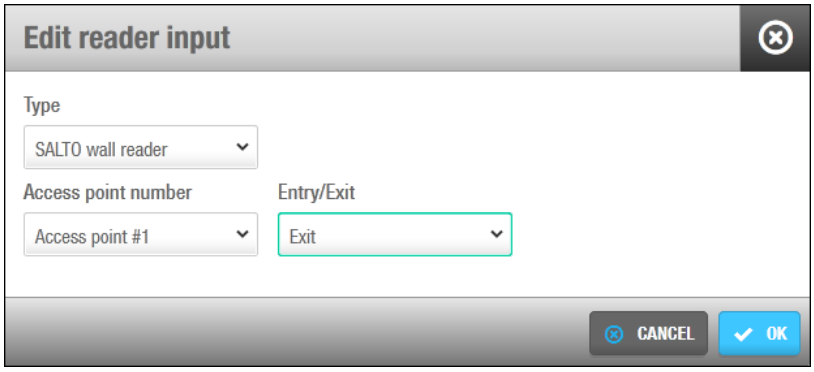


Figure 256: CU4200 node Reader Input

The **Reader input** fields are described in the following table.

Table 62: Reader Inputs fields

Field	Functionality
Type	You can select **None** if no SALTO wall reader is connected or **SALTO wall reader** if it is a SALTO wall reader. Other options may appear in the future. If **None** is selected, inputs 3, 4 and 5, 6 can be used with a third party wall reader.
Access point number	As the CU4200 can manage up to two different access points, you can decide whether the reader will trigger an opening in access point #1 or #2. See *Adding CU4200 Nodes* for more information.
Entry/Exit	Select whether the wall reader is an Entry or an Exit.

The CU4200 node can manage inputs from third party devices. Depending the

signal or data arrived to the input the CU4200 Node can act accordingly. Select the **Input ID** and click **Edit**.

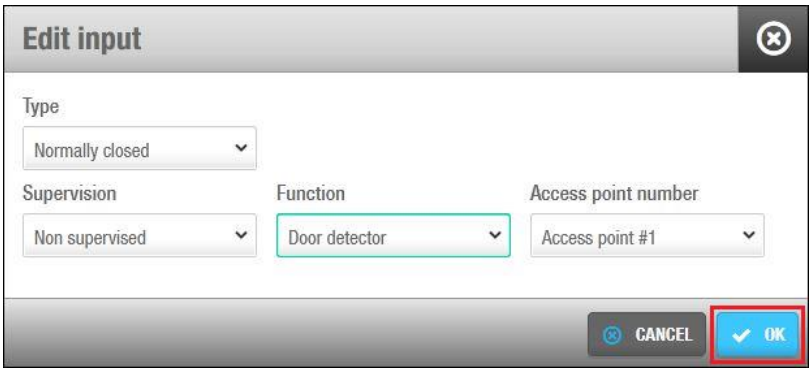


Figure 257: CU4200 node Reader Input

The **Inputs** fields are described in the table below,

Table 63: Inputs fields

Field	Functionality
Type	Status of the relay in normal position. The relay can be normally in closed position or opened position.
Supervision	Select the resistance as required for the supervision. A supervised input is protected against external attacks.
Function	Select the function you want for the relay. Options include doo Door detector, Office enabler, Intrusion inhibition, Request to open roller blind, Request to close roller blind, Request to Exit or Request to Open.

For example, according to the image below, a relay in normally opened position could send a request to open a roller blind when presenting a valid key in reader #1 from IN1 and request to close the roller blind from IN2.

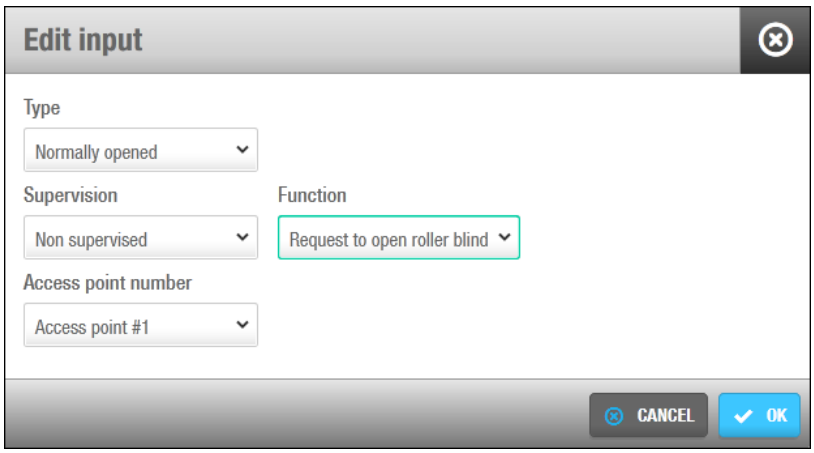


Figure 258: Roller blind example

A reader that is not from SALTO can also be used. **Edit Reader Input** Type must be set to **None**. **Type** field in **Edit Input** shows the **Third party reader** option in the dropdown menu. Only a **Wiegand** code is supported. See *Devices Tab* in General

options for more information about how to configure the Wiegand format. An authorization code has to be entered for each user in the **Authorization code** field on the **User** profile. See *Users* in **Cardholders** menu for more information. Select the **Access point** from the **Access point number** dropdown menu and if it will be an **Entry** or an **Exit.**

5. 29. 1. 7. Managing CU4200 Relays

A relay is an electrically operated switch. It is used where it is necessary to control a circuit by a low-power signal. For example, you can control an electric or magnetic strike, trigger a camera recording or turn an alarm off.

The CU4200 node has 4 relays that can be configured independently. Select the relay ID and click **Edit**. The **Edit Relay** fields are described in the table below

Table 64: Edit Relay fields

Field	Functionality
Type	Select the appropriate type as needed.
Access point number	Select the access point in question. It can be **Access point #1, Access point #2** or both.
Output	The **Output** dropdown menu is shown when Output is selected in **Type** dropdown menu. Select the Output from the dropdown menu. The list of outputs have to be created first in **Outputs** list, in the **Access points** menu. See Access points *Outputs* for more information about how to create Outputs. The relay will be triggered when a key with a valid output is presented to the wall reader. See User *Outputs* for more information about how to add outputs in the user access.
Conditions	Select **Combined** in the **Type** dropdown menu to select a combination of conditions. According to the image below, the relay will be triggered if in Access point #1 the **Door is left opened**, if there is an **Intrusion** or if there is a **Card rejected**.

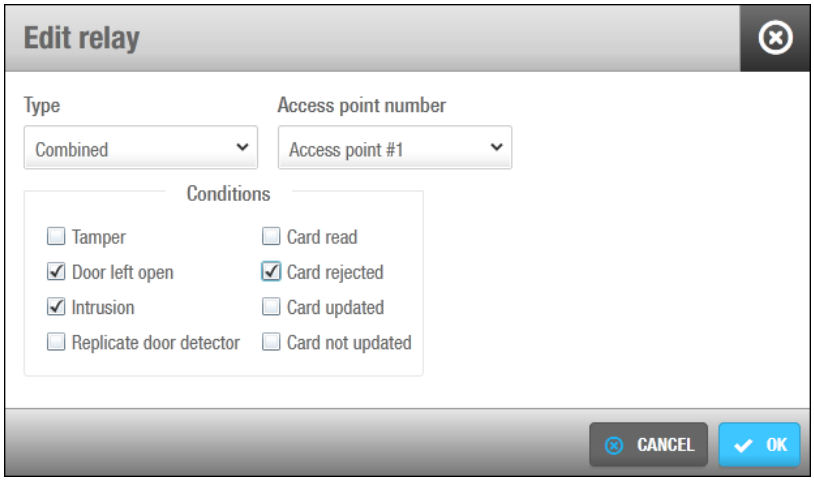


Figure 259: Combined relay type

5. 29. 1. 8. CU42X0 devices initialization and update

The CU42E0 gateways and CU4200 nodes are initialized and updated automatically. See table below for the frequency of each.

Table 65: CU42x0 Initialization and Update

Automatic process	Check Frequency	Notes
CU4K doors initialization	1 minute	Includes initialization + update
CU4K doors update	5 minutes	Can be executed on request
CU4K nodes initialization	1 minute	Includes initialization + update
CU4K nodes update	5 minutes	Can be executed on request

NOTE: Even if updates are performed automatically every 5 minutes for the CU42x0, a manual update can be performed immediately by selecting the device and clicking the **Update** button in **SALTO network**.

5. 29. 2. Filtering SALTO Network Data

You can filter SALTO network data by type, name, description, and/or IP address.

You can filter by the following item types:

- Online IP (CU5000)
- CU42E0 gateway
- CU4200 node
- Online IP (CU4200)
- Encoder
- RF gateway
- RF node
- Online RF (SALTO)
- BAS gateway
- Online RF (BAS integration)

To filter the SALTO network data, perform the following steps:

124. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
125. Click **Filters**. The **Items filtering** dialog box is displayed.
126. Select a pre-defined search term from the **Type** drop-down list.
127. Type the name of the item you want to search for in the **Name** field.
128. Type the description of the item you want to search for in the **Description** field.
129. Type the IP address in the **IP address** field if appropriate.

    The **IP address** field is only displayed for relevant search term types.
130. Click **Apply Filter**. A filtered SALTO network list is displayed.

    When a filter has been applied, on the **SALTO Network** screen when you have applied a filter, the search type is displayed in light blue. You can click the search type to once again display all items on the list screen. You can click **Delete Filter** to delete the filter and to redefine the filter parameters.
131. Click the **Close** icon in the **Applied Filters** field when you have finished reviewing the filtered list or click **Filters** to apply another filter.

5. 29. 3. Configuring Online Connection Types

When adding a door or room to the system, you must specify the appropriate connection type – either online or offline. When you select an online connection type, the door or room is displayed on the **SALTO Network** screen, and you can double-click the entry to configure it.

There are four online connection types:

- Online IP (CU5000)
- Online IP (CU4200)
- Online RF (SALTO)
- Online RF (BAS integration)

NOTE: Your BAS integration must be fully configured in ProAccess SPACE General options before you can select this option. See *BAS Tab* for more information.

See *Connection Types* for more information about selecting the correct connection types in non-hotel sites. For information about connection types in non-hotel sites, see *Connection Types*.

5. 29. 3. 1. Online IP (CU5000)

To configure an online IP (CU5000) door, perform the following steps:

132. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
133. Double-click the online IP (CU5000) door that you want to configure. The **Access point: Online IP (CU5000)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU5000) doors are online SVN points.

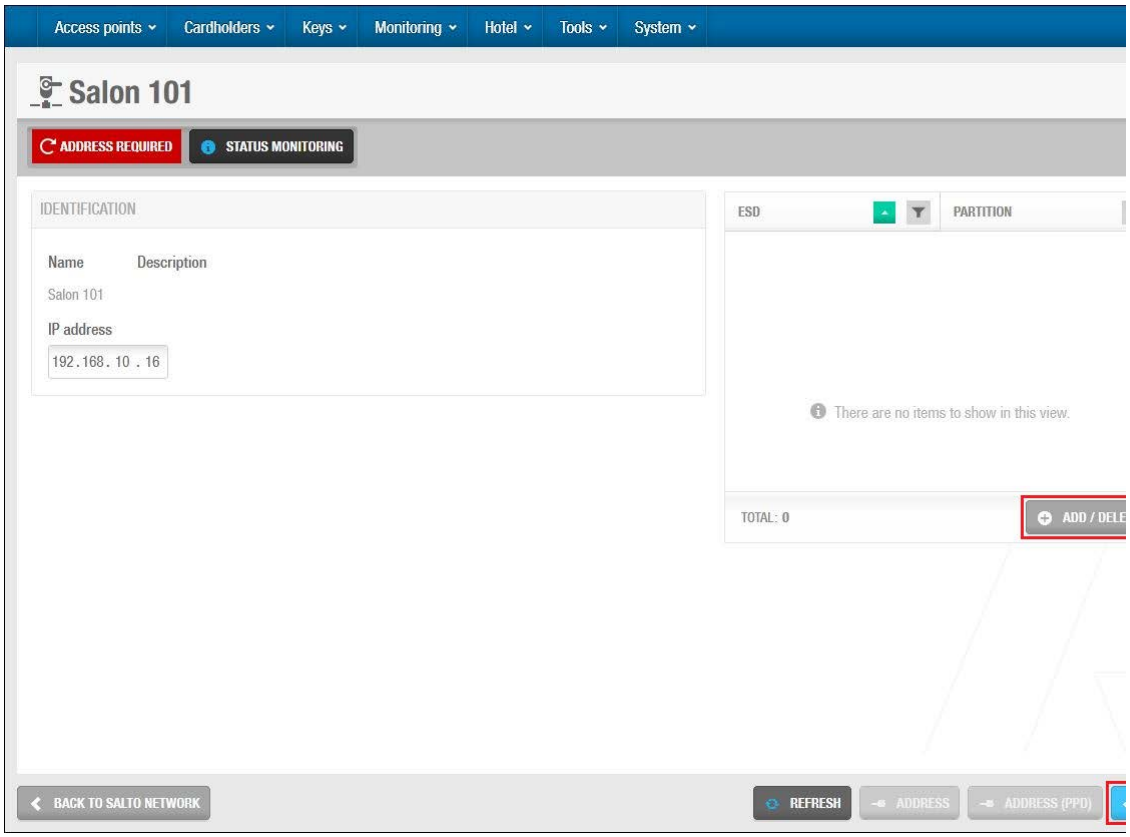


Figure 260: Access point: Online IP (CU5000) information screen

134. Type an IP address for the door in the **IP address** field.
135. Click **Add/Delete** in the **ESD** panel. The **Add/Delete** dialog box, showing a list of ESDs, is displayed. See *ESDs* for more information about ESDs.
136. Select the required ESD in the left-hand panel and click the chevron. The selected ESD is displayed in the right-hand panel.

You can hold down the Ctrl key while clicking the ESDs to make multiple selections.

137. Click **Accept**. The selected ESD is displayed in the **ESD** panel.
138. Click **Save**.

5. 29. 3. 2. Online IP (CU4200)

To configure an online IP (CU4200) door, perform the following steps:

139. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
140. Double-click the online IP (CU4200) door that you want to configure. The **Online IP (CU 4200)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU4200) doors that are not connected to CU4200 nodes are displayed in the **Unreachable items** tab. See *Adding CU4200 Nodes* for more information about CU4200 nodes.

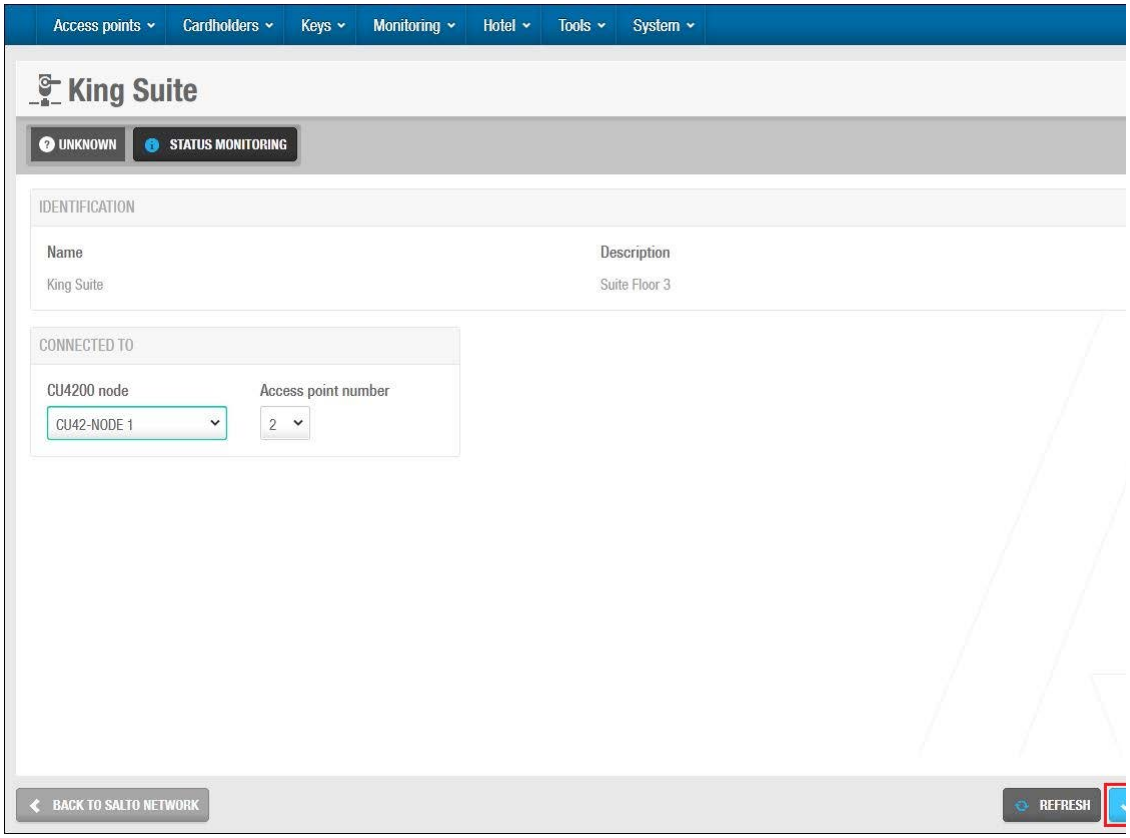


Figure 261: Online IP (CU4200) information screen

141. Select the CU4200 node to which you want to connect the door from the **Connected to** drop-down list.
142. Select either **1** or **2** from the **Door number** drop-down list.

You cannot select **2** unless you have selected **2** in the **Access point count** drop-down list on the **CU4200 node** information screen. Otherwise, this exceeds the door number count for the node. See *Adding CU4200 Nodes* for more information.

143. Click **Save**.

5. 29. 3. 3. Online RF (SALTO)

To configure an online RF (SALTO) door, perform the following steps:

144. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
145. Double-click the online RF (SALTO) door that you want to configure. The **Online RF (SALTO)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online RF (SALTO) doors that are not yet connected to RF nodes are displayed in the **Unreachable items** tab. See *Adding RF Nodes* for more information about RF nodes.

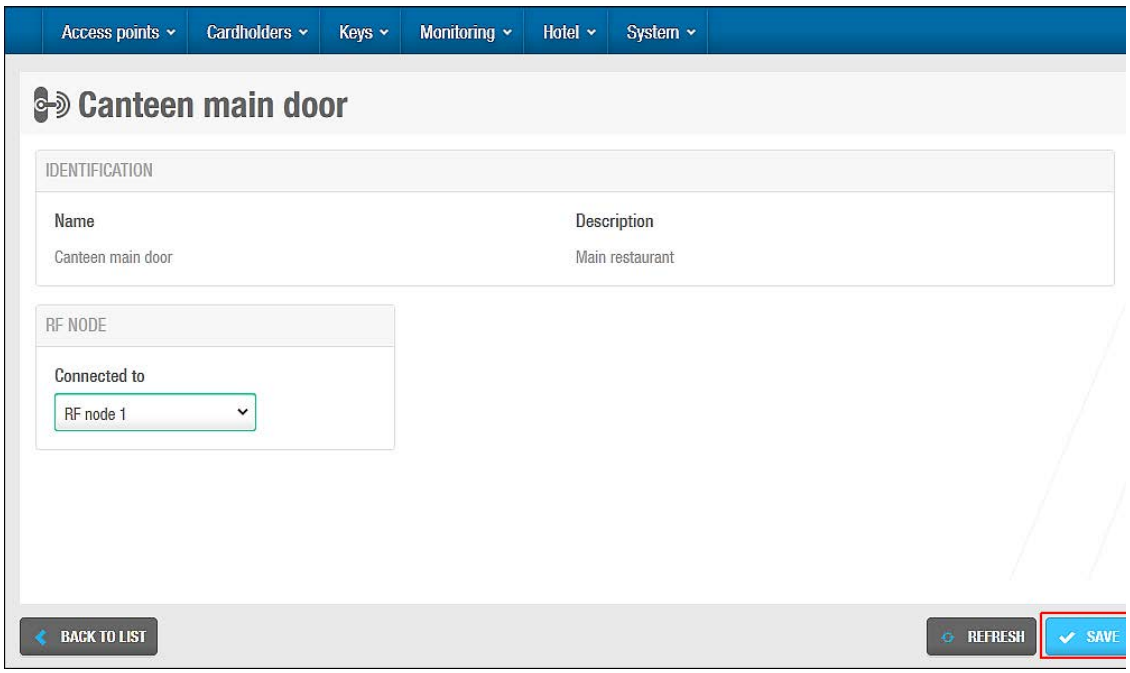


Figure 262: Online RF (SALTO) information screen

146. Select the RF node to which you want to connect the door from the **Connected to** drop-down list.
147. Click **Save**

5. 29. 4. Peripherals Addressing and Maintenance

SALTO network items like Control units, Ethernet encoders, gateways and RF nodes can be added and managed in ProAccess SPACE where you can also make changes such as updating online CUs or updating firmware.

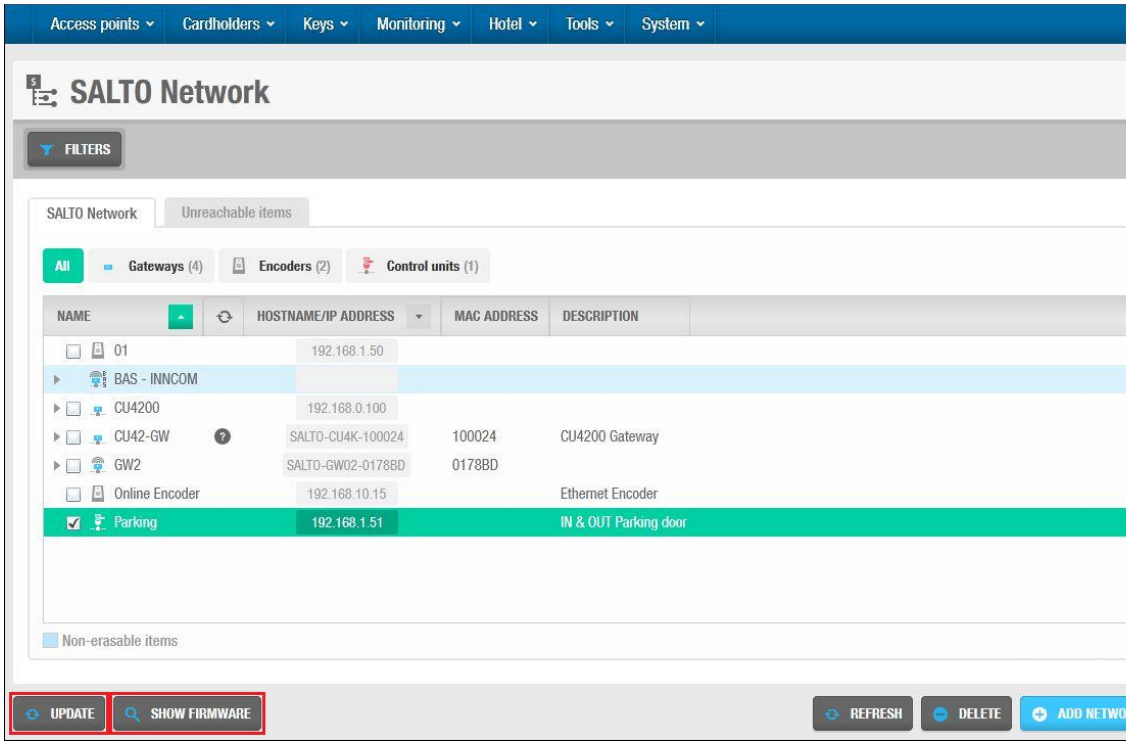


Figure 263: Address and Maintenance

The **Address** and **Maintenance** tab buttons are described in the following table.

Table 66: Maintenance buttons

Button	Functionality
Update	Allows updates to the SALTO database to be communicated to the selected network items. In addition, it allows blacklists to be transmitted automatically to doors without the need to visit each door with an updated key. SAM cards can also be used to transfer information to online doors and to update offline escutcheons and cylinders. See *SAM and Issuing Data* for more information. To SAM a local encoder, click **Supported Keys** on the **Settings** screen in ProAccess SPACE. See *Encoder Settings* for more information. You will find this button in all updatable devices such as control unit CU5000 and CU4200.
Show firmware	Displays the firmware version of the selected item. You can check the firmware version for any online device, CU, RF door, or Ethernet encoder. We recommended that you use the latest firmware version with the SALTO system. Online CUs consist of an Ethernet board and a CU board. This may require updating an individual or multiple online CUs to the most recent firmware version. See *Updating Firmware* for more information about updating multiple online CUs simultaneously. You will find this button in all firmware updatable devices such as control unit CU5000, CU4200 gateways and Ethernet encoders.
Address	Assigns an IP address that you have entered on the system for an Ethernet encoder or an online IP (CU5000) door if the peripheral is in the same network. When you click **CLR** on the online CU, for example, the device enters listening mode. When you click **Address** on the **Monitoring** tab, the software sends a broadcast to the online CU. When the broadcast reaches the online CU, it initializes it with the new IP and other door parameters. Note that you can only address one peripheral at a

	time when using this option. See *Adding Ethernet Encoders* and *Online IP (CU5000)* for more information about entering IP addresses for Ethernet encoders and online IP (CU5000) doors. You will find this button in all updatable devices such as control unit CU5000 and Ethernet encoders.
Address (PPD)	Assigns an IP address, using a PPD, to an online CU if the peripheral is in a different network. When the online CU is initialized by the PPD, click **Address (PPD)** on the **Monitoring** tab. This creates an authentication between the system and the peripheral. You must enable this option by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices** in ProAccess SPACE. See *Devices Tab* for more information. See also *PPD* for more information. You will find this button in all updatable devices such as control unit CU5000.
Signal	Used to help identify the physical Ethernet encoder that corresponds to the applicable IP/peripheral. After you select the peripheral in the list and click **Signal**, the LED of the applicable encoder starts flashing. At this point, the SAMing process can take place. See *SAM and Issuing Data* for more information.

The columns at the top of the **Maintenance** tab are described in the following table.

Table 67: Maintenance columns

Column	Functionality
Name	Specifies the name of the item (the icon immediately before the item name indicates the peripheral type)
 Update Status	Shows the peripheral update status. If no update is required, no icon will be shown. The status could be **Update required**, **Address required** or **Unknown.** Note that this column does not have a title on the screen.
Hostname/ IP address	Specifies the network name that identifies the item
MAC Address	Specifies the MAC address of the device.
Description	Matches the details of the item entered in the **Description** field in ProAccess SPACE

5. 29. 4. 1. Updating Firmware

Firmware is software that is programmed on the ROM of hardware devices.

NOTE: SALTO provides firmware updates when new functionality is available or when a software bug is fixed. Each component has a unique file. Contact your SALTO technical support contact before updating any firmware file.

To update the firmware version of an item, perform the following steps:

148. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
149. Select the required item and click **Show firmware**. The **Firmware information** dialog box is displayed.

Figure 264: Peripheral firmware update dialog box

You can select multiple items on the **SALTO Network** peripheral list if required.

150. Select the checkbox next to the item that you want to update. The **Browse** button is enabled.

    If required, you can click **Check all** to update the firmware for multiple items simultaneously. You can only update multiples of the same item (for example, online CUs only or Ethernet encoders only) simultaneously.

151. Click **Browse** to select the required firmware file.

152. Click **Send firmware**. A confirmation screen is displayed when the firmware update is complete.

NOTE: You can update the firmware for local encoders by using the **Show Firmware** button on the **Settings** screen in ProAccess SPACE. See *Updating Encoder Firmware* for more information.

Calendars for more information.

5. 29. 5. Creating Access Point Timed Periods

To create an access point timed period, perform the following steps:

1. Select **Access points** > **Access point timed periods**. The **Access point timed periods** information screen is displayed.

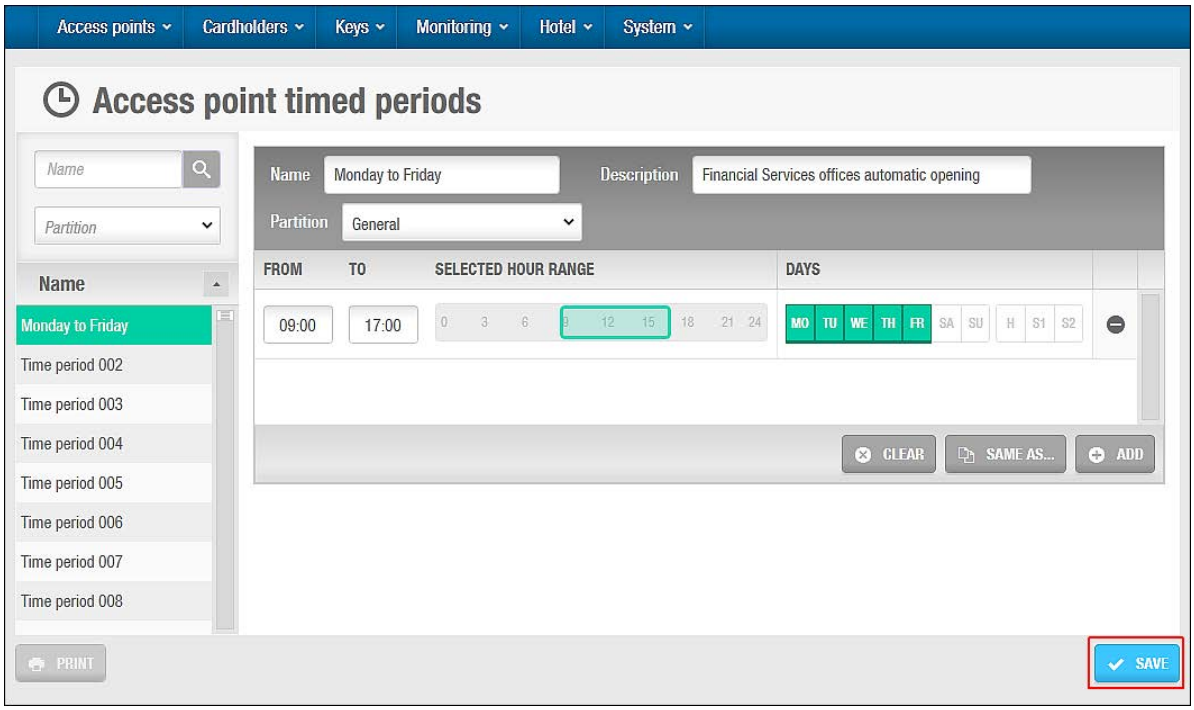


Figure 78: Access point timed periods information screen

2. Select a time period from the **Name** panel.

   You can rename the timed period to something more relevant to your organization, for example, Monday to Friday.
   Time period 001 is automatically selected. If you have already configured this period entry, select the next time period. Up to 1024 time periods can be created.
3. Type a description of the access point timed opening in the **Description** field.
4. Select the relevant partition from the **Partition** drop-down list, if required.

   See *System* Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

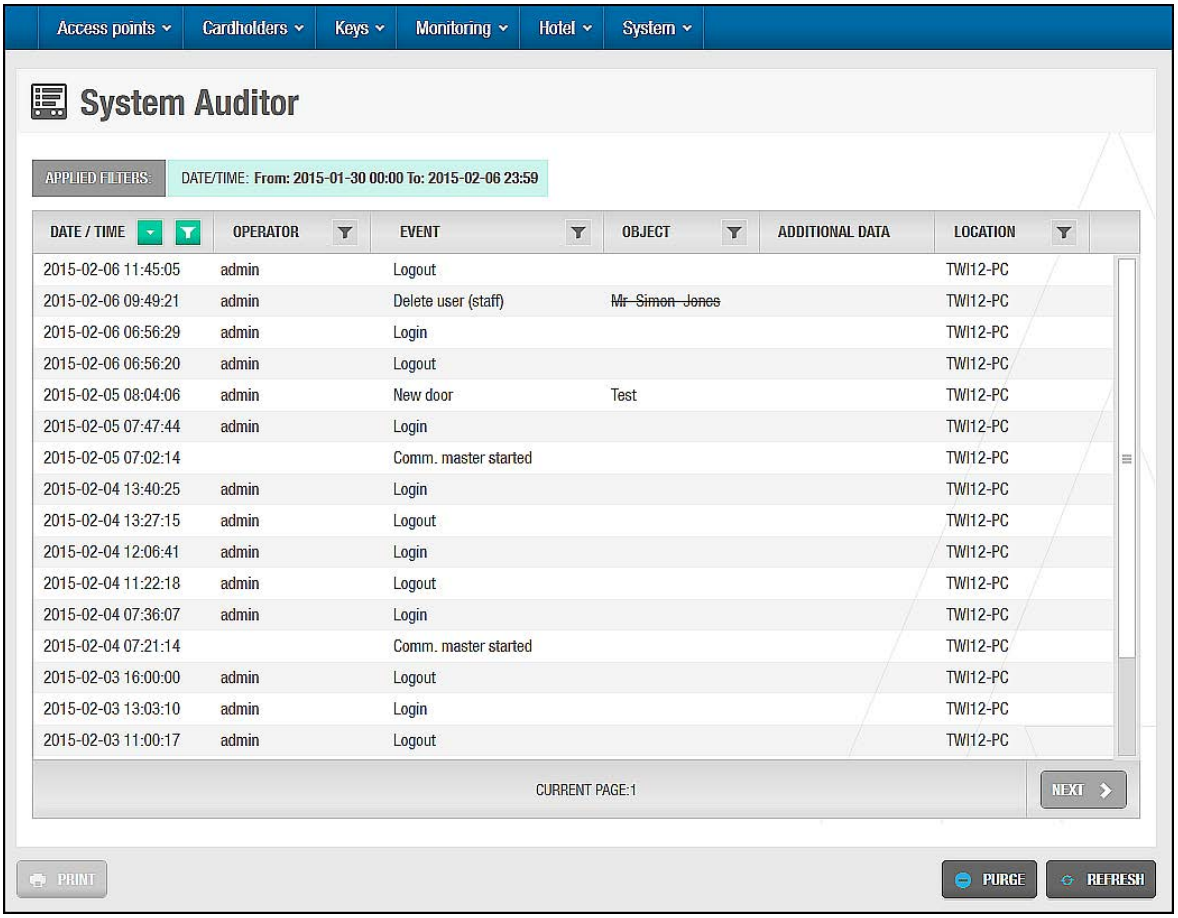


Figure 228: System Auditor information screen

5. 29. 6. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

5. 29. 7. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

5. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

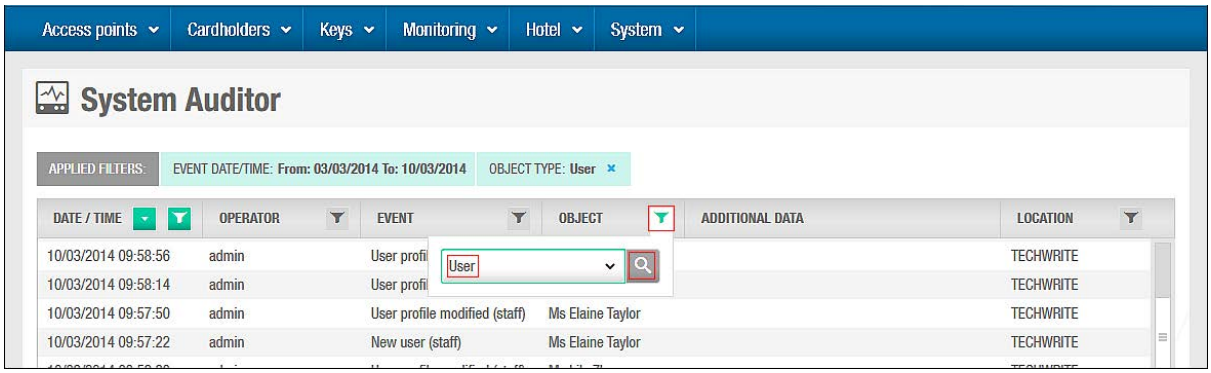


Figure 229: System Auditor information screen

6. Click the **Funnel** icon above the filter item. A search dialog box is displayed.

   For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.
   For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.
   For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.
7. Type your search term.

   Or
   Select a predefined search term from the drop-down list.
   Or
   Select a date range.
   You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.
   However, you cannot remove the **Date/Time** filter.
8. Click the **Search** icon. A filtered audit trail list is displayed.

5. 29. 7. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

5. 29. 8. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic System Auditor Purging* for more information.

To purge the system auditor, perform the following steps:

9. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
10. Click **Purge**. The **Purge system auditor** dialog box is displayed.

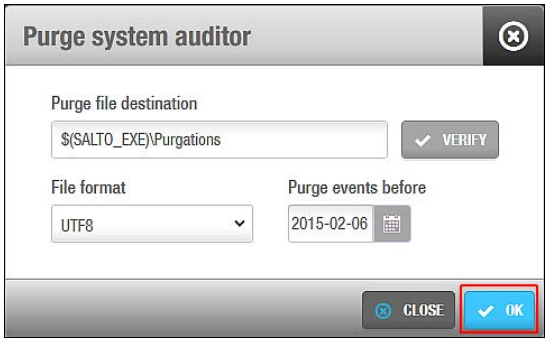


Figure 230: Purge system auditor dialog box

11. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
12. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
13. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
14. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
15. Click **OK**.

5. 30. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

5. 30. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

16. Select **System** > **Operators**. The **Operators** screen is displayed.

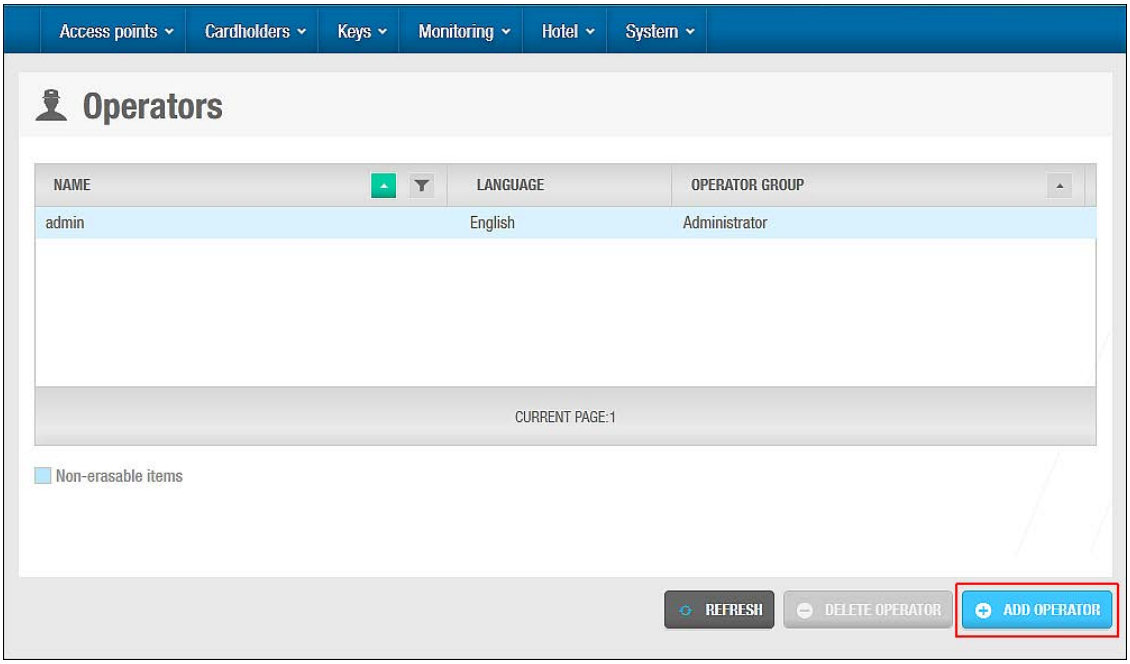


Figure 231: Operators screen

17. Click **Add Operator**. The **Operator** information screen is displayed.

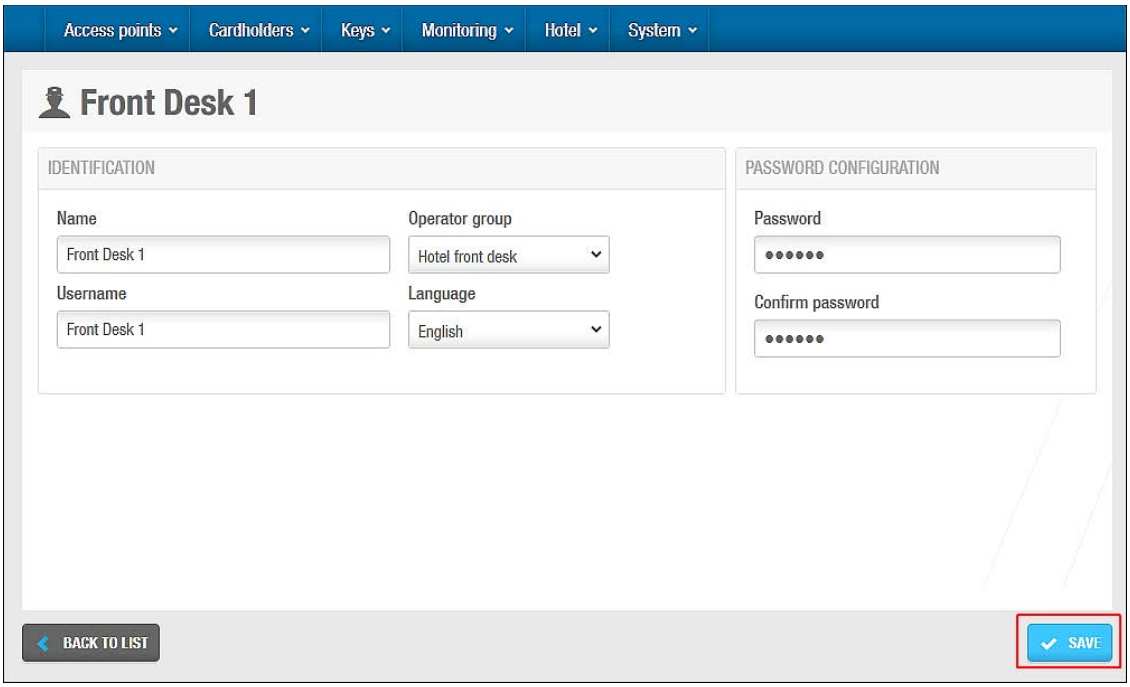


Figure 232: Operator information screen

18. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

19. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

    A maximum of 64 characters can be entered. The user name is not case sensitive.

20. Select the appropriate operator group from the **Operator group** drop-down list.
21. Select the display language for the operator in the **Language** drop-down list.

22. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.

23. Confirm the password.
24. Click **Save**.

5. 31. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

5. 31. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

25. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

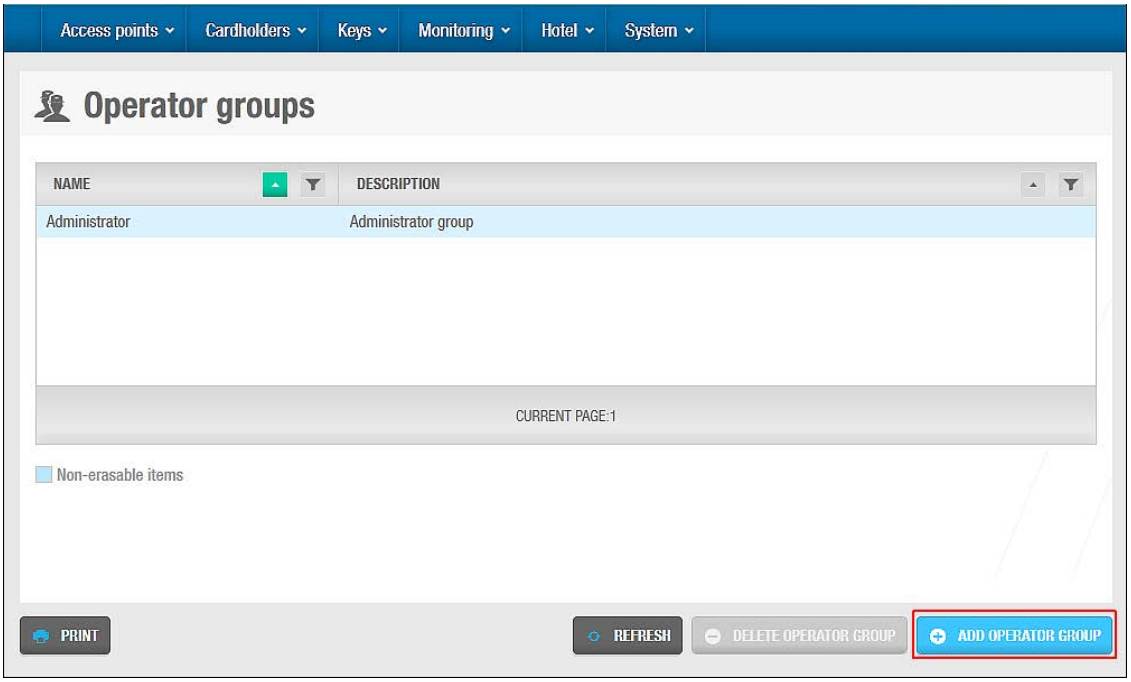


Figure 233: Operator groups screen

26. Click **Add Operator Group**. The **Operator group** information screen is displayed.

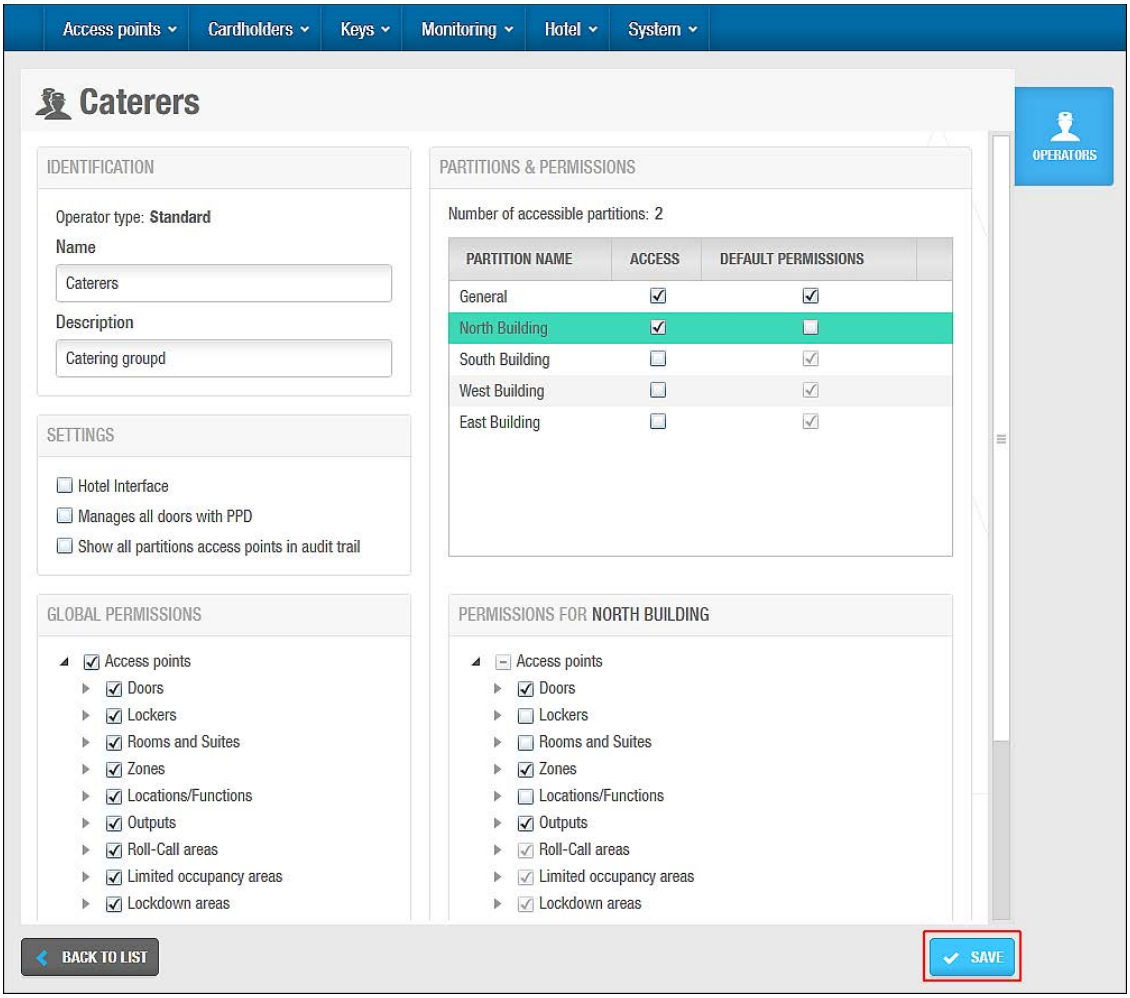


Figure 234: Operator group information screen

27. Type the name of the operator group in the **Name** field.
28. Type a description for the group in the **Description** field.
29. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.
30. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.
31. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes

in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.

32. Click **Save**.

5. 31. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

5. 31. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level **Monitoring** checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors

Permission	Description
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas

Permission	Description
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

5. 31. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

33. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
34. Double-click the operator group with the operator list you want to view.
35. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

    Partitions for more information.
36. Click **Add**. The **Access point timed periods** panel is displayed.
37. Type a start time for the timed period in the **From** field.
38. Type an end time for the timed period in the **To** field.
39. Click the applicable days in the **Days** panel.

    In addition to the days of the week, you can also create timed periods for holidays (H1) and special days (S1 and S2). You can create up to eight different periods for each timed period by clicking **Add**. See *PPD*

PPDs are connected to the operator's local PC through either a USB or COM port. See *PPD Settings* for more information. PPDs allow data to be transferred between the operator's PC and the locks. Data is downloaded from the PC to the PPD, and the PPD is used to perform tasks such as lock initialization and emergency openings. In the process, the PPD retrieves information (such as battery status) from the locks. This information is communicated to the system when the PPD is connected to the operator's PC.

See the *Portable Programming Device by SALTO* document for more information about PPDs and their configuration settings.

Table 56: PPD

 Portable Programming Device (PPD)	Used by admin operators to transfer configuration changes to a lock or by maintenance operators to check the battery status of the lock and collect the lock's audit trail

NOTE: It is important that the time is set correctly for the PC on which the SALTO software is running, as this controls the time and date settings for locks.

5. 31. 3. Peripheral Types

The functionality of the PPD is described in the following table.

Table 57: Peripheral types

Peripheral	Functionality
PPD	Communicates information to the locks such as door identification and configuration details. The operator downloads the information from their PC to the PPD and the PPD can then be connected to the lock. In this way, information is transferred to the lock. PPDs are used to: ▪ Update configuration changes to the lock (door profile,

	calendars etc.) ▪ Manually retrieve the audit trail stored on the lock for uploading to the server ▪ Perform a firmware diagnostic evaluation of the locking electronic components ▪ Upgrade the firmware of the locking components ▪ Open a door in the event of an emergency ▪ Read the battery status of the lock ▪ Perform a general diagnostic evaluation of the system

PPDs are configured in ProAccess SPACE General options. See *Devices Tab* for more information. The **PPD** information screen in ProAccess SPACE is used to download access point data to PPDs. This allows you to perform tasks with PPDs such as initializing and updating locks. You can also view the status of PPDs and update their firmware by using the **PPD** information screen.

5. 31. 4. PPD Menu Options

PPDs have seven menu options. Some of the menu options are available by default. Others are enabled when you select particular options on the **PPD** information screen in ProAccess SPACE, and download access point data to the PPD. See the *Portable Programming Device by SALTO* document for more information about using PPDs.

The options are described in the following table.

Table 58: PPD menu options

Option	Description
Update locks	Used to update a lock when the PPD is connected to it. To enable this menu option, you must download the appropriate access point data to the PPD by using the **PPD** information screen.
Firmware diagnostic	Used to perform a firmware diagnostic of the locking electronic components
Update firmware	Used to update the firmware of the locking electronic components
Collect audit trail	Used to collect audit trail data from offline doors and transfer it to the operator's local PC
Emergency opening	Used to perform an emergency opening if the lock battery dies or a reader error occurs. To enable this menu option, you must select the **Allow emergency opening** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. Alternatively, you can set this as a default option in ProAccess SPACE General options. You can also set a password for performing emergency openings using the PPD if required. See *Performing Emergency Door Openings* and *Devices Tab* for more information.
Initialize lock	Used to transfer access data to new locks or existing locks that have been fitted on a different access point and renamed. To enable this menu option, you must select the **Initialize locks** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. See *Initializing Locks* for more information.
Diagnostic	Used to retrieve information from the lock such as the battery status or serial number

5. 31. 5. Viewing PPD Status

You can view the status of a PPD you have connected to the PC by selecting **System** > **PPD**.

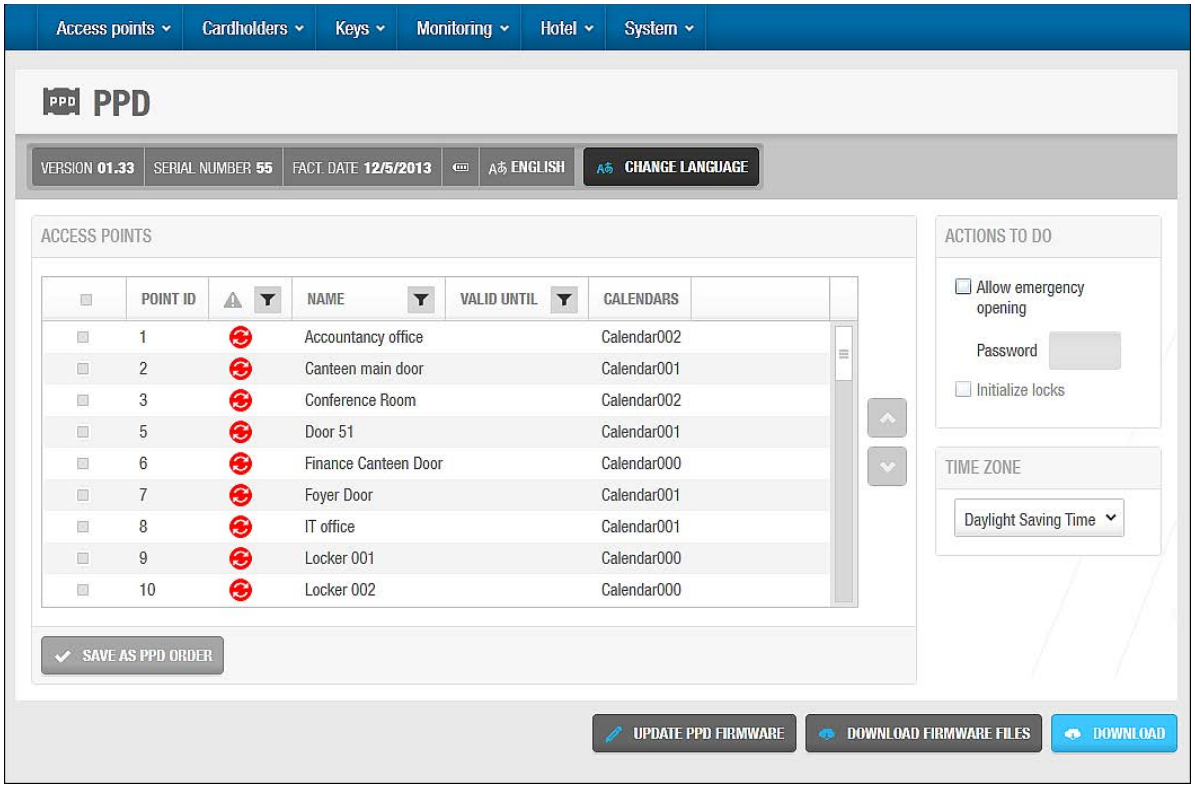


Figure 238: PPD information screen

The **PPD** information screen shows the following information about the PPD:

- Version
- Serial number
- Factory date (or date of manufacture)
- Battery status
- Language

5. 31. 6. Changing the PPD Language

You can change the language of the display messages in the PPDs if required.

To change the language displayed in a PPD, perform the following steps:

40. Connect the PPD to the PC.
41. Select **System** > **PPD**. The **PPD** information screen is displayed.
42. Click **Change Language**. The **Change language** dialog box is displayed.

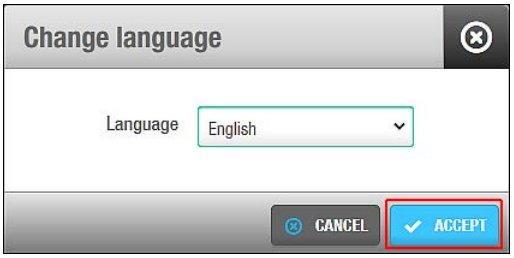


Figure 239: Change language dialog box

43. Select the required language from the **Language** drop-down list.
44. Click **Accept**. The **PPD** progress screen is displayed.
45. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
46. Click **OK**.

5. 31. 7. Using the PPD Information Screen

The **PPD** information screen displays a list of access points. This list varies depending on which time zone is selected in the **Time Zone** panel. It is important to remember that only access points for the selected time zone are displayed. Note that you must enable the multiple time zones functionality in ProAccess SPACE General options to display this panel in ProAccess SPACE. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Access points that need to be updated have a red **Update required** icon on the left-hand side of their name. You can download access point data to a PPD you have connected to the PC by selecting the required access points and clicking **Download**. You can then perform tasks such as updating locks with the PPD. See *Updating Locks* for more information. You must select additional options in the **Actions To Do** panel for certain tasks, for example, initializing locks. See *Initializing Locks* and *Performing Emergency Door Openings* for more information about this panel.

The following table describes some useful screen items.

Table 59: PPD information screen items

Item	Description
Access point checkboxes	Allow you to select individual access points
Checkbox column header	Allows you to select all of the displayed access points. To do so, select the checkbox in the column header.
Chevrons	Allow you to move entries up and down in the access point list
Save As PPD Order button	Allows you to save the access point list order. This specifies the order in which access point data is downloaded to the PPD and displayed in the PPD's menu.
Expand icon	Allows you to view the ESDs for rooms and suites. This icon is displayed on the left-hand side of the room and suite names.

5. 31. 8. Updating PPD Firmware

Firmware is software that is programmed on the read-only memory (ROM) of hardware devices. Firmware updates are available when a new version of the SALTO software is downloaded. Your SALTO technical support contact may also recommend specific firmware updates if required.

To update the firmware of a PPD, perform the following steps:

47. Connect the PPD to the PC.
48. Select **System** > **PPD**. The **PPD** information screen is displayed.

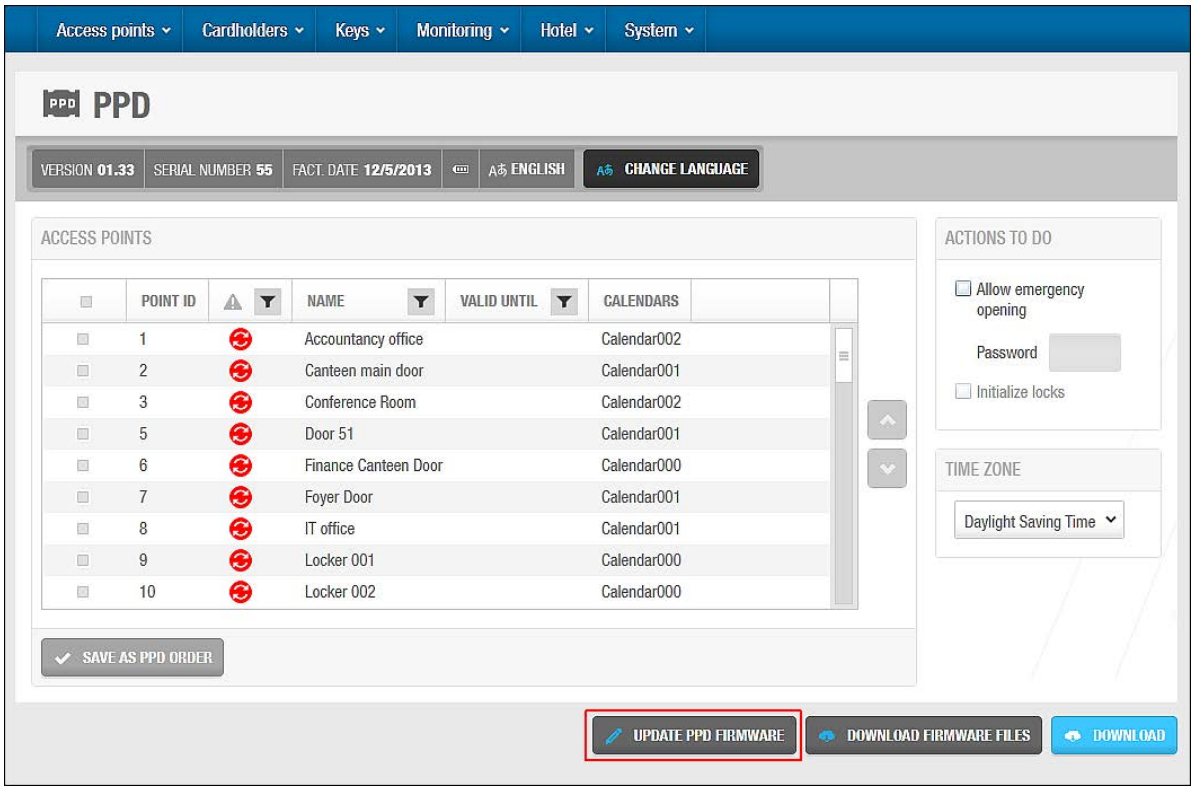


Figure 240: PPD information screen

49. Click **Update PPD Firmware**. The **Update PPD Firmware** dialog box, showing the available firmware files, is displayed.

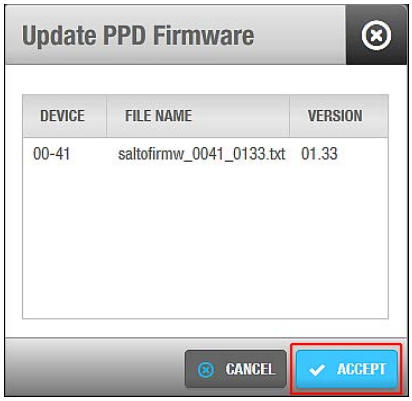


Figure 241: Update PPD Firmware dialog box

50. Select the required file.
51. Click **Accept**. The **PPD** progress screen is displayed.
52. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
53. Click **OK**.

5. 31. 9. Downloading Firmware Files

You can download firmware files to the PPD and use it to update the locking electronic components.

To download a firmware file to a PPD, perform the following steps:

54. Connect the PPD to the PC.
55. Select **System** > **PPD**. The **PPD** information screen is displayed.

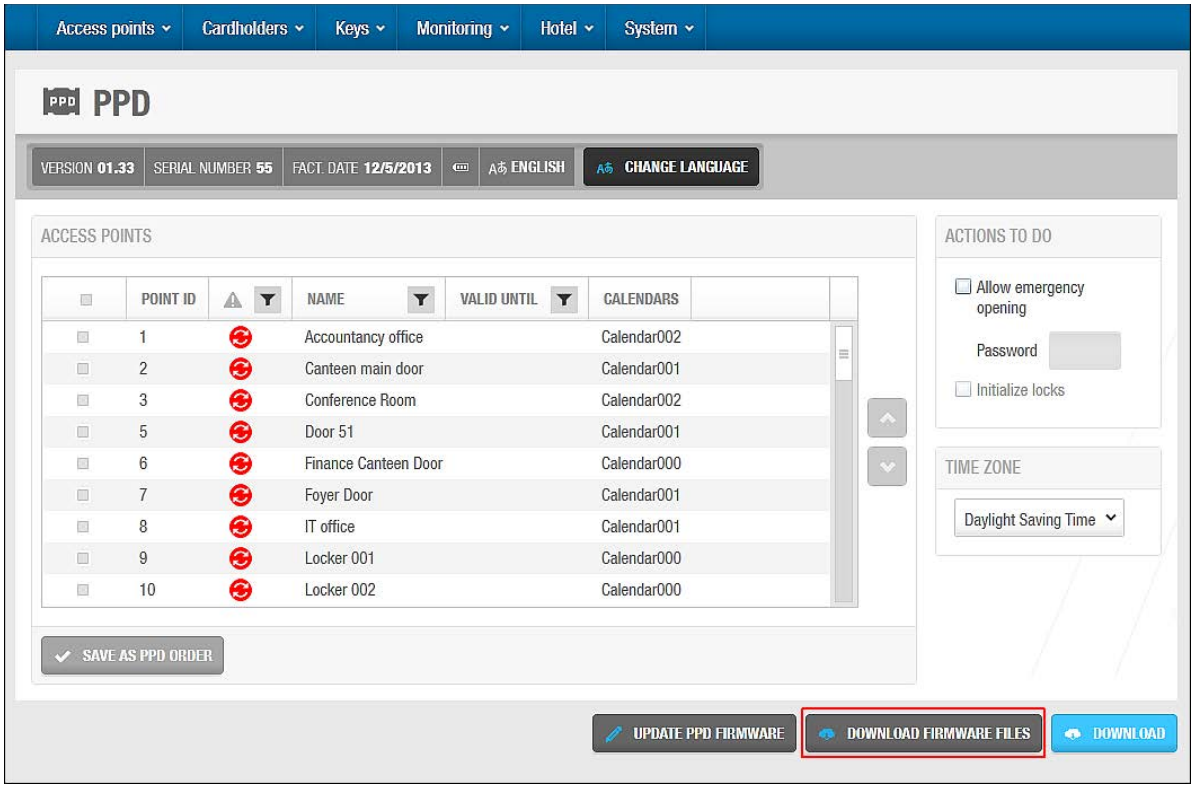


Figure 242: PPD information screen

56. Click **Download Firmware Files**. The **Download Firmware files** dialog box, showing the available firmware files, is displayed.

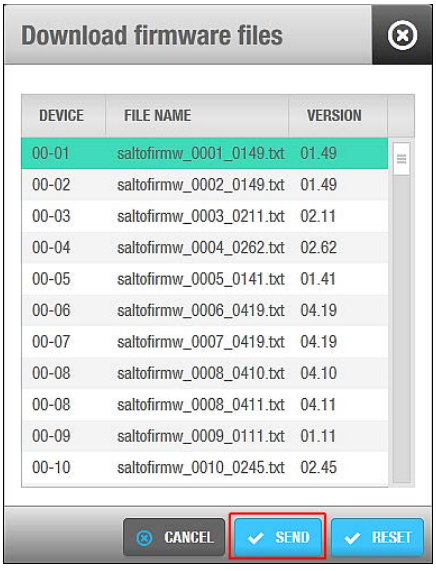


Figure 243: Download firmware files dialog box

57. Select the required file.

    You can hold down the Ctrl key while clicking the files to make multiple selections. Note that you can click **Reset** to delete any firmware files you have already downloaded.

58. Click **Send**. The **PPD** progress screen is displayed.
59. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
60. Click **OK**.

    You can now use the PPD to update the firmware of locking electronic components by selecting **Update Firmware** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

5. 31. 10. Initializing Locks

You must initialize each lock when it is installed. This programmes the lock, and transfers access point data relating to time zones and calendars, for example.

It is recommended that you connect the PPD to the PC after you initialize locks to communicate the most up-to-date information about the locks to the system.

NOTE: You can configure PPDs to assign IP addresses to online IP (CU5000) doors during initialization if required. You must enter each IP address on the system by using the **Access point: Online IP CU5000** information screen. Note that you must select **System** > **SALTO Network** and double-click the required online IP (CU5000) door on the **SALTO Network** screen to view the information screen. You must enable this option in ProAccess SPACE General options by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

PPDs can also be used to transfer SAM data to SALTO locks and wall readers during initialization (or when you perform updates). See *SAM and Issuing options General* options

See *General options* section.

SAM and Issuing Data for more information.

To initialize a lock, perform the following steps:

61. Connect the PPD to the PC.
62. Select **System** > **PPD**. The **PPD** information screen is displayed.

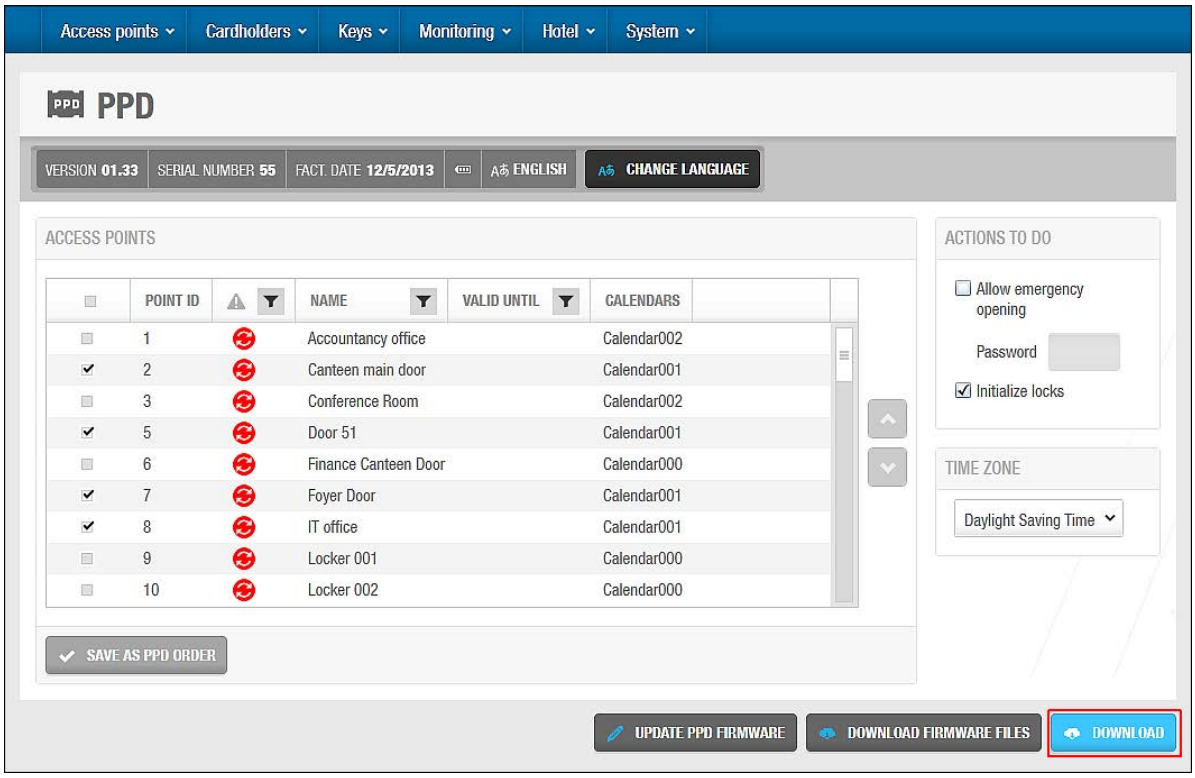


Figure 244: PPD information screen

63. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

64. Select the checkbox of the access point for which you want to initialize the lock.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

65. Select the **Initialize locks** checkbox in the **Actions To Do** panel.
66. Click **Download**. The **PPD** progress screen is displayed.
67. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.

    You can now use the PPD to initialize the lock of the selected access point by selecting **Initialize Lock** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: If you initialize a lock that is already in use, its audit trail is deleted.

5. 31. 11. Initializing Rooms and ESDs

The procedure for initializing rooms and ESDs is the same as for initializing locks. See *Initializing Locks* for more information and a description of the steps you should follow.

NOTE: You can initialize rooms and their associated ESDs either together or separately. However, all of the rooms and ESDs that you select during the initialization process must have the same calendar.

5. 31. 12. Updating Locks

You must update offline locks when you make certain changes to access point data, such as enabling anti-passback or changing the opening mode of doors. You can view locks that need to be updated on the **PPD** information screen by selecting **System** > **PPD**. Note that you must connect a PPD to the PC before you can access the **PPD** information screen. Access points that need to be updated have a red **Update required** icon on the left-hand side of their name.

It is recommended to update offline locks at least every six months to ensure that the clock and calendars are up to date. You must also update locks after you replace their batteries. This is because access point data relating to time zones and calendars, for example, must be restored after a lock's battery dies.

You should connect the PPD to the PC after you update locks to communicate the most up-to-date information about the locks to the system.

To update a lock, perform the following steps:

68. Connect the PPD to the PC.
69. Select **System** > **PPD**. The **PPD** information screen is displayed.

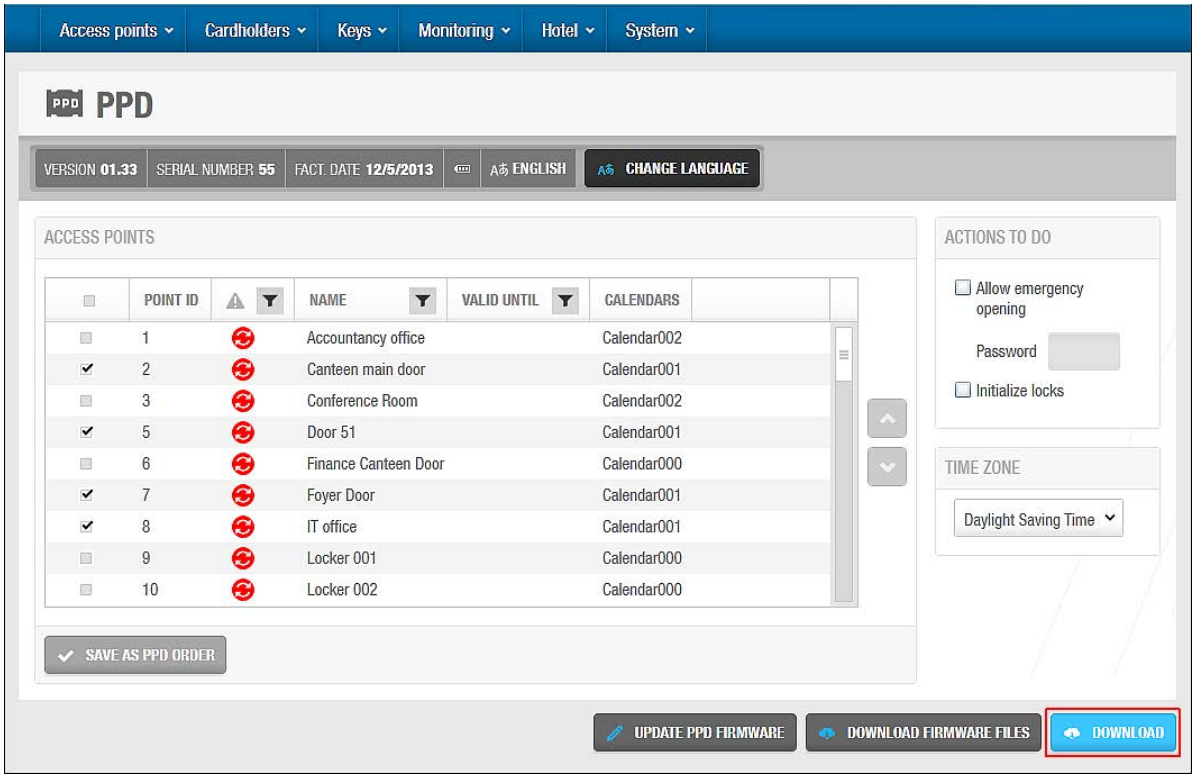


Figure 245: PPD information screen

70. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have

enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

71. Select the checkbox of the access point for which you want to update the lock.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.
72. Click **Download**. The **PPD** progress screen is displayed.
73. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
74. Click **OK**.

    You can now use the PPD to update the lock of the selected access point by selecting **Update Locks** in the PPD's menu and connecting the PPD to the lock. Alternatively, you can simply connect the PPD to the lock. In this case, it recognizes the lock and automatically displays the appropriate data. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: You can configure PPDs to automatically collect audit trail data when they are used to update locks. You must enable this option in ProAccess SPACE General options by selecting the **Collect audit trails automatically when updating locks** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

5. 31. 13. Performing Emergency Door Openings

You can use the PPD to perform an emergency opening if the lock battery dies or a reader error occurs, for example.

NOTE: You can perform emergency openings of online doors without using a PPD. See *Lockdown* for more information.

To perform an emergency opening, perform the following steps:

75. Connect the PPD to the PC.
76. Select **System** > **PPD**. The **PPD** information screen is displayed.

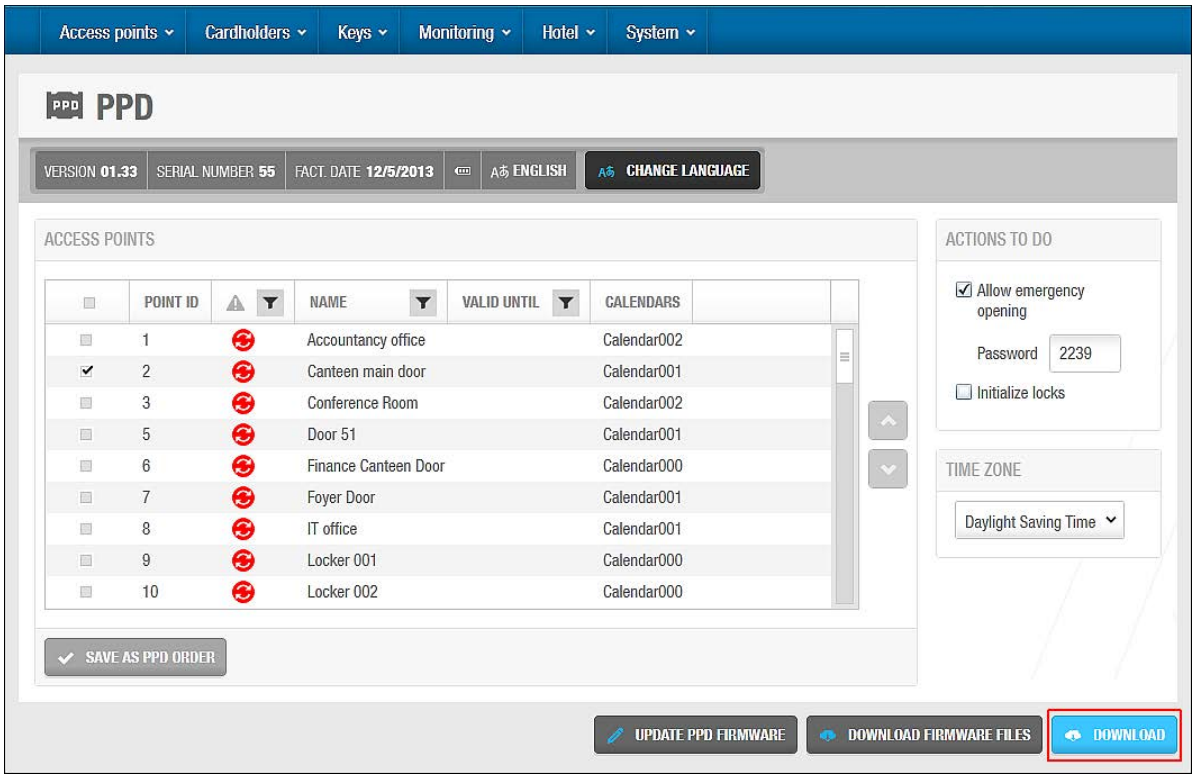


Figure 246: PPD information screen

77. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

78. Select the checkbox of the access point for which you want to perform the emergency opening.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

79. Select the **Allow emergency opening** checkbox in the **Actions To Do** panel.

    The checkbox is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options. See *PPD Tab* for more information. Otherwise, you must select it each time you want to perform an emergency opening.

80. Type a password for the emergency opening in the **Password** field if required.

    The password can only contain digits. If you type a password, you must enter this password in the PPD before you can perform the emergency opening. Otherwise, the PPD does not require a password. The **Password** field is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options and entered a password there already for the option. See *Devices Tab* for more information. Your PPD firmware must be version 01.29 or higher to use this option.

81. Click **Download**. The **PPD** progress screen is displayed.

82. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
83. Click **OK**.

    You can now use the PPD to perform an emergency opening of the selected access point by selecting **Emergency Opening** in the PPD's menu and connecting the PPD to the lock. Note that you are required to enter a password in the PPD if you have enabled this option in either ProAccess SPACE PPD window or ProAccess SPACE Devices window. See the *Portable Programming Device by SALTO* document for more information about this process.

5. 31. 14. Collecting Audit Trail Data from Offline Doors

See *Audit Trails* for more information about audit trails. You must use a PPD to collect audit trail data from offline doors. See the *Portable Programming Device by SALTO* document for more information about this process. When you have collected the data, you can view it in ProAccess SPACE.

To view the audit trail data on the system, perform the following steps:

84. Connect the PPD to the PC.
85. Select **System** > **PPD**. The **PPD** information screen is displayed.

    The **Audit Trail** information screen is automatically updated with the information from the connected PPD when you display the **PPD** information screen.
86. Select **Monitoring** > **Audit Trail**. The **Audit trail** information screen, showing the new audit trail data, is displayed.

5. 32. SALTO Network

The SALTO network includes items like encoders, gateways, radio frequency (RF) nodes, CU4200 nodes, online doors, and CUs. These are added and managed in ProAccess SPACE. See *SALTO Virtual Network* for more information about the SALTO network.

The RF and CU4200 functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

NOTE: You can view the enabled channels for RF signals in ProAccess SPACE General options. To do so, select **System** > **General options** > **Devices**. There are 16 channels available and all of these are enabled by default. The frequency range of each channel is also displayed. You can disable a channel if required by clearing the checkbox for the channel and clicking **Save**.

RF mode 2 technology is compatible with ProAccess SPACE. However, RF mode 1 technology is not. If your site uses RF mode 1, an upgrade to ProAccess SPACE is not possible, which means that you must continue to use HAMS or ProAccess RW.

You can view the list of SALTO network items by selecting **System** > **SALTO Network**.

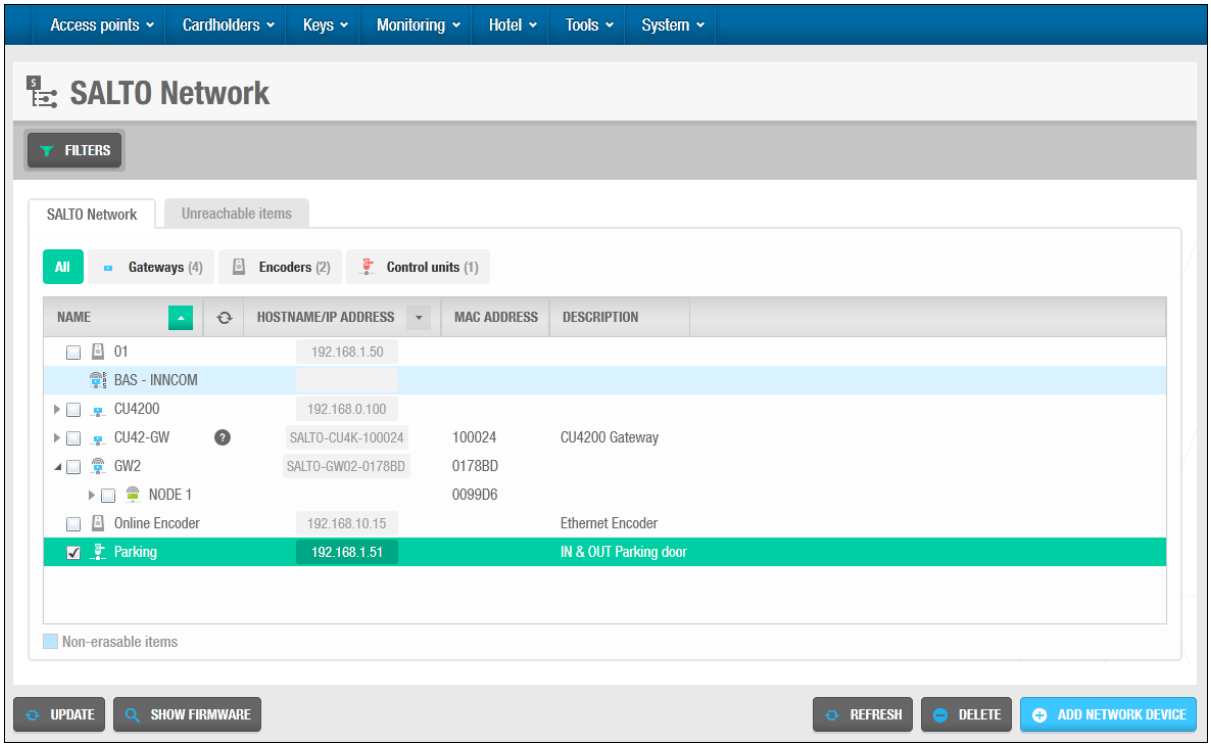


Figure 247: SALTO Network screen

The **SALTO Network** screen displays a list of all network items that have been added and are currently connected to the system.

The information is displayed in four different filtered views:

- **All**: This view shows all of the gateways, encoders, and CUs on the system.
- **Gateways**: This view shows RF gateways and CU4200 gateways. When you click the triangular **Expand** icon on the left-hand side of gateway names, all of the items to which they are connected are displayed. You can view all of the RF nodes and online RF (SALTO) access points connected to each RF gateway, and all of the CU4200 nodes and online IP (CU4200) access points connected to each CU4200 gateway. See *Configuring Online Connection Types* for more information.

NOTE: A BAS gateway may also be displayed on the **SALTO Network** screen. This gateway is created by default if you have fully configured your BAS integration in ProAccess SPACE General options. See *BAS Integration Tab* for more information.

- **Encoders**: This view shows the encoders on the system.
- **Control units**: This view shows online IP (CU5000) access points. See *Configuring Online Connection Types* for more information.

Click the appropriate tab to display each filtered view. The screen also includes an **Unreachable items** tab. Click on this tab to view and configure all items that require additional connection information.

The following table describes the buttons use on the SALTO network main screen.

Table 60: SALTO Network main screen buttons

Item	Description

Item	Description
Update	Allows you to update the selected access point.
Show firmware	Allows you to show the firmware of the selected access point and update it.
Refresh	Allows you to refresh the window with the most updated peripherals status.
Delete	Allows you to delete the selected peripheral.
Add Network device	Allows you to add a new online device.

5. 32. 1. Adding Network Devices

You can add the following network devices to the system:

- Ethernet encoders
- RF gateways
- RF nodes
- CU42E0 gateways
- CU4200 nodes

The following sections describe how to add these devices.

5. 32. 1. 1. Adding Ethernet Encoders

See *Encoders* for more information about encoders.

To add an Ethernet encoder, perform the following steps:

87. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
88. Click **Add Network Device**. The **Add network device** dialog box is displayed.
89. Select **Encoder** from the drop-down list.
90. Click **OK**. The **Encoder** information screen is displayed.

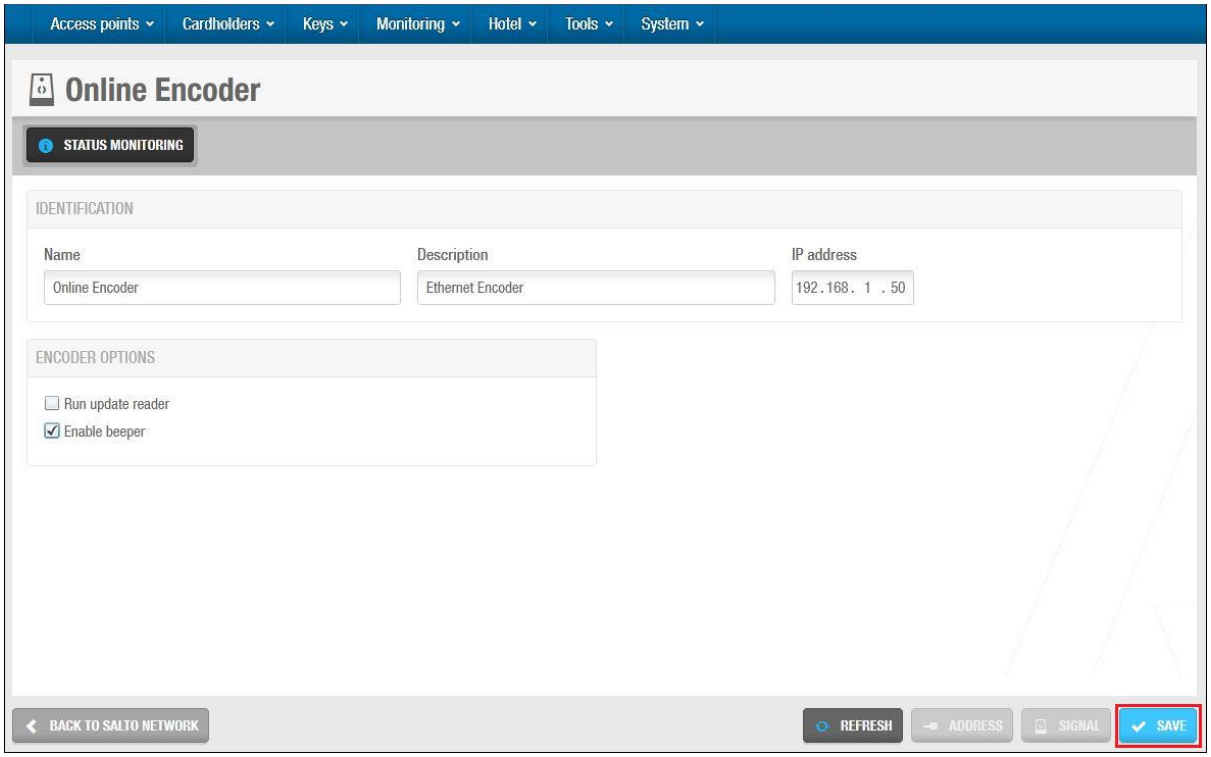


Figure 248: Encoder information screen

91. Type a name for the encoder in the **Name** field.
92. Type a description for the encoder in the **Description** field.
93. Type an IP address for the encoder in the **IP address** field.
94. Select the **Run update reader** checkbox if required.

    This option is used to configure an Ethernet encoder to update user keys automatically when users present their keys to it. If you select this option, the encoder runs continuously but it can only update keys. It cannot be used to encode keys with access data from the SALTO software. See *Updating Keys* for more information.
95. Select the **Enable beeper** checkbox if required.

    If you select this option, the encoder emits beeps when in use.
96. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Click **Save**.

5. 32. 1. 2. Adding RF Gateways

Gateways are hardware devices that provide a link between networks that use different base protocols. RF gateways allow data to be transmitted from the system to the SALTO RF locks, and from the RF locks to the system. RF gateways control RF nodes. See *Adding RF Nodes* for more information about RF nodes.

You must physically connect RF nodes to an RF gateway using an RS485 cable to establish communication between the RF nodes and the RF gateway. See the *SALTO Datasheet_Gatewayx2_xxx* document for more information about this process. You must also connect RF nodes and RF gateways in ProAccess SPACE so the system can show which nodes and gateways are connected.

To add an RF gateway, perform the following steps:

97. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
98. Click **Add Network Device**. The **Add network device** dialog box is displayed.
99. Select **RF gateway** from the drop-down list.
100. Click **OK**. The **RF gateway** information screen is displayed.

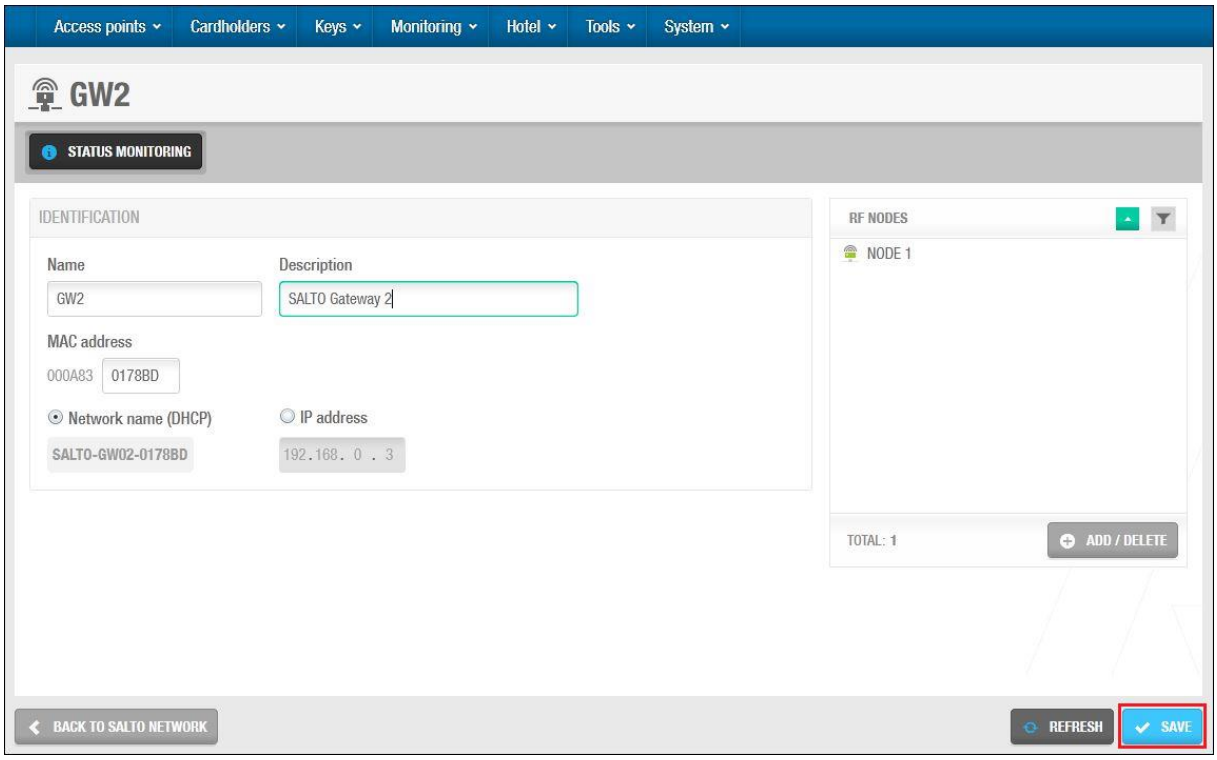


Figure 249: RF gateway information screen

101. Type a name for the RF gateway in the **Name** field.
102. Type a description for the RF gateway in the **Description** field.
103. Type the media access control (MAC) address in the **MAC address** field.

    This is usually displayed on the Ethernet board of the RF gateway.

104. Select either the **Network name (DHCP)** or **IP address** option.

    If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the RF gateway. A Dynamic Host Configuration Protocol (DHCP) server and a DNS are required for this option. If you select the **IP address** option, you must type a static IP address in the field.

105. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

106. Click **Add/Delete** in the **RF Nodes** panel. The **Add/Delete** dialog box, showing a list of RF nodes, is displayed.

    The **Add/Delete** dialog box only displays RF nodes if you have already added them to the system. You can also connect RF nodes to RF gateways when you add RF nodes to the system. See *Adding RF Nodes* for more information.

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

    You can hold down the Ctrl key while clicking the RF nodes to make multiple selections. You cannot add RF nodes that already belong to another gateway.

108. Click **Accept**. The selected RF node is displayed in the **RF Nodes** panel.
109. Click **Save**.

5. 32. 1. 3. Adding RF Nodes

RF nodes are network connection points that are physically connected to an RF gateway using an RS485 cable. See *Adding RF Gateways* for more information. This establishes communication between the RF nodes and the RF gateways. Also, in ProAccess SPACE you must connect RF nodes to RF gateways, and RF access points to RF nodes. This means that the system can show which items are connected.

NOTE: You must select **Online RF (SALTO)** in the **Connection Type** panel on the **Door** or **Room** information screen to define a door as an RF access point.

To add an RF node, perform the following steps:

110. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
111. Click **Add Network Device**. The **Add network device** dialog box is displayed.
112. Select **RF node** from the drop-down list.
113. Click **OK**. The **RF node** information screen is displayed.

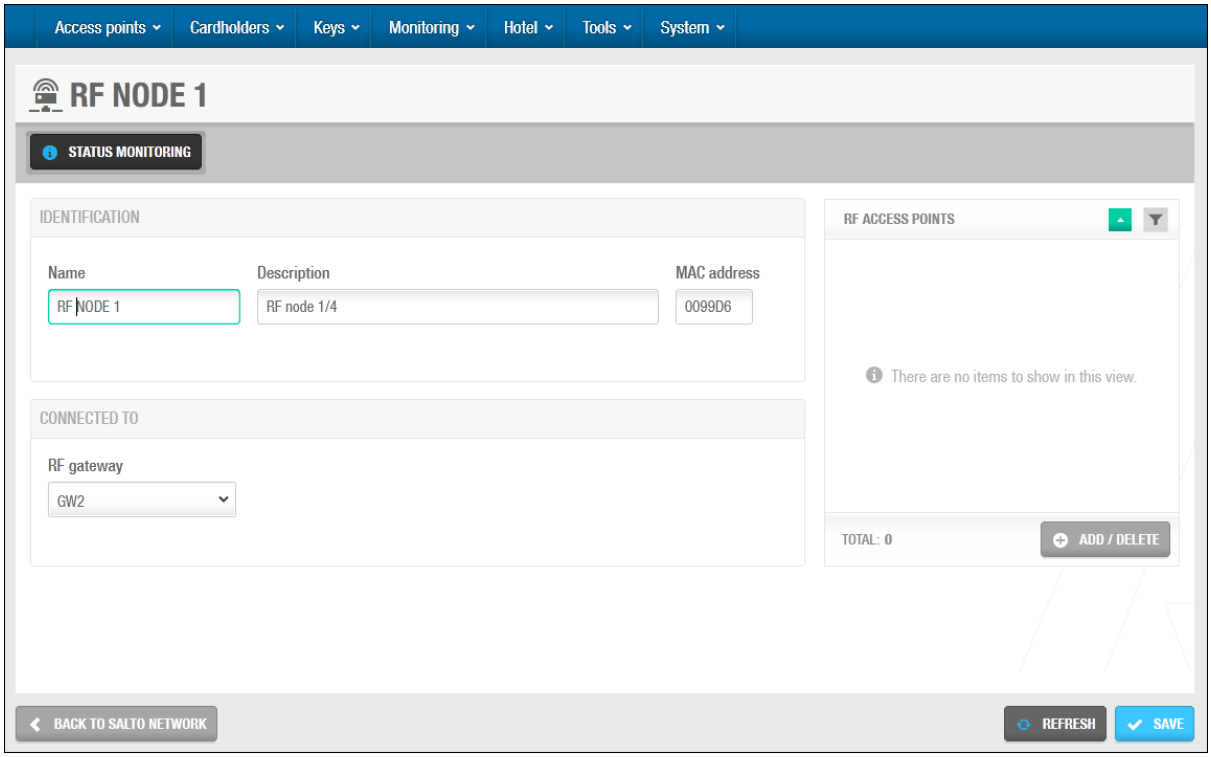


Figure 250: RF node information screen

114. Type a name for the RF node in the **Name** field.
115. Type a description for the RF node in the **Description** field.
116. Type the MAC address of the antenna in the **MAC address** field.
117. Select the RF gateway to which you want to connect the RF node from the **Connected to** drop-down list.

    The default option is **None**.
118. Click **Add/Delete** in the **RF Access Points** panel. The **Add/Delete** dialog box, showing a list of RF access points, is displayed.

    The **Add/Delete** dialog box only displays RF access points if you have already defined doors as RF access points by selecting **Online RF (SALTO)** in the **Connection Type** panel on the **Door** or **Room** information screens. You can also connect online RF

(SALTO) doors to RF nodes by using the **Connected to** field on the **Online RF (SALTO)** information screen. See *Online RF (SALTO)* for more information.

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

    You can hold down the Ctrl key while clicking the RF access points to make multiple selections. You cannot add RF access points that already belong to another RF node.

120. Click **Accept**. The selected RF access point is displayed in the **RF Access Points** panel.
121. Click **Save**.

NOTE: RF gateways have a mini node connected to them. You must add this node in ProAccess SPACE by following the procedure for adding RF nodes. Also, you must connect the mini node to the RF gateway in ProAccess SPACE.

5. 32. 1. 4. Adding CU42E0 Gateways

CU42E0 gateways are CUs that are connected to a local area network (LAN) using a network cable. They connect to the SALTO network using a TCP/IP connection. CU42E0 gateways can control CU4200 nodes. See *Adding CU4200 Nodes* section below for more information about CU4200 nodes.

The CU42E0 gateways provide a link between the CU4200 nodes and the SALTO system, and transmit data to the nodes. This means the CU4200 nodes do not require a TCP/IP connection. You must physically connect CU4200 nodes to a CU42E0 gateway using an RS485 cable. This establishes communication between the CU4200 nodes and the CU42E0 gateway. You must also link CU42E0 gateways and CU4200 nodes in ProAccess SPACE so the system can show which nodes and gateways are connected.

CU42E0 gateways control access to doors by activating their relays. Each CU42E0 gateway can control a maximum of two doors. They can also update user keys.

The CU42E0 supports up to 4 auxiliary CU4200 nodes, meaning this that up to 10 online doors can be controlled using a single IP address (1 CU42E0 gateways + 4 CU4200 nodes)

In stand-alone mode, dipswitches on the CU4200 node units must be set up to 0000, if online, each node should have its own configured address, using the suitable dipswitch combination in binary format. See the CU42X0 installation guide for more details. See image below for an example.

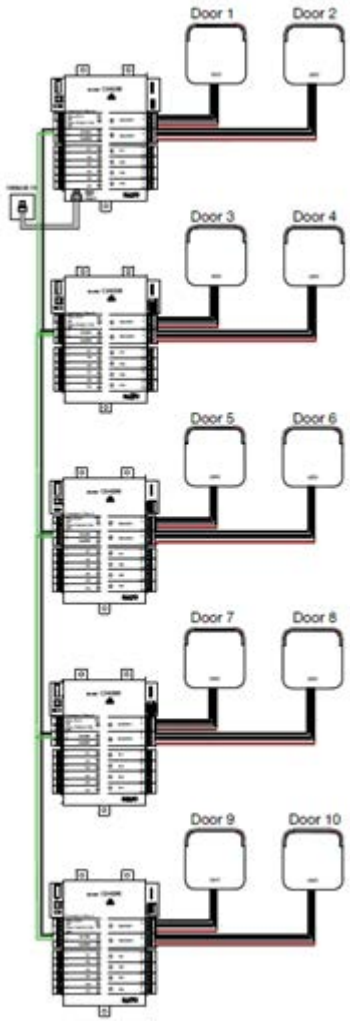


Figure 251: CU42E0 and CU4200 example

NOTE: The maximum distance between the gateway (CU42E0) and the last node (CU4200) in line cannot be over 300 meters.

To add a CU42E0 gateway, perform the following steps:

122. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
123. Click **Add Network Device**. The **Add network device** dialog box is displayed.
124. Select **CU42E0 gateway** from the drop-down list.
125. Click **OK**. The **CU42E0 gateway** information screen is displayed.

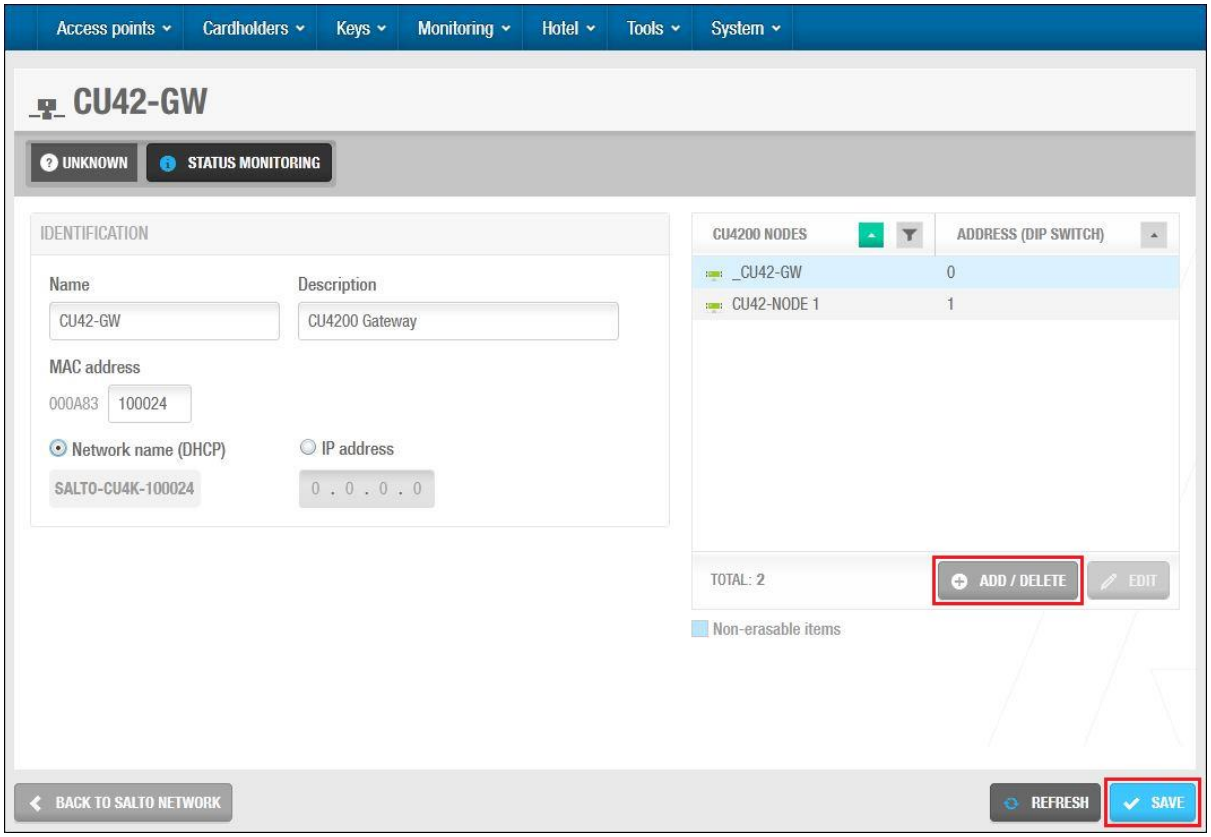


Figure 252: CU4200 gateway information screen

126. Type a name for the CU42E0 gateway in the **Name** field.
127. Type a description for the CU42E0 gateway in the **Description** field.
128. Type the MAC address in the **MAC address** field.

    The MAC address is displayed on a sticker on the CU.

129. Select either the **Network name (DHCP)** or **IP address** radio button.

    If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the CU42E0 gateway. A DHCP server and a DNS are required for this option. If you select the **IP address** option, you must type an IP address in the field.

130. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

131. Click **Add/Delete** in the **CU4200 Node** panel. The **Add/Delete** dialog box, showing a list of CU4200 nodes, is displayed.

    The **Add/Delete** dialog box only displays CU4200 nodes if you have already added them to the system. You can also connect CU4200 nodes to CU42E0 gateways when you add CU4200 nodes to the system. See *Adding CU4200 Nodes* for more information.

132. Select the required CU4200 node in the left-hand panel and click the chevron. The selected CU4200 node is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the CU4200 nodes to make multiple selections. You cannot add CU4200 nodes that already belong to another CU4200 gateway.

NOTE: When you add a CU42E0 gateway, an embedded CU4200 node is automatically created. This cannot be deleted. Each CU42E0 gateway can support its embedded CU4200 node and a maximum of four other CU4200 nodes. The name of the embedded node will be always the same than the parent CU42E0 gateway preceeded by an underscore. For example: **_CU4200.**

133. Click **Accept**. The selected CU4200 node is displayed in the **CU4200 Node** panel.

    You can select the CU4200 node and click **Edit** to change the number in the **Address (dip switch)** column if required. See *Adding CU4200 Nodes* for more information about the **Address (dip switch)** field. Note that embedded CU4200 nodes have a fixed number (0). This cannot be changed.

134. Click **Save**.

5. 32. 1. 5. Adding CU4200 Nodes

CU4200 nodes are network connection points that are physically connected to a CU42E0 gateway using an RS485 cable. See *Adding CU42E0 Gateways* for more information about CU42E0 gateways. This establishes communication between the CU4200 nodes and the CU42E0 gateway.

The CU4200 nodes receive data from the CU42E0 gateway so they do not require a TCP/IP connection. Instead, they communicate with the SALTO network through the CU42E0 gateway to which they are connected.

You must connect CU4200 nodes to CU42E0 gateways in ProAccess SPACE. You must also connect CU4200 nodes to access points. This means that the system can show which items are connected. Each CU4200 node can control a maximum of two doors.

NOTE: You must select **Online IP (CU4200)** in the **Connection Type** panel on the **Door** and in **Room** information screen before you can connect an access point to a CU4200 node.

To add a CU4200 node, perform the following steps:

135. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
136. Click **Add Network Device**. The **Add network device** dialog box is displayed.
137. Select **CU4200 node** from the drop-down list.
138. Click **OK**. The **CU4200 node** information screen is displayed.

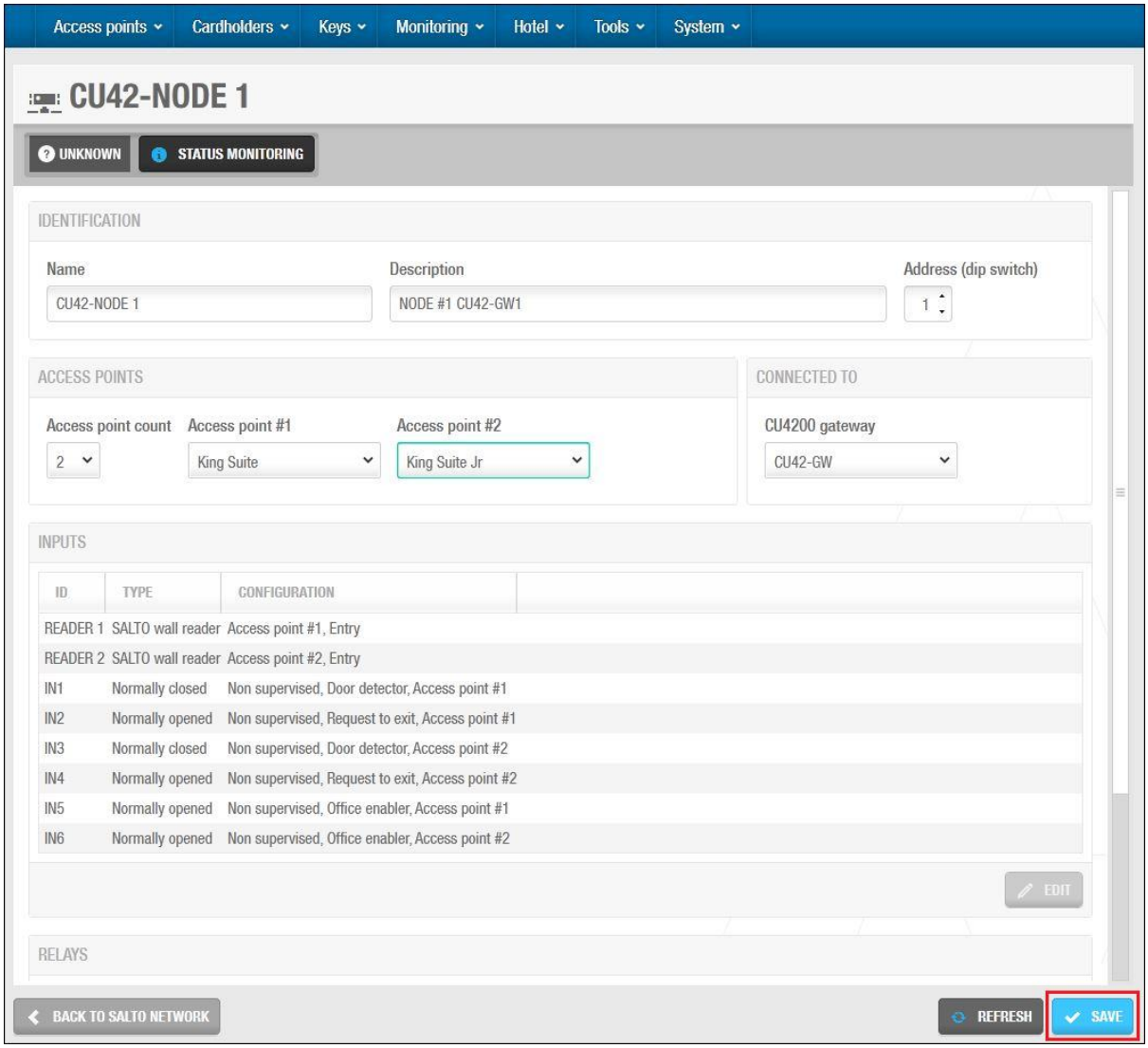


Figure 253: CU4200 node information screen

139. Type a name for the CU4200 node in the **Name** field.
140. Type a description for the CU4200 node in the **Description** field.
141. Select the required number by using the up and down arrows in the **Address (dip switch)** field.

    This number corresponds to the switches on the dip switch panel. The system allows you to select any number between 1 and 99. However, you must select a number between 1 and 15 due to hardware limitations. A CU42E0 gateway can support an embedded CU4200 node and a maximum of four other CU4200 nodes. Each CU4200 node that you connect to a specific CU42E0 gateway must have a unique number, for example, 1, 2, 3, until 15. Note that the value 0 is used for embedded CU4200 nodes. Bear in mind that addresses set up on the nodes should follow the physical dipswitches' configuration on each CU4200 unit.

Table 61: Dipswitch configuration

Dip switch	Address (dip switch)
0000	Address 0, only for embedded CU4200 nodes.
0001	Address 1

Dip switch	Address (dip switch)
0010	Address 2
0011	Address 3
0100	Address 4
0101	Address 5
0110	Address 6
0111	Address 7
1000	Address 8
1001	Address 9
1010	Address 10
1011	Address 11
1100	Address 12
1101	Address 13
1110	Address 14
1111	Address 15

See the following image as an example;

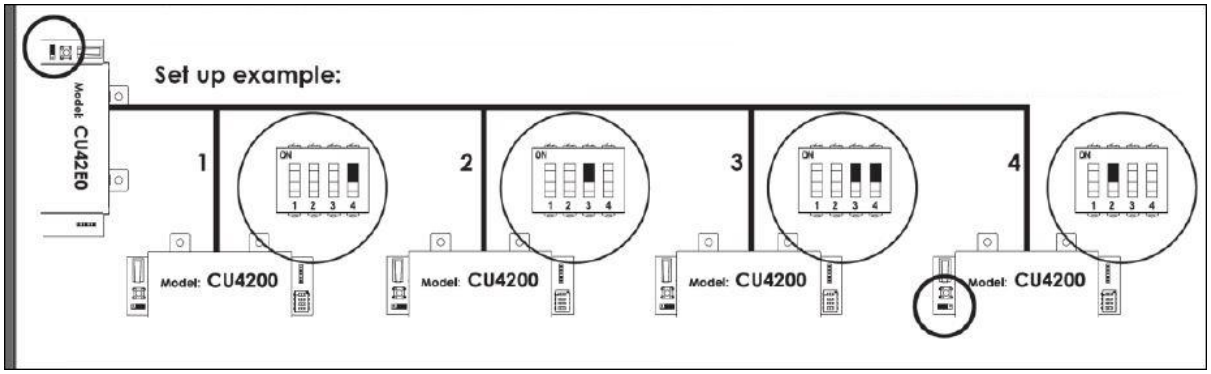


Figure 254: CU4200 dip switches set up

142. Select the required number from the **Access point count** drop-down list.

You can select either **1** or **2.** This defines the number of doors you want the CU4200 node to control. Each CU4200 node can control two readers. This means it can control either one door that has two readers or two doors where each has one reader. If a door has two readers, one reader controls access from inside to outside, and the other reader controls access from outside to inside. You should select **1** if a door has two readers. If you select **2,** an **Access point #2** field is displayed on the right-hand side of the **Access point #1** field, and you can select an additional door from the drop-down list.

143. Select the required door from the **Access point #1** drop-down list.

The **Access point** drop-down lists only display doors if you have already defined some as CU4200 access points. This is done by selecting **Online IP (CU4200)** in the **Connection Type** panel on the **Door** information screen. You can also connect online IP (CU4200) doors to CU4200 nodes in the **Connected to** field on the **Online IP (CU4200)** information screen. See *Online IP (CU4200)* for more information.

144. Select the CU42E0 gateway to which you want to connect the CU4200 node from the **Connected to** drop-down list.
145. Click **Save**.

5. 32. 1. 6. Using CU4200 Inputs

Inputs are the signals or data received by the CU4200. You can setup the inputs in ProAccess SPACE so the CU4200 can understand how to act. You can set Inputs for **Reader 1** and **Reader 2.** You can also set up to 6 inputs from third party devices.

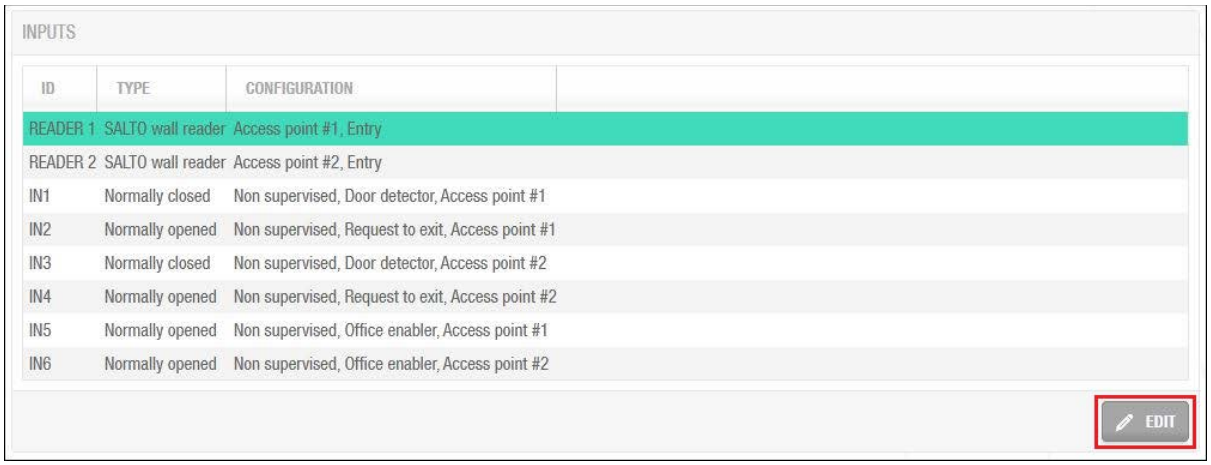


Figure 255: CU4200 node Inputs

You can set the CU4200 outputs according with the wall reader input. To manage the wall reader input, select the reader and click **Edit**.

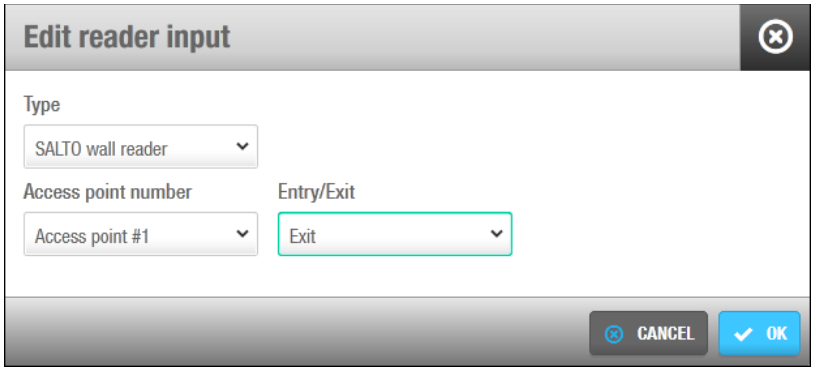


Figure 256: CU4200 node Reader Input

The **Reader input** fields are described in the following table.

Table 62: Reader Inputs fields

Field	Functionality
Type	You can select **None** if no SALTO wall reader is connected or **SALTO wall reader** if it is a SALTO wall reader. Other options may appear in the future. If **None** is selected, inputs 3, 4 and 5, 6 can be used with a third party wall reader.
Access point number	As the CU4200 can manage up to two different access points, you can decide whether the reader will trigger an opening in access point #1 or #2. See *Adding CU4200 Nodes* for more information.

Field	Functionality
Entry/Exit	Select whether the wall reader is an Entry or an Exit.

The CU4200 node can manage inputs from third party devices. Depending the signal or data arrived to the input the CU4200 Node can act accordingly. Select the **Input ID** and click **Edit**.

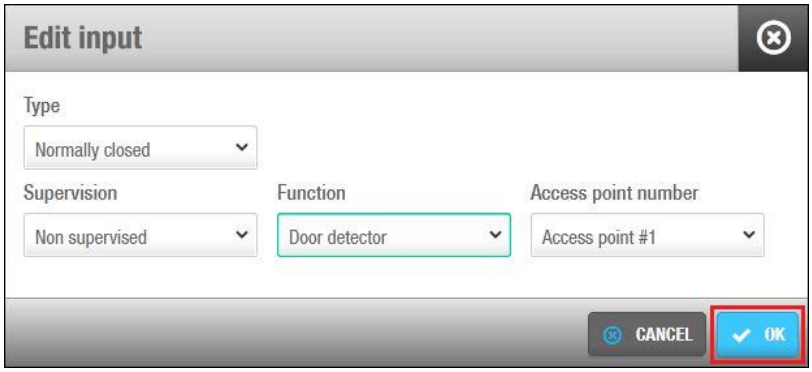


Figure 257: CU4200 node Reader Input

The **Inputs** fields are described in the table below,

Table 63: Inputs fields

Field	Functionality
Type	Status of the relay in normal position. The relay can be normally in closed position or opened position.
Supervision	Select the resistance as required for the supervision. A supervised input is protected against external attacks.
Function	Select the function you want for the relay. Options include doo Door detector, Office enabler, Intrusion inhibition, Request to open roller blind, Request to close roller blind, Request to Exit or Request to Open.

For example, according to the image below, a relay in normally opened position could send a request to open a roller blind when presenting a valid key in reader #1 from IN1 and request to close the roller blind from IN2.

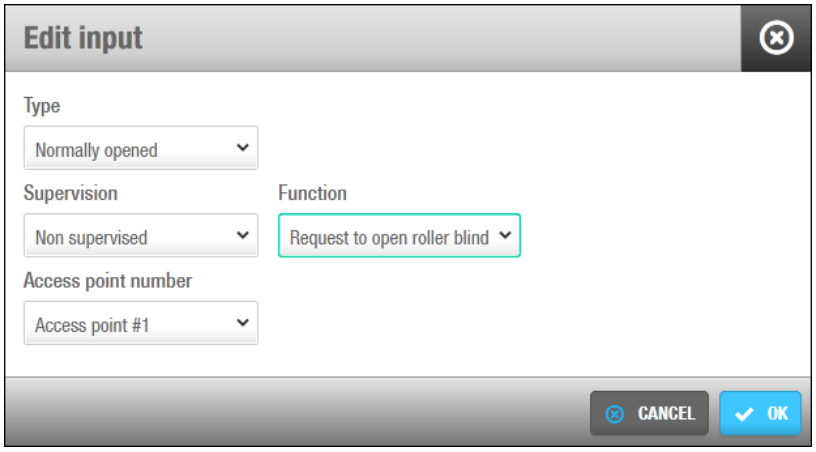


Figure 258: Roller blind example

A reader that is not from SALTO can also be used. **Edit Reader Input** Type must be set to **None**. **Type** field in **Edit Input** shows the **Third party reader** option in the dropdown menu. Only a **Wiegand** code is supported. See *Devices Tab* in General options for more information about how to configure the Wiegand format. An authorization code has to be entered for each user in the **Authorization code** field on the **User** profile. See *Users* in **Cardholders** menu for more information. Select the **Access point** from the **Access point number** dropdown menu and if it will be an **Entry** or an **Exit.**

5. 32. 1. 7. Managing CU4200 Relays

A relay is an electrically operated switch. It is used where it is necessary to control a circuit by a low-power signal. For example, you can control an electric or magnetic strike, trigger a camera recording or turn an alarm off.

The CU4200 node has 4 relays that can be configured independently. Select the relay ID and click **Edit**. The **Edit Relay** fields are described in the table below

Table 64: Edit Relay fields

Field	Functionality
Type	Select the appropriate type as needed.
Access point number	Select the access point in question. It can be **Access point #1, Access point #2** or both.
Output	The **Output** dropdown menu is shown when Output is selected in **Type** dropdown menu. Select the Output from the dropdown menu. The list of outputs have to be created first in **Outputs** list, in the **Access points** menu. See Access points *Outputs* for more information about how to create Outputs. The relay will be triggered when a key with a valid output is presented to the wall reader. See User *Outputs* for more information about how to add outputs in the user access.
Conditions	Select **Combined** in the **Type** dropdown menu to select a combination of conditions. According to the image below, the relay will be triggered if in Access point #1 the **Door is left opened**, if there is an **Intrusion** or if there is a **Card rejected**.

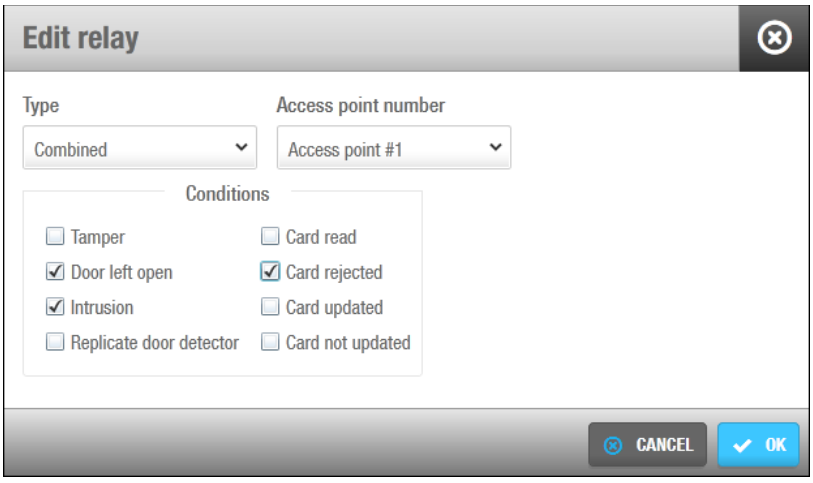


Figure 259: Combined relay type

5. 32. 1. 8. CU42X0 devices initialization and update

The CU42E0 gateways and CU4200 nodes are initialized and updated automatically. See table below for the frequency of each.

Table 65: CU42x0 Initialization and Update

Automatic process	Check Frequency	Notes
CU4K doors initialization	1 minute	Includes initialization + update
CU4K doors update	5 minutes	Can be executed on request
CU4K nodes initialization	1 minute	Includes initialization + update
CU4K nodes update	5 minutes	Can be executed on request

NOTE: Even if updates are performed automatically every 5 minutes for the CU42x0, a manual update can be performed immediately by selecting the device and clicking the **Update** button in **SALTO network**.

5. 32. 2. Filtering SALTO Network Data

You can filter SALTO network data by type, name, description, and/or IP address.

You can filter by the following item types:

- Online IP (CU5000)
- CU42E0 gateway
- CU4200 node
- Online IP (CU4200)
- Encoder
- RF gateway
- RF node
- Online RF (SALTO)
- BAS gateway
- Online RF (BAS integration)

To filter the SALTO network data, perform the following steps:

146. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
147. Click **Filters**. The **Items filtering** dialog box is displayed.
148. Select a pre-defined search term from the **Type** drop-down list.
149. Type the name of the item you want to search for in the **Name** field.
150. Type the description of the item you want to search for in the **Description** field.
151. Type the IP address in the **IP address** field if appropriate.

    The **IP address** field is only displayed for relevant search term types.

152. Click **Apply Filter**. A filtered SALTO network list is displayed.

    When a filter has been applied, on the **SALTO Network** screen when you have applied a filter, the search type is displayed in light blue. You can click the search type to once again display all items on the list screen. You can click **Delete Filter** to delete the filter and to redefine the filter parameters.

153. Click the **Close** icon in the **Applied Filters** field when you have finished reviewing the filtered list or click **Filters** to apply another filter.

5. 32. 3. Configuring Online Connection Types

When adding a door or room to the system, you must specify the appropriate connection type – either online or offline. When you select an online connection type, the door or room is displayed on the **SALTO Network** screen, and you can double-click the entry to configure it.

There are four online connection types:

- Online IP (CU5000)
- Online IP (CU4200)
- Online RF (SALTO)
- Online RF (BAS integration)

NOTE: Your BAS integration must be fully configured in ProAccess SPACE General options before you can select this option. See *BAS Tab* for more information.

See *Connection Types* for more information about selecting the correct connection types in non-hotel sites. For information about connection types in non-hotel sites, see *Connection Types*.

5. 32. 3. 1. Online IP (CU5000)

To configure an online IP (CU5000) door, perform the following steps:

154. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
155. Double-click the online IP (CU5000) door that you want to configure. The **Access point: Online IP (CU5000)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU5000) doors are online SVN points.

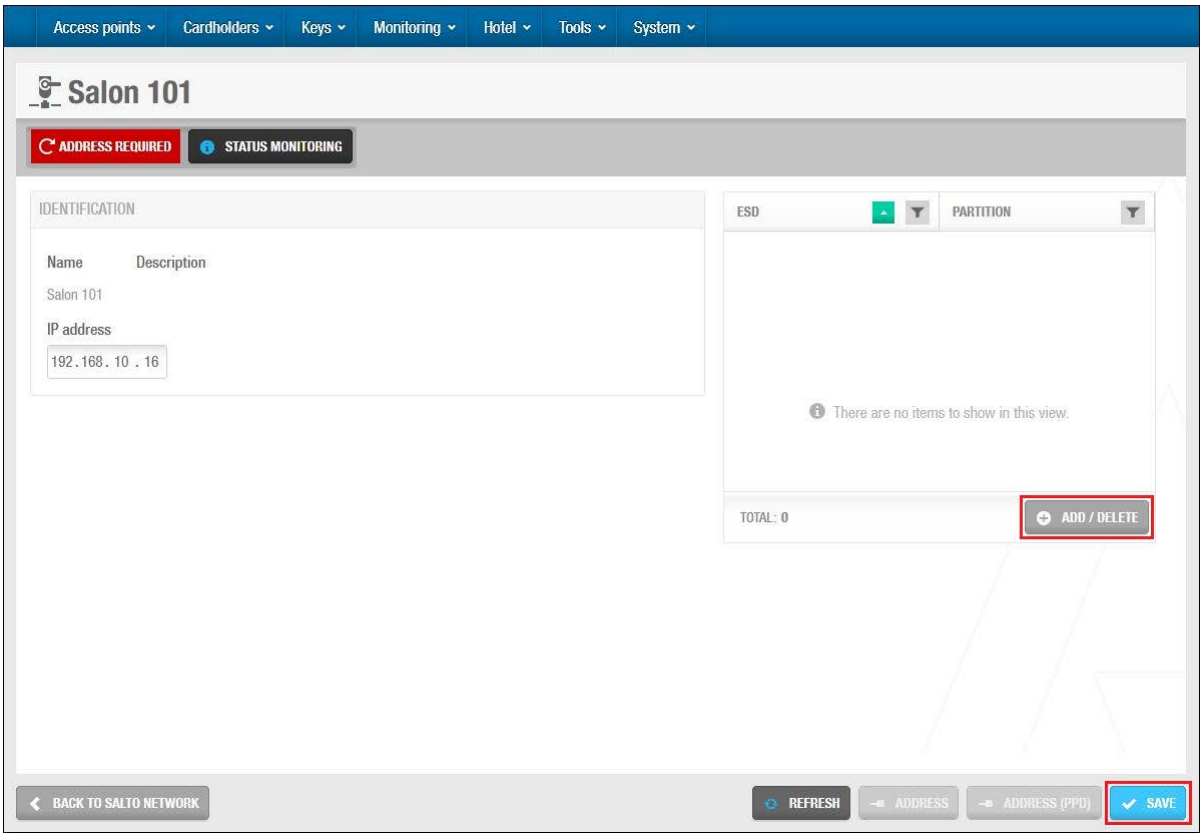


Figure 260: Access point: Online IP (CU5000) information screen

156. Type an IP address for the door in the **IP address** field.
157. Click **Add/Delete** in the **ESD** panel. The **Add/Delete** dialog box, showing a list of ESDs, is displayed. See *ESDs* for more information about ESDs.
158. Select the required ESD in the left-hand panel and click the chevron. The selected ESD is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the ESDs to make multiple selections.
159. Click **Accept**. The selected ESD is displayed in the **ESD** panel.
160. Click **Save**.

5. 32. 3. 2. Online IP (CU4200)

To configure an online IP (CU4200) door, perform the following steps:

161. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
162. Double-click the online IP (CU4200) door that you want to configure. The **Online IP (CU 4200)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU4200) doors that are not connected to CU4200 nodes are displayed in the **Unreachable items** tab. See *Adding CU4200 Nodes* for more information about CU4200 nodes.

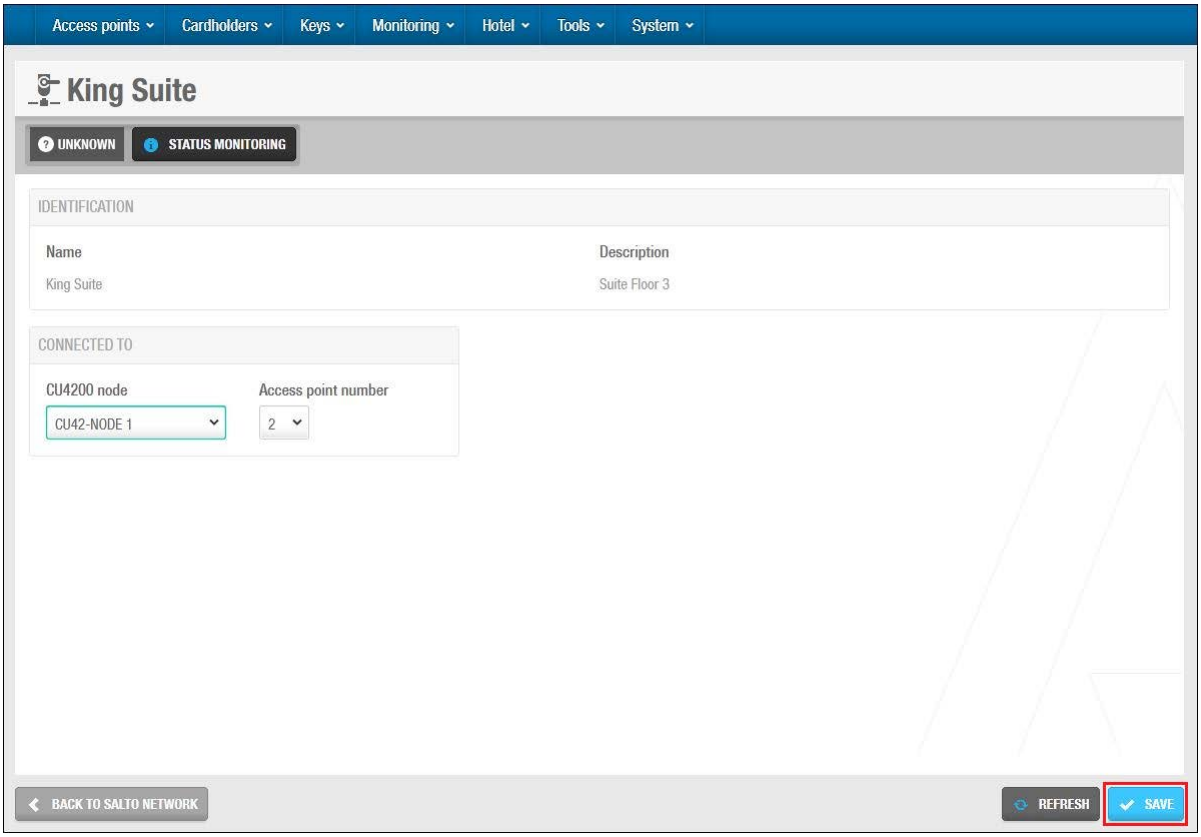


Figure 261: Online IP (CU4200) information screen

163. Select the CU4200 node to which you want to connect the door from the **Connected to** drop-down list.
164. Select either **1** or **2** from the **Door number** drop-down list.

    You cannot select **2** unless you have selected **2** in the **Access point count** drop-down list on the **CU4200 node** information screen. Otherwise, this exceeds the door number count for the node. See *Adding CU4200 Nodes* for more information.
165. Click **Save**.

5. 32. 3. 3. Online RF (SALTO)

To configure an online RF (SALTO) door, perform the following steps:

166. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
167. Double-click the online RF (SALTO) door that you want to configure. The **Online RF (SALTO)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online RF (SALTO) doors that are not yet connected to RF nodes are displayed in the **Unreachable items** tab. See *Adding RF Nodes* for more information about RF nodes.

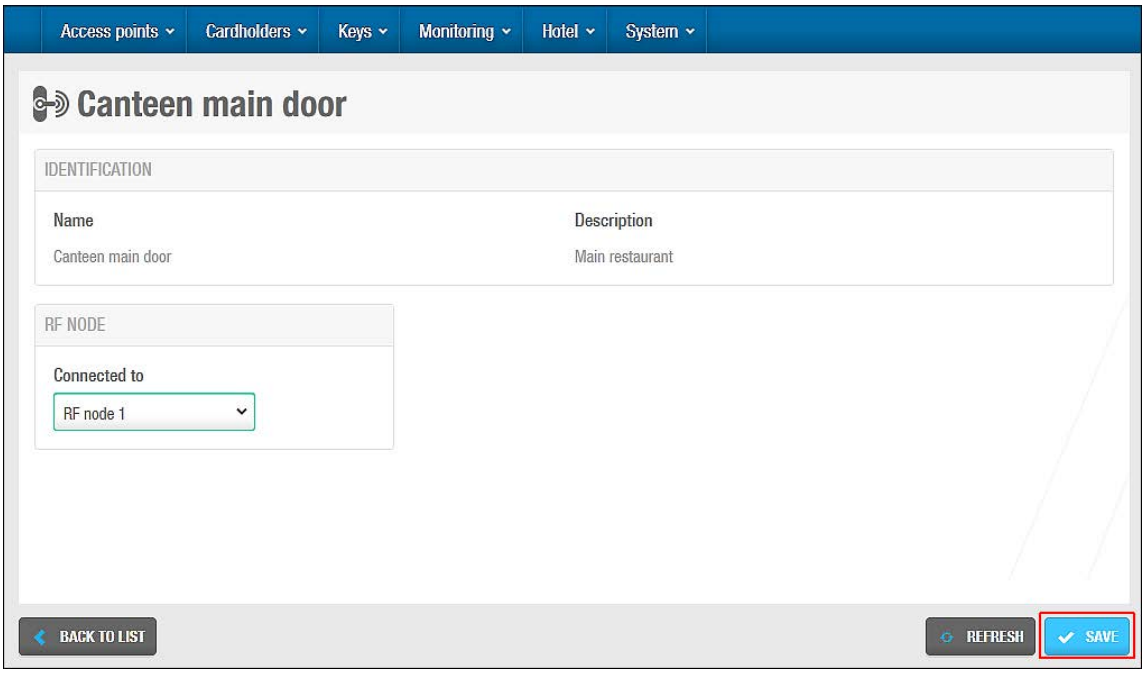


Figure 262: Online RF (SALTO) information screen

168. Select the RF node to which you want to connect the door from the **Connected to** drop-down list.
169. Click **Save**

5. 32. 4. Peripherals Addressing and Maintenance

SALTO network items like Control units, Ethernet encoders, gateways and RF nodes can be added and managed in ProAccess SPACE where you can also make changes such as updating online CUs or updating firmware.

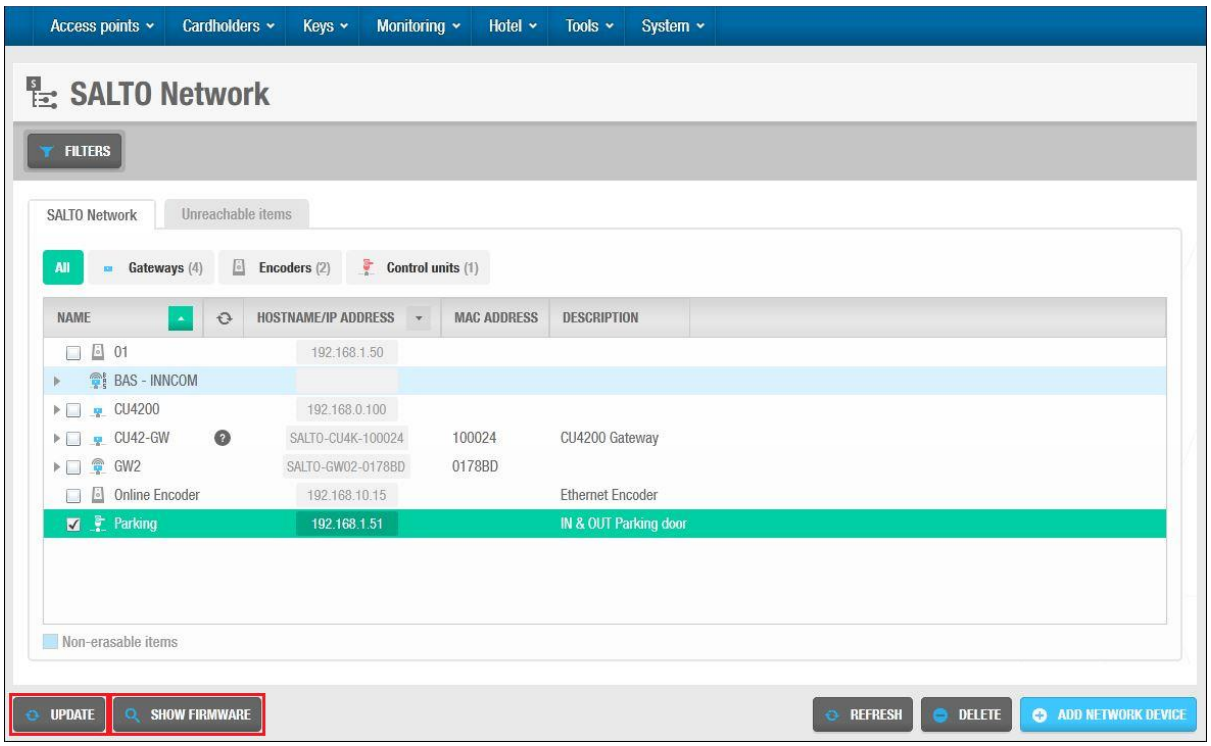


Figure 263: Address and Maintenance

The **Address** and **Maintenance** tab buttons are described in the following table.

Table 66: Maintenance buttons

Button	Functionality
Update	Allows updates to the SALTO database to be communicated to the selected network items. In addition, it allows blacklists to be transmitted automatically to doors without the need to visit each door with an updated key. SAM cards can also be used to transfer information to online doors and to update offline escutcheons and cylinders. See *SAM and Issuing Data* for more information. To SAM a local encoder, click **Supported Keys** on the **Settings** screen in ProAccess SPACE. See *Encoder Settings* for more information. You will find this button in all updatable devices such as control unit CU5000 and CU4200.
Show firmware	Displays the firmware version of the selected item. You can check the firmware version for any online device, CU, RF door, or Ethernet encoder. We recommended that you use the latest firmware version with the SALTO system. Online CUs consist of an Ethernet board and a CU board. This may require updating an individual or multiple online CUs to the most recent firmware version. See *Updating Firmware* for more information about updating multiple online CUs simultaneously. You will find this button in all firmware updatable devices such as control unit CU5000, CU4200 gateways and Ethernet encoders.
Address	Assigns an IP address that you have entered on the system for an Ethernet encoder or an online IP (CU5000) door if the peripheral is in the same network. When you click **CLR** on the online CU, for example, the device enters listening mode. When you click **Address** on the **Monitoring** tab, the software sends a broadcast to the online CU. When the broadcast reaches the online CU, it initializes it with the new IP and other door parameters. Note that you can only address one peripheral at a time when using this option. See *Adding Ethernet Encoders* and *Online IP (CU5000)* for more information about entering IP addresses for Ethernet encoders and online IP (CU5000) doors. You will find this button in all updatable devices such as control unit CU5000 and Ethernet encoders.
Address (PPD)	Assigns an IP address, using a PPD, to an online CU if the peripheral is in a different network. When the online CU is initialized by the PPD, click **Address (PPD)** on the **Monitoring** tab. This creates an authentication between the system and the peripheral. You must enable this option by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices** in ProAccess SPACE. See *Devices Tab* for more information. See also *PPD* for more information. You will find this button in all updatable devices such as control unit CU5000.
Signal	Used to help identify the physical Ethernet encoder that corresponds to the applicable IP/peripheral. After you select the peripheral in the list and click **Signal**, the LED of the applicable encoder starts flashing. At this point, the SAMing process can take place. See *SAM and Issuing Data* for more information.

The columns at the top of the **Maintenance** tab are described in the following table.

Table 67: Maintenance columns

Column	Functionality

Column	Functionality
Name	Specifies the name of the item (the icon immediately before the item name indicates the peripheral type)
Update Status	Shows the peripheral update status. If no update is required, no icon will be shown. The status could be **Update required**, **Address required** or **Unknown.** Note that this column does not have a title on the screen.
Hostname/ IP address	Specifies the network name that identifies the item
MAC Address	Specifies the MAC address of the device.
Description	Matches the details of the item entered in the **Description** field in ProAccess SPACE

5. 32. 4. 1. Updating Firmware

Firmware is software that is programmed on the ROM of hardware devices.

NOTE: SALTO provides firmware updates when new functionality is available or when a software bug is fixed. Each component has a unique file. Contact your SALTO technical support contact before updating any firmware file.

To update the firmware version of an item, perform the following steps:

170. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
171. Select the required item and click **Show firmware**. The **Firmware information** dialog box is displayed.

Figure 264: Peripheral firmware update dialog box

You can select multiple items on the **SALTO Network** peripheral list if required.

172. Select the checkbox next to the item that you want to update. The **Browse** button is enabled.

    If required, you can click **Check all** to update the firmware for multiple items simultaneously. You can only update multiples of the same item (for example, online CUs only or Ethernet encoders only) simultaneously.
173. Click **Browse** to select the required firmware file.
174. Click **Send firmware**. A confirmation screen is displayed when the firmware update is complete.

NOTE: You can update the firmware for local encoders by using the **Show Firmware** button on the **Settings** screen in ProAccess SPACE. See *Updating Encoder*

Firmware for more information.

Calendars for more information about holidays and special days.

175. Click **Save**.

5. 33. Access Point Automatic Changes

You can use access point automatic changes to allow a number of different opening modes to switch automatically and vary across different time periods. Opening modes are defined when you set up doors and/or lockers. See *Configuring Doors* and *Configuring Lockers* for more information.

For example, a door's opening mode may have automatic changes enabled as follows:

- 00.00 to 08.00 Office
- 08.00 to 18.00 Automatic
- 18.00 to 00.00 Standard

Three parameters define an automatic change: start time, end time, and opening mode. For a specified day, up to eight automatic changes can be defined. In order to allow varying combinations, the system includes 1024 automatic change tables. Each table contains four day types as follows:

- Monday to Sunday
- Holiday
- Special 1
- Special 2

See *Opening Modes and Timed Periods* for more information about defined opening modes.

You must configure the system calendar before you create access point automatic changes. See *PPD*

PPDs are connected to the operator's local PC through either a USB or COM port. See *PPD Settings* for more information. PPDs allow data to be transferred between the operator's PC and the locks. Data is downloaded from the PC to the PPD, and the PPD is used to perform tasks such as lock initialization and emergency openings. In the process, the PPD retrieves information (such as battery status) from the locks. This information is communicated to the system when the PPD is connected to the operator's PC.

See the *Portable Programming Device by SALTO* document for more information about PPDs and their configuration settings.

Table 56: PPD

 Portable Programming Device (PPD)	Used by admin operators to transfer configuration changes to a lock or by maintenance operators to check the battery status of the lock and collect the lock's audit trail

NOTE: It is important that the time is set correctly for the PC on which the SALTO software is running, as this controls the time and date settings for locks.

5. 33. 1. Peripheral Types

The functionality of the PPD is described in the following table.

Table 57: Peripheral types

Peripheral	Functionality
PPD	Communicates information to the locks such as door identification and configuration details. The operator downloads the information from their PC to the PPD and the PPD can then be connected to the lock. In this way, information is transferred to the lock. PPDs are used to: ▪ Update configuration changes to the lock (door profile, calendars etc.) ▪ Manually retrieve the audit trail stored on the lock for uploading to the server ▪ Perform a firmware diagnostic evaluation of the locking electronic components ▪ Upgrade the firmware of the locking components ▪ Open a door in the event of an emergency ▪ Read the battery status of the lock ▪ Perform a general diagnostic evaluation of the system

PPDs are configured in ProAccess SPACE General options. See *Devices Tab* for more information. The **PPD** information screen in ProAccess SPACE is used to download access point data to PPDs. This allows you to perform tasks with PPDs such as initializing and updating locks. You can also view the status of PPDs and update their firmware by using the **PPD** information screen.

5. 33. 2. PPD Menu Options

PPDs have seven menu options. Some of the menu options are available by default. Others are enabled when you select particular options on the **PPD** information screen in ProAccess SPACE, and download access point data to the PPD. See the *Portable Programming Device by SALTO* document for more information about using PPDs.

The options are described in the following table.

Table 58: PPD menu options

Option	Description
Update locks	Used to update a lock when the PPD is connected to it. To enable this menu option, you must download the appropriate access point data to the PPD by using the **PPD** information screen.
Firmware diagnostic	Used to perform a firmware diagnostic of the locking electronic components
Update firmware	Used to update the firmware of the locking electronic components
Collect audit trail	Used to collect audit trail data from offline doors and transfer it to the operator's local PC

Option	Description
Emergency opening	Used to perform an emergency opening if the lock battery dies or a reader error occurs. To enable this menu option, you must select the **Allow emergency opening** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. Alternatively, you can set this as a default option in ProAccess SPACE General options. You can also set a password for performing emergency openings using the PPD if required. See *Performing Emergency Door Openings* and *Devices Tab* for more information.
Initialize lock	Used to transfer access data to new locks or existing locks that have been fitted on a different access point and renamed. To enable this menu option, you must select the **Initialize locks** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. See *Initializing Locks* for more information.
Diagnostic	Used to retrieve information from the lock such as the battery status or serial number

5. 33. 3. Viewing PPD Status

You can view the status of a PPD you have connected to the PC by selecting **System** > **PPD**.

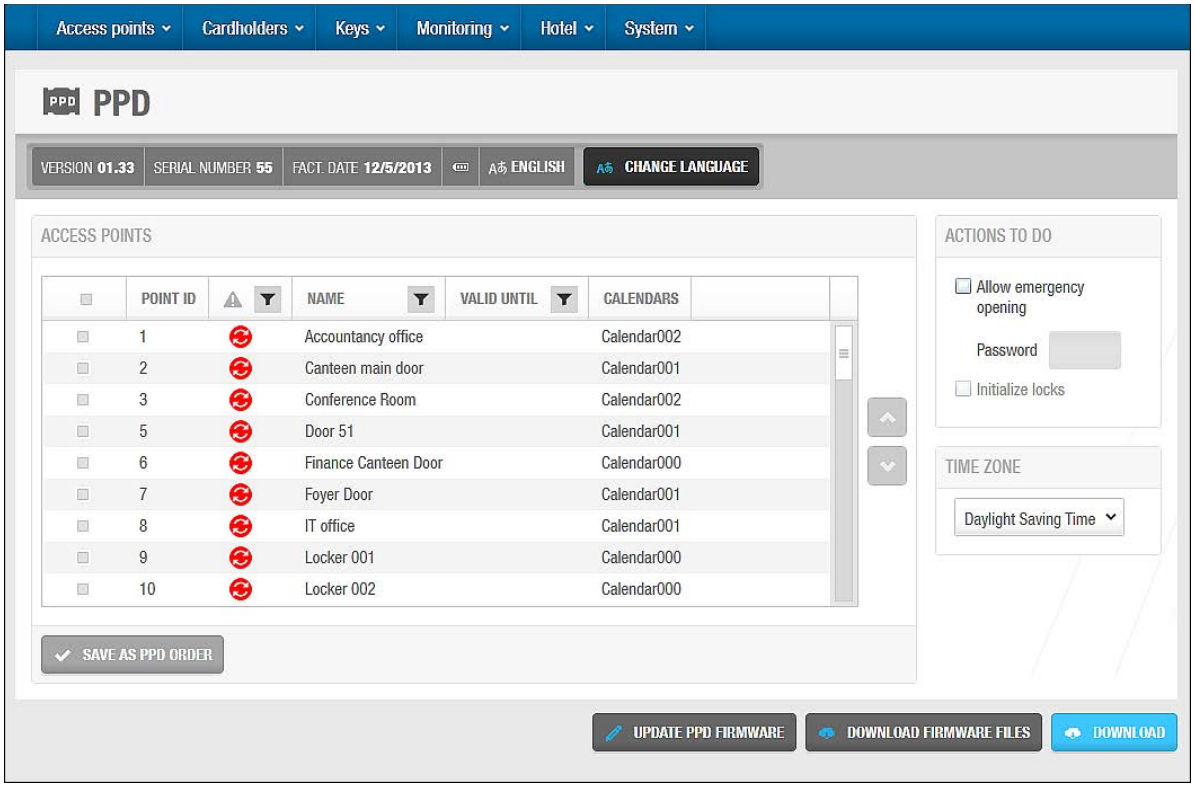


Figure 238: PPD information screen

The **PPD** information screen shows the following information about the PPD:

- Version
- Serial number
- Factory date (or date of manufacture)
- Battery status

- Language

5. 33. 4. Changing the PPD Language

You can change the language of the display messages in the PPDs if required.

To change the language displayed in a PPD, perform the following steps:

176. Connect the PPD to the PC.
177. Select **System** > **PPD**. The **PPD** information screen is displayed.
178. Click **Change Language**. The **Change language** dialog box is displayed.

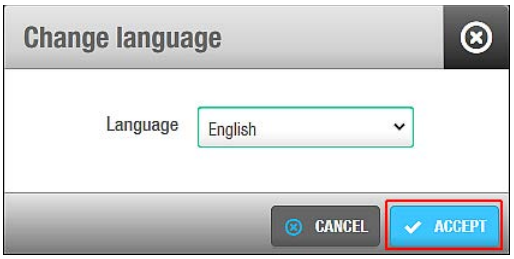


Figure 239: Change language dialog box

179. Select the required language from the **Language** drop-down list.
180. Click **Accept**. The **PPD** progress screen is displayed.
181. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
182. Click **OK**.

5. 33. 5. Using the PPD Information Screen

The **PPD** information screen displays a list of access points. This list varies depending on which time zone is selected in the **Time Zone** panel. It is important to remember that only access points for the selected time zone are displayed. Note that you must enable the multiple time zones functionality in ProAccess SPACE General options to display this panel in ProAccess SPACE. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Access points that need to be updated have a red **Update required** icon on the left-hand side of their name. You can download access point data to a PPD you have connected to the PC by selecting the required access points and clicking **Download**. You can then perform tasks such as updating locks with the PPD. See *Updating Locks* for more information. You must select additional options in the **Actions To Do** panel for certain tasks, for example, initializing locks. See *Initializing Locks* and *Performing Emergency Door Openings* for more information about this panel.

The following table describes some useful screen items.

Table 59: PPD information screen items

Item	Description
Access point checkboxes	Allow you to select individual access points
Checkbox column header	Allows you to select all of the displayed access points. To do so, select the checkbox in the column header.
Chevrons	Allow you to move entries up and down in the access point list

Item	Description
Save As PPD Order button	Allows you to save the access point list order. This specifies the order in which access point data is downloaded to the PPD and displayed in the PPD's menu.
Expand icon	Allows you to view the ESDs for rooms and suites. This icon is displayed on the left-hand side of the room and suite names.

5. 33. 6. Updating PPD Firmware

Firmware is software that is programmed on the read-only memory (ROM) of hardware devices. Firmware updates are available when a new version of the SALTO software is downloaded. Your SALTO technical support contact may also recommend specific firmware updates if required.

To update the firmware of a PPD, perform the following steps:

183. Connect the PPD to the PC.
184. Select **System** > **PPD**. The **PPD** information screen is displayed.

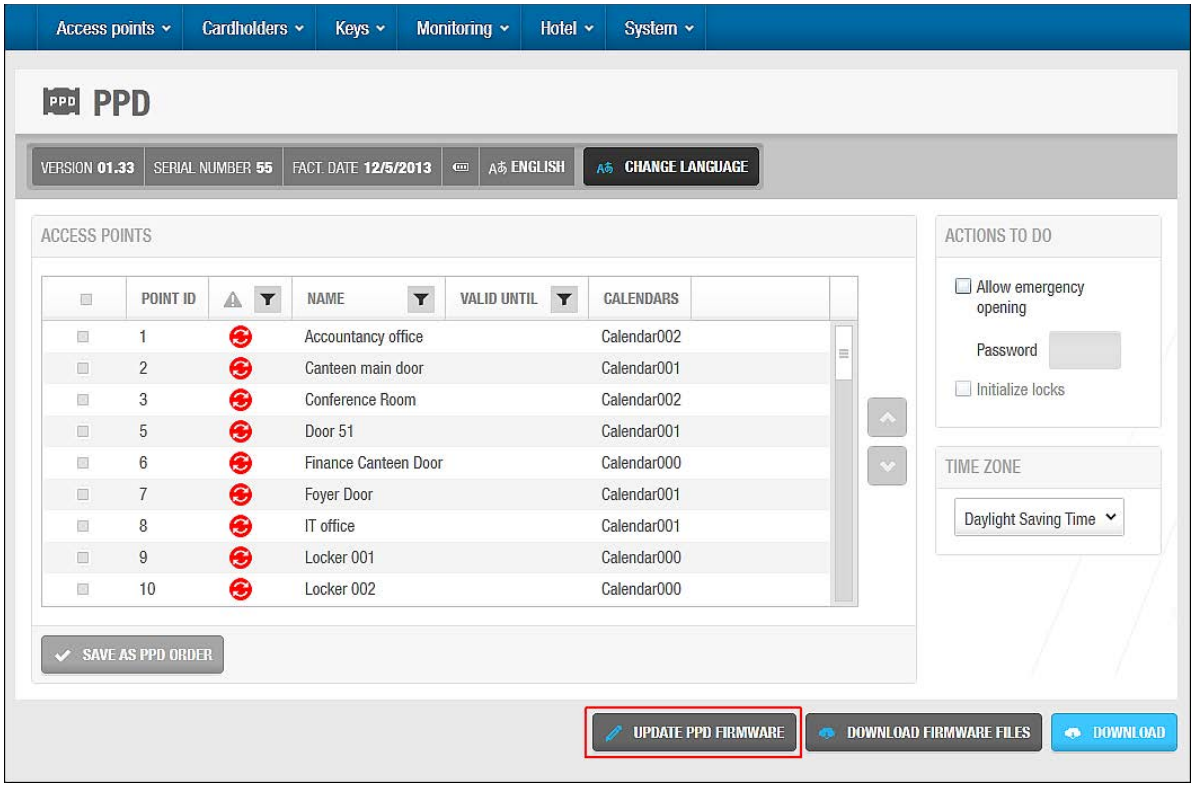


Figure 240: PPD information screen

185. Click **Update PPD Firmware**. The **Update PPD Firmware** dialog box, showing the available firmware files, is displayed.

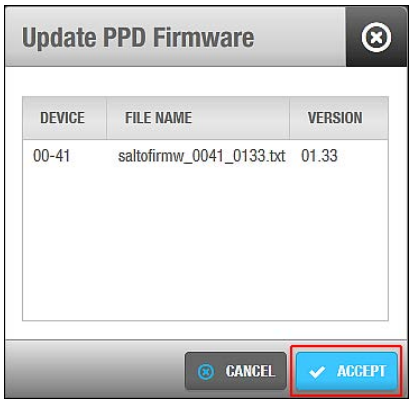


Figure 241: Update PPD Firmware dialog box

186. Select the required file.
187. Click **Accept**. The **PPD** progress screen is displayed.
188. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
189. Click **OK**.

5. 33. 7. Downloading Firmware Files

You can download firmware files to the PPD and use it to update the locking electronic components.

To download a firmware file to a PPD, perform the following steps:

190. Connect the PPD to the PC.
191. Select **System** > **PPD**. The **PPD** information screen is displayed.

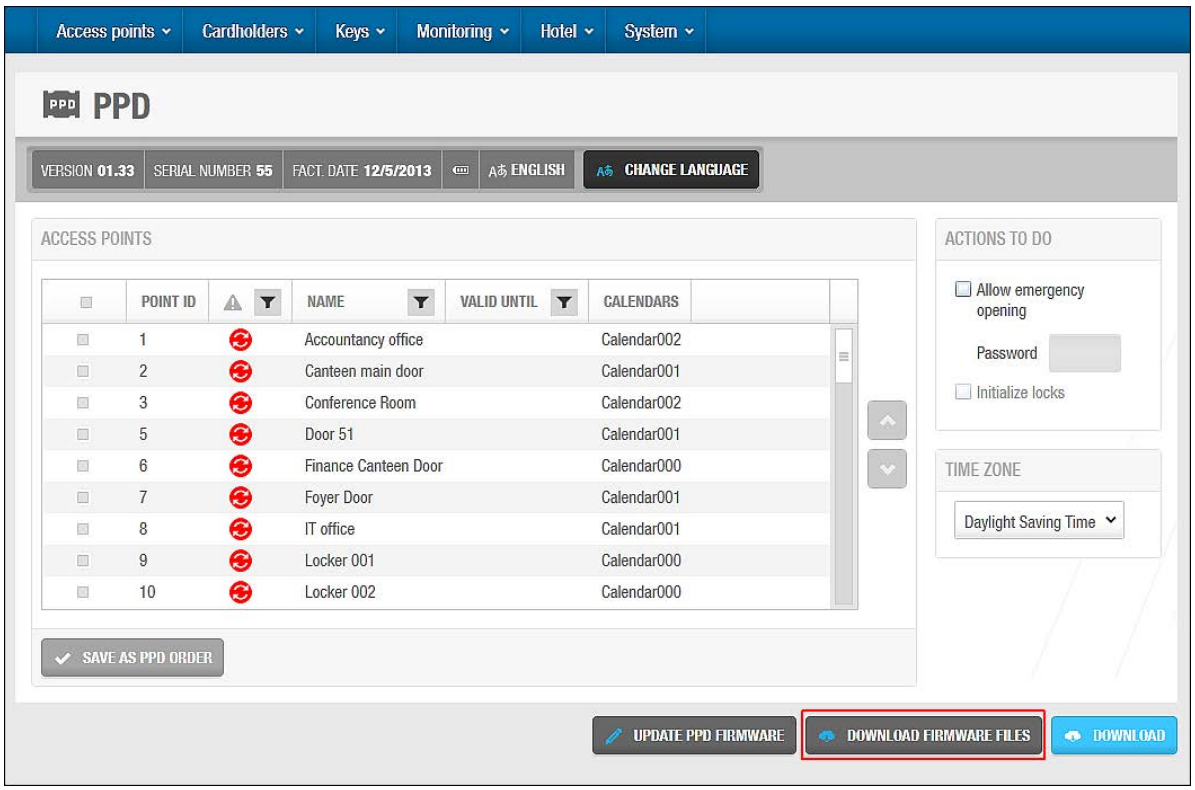


Figure 242: PPD information screen

192. Click **Download Firmware Files**. The **Download Firmware files** dialog box, showing the available firmware files, is displayed.

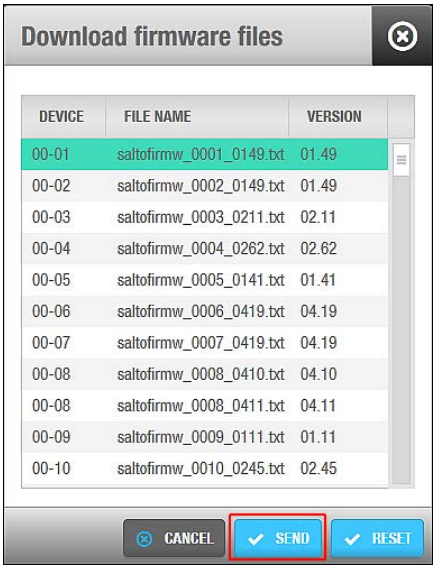


Figure 243: Download firmware files dialog box

193. Select the required file.

You can hold down the Ctrl key while clicking the files to make multiple selections. Note that you can click **Reset** to delete any firmware files you have already downloaded.

194. Click **Send**. The **PPD** progress screen is displayed.

195. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.

196. Click **OK**.

You can now use the PPD to update the firmware of locking electronic components by selecting **Update Firmware** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

5. 33. 8. Initializing Locks

You must initialize each lock when it is installed. This programmes the lock, and transfers access point data relating to time zones and calendars, for example.

It is recommended that you connect the PPD to the PC after you initialize locks to communicate the most up-to-date information about the locks to the system.

NOTE: You can configure PPDs to assign IP addresses to online IP (CU5000) doors during initialization if required. You must enter each IP address on the system by using the **Access point: Online IP CU5000** information screen. Note that you must select **System** > **SALTO Network** and double-click the required online IP (CU5000) door on the **SALTO Network** screen to view the information screen. You must enable this option in ProAccess SPACE General options by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

PPDs can also be used to transfer SAM data to SALTO locks and wall readers during initialization (or when you perform updates). See *SAM and Issuing options General* options

See *General options* section.

SAM and Issuing Data for more information.

To initialize a lock, perform the following steps:

197. Connect the PPD to the PC.
198. Select **System** > **PPD**. The **PPD** information screen is displayed.

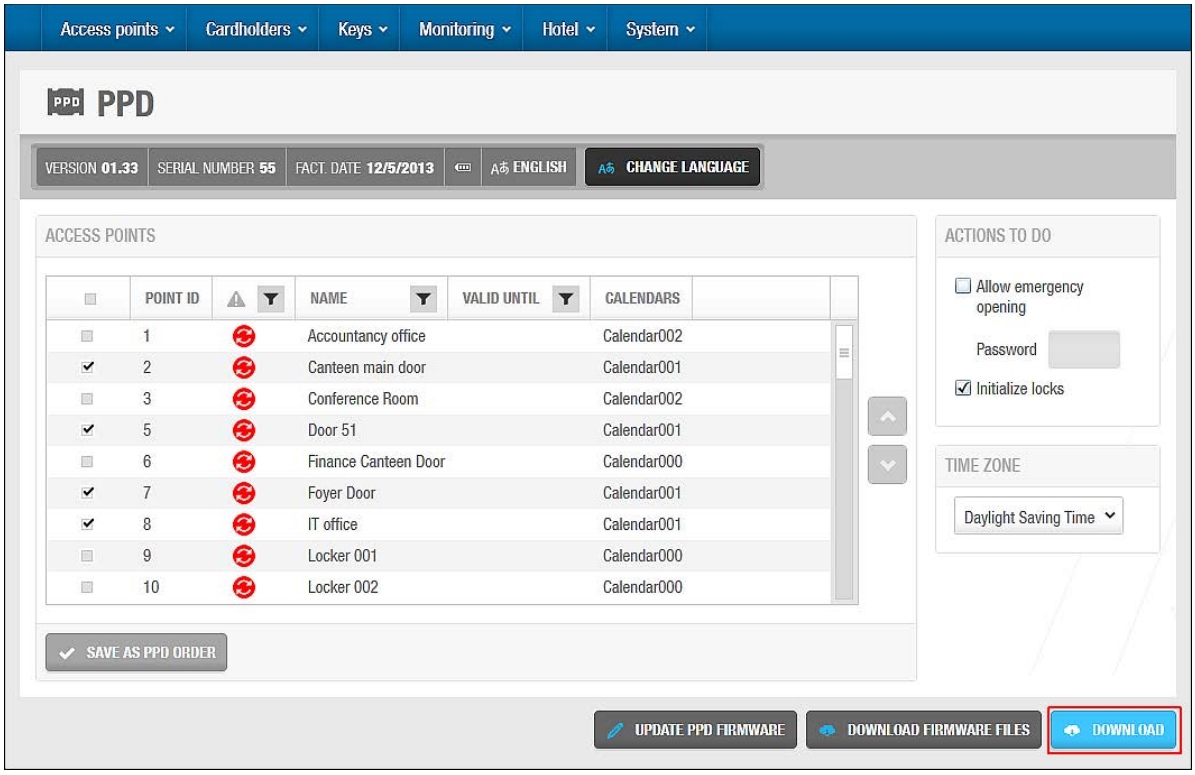


Figure 244: PPD information screen

199. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

200. Select the checkbox of the access point for which you want to initialize the lock.

You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

201. Select the **Initialize locks** checkbox in the **Actions To Do** panel.
202. Click **Download**. The **PPD** progress screen is displayed.
203. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.

You can now use the PPD to initialize the lock of the selected access point by selecting **Initialize Lock** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: If you initialize a lock that is already in use, its audit trail is deleted.

5. 33. 9. Initializing Rooms and ESDs

The procedure for initializing rooms and ESDs is the same as for initializing locks. See *Initializing Locks* for more information and a description of the steps you should follow.

NOTE: You can initialize rooms and their associated ESDs either together or separately. However, all of the rooms and ESDs that you select during the initialization process must have the same calendar.

5. 33. 10. Updating Locks

You must update offline locks when you make certain changes to access point data, such as enabling anti-passback or changing the opening mode of doors. You can view locks that need to be updated on the **PPD** information screen by selecting **System** > **PPD**. Note that you must connect a PPD to the PC before you can access the **PPD** information screen. Access points that need to be updated have a red **Update required** icon on the left-hand side of their name.

It is recommended to update offline locks at least every six months to ensure that the clock and calendars are up to date. You must also update locks after you replace their batteries. This is because access point data relating to time zones and calendars, for example, must be restored after a lock's battery dies.

You should connect the PPD to the PC after you update locks to communicate the most up-to-date information about the locks to the system.

To update a lock, perform the following steps:

204. Connect the PPD to the PC.
205. Select **System** > **PPD**. The **PPD** information screen is displayed.

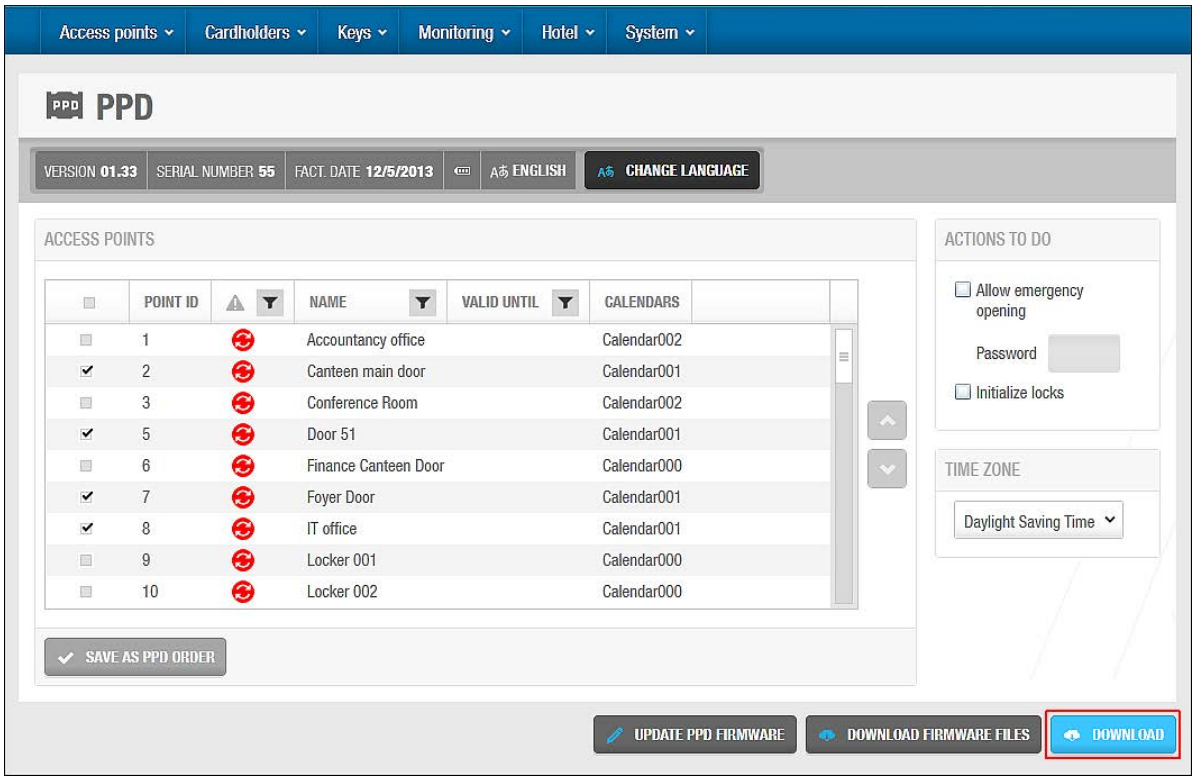


Figure 245: PPD information screen

206. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

207. Select the checkbox of the access point for which you want to update the lock.

You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

208. Click **Download**. The **PPD** progress screen is displayed.

209. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.

210. Click **OK**.

You can now use the PPD to update the lock of the selected access point by selecting **Update Locks** in the PPD's menu and connecting the PPD to the lock. Alternatively, you can simply connect the PPD to the lock. In this case, it recognizes the lock and automatically displays the appropriate data. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: You can configure PPDs to automatically collect audit trail data when they are used to update locks. You must enable this option in ProAccess SPACE General options by selecting the **Collect audit trails automatically when updating locks** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

5. 33. 11. Performing Emergency Door Openings

You can use the PPD to perform an emergency opening if the lock battery dies or a reader error occurs, for example.

NOTE: You can perform emergency openings of online doors without using a PPD. See *Lockdown* for more information.

To perform an emergency opening, perform the following steps:

211. Connect the PPD to the PC.
212. Select **System** > **PPD**. The **PPD** information screen is displayed.

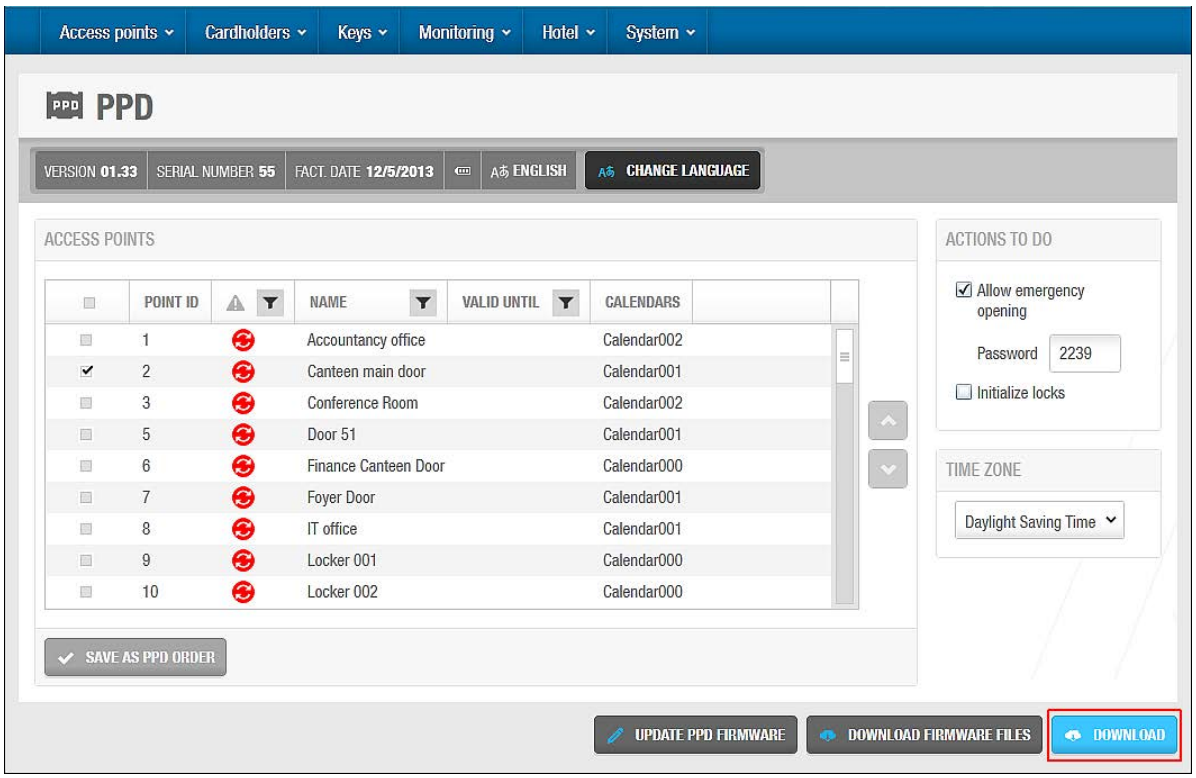


Figure 246: PPD information screen

213. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

214. Select the checkbox of the access point for which you want to perform the emergency opening.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

215. Select the **Allow emergency opening** checkbox in the **Actions To Do** panel.

    The checkbox is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options. See *PPD Tab* for more information. Otherwise, you must select it each time you want to perform an emergency opening.

216. Type a password for the emergency opening in the **Password** field if required.

The password can only contain digits. If you type a password, you must enter this password in the PPD before you can perform the emergency opening. Otherwise, the PPD does not require a password. The **Password** field is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options and entered a password there already for the option. See *Devices Tab* for more information. Your PPD firmware must be version 01.29 or higher to use this option.

217. Click **Download**. The **PPD** progress screen is displayed.
218. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
219. Click **OK**.

You can now use the PPD to perform an emergency opening of the selected access point by selecting **Emergency Opening** in the PPD's menu and connecting the PPD to the lock. Note that you are required to enter a password in the PPD if you have enabled this option in either ProAccess SPACE PPD window or ProAccess SPACE Devices window. See the *Portable Programming Device by SALTO* document for more information about this process.

5. 33. 12. Collecting Audit Trail Data from Offline Doors

See *Audit Trails* for more information about audit trails. You must use a PPD to collect audit trail data from offline doors. See the *Portable Programming Device by SALTO* document for more information about this process. When you have collected the data, you can view it in ProAccess SPACE.

To view the audit trail data on the system, perform the following steps:

220. Connect the PPD to the PC.
221. Select **System** > **PPD**. The **PPD** information screen is displayed.

The **Audit Trail** information screen is automatically updated with the information from the connected PPD when you display the **PPD** information screen.

222. Select **Monitoring** > **Audit Trail**. The **Audit trail** information screen, showing the new audit trail data, is displayed.

5. 34. SALTO Network

The SALTO network includes items like encoders, gateways, radio frequency (RF) nodes, CU4200 nodes, online doors, and CUs. These are added and managed in ProAccess SPACE. See *SALTO Virtual Network* for more information about the SALTO network.

The RF and CU4200 functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

NOTE: You can view the enabled channels for RF signals in ProAccess SPACE General options. To do so, select **System** > **General options** > **Devices**. There are 16 channels available and all of these are enabled by default. The frequency range of each channel is also displayed. You can disable a channel if required by clearing the checkbox for the channel and clicking **Save**.

RF mode 2 technology is compatible with ProAccess SPACE. However, RF mode

1 technology is not. If your site uses RF mode 1, an upgrade to ProAccess SPACE is not possible, which means that you must continue to use HAMS or ProAccess RW.

You can view the list of SALTO network items by selecting **System** > **SALTO Network**.

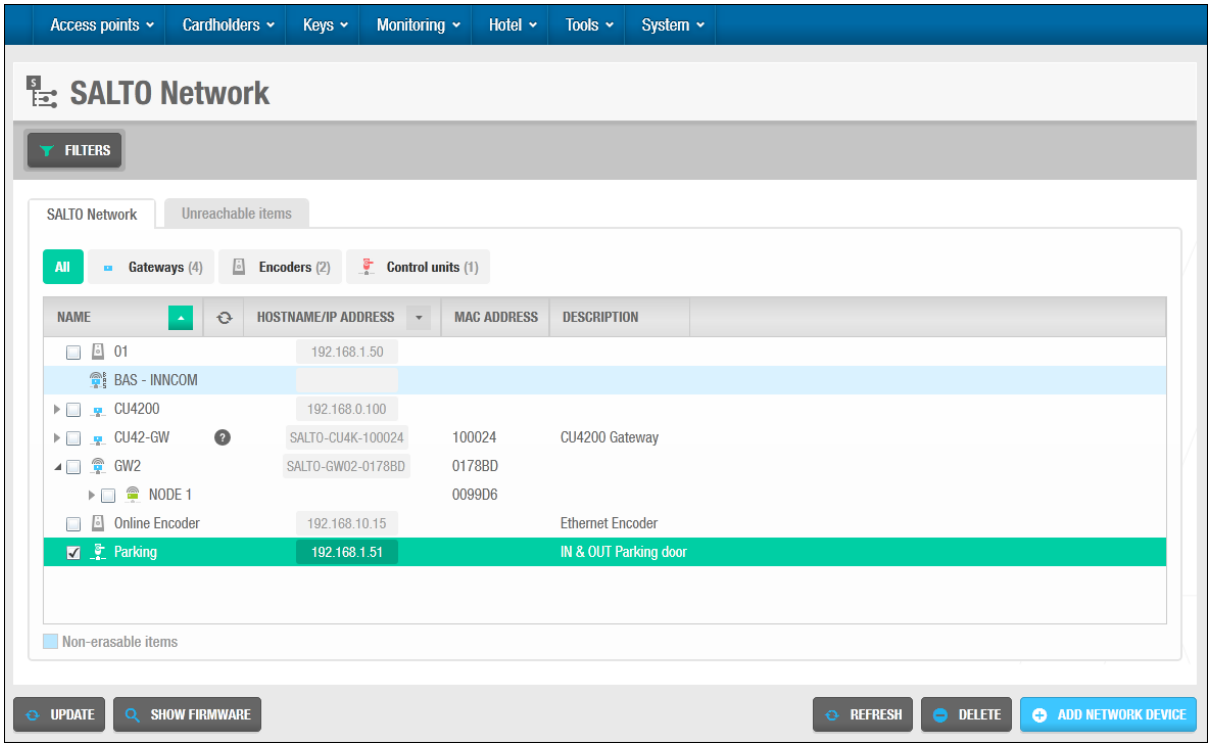


Figure 247: SALTO Network screen

The **SALTO Network** screen displays a list of all network items that have been added and are currently connected to the system.

The information is displayed in four different filtered views:

- **All**: This view shows all of the gateways, encoders, and CUs on the system.
- **Gateways**: This view shows RF gateways and CU4200 gateways. When you click the triangular **Expand** icon on the left-hand side of gateway names, all of the items to which they are connected are displayed. You can view all of the RF nodes and online RF (SALTO) access points connected to each RF gateway, and all of the CU4200 nodes and online IP (CU4200) access points connected to each CU4200 gateway. See *Configuring Online Connection Types* for more information.

NOTE: A BAS gateway may also be displayed on the **SALTO Network** screen. This gateway is created by default if you have fully configured your BAS integration in ProAccess SPACE General options. See *BAS Integration Tab* for more information.

- **Encoders**: This view shows the encoders on the system.
- **Control units**: This view shows online IP (CU5000) access points. See *Configuring Online Connection Types* for more information.

Click the appropriate tab to display each filtered view. The screen also includes an **Unreachable items** tab. Click on this tab to view and configure all items that require additional connection information.

The following table describes the buttons use on the SALTO network main screen.

Table 60: SALTO Network main screen buttons

Item	Description
Update	Allows you to update the selected access point.
Show firmware	Allows you to show the firmware of the selected access point and update it.
Refresh	Allows you to refresh the window with the most updated peripherals status.
Delete	Allows you to delete the selected peripheral.
Add Network device	Allows you to add a new online device.

5. 34. 1. Adding Network Devices

You can add the following network devices to the system:

- Ethernet encoders
- RF gateways
- RF nodes
- CU42E0 gateways
- CU4200 nodes

The following sections describe how to add these devices.

5. 34. 1. 1. Adding Ethernet Encoders

See *Encoders* for more information about encoders.

To add an Ethernet encoder, perform the following steps:

223. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
224. Click **Add Network Device**. The **Add network device** dialog box is displayed.
225. Select **Encoder** from the drop-down list.
226. Click **OK**. The **Encoder** information screen is displayed.

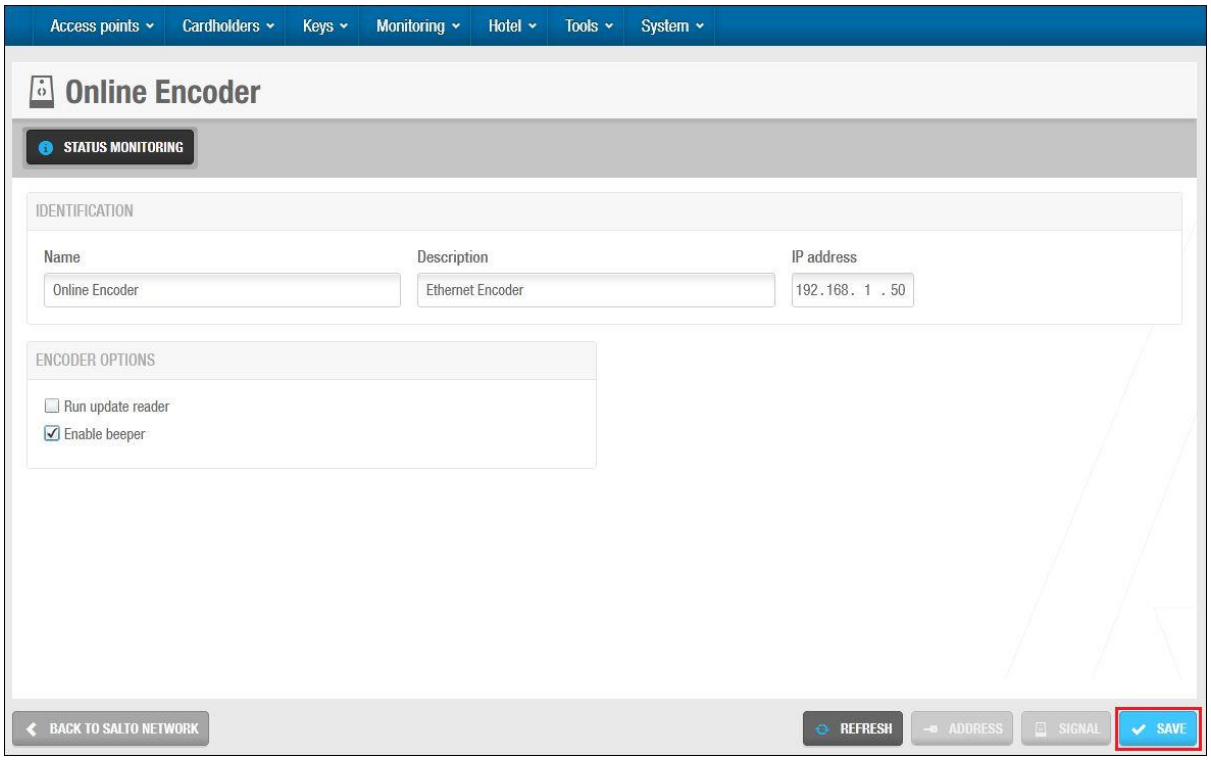


Figure 248: Encoder information screen

227. Type a name for the encoder in the **Name** field.
228. Type a description for the encoder in the **Description** field.
229. Type an IP address for the encoder in the **IP address** field.
230. Select the **Run update reader** checkbox if required.

    This option is used to configure an Ethernet encoder to update user keys automatically when users present their keys to it. If you select this option, the encoder runs continuously but it can only update keys. It cannot be used to encode keys with access data from the SALTO software. See *Updating Keys* for more information.

231. Select the **Enable beeper** checkbox if required.

    If you select this option, the encoder emits beeps when in use.

232. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Click **Save**.

5. 34. 1. 2. Adding RF Gateways

Gateways are hardware devices that provide a link between networks that use different base protocols. RF gateways allow data to be transmitted from the system to the SALTO RF locks, and from the RF locks to the system. RF gateways control RF nodes. See *Adding RF Nodes* for more information about RF nodes.

You must physically connect RF nodes to an RF gateway using an RS485 cable to establish communication between the RF nodes and the RF gateway. See the *SALTO Datasheet_Gatewayx2_xxx* document for more information about this process. You must

also connect RF nodes and RF gateways in ProAccess SPACE so the system can show which nodes and gateways are connected.

To add an RF gateway, perform the following steps:

233. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
234. Click **Add Network Device**. The **Add network device** dialog box is displayed.
235. Select **RF gateway** from the drop-down list.
236. Click **OK**. The **RF gateway** information screen is displayed.

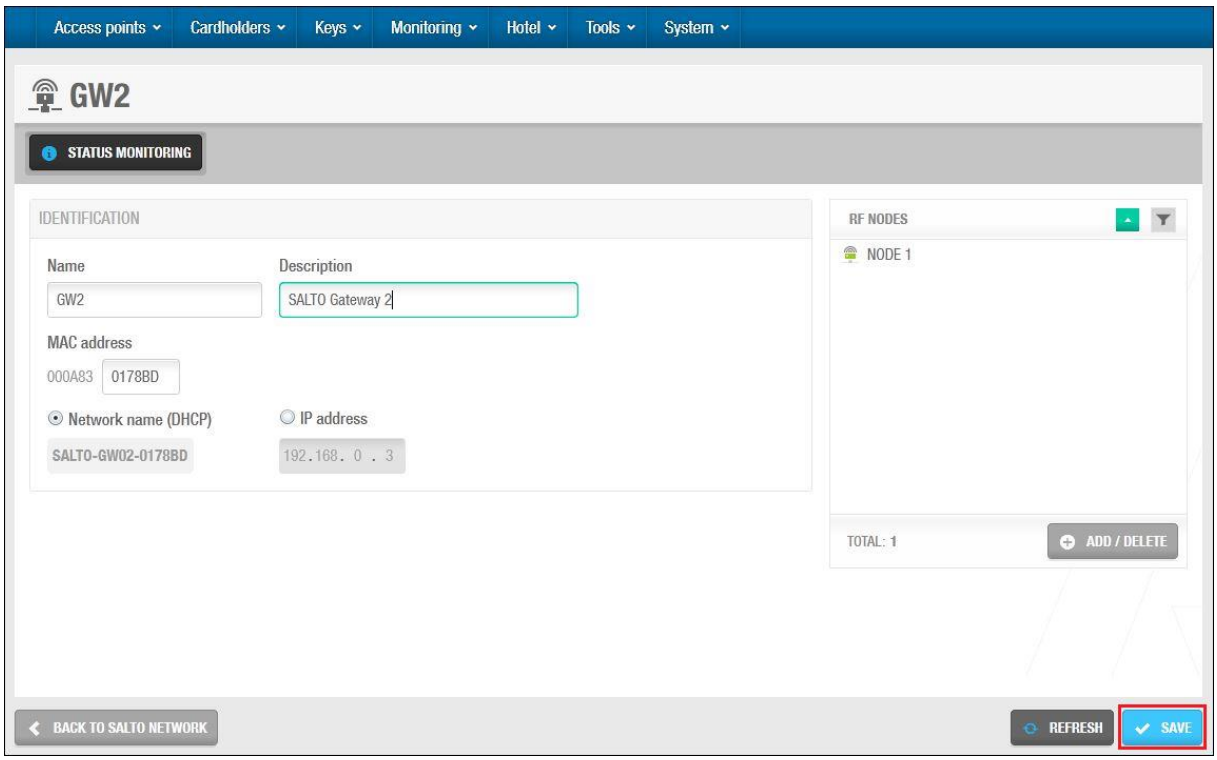


Figure 249: RF gateway information screen

237. Type a name for the RF gateway in the **Name** field.
238. Type a description for the RF gateway in the **Description** field.
239. Type the media access control (MAC) address in the **MAC address** field.

    This is usually displayed on the Ethernet board of the RF gateway.

240. Select either the **Network name (DHCP)** or **IP address** option.

    If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the RF gateway. A Dynamic Host Configuration Protocol (DHCP) server and a DNS are required for this option. If you select the **IP address** option, you must type a static IP address in the field.

241. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

242. Click **Add/Delete** in the **RF Nodes** panel. The **Add/Delete** dialog box, showing a list of RF nodes, is displayed.

The **Add/Delete** dialog box only displays RF nodes if you have already added them to the system. You can also connect RF nodes to RF gateways when you add RF nodes to the system. See *Adding RF Nodes* for more information.

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

    You can hold down the Ctrl key while clicking the RF nodes to make multiple selections. You cannot add RF nodes that already belong to another gateway.

244. Click **Accept**. The selected RF node is displayed in the **RF Nodes** panel.
245. Click **Save**.

5. 34. 1. 3. Adding RF Nodes

RF nodes are network connection points that are physically connected to an RF gateway using an RS485 cable. See *Adding RF Gateways* for more information. This establishes communication between the RF nodes and the RF gateways. Also, in ProAccess SPACE you must connect RF nodes to RF gateways, and RF access points to RF nodes. This means that the system can show which items are connected.

NOTE: You must select **Online RF (SALTO)** in the **Connection Type** panel on the **Door** or **Room** information screen to define a door as an RF access point.

To add an RF node, perform the following steps:

246. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
247. Click **Add Network Device**. The **Add network device** dialog box is displayed.
248. Select **RF node** from the drop-down list.
249. Click **OK**. The **RF node** information screen is displayed.

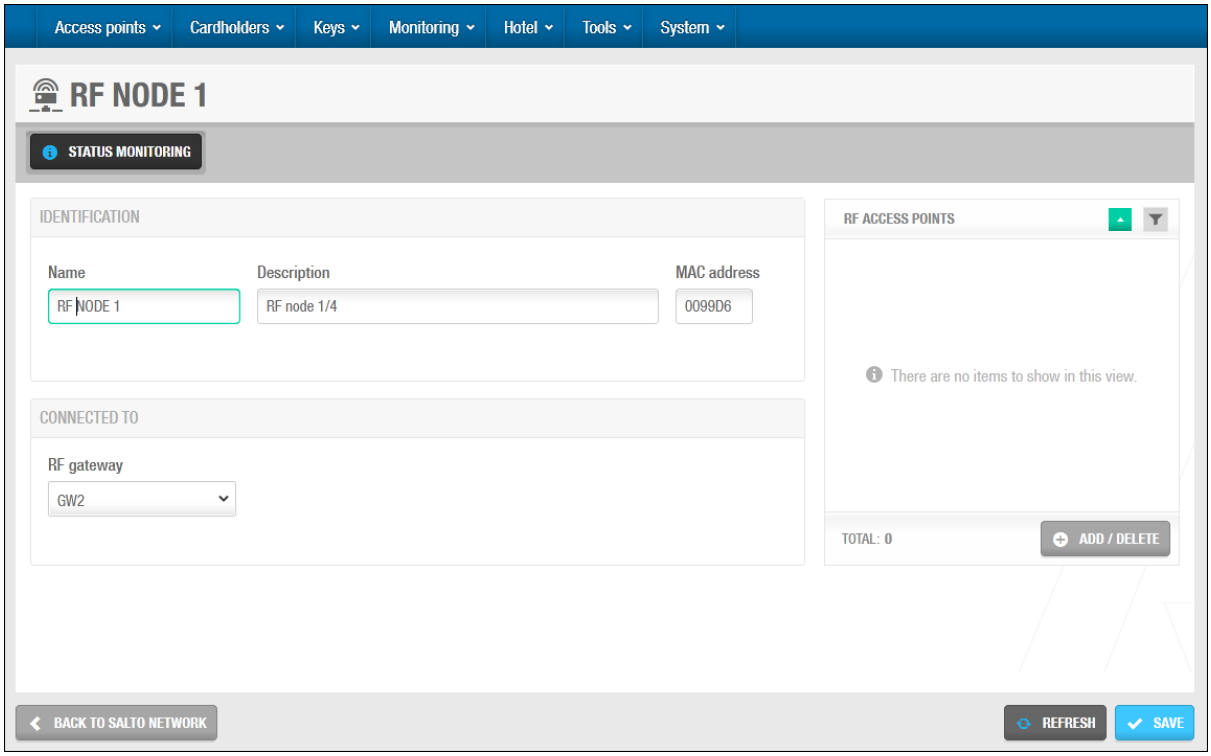


Figure 250: RF node information screen

250. Type a name for the RF node in the **Name** field.

251. Type a description for the RF node in the **Description** field.
252. Type the MAC address of the antenna in the **MAC address** field.
253. Select the RF gateway to which you want to connect the RF node from the **Connected to** drop-down list.

    The default option is **None**.
254. Click **Add/Delete** in the **RF Access Points** panel. The **Add/Delete** dialog box, showing a list of RF access points, is displayed.

    The **Add/Delete** dialog box only displays RF access points if you have already defined doors as RF access points by selecting **Online RF (SALTO)** in the **Connection Type** panel on the **Door** or **Room** information screens. You can also connect online RF (SALTO) doors to RF nodes by using the **Connected to** field on the **Online RF (SALTO)** information screen. See *Online RF (SALTO)* for more information.
255. Select the required RF access point in the left-hand panel and click the chevron. The selected RF access point is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the RF access points to make multiple selections. You cannot add RF access points that already belong to another RF node.
256. Click **Accept**. The selected RF access point is displayed in the **RF Access Points** panel.
257. Click **Save**.

NOTE: RF gateways have a mini node connected to them. You must add this node in ProAccess SPACE by following the procedure for adding RF nodes. Also, you must connect the mini node to the RF gateway in ProAccess SPACE.

5. 34. 1. 4. Adding CU42E0 Gateways

CU42E0 gateways are CUs that are connected to a local area network (LAN) using a network cable. They connect to the SALTO network using a TCP/IP connection. CU42E0 gateways can control CU4200 nodes. See *Adding CU4200 Nodes* section below for more information about CU4200 nodes.

The CU42E0 gateways provide a link between the CU4200 nodes and the SALTO system, and transmit data to the nodes. This means the CU4200 nodes do not require a TCP/IP connection. You must physically connect CU4200 nodes to a CU42E0 gateway using an RS485 cable. This establishes communication between the CU4200 nodes and the CU42E0 gateway. You must also link CU42E0 gateways and CU4200 nodes in ProAccess SPACE so the system can show which nodes and gateways are connected.

CU42E0 gateways control access to doors by activating their relays. Each CU42E0 gateway can control a maximum of two doors. They can also update user keys.

The CU42E0 supports up to 4 auxiliary CU4200 nodes, meaning this that up to 10 online doors can be controlled using a single IP address (1 CU42E0 gateways + 4 CU4200 nodes)

In stand-alone mode, dipswitches on the CU4200 node units must be set up to 0000, if online, each node should have its own configured address, using the suitable dipswitch combination in binary format. See the CU42X0 installation guide for more details. See image below for an example.

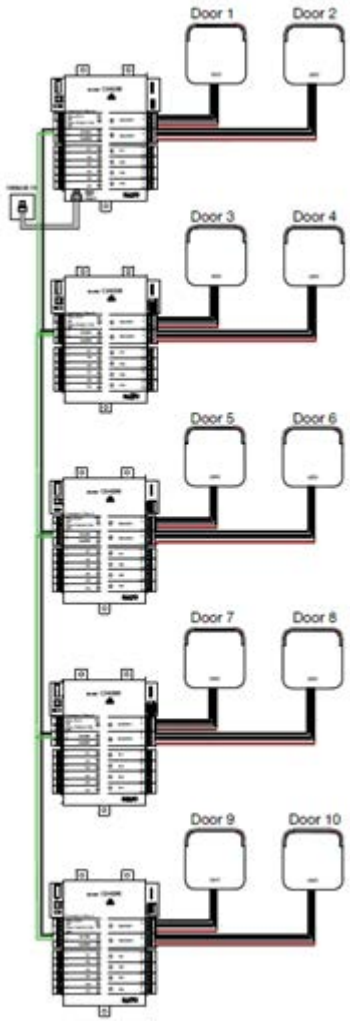


Figure 251: CU42E0 and CU4200 example

NOTE: The maximum distance between the gateway (CU42E0) and the last node (CU4200) in line cannot be over 300 meters.

To add a CU42E0 gateway, perform the following steps:

258. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
259. Click **Add Network Device**. The **Add network device** dialog box is displayed.
260. Select **CU42E0 gateway** from the drop-down list.
261. Click **OK**. The **CU42E0 gateway** information screen is displayed.

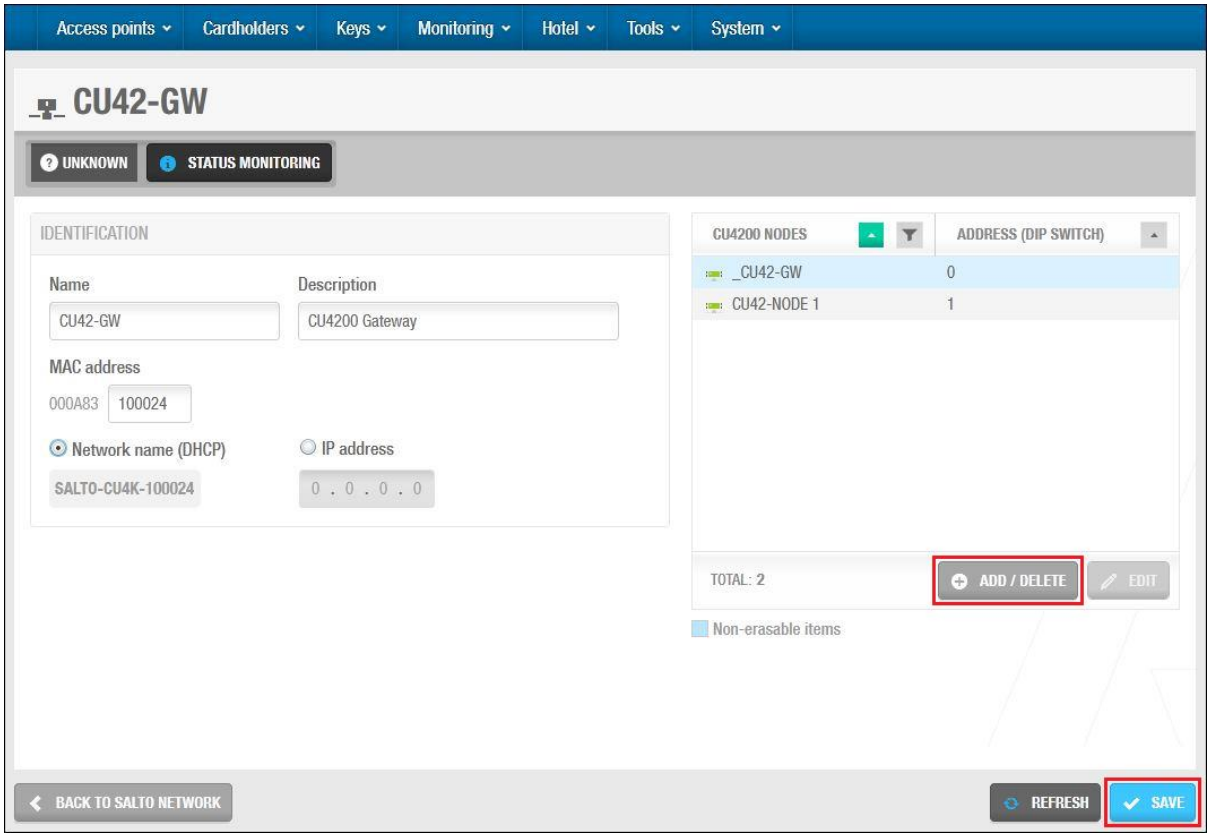


Figure 252: CU4200 gateway information screen

262. Type a name for the CU42E0 gateway in the **Name** field.
263. Type a description for the CU42E0 gateway in the **Description** field.
264. Type the MAC address in the **MAC address** field.

    The MAC address is displayed on a sticker on the CU.

265. Select either the **Network name (DHCP)** or **IP address** radio button.

    If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the CU42E0 gateway. A DHCP server and a DNS are required for this option. If you select the **IP address** option, you must type an IP address in the field.

266. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

267. Click **Add/Delete** in the **CU4200 Node** panel. The **Add/Delete** dialog box, showing a list of CU4200 nodes, is displayed.

    The **Add/Delete** dialog box only displays CU4200 nodes if you have already added them to the system. You can also connect CU4200 nodes to CU42E0 gateways when you add CU4200 nodes to the system. See *Adding CU4200 Nodes* for more information.

268. Select the required CU4200 node in the left-hand panel and click the chevron. The selected CU4200 node is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the CU4200 nodes to make multiple selections. You cannot add CU4200 nodes that already belong to another CU4200 gateway.

NOTE: When you add a CU42E0 gateway, an embedded CU4200 node is automatically created. This cannot be deleted. Each CU42E0 gateway can support its embedded CU4200 node and a maximum of four other CU4200 nodes. The name of the embedded node will be always the same than the parent CU42E0 gateway preceeded by an underscore. For example: **_CU4200.**

269. Click **Accept**. The selected CU4200 node is displayed in the **CU4200 Node** panel.

    You can select the CU4200 node and click **Edit** to change the number in the **Address (dip switch)** column if required. See *Adding CU4200 Nodes* for more information about the **Address (dip switch)** field. Note that embedded CU4200 nodes have a fixed number (0). This cannot be changed.

270. Click **Save**.

5. 34. 1. 5. Adding CU4200 Nodes

CU4200 nodes are network connection points that are physically connected to a CU42E0 gateway using an RS485 cable. See *Adding CU42E0 Gateways* for more information about CU42E0 gateways. This establishes communication between the CU4200 nodes and the CU42E0 gateway.

The CU4200 nodes receive data from the CU42E0 gateway so they do not require a TCP/IP connection. Instead, they communicate with the SALTO network through the CU42E0 gateway to which they are connected.

You must connect CU4200 nodes to CU42E0 gateways in ProAccess SPACE. You must also connect CU4200 nodes to access points. This means that the system can show which items are connected. Each CU4200 node can control a maximum of two doors.

NOTE: You must select **Online IP (CU4200)** in the **Connection Type** panel on the **Door** and in **Room** information screen before you can connect an access point to a CU4200 node.

To add a CU4200 node, perform the following steps:

271. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
272. Click **Add Network Device**. The **Add network device** dialog box is displayed.
273. Select **CU4200 node** from the drop-down list.
274. Click **OK**. The **CU4200 node** information screen is displayed.

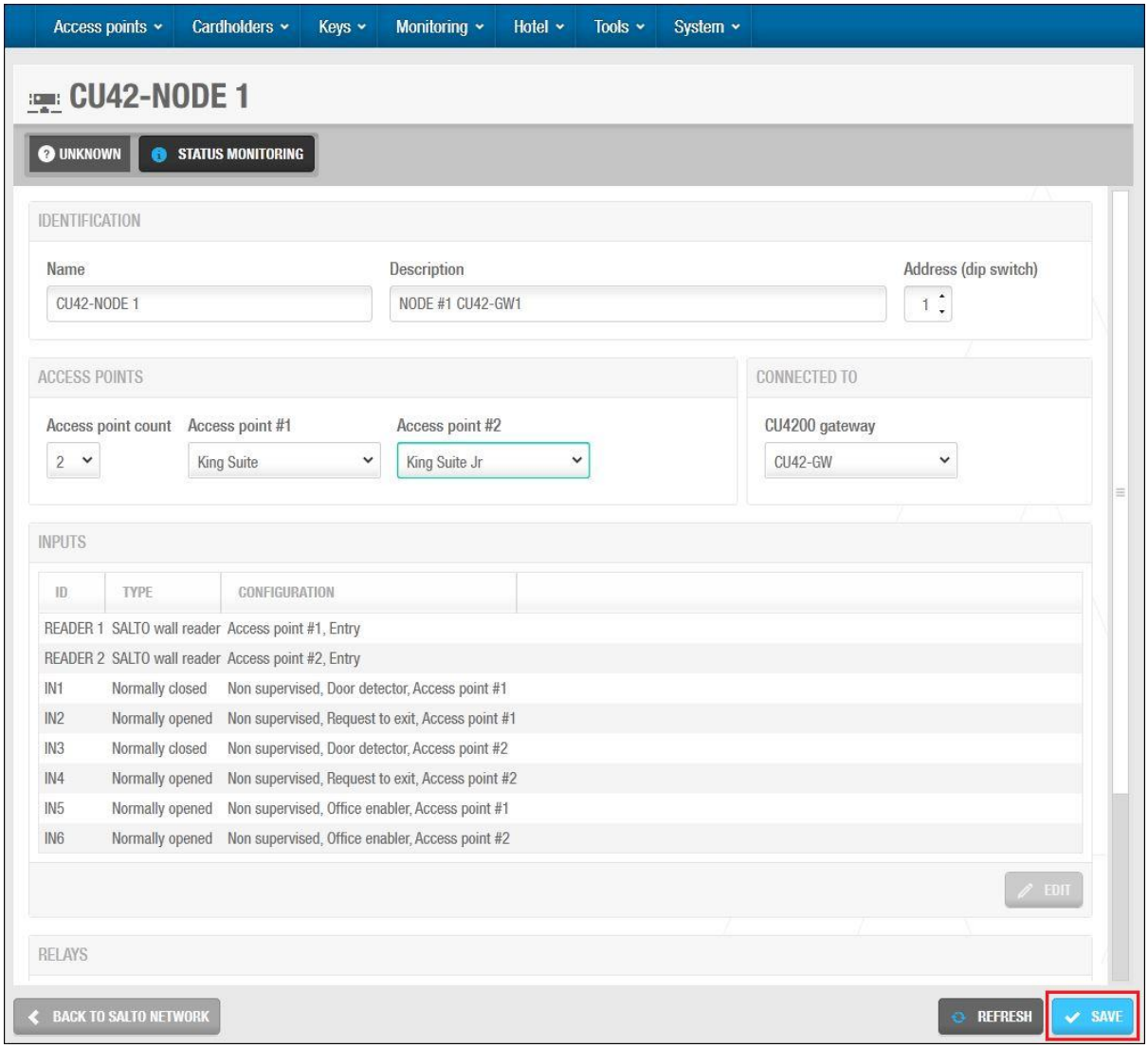


Figure 253: CU4200 node information screen

275. Type a name for the CU4200 node in the **Name** field.
276. Type a description for the CU4200 node in the **Description** field.
277. Select the required number by using the up and down arrows in the **Address (dip switch)** field.

    This number corresponds to the switches on the dip switch panel. The system allows you to select any number between 1 and 99. However, you must select a number between 1 and 15 due to hardware limitations. A CU42E0 gateway can support an embedded CU4200 node and a maximum of four other CU4200 nodes. Each CU4200 node that you connect to a specific CU42E0 gateway must have a unique number, for example, 1, 2, 3, until 15. Note that the value 0 is used for embedded CU4200 nodes. Bear in mind that addresses set up on the nodes should follow the physical dipswitches' configuration on each CU4200 unit.

Table 61: Dipswitch configuration

Dip switch	Address (dip switch)
0000	Address 0, only for embedded CU4200 nodes.
0001	Address 1

Dip switch	Address (dip switch)
0010	Address 2
0011	Address 3
0100	Address 4
0101	Address 5
0110	Address 6
0111	Address 7
1000	Address 8
1001	Address 9
1010	Address 10
1011	Address 11
1100	Address 12
1101	Address 13
1110	Address 14
1111	Address 15

See the following image as an example;

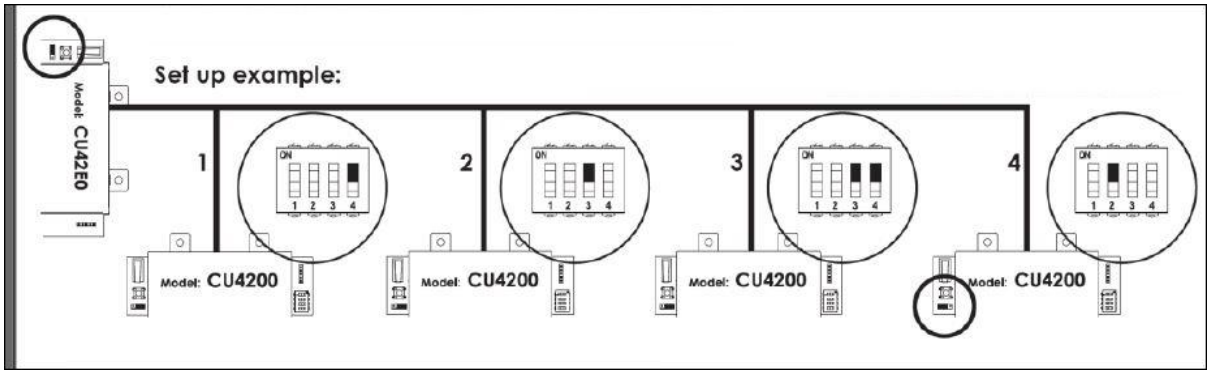


Figure 254: CU4200 dip switches set up

278. Select the required number from the **Access point count** drop-down list.

You can select either **1** or **2.** This defines the number of doors you want the CU4200 node to control. Each CU4200 node can control two readers. This means it can control either one door that has two readers or two doors where each has one reader. If a door has two readers, one reader controls access from inside to outside, and the other reader controls access from outside to inside. You should select **1** if a door has two readers. If you select **2,** an **Access point #2** field is displayed on the right-hand side of the **Access point #1** field, and you can select an additional door from the drop-down list.

279. Select the required door from the **Access point #1** drop-down list.

The **Access point** drop-down lists only display doors if you have already defined some as CU4200 access points. This is done by selecting **Online IP (CU4200)** in the **Connection Type** panel on the **Door** information screen. You can also connect online IP (CU4200) doors to CU4200 nodes in the **Connected to** field on the **Online IP (CU4200)** information screen. See *Online IP (CU4200)* for more information.

280. Select the CU42E0 gateway to which you want to connect the CU4200 node from the **Connected to** drop-down list.
281. Click **Save**.

5. 34. 1. 6. Using CU4200 Inputs

Inputs are the signals or data received by the CU4200. You can setup the inputs in ProAccess SPACE so the CU4200 can understand how to act. You can set Inputs for **Reader 1** and **Reader 2.** You can also set up to 6 inputs from third party devices.

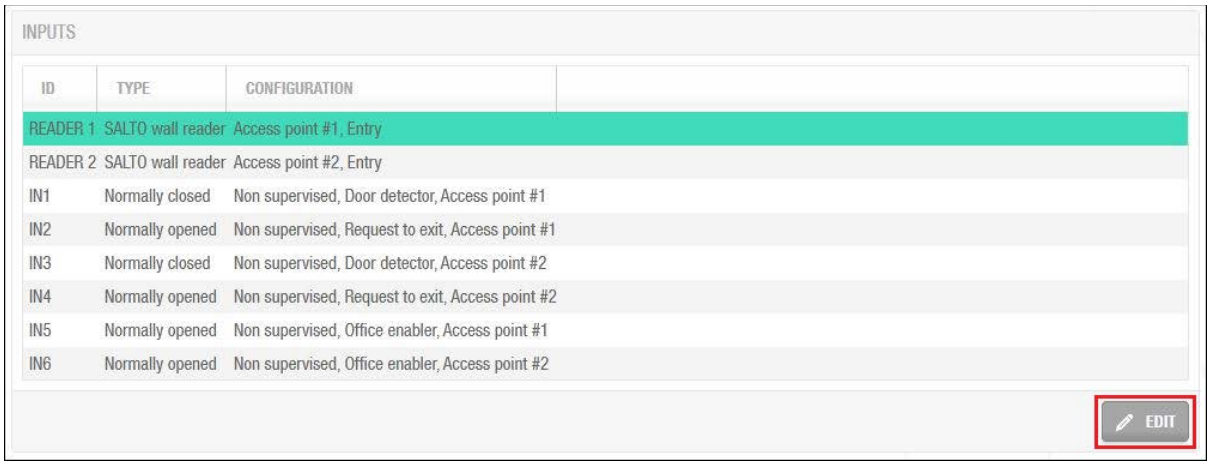


Figure 255: CU4200 node Inputs

You can set the CU4200 outputs according with the wall reader input. To manage the wall reader input, select the reader and click **Edit**.

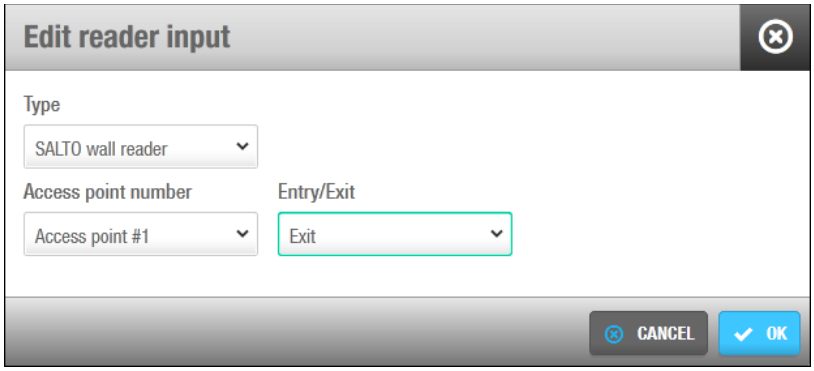


Figure 256: CU4200 node Reader Input

The **Reader input** fields are described in the following table.

Table 62: Reader Inputs fields

Field	Functionality
Type	You can select **None** if no SALTO wall reader is connected or **SALTO wall reader** if it is a SALTO wall reader. Other options may appear in the future. If **None** is selected, inputs 3, 4 and 5, 6 can be used with a third party wall reader.
Access point number	As the CU4200 can manage up to two different access points, you can decide whether the reader will trigger an opening in access point #1 or #2. See *Adding CU4200 Nodes* for more information.

Field	Functionality
Entry/Exit	Select whether the wall reader is an Entry or an Exit.

The CU4200 node can manage inputs from third party devices. Depending the signal or data arrived to the input the CU4200 Node can act accordingly. Select the **Input ID** and click **Edit**.

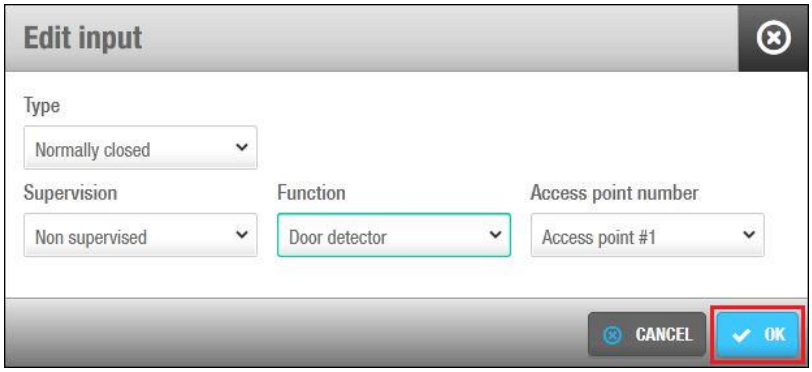


Figure 257: CU4200 node Reader Input

The **Inputs** fields are described in the table below,

Table 63: Inputs fields

Field	Functionality
Type	Status of the relay in normal position. The relay can be normally in closed position or opened position.
Supervision	Select the resistance as required for the supervision. A supervised input is protected against external attacks.
Function	Select the function you want for the relay. Options include doo Door detector, Office enabler, Intrusion inhibition, Request to open roller blind, Request to close roller blind, Request to Exit or Request to Open.

For example, according to the image below, a relay in normally opened position could send a request to open a roller blind when presenting a valid key in reader #1 from IN1 and request to close the roller blind from IN2.

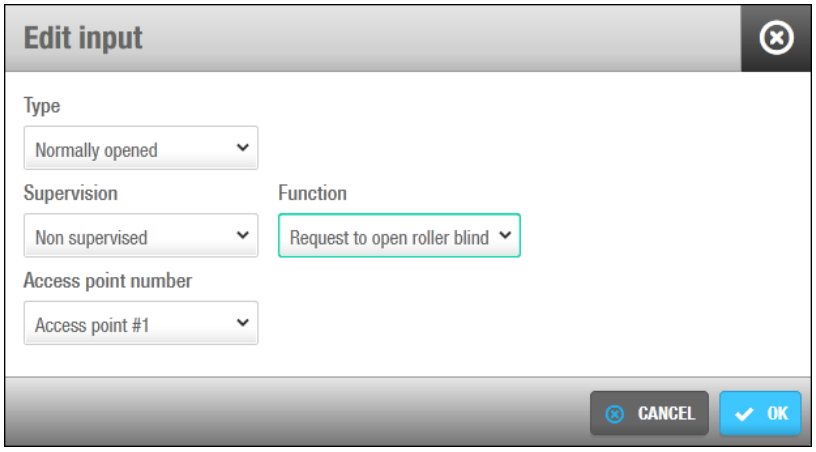


Figure 258: Roller blind example

A reader that is not from SALTO can also be used. **Edit Reader Input** Type must be set to **None**. **Type** field in **Edit Input** shows the **Third party reader** option in the dropdown menu. Only a **Wiegand** code is supported. See *Devices Tab* in General options for more information about how to configure the Wiegand format. An authorization code has to be entered for each user in the **Authorization code** field on the **User** profile. See *Users* in **Cardholders** menu for more information. Select the **Access point** from the **Access point number** dropdown menu and if it will be an **Entry** or an **Exit.**

5. 34. 1. 7. Managing CU4200 Relays

A relay is an electrically operated switch. It is used where it is necessary to control a circuit by a low-power signal. For example, you can control an electric or magnetic strike, trigger a camera recording or turn an alarm off.

The CU4200 node has 4 relays that can be configured independently. Select the relay ID and click **Edit**. The **Edit Relay** fields are described in the table below

Table 64: Edit Relay fields

Field	Functionality
Type	Select the appropriate type as needed.
Access point number	Select the access point in question. It can be **Access point #1, Access point #2** or both.
Output	The **Output** dropdown menu is shown when Output is selected in **Type** dropdown menu. Select the Output from the dropdown menu. The list of outputs have to be created first in **Outputs** list, in the **Access points** menu. See Access points *Outputs* for more information about how to create Outputs. The relay will be triggered when a key with a valid output is presented to the wall reader. See User *Outputs* for more information about how to add outputs in the user access.
Conditions	Select **Combined** in the **Type** dropdown menu to select a combination of conditions. According to the image below, the relay will be triggered if in Access point #1 the **Door is left opened**, if there is an **Intrusion** or if there is a **Card rejected**.

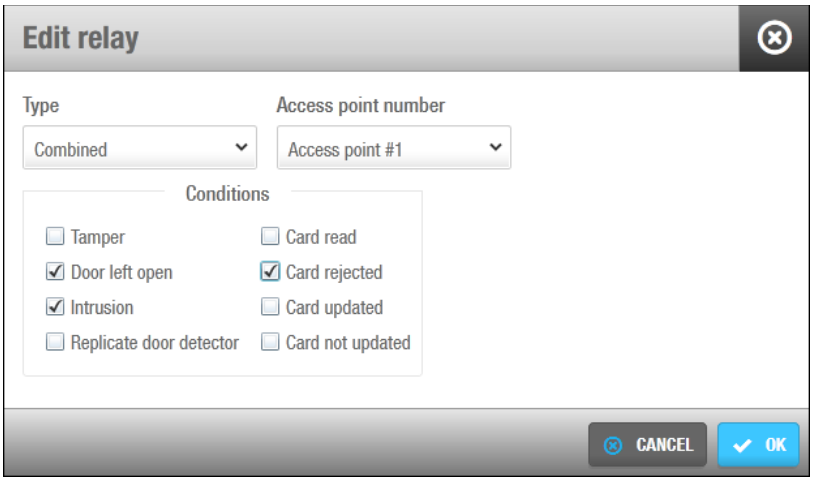


Figure 259: Combined relay type

5. 34. 1. 8. CU42X0 devices initialization and update

The CU42E0 gateways and CU4200 nodes are initialized and updated automatically. See table below for the frequency of each.

Table 65: CU42x0 Initialization and Update

Automatic process	Check Frequency	Notes
CU4K doors initialization	1 minute	Includes initialization + update
CU4K doors update	5 minutes	Can be executed on request
CU4K nodes initialization	1 minute	Includes initialization + update
CU4K nodes update	5 minutes	Can be executed on request

NOTE: Even if updates are performed automatically every 5 minutes for the CU42x0, a manual update can be performed immediately by selecting the device and clicking the **Update** button in **SALTO network**.

5. 34. 2. Filtering SALTO Network Data

You can filter SALTO network data by type, name, description, and/or IP address.

You can filter by the following item types:

- Online IP (CU5000)
- CU42E0 gateway
- CU4200 node
- Online IP (CU4200)
- Encoder
- RF gateway
- RF node
- Online RF (SALTO)
- BAS gateway
- Online RF (BAS integration)

To filter the SALTO network data, perform the following steps:

282. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
283. Click **Filters**. The **Items filtering** dialog box is displayed.
284. Select a pre-defined search term from the **Type** drop-down list.
285. Type the name of the item you want to search for in the **Name** field.
286. Type the description of the item you want to search for in the **Description** field.
287. Type the IP address in the **IP address** field if appropriate.

    The **IP address** field is only displayed for relevant search term types.

288. Click **Apply Filter**. A filtered SALTO network list is displayed.

    When a filter has been applied, on the **SALTO Network** screen when you have applied a filter, the search type is displayed in light blue. You can click the search type to once again display all items on the list screen. You can click **Delete Filter** to delete the filter and to redefine the filter parameters.

289. Click the **Close** icon in the **Applied Filters** field when you have finished reviewing the filtered list or click **Filters** to apply another filter.

5. 34. 3. Configuring Online Connection Types

When adding a door or room to the system, you must specify the appropriate connection type – either online or offline. When you select an online connection type, the door or room is displayed on the **SALTO Network** screen, and you can double-click the entry to configure it.

There are four online connection types:

- Online IP (CU5000)
- Online IP (CU4200)
- Online RF (SALTO)
- Online RF (BAS integration)

NOTE: Your BAS integration must be fully configured in ProAccess SPACE General options before you can select this option. See *BAS Tab* for more information.

See *Connection Types* for more information about selecting the correct connection types in non-hotel sites. For information about connection types in non-hotel sites, see *Connection Types*.

5. 34. 3. 1. Online IP (CU5000)

To configure an online IP (CU5000) door, perform the following steps:

290. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
291. Double-click the online IP (CU5000) door that you want to configure. The **Access point: Online IP (CU5000)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU5000) doors are online SVN points.

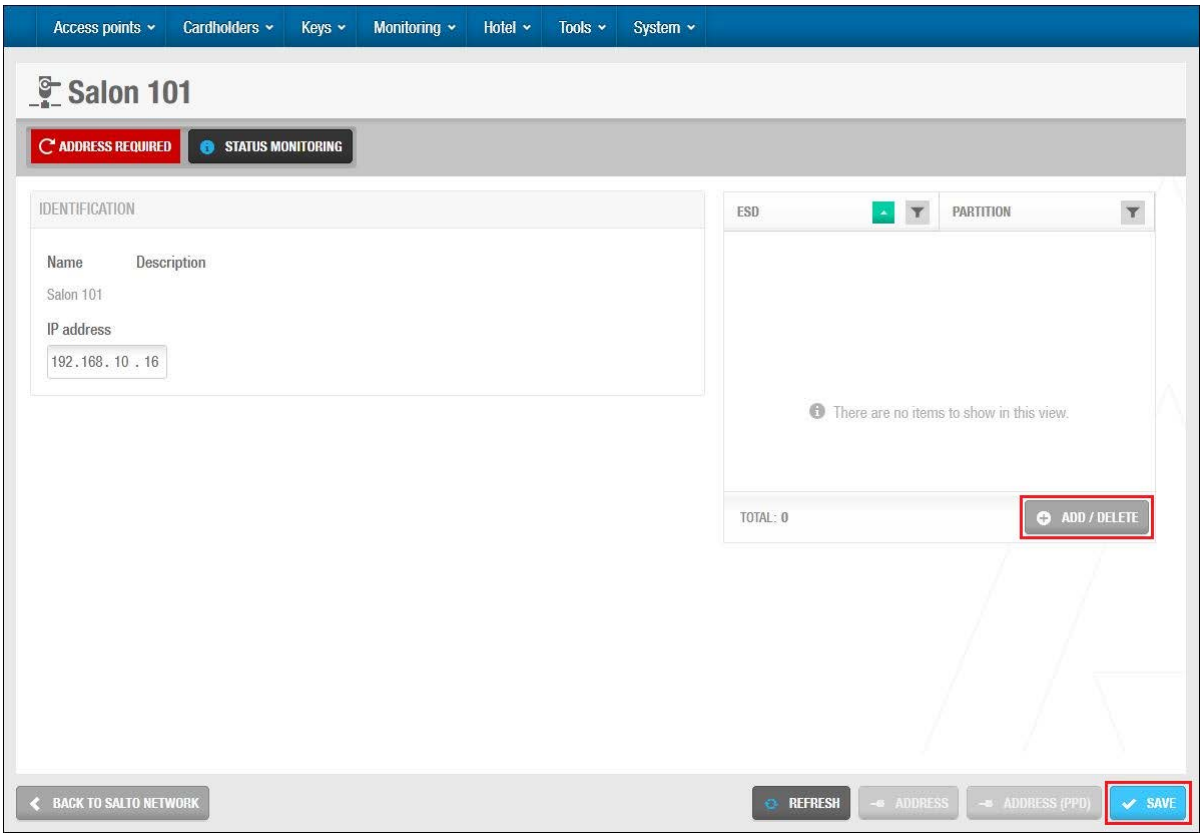


Figure 260: Access point: Online IP (CU5000) information screen

292. Type an IP address for the door in the **IP address** field.
293. Click **Add/Delete** in the **ESD** panel. The **Add/Delete** dialog box, showing a list of ESDs, is displayed. See *ESDs* for more information about ESDs.
294. Select the required ESD in the left-hand panel and click the chevron. The selected ESD is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the ESDs to make multiple selections.
295. Click **Accept**. The selected ESD is displayed in the **ESD** panel.
296. Click **Save**.

5. 34. 3. 2. Online IP (CU4200)

To configure an online IP (CU4200) door, perform the following steps:

297. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
298. Double-click the online IP (CU4200) door that you want to configure. The **Online IP (CU 4200)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU4200) doors that are not connected to CU4200 nodes are displayed in the **Unreachable items** tab. See *Adding CU4200 Nodes* for more information about CU4200 nodes.

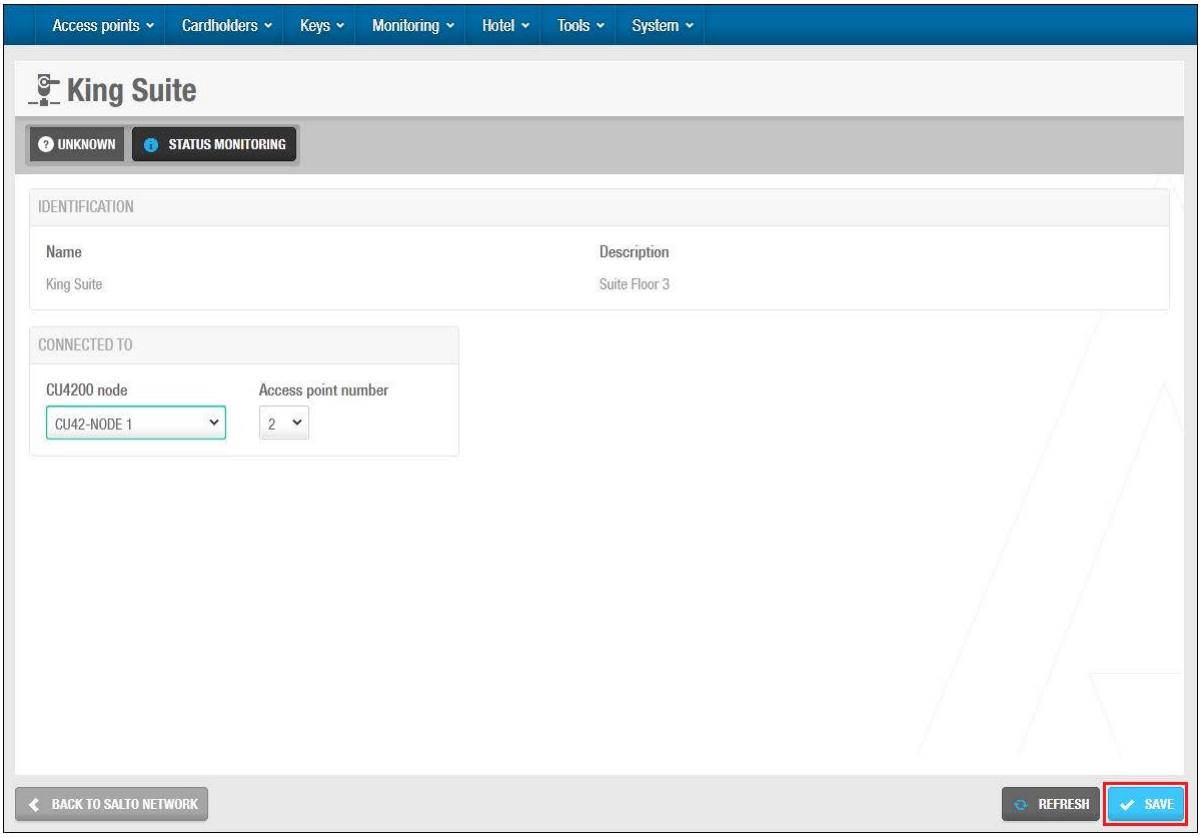


Figure 261: Online IP (CU4200) information screen

299. Select the CU4200 node to which you want to connect the door from the **Connected to** drop-down list.
300. Select either **1** or **2** from the **Door number** drop-down list.

    You cannot select **2** unless you have selected **2** in the **Access point count** drop-down list on the **CU4200 node** information screen. Otherwise, this exceeds the door number count for the node. See *Adding CU4200 Nodes* for more information.
301. Click **Save**.

5. 34. 3. 3. Online RF (SALTO)

To configure an online RF (SALTO) door, perform the following steps:

302. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
303. Double-click the online RF (SALTO) door that you want to configure. The **Online RF (SALTO)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online RF (SALTO) doors that are not yet connected to RF nodes are displayed in the **Unreachable items** tab. See *Adding RF Nodes* for more information about RF nodes.

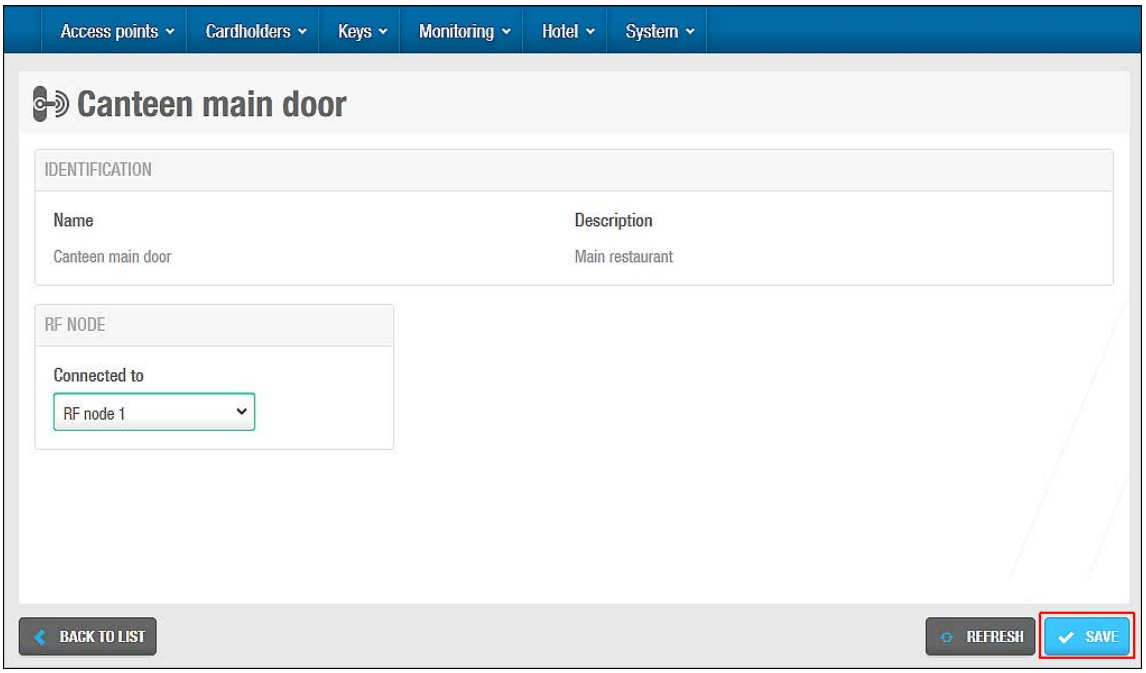


Figure 262: Online RF (SALTO) information screen

304. Select the RF node to which you want to connect the door from the **Connected to** drop-down list.
305. Click **Save**

5. 34. 4. Peripherals Addressing and Maintenance

SALTO network items like Control units, Ethernet encoders, gateways and RF nodes can be added and managed in ProAccess SPACE where you can also make changes such as updating online CUs or updating firmware.

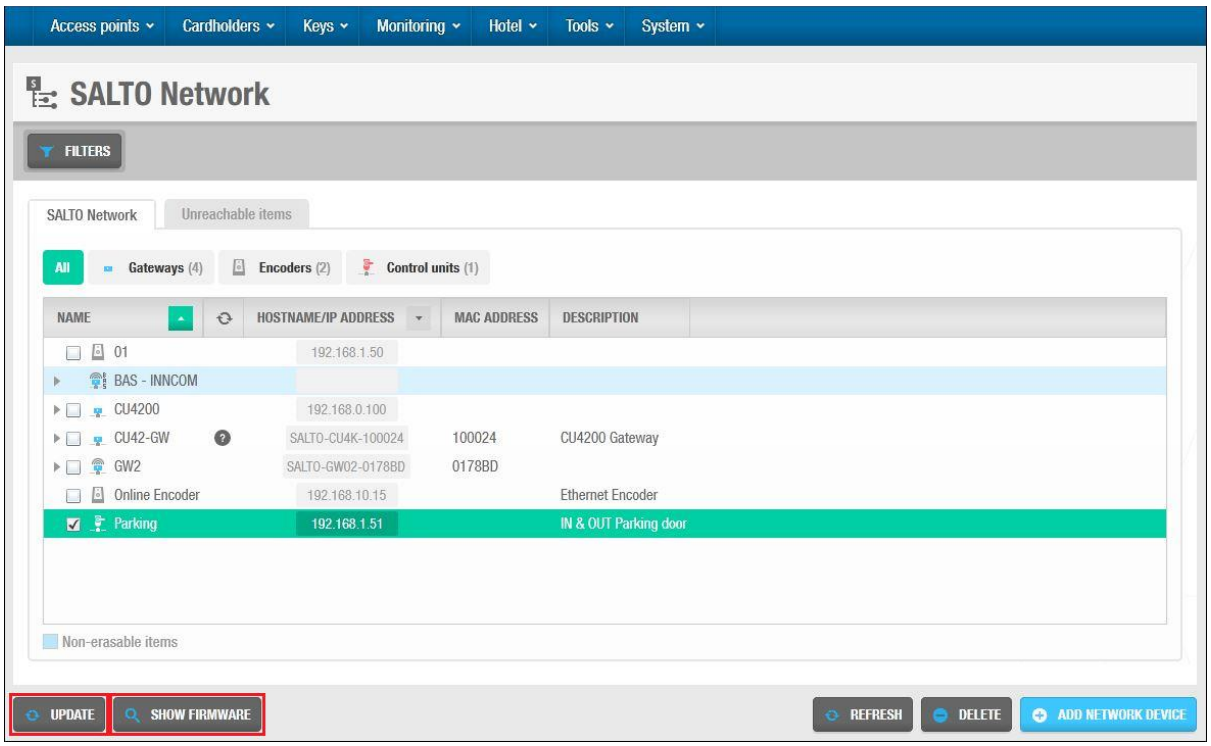


Figure 263: Address and Maintenance

The **Address** and **Maintenance** tab buttons are described in the following table.

Table 66: Maintenance buttons

Button	Functionality
Update	Allows updates to the SALTO database to be communicated to the selected network items. In addition, it allows blacklists to be transmitted automatically to doors without the need to visit each door with an updated key. SAM cards can also be used to transfer information to online doors and to update offline escutcheons and cylinders. See *SAM and Issuing Data* for more information. To SAM a local encoder, click **Supported Keys** on the **Settings** screen in ProAccess SPACE. See *Encoder Settings* for more information. You will find this button in all updatable devices such as control unit CU5000 and CU4200.
Show firmware	Displays the firmware version of the selected item. You can check the firmware version for any online device, CU, RF door, or Ethernet encoder. We recommended that you use the latest firmware version with the SALTO system. Online CUs consist of an Ethernet board and a CU board. This may require updating an individual or multiple online CUs to the most recent firmware version. See *Updating Firmware* for more information about updating multiple online CUs simultaneously. You will find this button in all firmware updatable devices such as control unit CU5000, CU4200 gateways and Ethernet encoders.
Address	Assigns an IP address that you have entered on the system for an Ethernet encoder or an online IP (CU5000) door if the peripheral is in the same network. When you click **CLR** on the online CU, for example, the device enters listening mode. When you click **Address** on the **Monitoring** tab, the software sends a broadcast to the online CU. When the broadcast reaches the online CU, it initializes it with the new IP and other door parameters. Note that you can only address one peripheral at a time when using this option. See *Adding Ethernet Encoders* and *Online IP (CU5000)* for more information about entering IP addresses for Ethernet encoders and online IP (CU5000) doors. You will find this button in all updatable devices such as control unit CU5000 and Ethernet encoders.
Address (PPD)	Assigns an IP address, using a PPD, to an online CU if the peripheral is in a different network. When the online CU is initialized by the PPD, click **Address (PPD)** on the **Monitoring** tab. This creates an authentication between the system and the peripheral. You must enable this option by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices** in ProAccess SPACE. See *Devices Tab* for more information. See also *PPD* for more information. You will find this button in all updatable devices such as control unit CU5000.
Signal	Used to help identify the physical Ethernet encoder that corresponds to the applicable IP/peripheral. After you select the peripheral in the list and click **Signal**, the LED of the applicable encoder starts flashing. At this point, the SAMing process can take place. See *SAM and Issuing Data* for more information.

The columns at the top of the **Maintenance** tab are described in the following table.

Table 67: Maintenance columns

Column	Functionality

Column	Functionality
Name	Specifies the name of the item (the icon immediately before the item name indicates the peripheral type)
Update Status	Shows the peripheral update status. If no update is required, no icon will be shown. The status could be **Update required**, **Address required** or **Unknown.** Note that this column does not have a title on the screen.
Hostname/ IP address	Specifies the network name that identifies the item
MAC Address	Specifies the MAC address of the device.
Description	Matches the details of the item entered in the **Description** field in ProAccess SPACE

5. 34. 4. 1. Updating Firmware

Firmware is software that is programmed on the ROM of hardware devices.

NOTE: SALTO provides firmware updates when new functionality is available or when a software bug is fixed. Each component has a unique file. Contact your SALTO technical support contact before updating any firmware file.

To update the firmware version of an item, perform the following steps:

306. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
307. Select the required item and click **Show firmware**. The **Firmware information** dialog box is displayed.

Figure 264: Peripheral firmware update dialog box

You can select multiple items on the **SALTO Network** peripheral list if required.

308. Select the checkbox next to the item that you want to update. The **Browse** button is enabled.

If required, you can click **Check all** to update the firmware for multiple items simultaneously. You can only update multiples of the same item (for example, online CUs only or Ethernet encoders only) simultaneously.

309. Click **Browse** to select the required firmware file.
310. Click **Send firmware**. A confirmation screen is displayed when the firmware update is complete.

NOTE: You can update the firmware for local encoders by using the **Show Firmware** button on the **Settings** screen in ProAccess SPACE. See *Updating Encoder*

Firmware for more information.

Calendars for more information.

NOTE: An access point automatic change differs from an access point timed period in that the access point timed period allows for only one opening mode to be applied to an access point. An access point automatic change allows multiple opening modes to be applied to one access point. See *Roll-Call Areas*

A roll call is used to list the individual users in a specified area at a particular time. For example, you can use a roll call to generate a report after a fire alarm goes off. This way, it is possible to check whether all the users in the area have been safely evacuated. The system generates the roll call by monitoring specific access points. By tracking when cardholders enter and exit using these access points, it is possible to see exactly who is inside or outside the roll-call area.

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

See *Roll-Call* for information about generating a list of individual user names in a roll-call area in ProAccess SPACE. You can also use ProAccess SPACE Roll-Call Monitoring to perform other roll-call tasks, such as searching all roll-call areas for a user and the time and date each user entered the roll-call area. See *Roll-Call* for more information.

5. 34. 5. Creating Roll-Call Areas

To create a roll-call area, perform the following steps:

311. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.

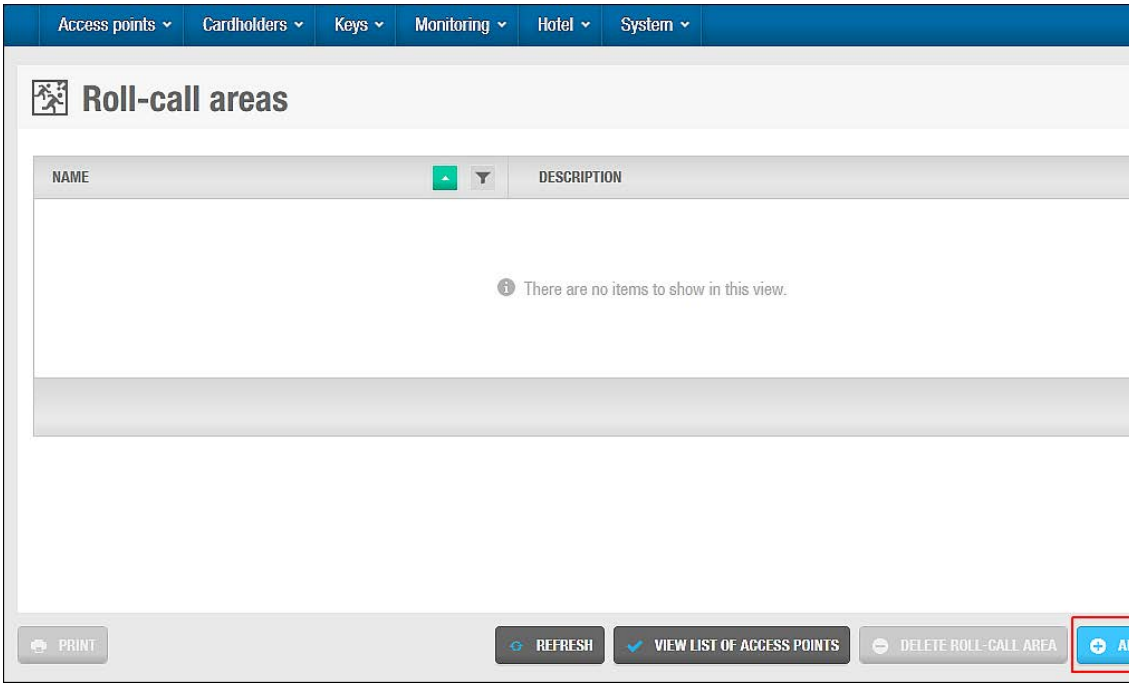


Figure 75: Roll-call areas screen

NOTE: The **View List of Access Points** button shows a list of access points associated with all roll-call areas.

312. Click **Add Roll-Call area**. The **Roll-call area** information screen is

displayed.

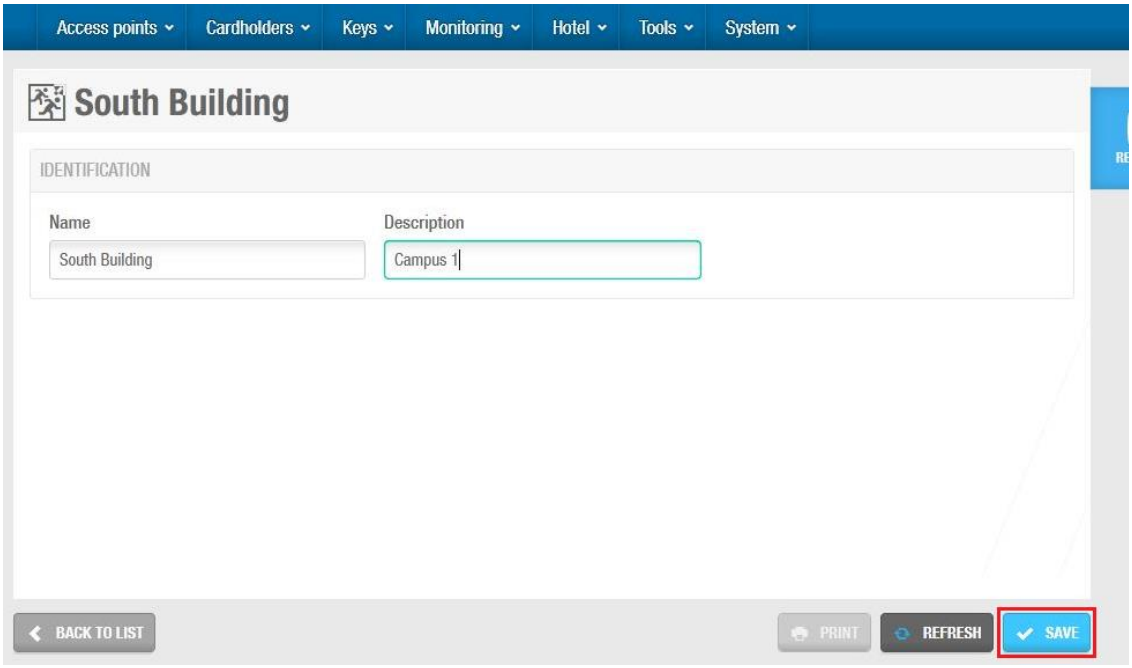


Figure 76: Roll-call area information screen

313. Type a name for the location in the **Name** field.
314. Type a description for the location in the **Description** field.
315. Click **Save**.

5. 34. 5. 1. Creating Roll-Call Exterior Areas

Roll-call areas list the individual users in a specified area at a particular time. To account for the individual users who are on a site but are not in any of the designated roll-call areas, you need to create a separate, exterior area, for example, an assembly area. This is an important concept to consider when creating roll-call areas.

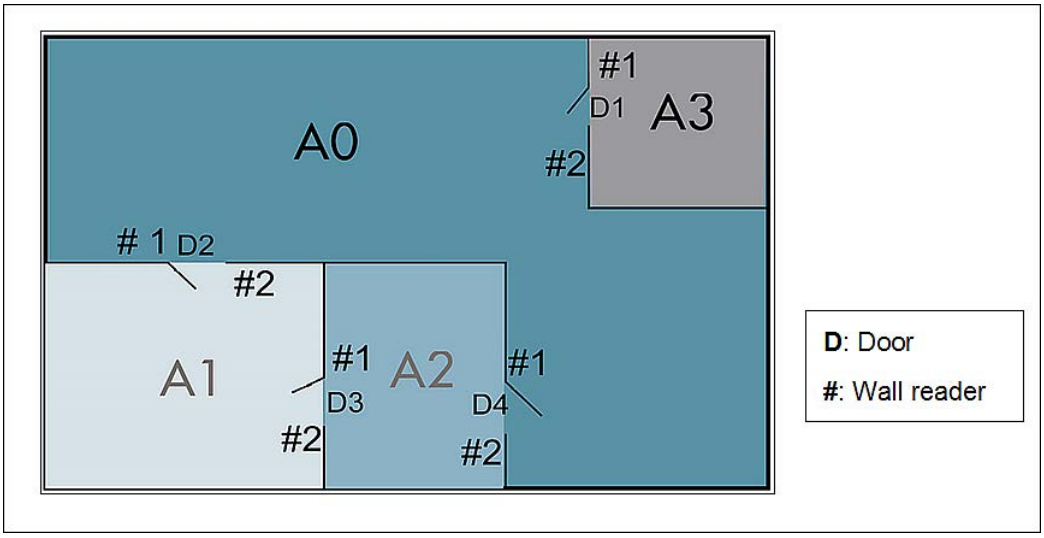


Figure 77: Designated roll-call areas and exterior area

In the above example, there are three standard roll-call areas: A1, A2, and A3. The exterior area is A0, which lists all users who are not in A1, A2, or A3.

A user in A1, A2, or A3 must present their key to a wall reader to exit that roll-call area. When a user presents their key, the system determines that the user has exited the area and entered the exterior area A0. The exterior area allows the system to create accurate roll-call lists, accounting for all the people who are present.

5. 34. 6. Associating Roll-Call Areas

Once you have created a roll-call area, you must associate wall readers with that roll-call area. Each roll-call area must have two wall readers: one to track users entering the area and another to track users exiting the area. The following section describes how to associate roll-call areas with readers.

5. 34. 6. 1. Readers

To associate a reader with a roll-call area, perform the following steps:

316. Select **Access points** > **Roll-call areas**. The **Roll-call areas** screen is displayed.
317. Double-click the roll-call area that you want to associate with a reader. The **Roll-call area** information screen is displayed.
318. Click **Readers** in the sidebar. The **Readers** dialog box is displayed.

    Note that the dialog box will be blank because you have not yet associated an access point with this particular roll-call area.
319. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.

    This list only applies to online CUs where there are two physical wall readers.
320. 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.
321. Click **Accept**. The roll-call area is now associated with the access point.

Access Point Timed Periods for more information.

5. 34. 7. Creating Access Point Automatic Changes

To create an access point automatic change, perform the following steps:

1. Select **Access points** > **Access points automatic changes**. The **Access point automatic changes** screen is displayed.

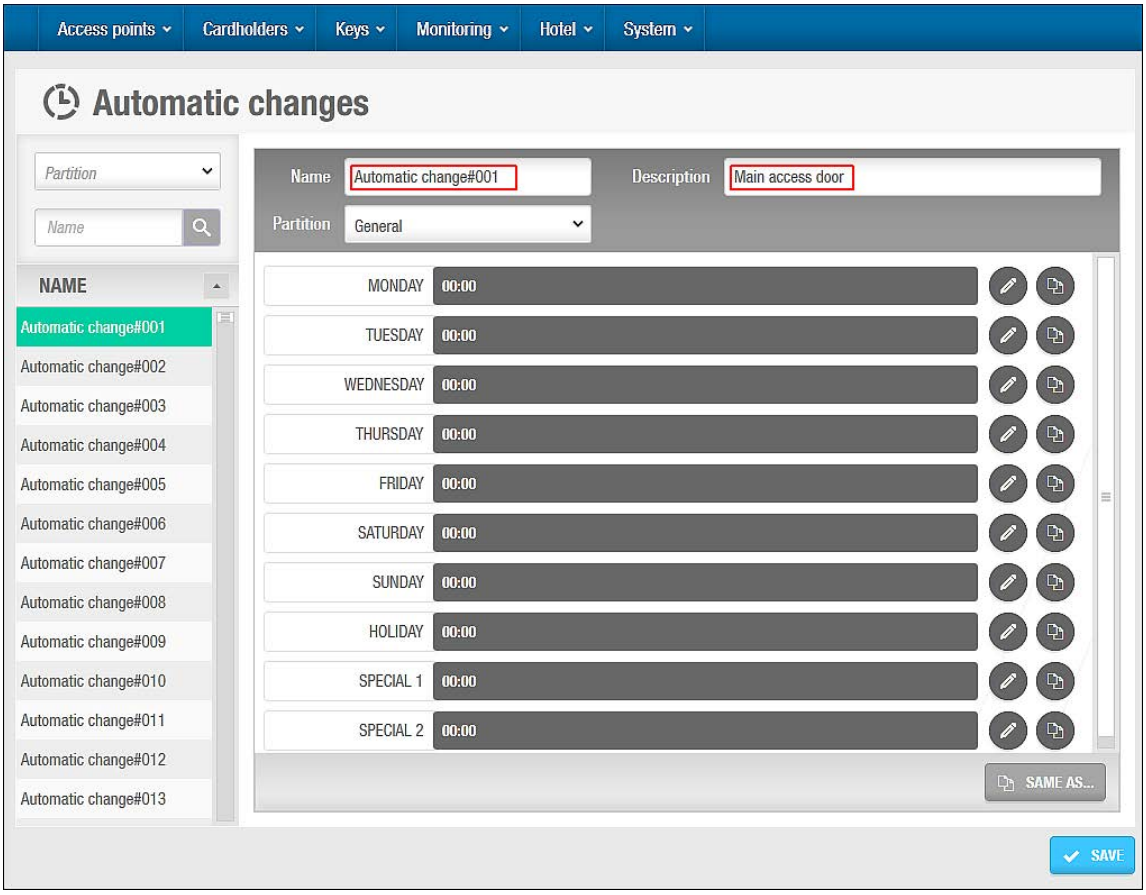


Figure 79: Automatic changes screen

2. Select an automatic change period from the **Name** panel.

   Automatic change#001 is automatically selected. You can rename the automatic change to something more relevant to your organization. If you have already configured this automatic change entry, select the next automatic change period.
3. Type a description of the automatic change period in the **Description** field.
4. Click the **Pencil** icon on the right-hand side of the applicable day. The **Edit automatic changes** dialog box is displayed.

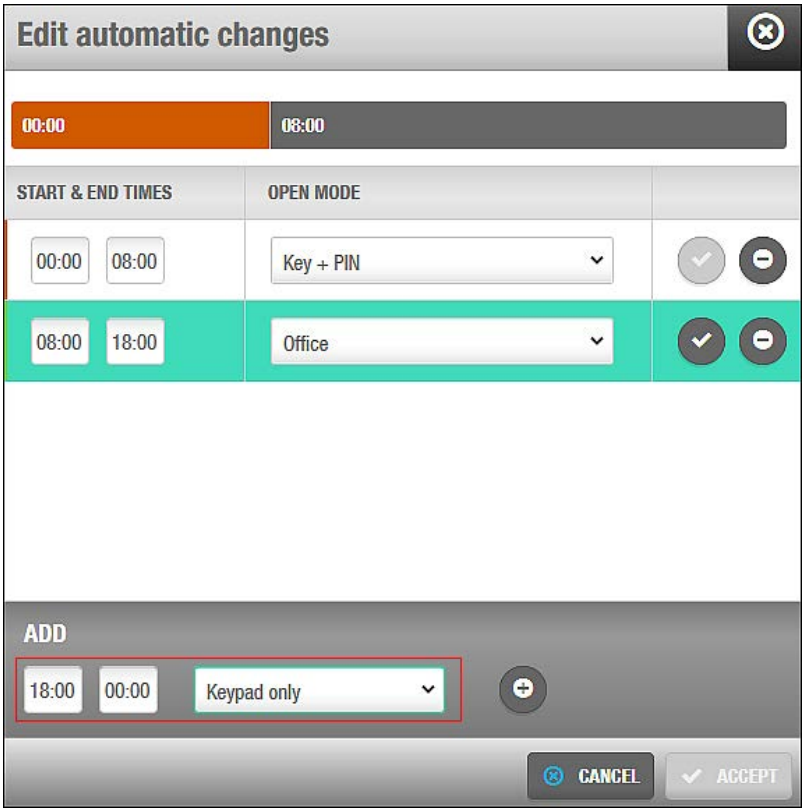


Figure 80: Edit automatic changes dialog box

5. Type a start time and end time for the automatic changes period in the **Add** panel.
6. Select an opening mode from the drop-down list in the **Add** panel.

   The opening modes drop-down list includes an extra mode in addition to those available for managing doors. This extra mode is called the Two-person rule. It can only be enabled from this dialog box. Enabling this mode means that two users must each present a valid key to open the door.
7. Click the **Plus** icon on the right-hand side of the **Add** panel. The automatic change is added.
8. Click the **Tick** icon on the right-hand side of the last automatic change entry to add another entry that starts when the last one ends.
9. Click **Accept** when you have finished adding all of the automatic changes for the specified day.

   The **Automatic changes** screen is displayed with the automatic changes added.

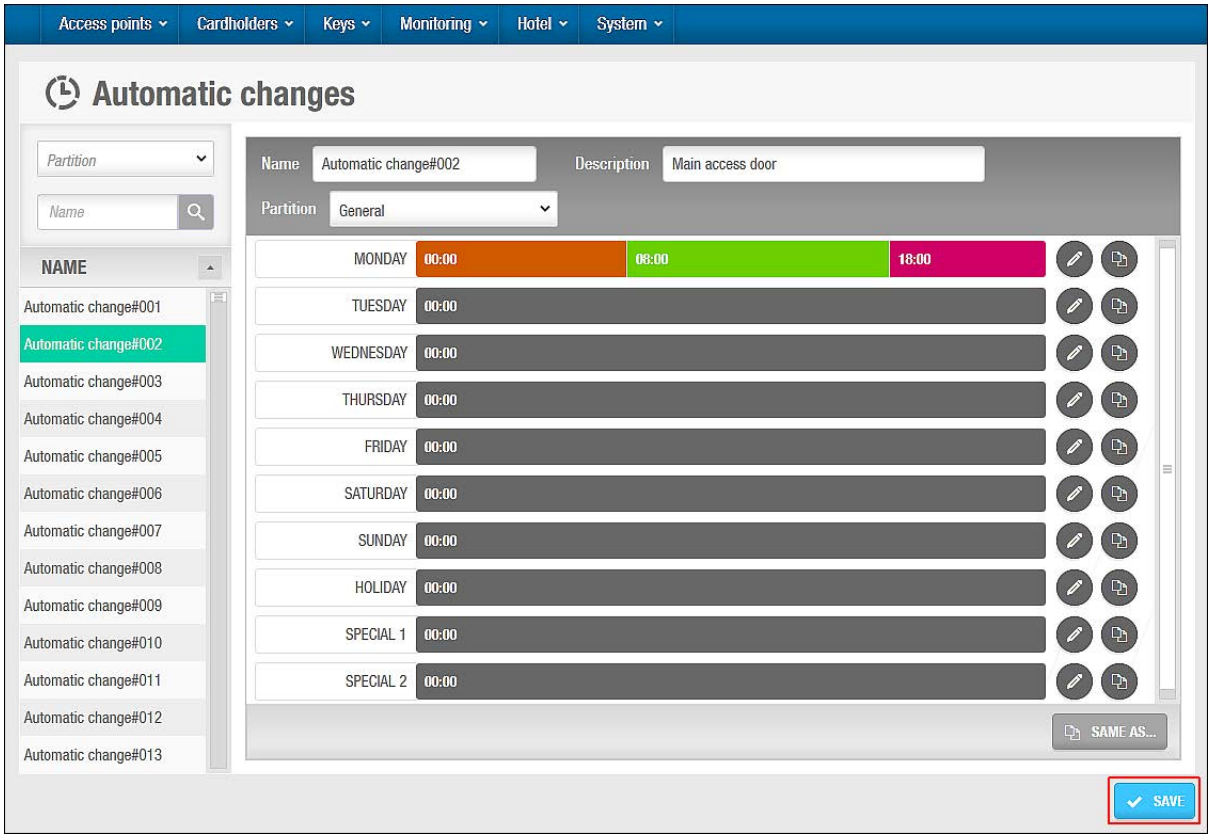


Figure 81: Automatic changes created

10. Click **Save**.

5. 34. 8. Managing Access Point Automatic Changes

You can copy saved automatic changes from one specified day to another day. You can also copy all the details from one saved automatic change entry to another.

5. 34. 8. 1. Copying Automatic Changes – Day to Day

The following example shows how to copy the saved automatic changes for Monday in Automatic change#002 to Monday in Automatic change#003:

1. Select **Access points** > **Access point automatic changes**. The **Access point automatic changes** screen is displayed.
2. Select **Automatic change#003** in the **Name** panel. The details for this automatic change are displayed.

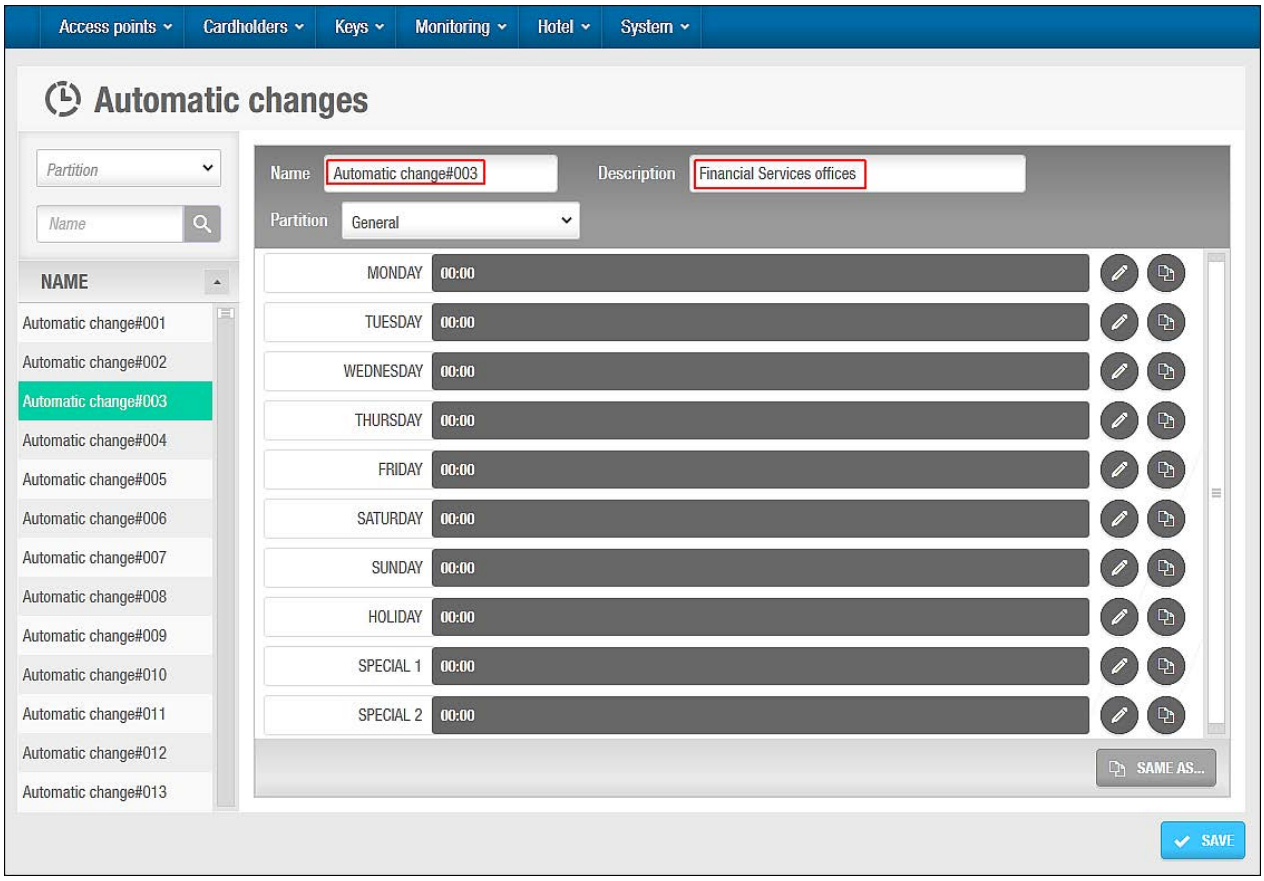


Figure 82: Automatic changes#003

3. Type a description in the **Description** field.
4. Click the **Copy** icon on the right-hand side of Monday. The **Copy automatic changes** dialog box is displayed.

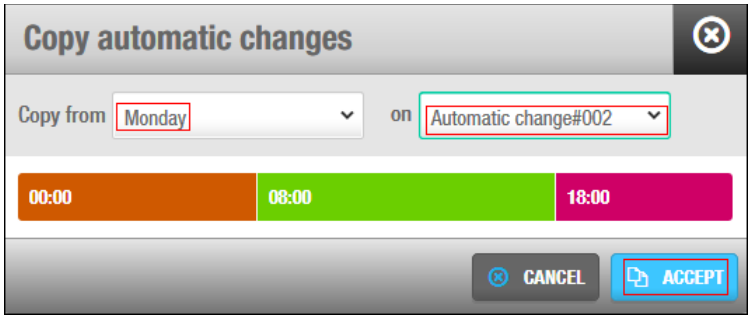


Figure 83: Copy automatic changes dialog box

5. Select **Monday** in the **Copy From** drop-down list.
6. Select **Automatic change#002** from the **on** drop-down list.
7. Click **Accept**. The saved automatic changes for Monday in Automatic change#002 are copied to Monday in Automatic change#003.

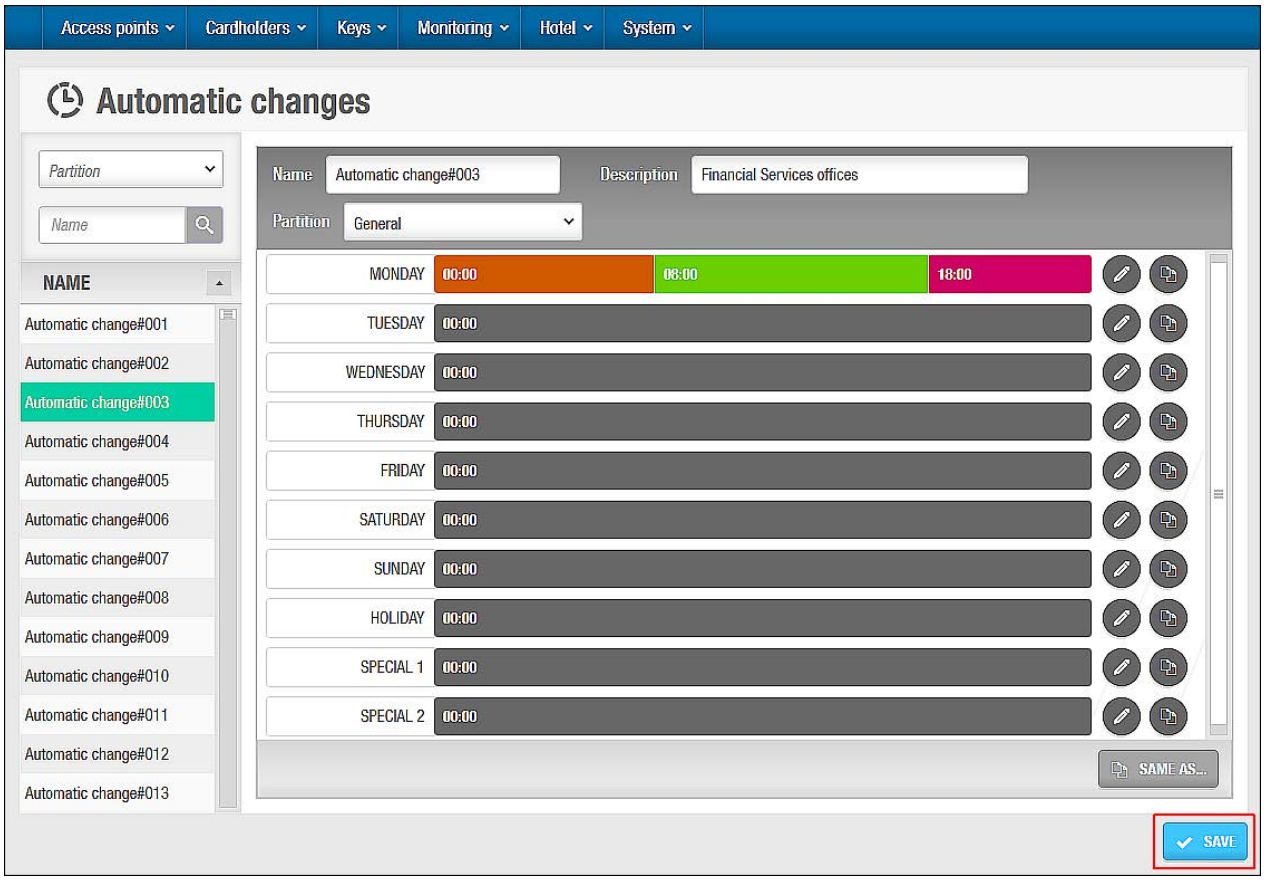


Figure 84: Automatic changes#003 created

8. Click **Save**.

5. 34. 8. 2. Copying Automatic Changes – Entry to Entry

The following example shows how to copy all the information from Automatic change#003 to Automatic change#004:

1. Select **Access points** > **Access point automatic changes**. The **Access point automatic changes** screen is displayed.
2. Select **Automatic change#004** in the **Name** panel. The details for this automatic change are displayed.

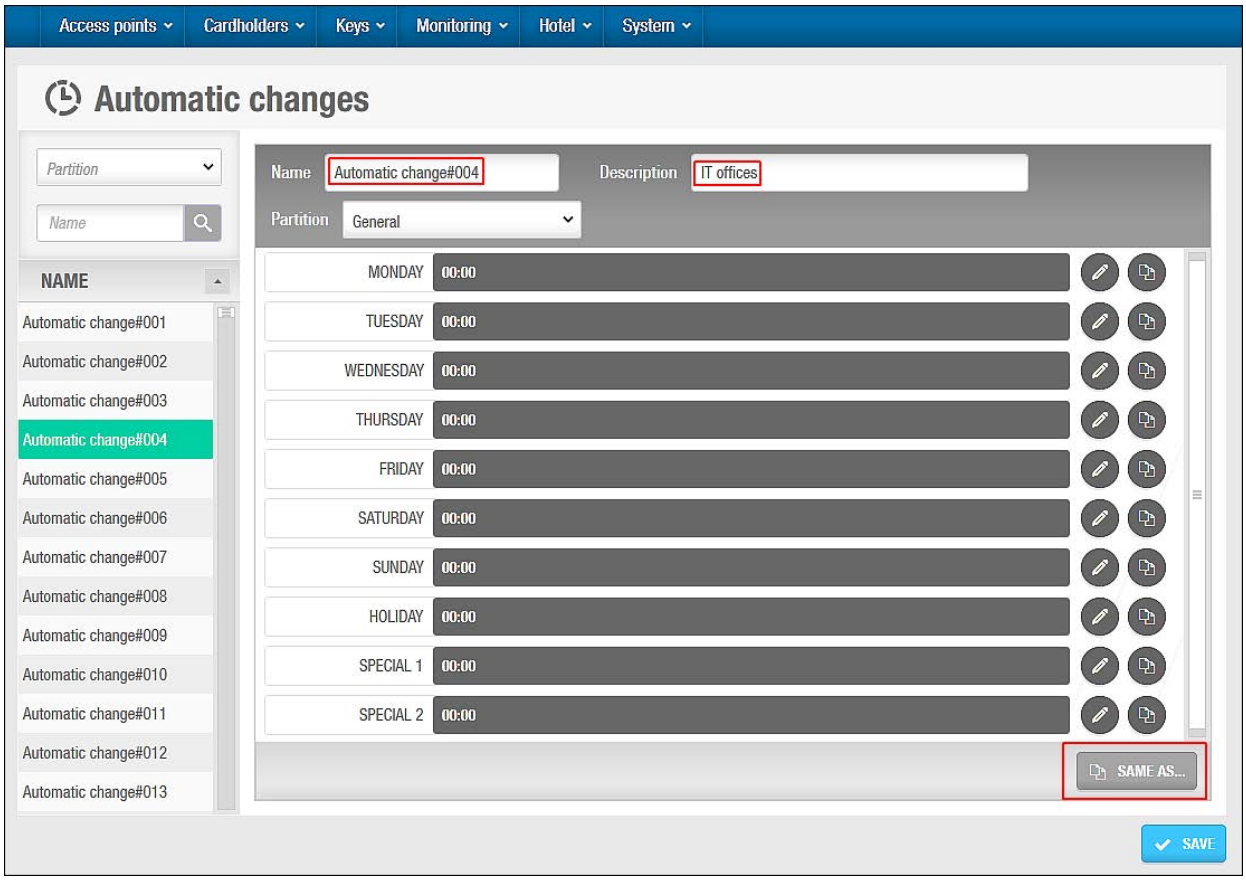


Figure 85: Automatic changes#004

3. Type a description in the **Description** field.
4. Click **Same As**. The **Same as…** dialog box is displayed.

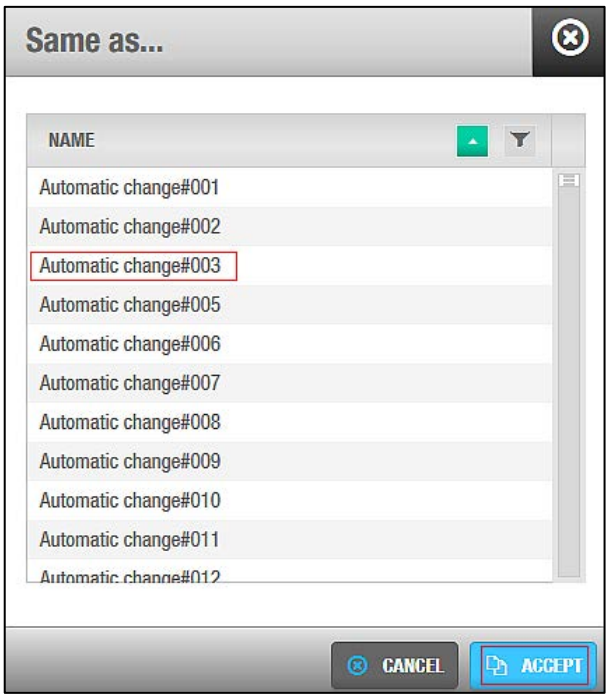


Figure 86: Same as dialog box

5. Select **Automatic change#003**.

6. Click **Accept**. The Automatic change#003 entry information is copied to the Automatic change#004 entry.

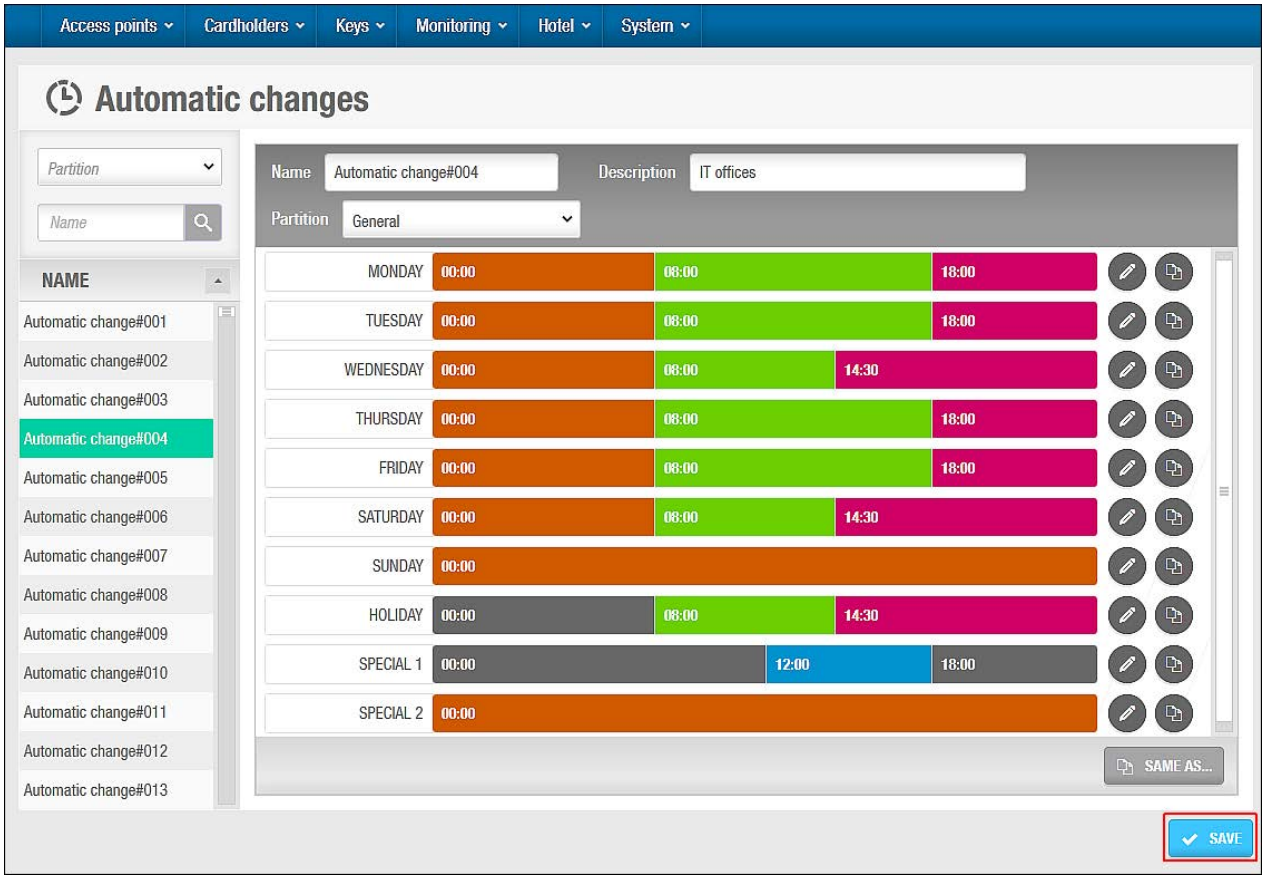


Figure 87: Automatic changes#004 created

7. Click **Save**.

6. CARDHOLDERS

This chapter contains the following sections:

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 ***Error! Reference source not found.*** for more information.

You can use the **Keys** tab to enable and configure tracks for user keys. See ***Error! Reference source not found.*** for more information.

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.
2. **Users associated**

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

   The admin operator creates user access levels and configures the user access level options.
4. **User access levels associated**

   The admin operator associates access points, zones, users, and outputs with the specified user access level.
5. **Limited occupancy groups created and configured**

   The admin operator creates limited occupancy groups and configures the limited occupancy groups options.
6. **Limited occupancy groups associated**

   The admin operator associates users and limited occupancy areas with the specified limited occupancy groups.
7. **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.

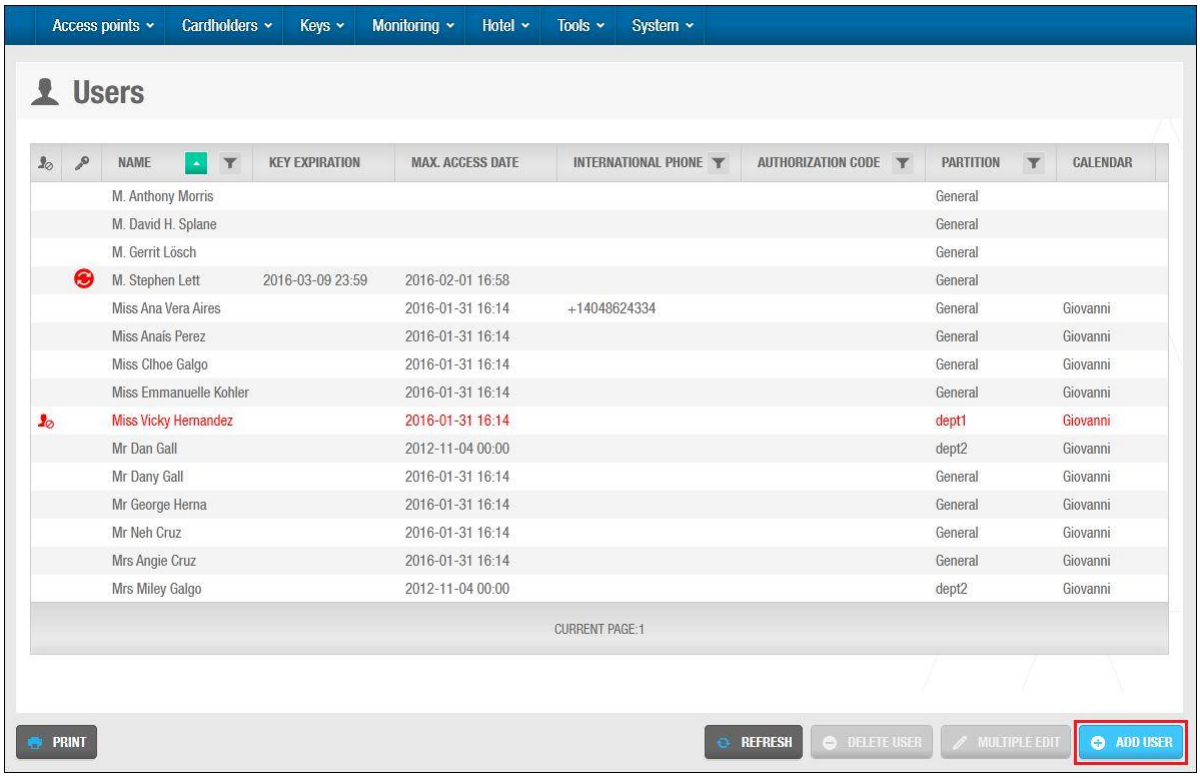


Figure 88: Users screen

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

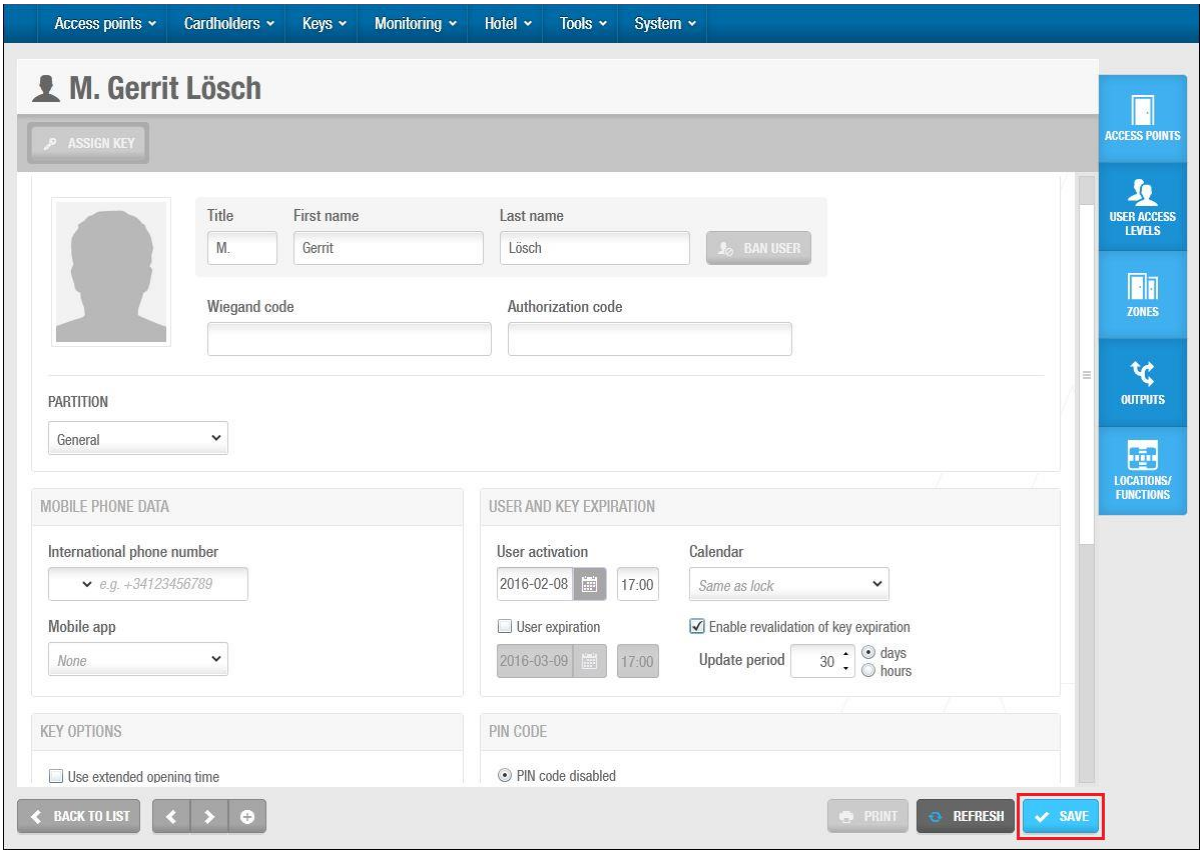


Figure 89: User information screen

3. 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.

4. Enter a **Wiegand code** if required. See *Wiegand code format* for more information.
5. 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.

6. Select the relevant partition from the **Partition** drop-down list, if required.

   See *Partitions* for more information.
7. Select the appropriate management options.

   The configuration and management fields are described in *Configuring Users*.
8. 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. 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.

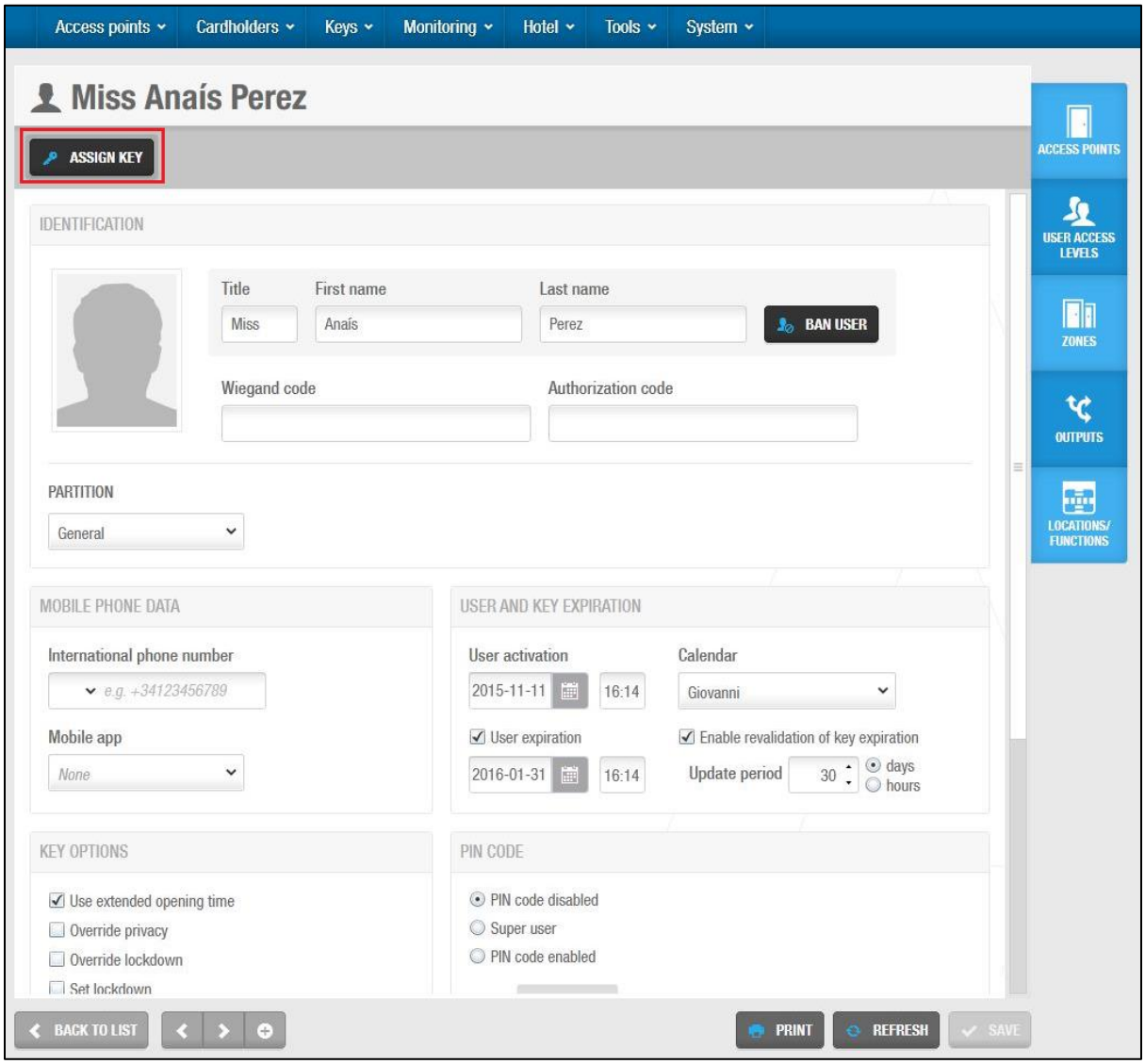


Figure 90: User information screen

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.

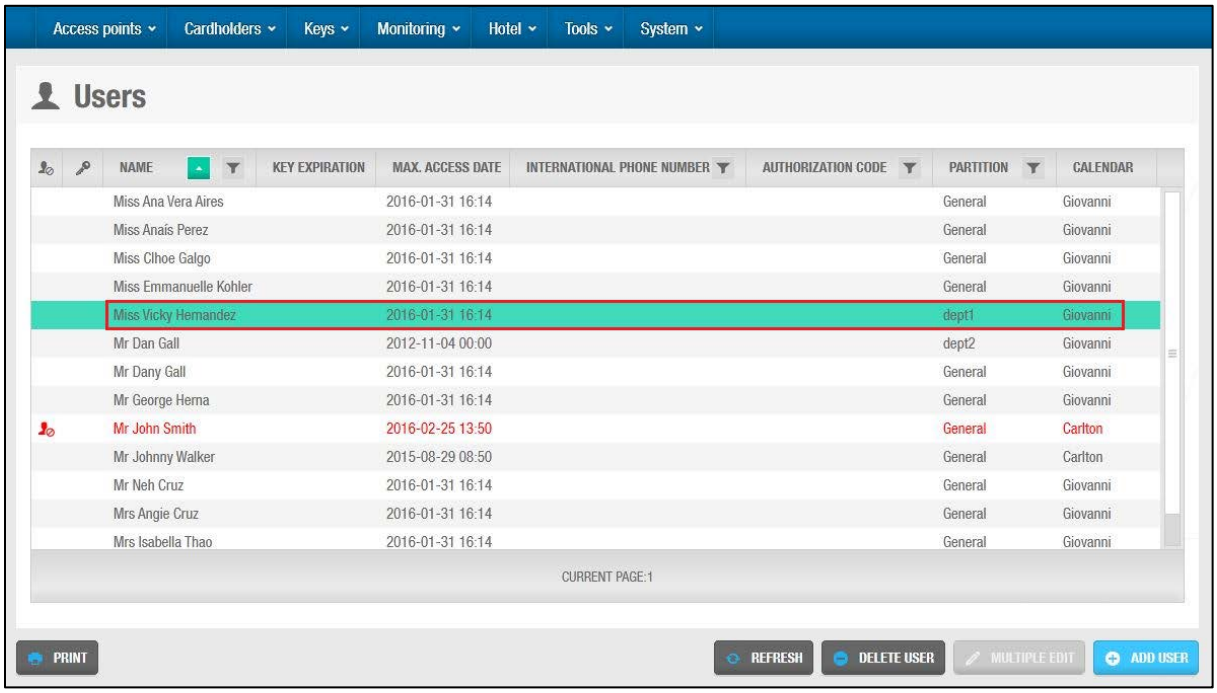


Figure 91: List of users

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

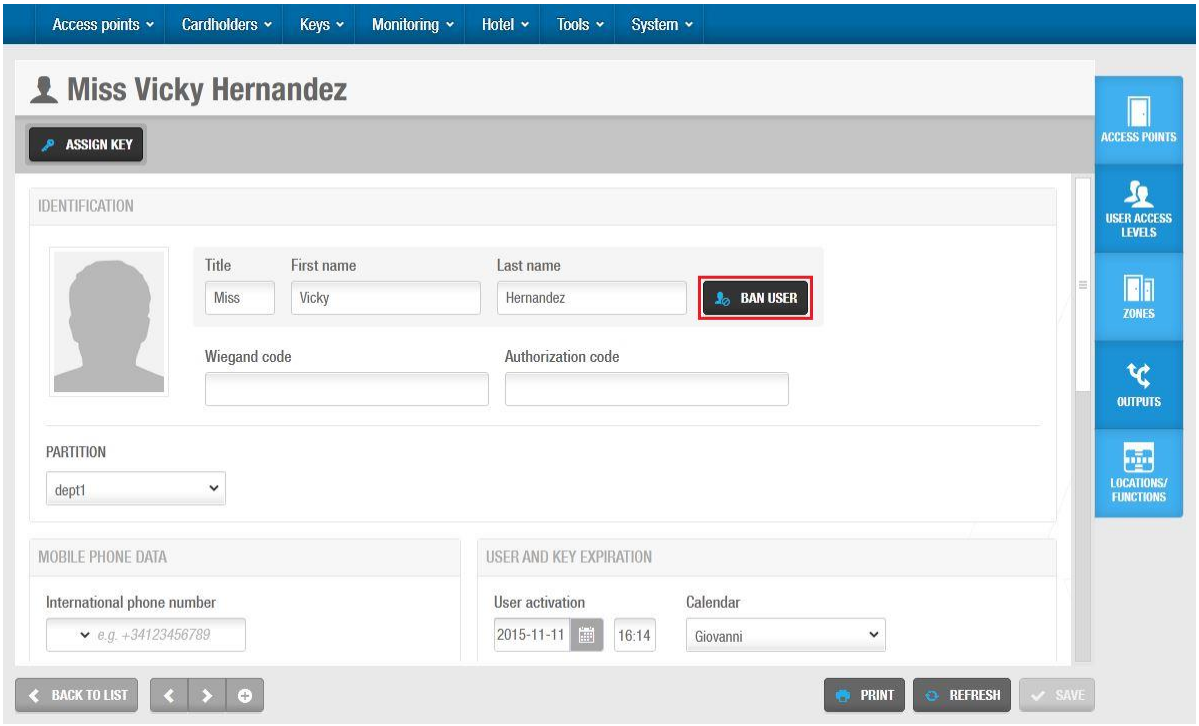


Figure 92: User information screen

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

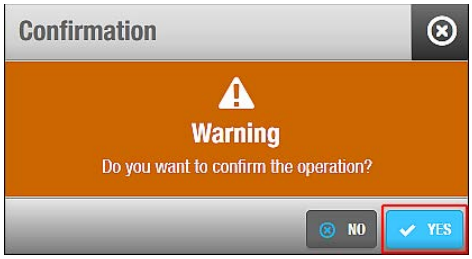


Figure 93: Ban user confirmation pop-up

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

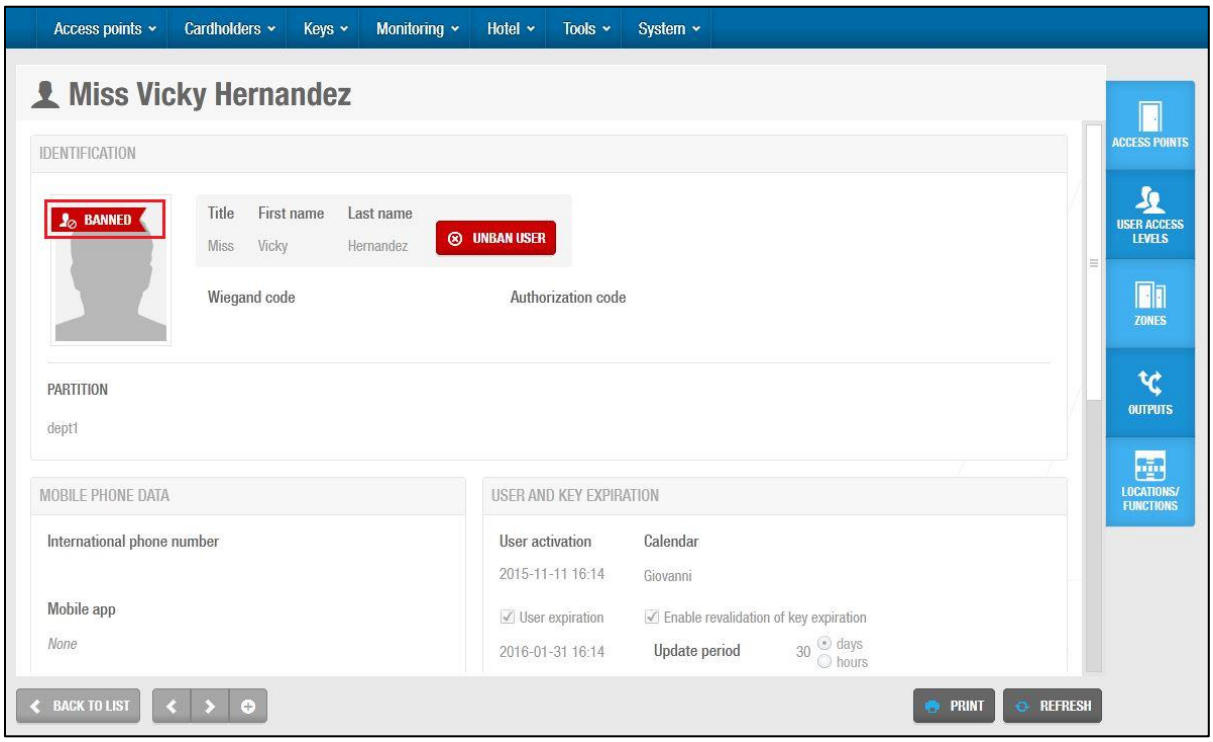


Figure 94: User information screen

To unban a user, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.
2. Double-click the user that you want to unban. The **User** information screen is displayed.
3. Click **Unban User**. A pop-up is displayed asking you to confirm that you want to unban the user.
4. 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.

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.
4. 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.
5. 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.

6. 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 ***Error! Reference source not found.*** and *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.
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.

Option	Description
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.
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.

Option	Description
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.
2. Double-click the user name that you want to associate with an access point. The **User** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.
5. 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.
6. Click **Accept**. The access point is associated with the user.
7. 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.

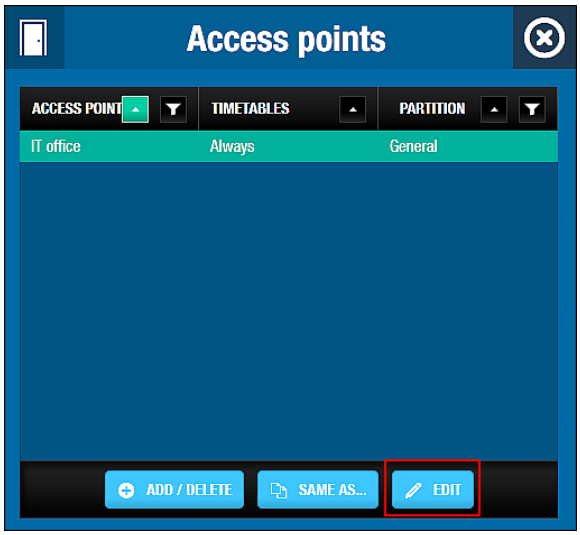


Figure 95: Users dialog box

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

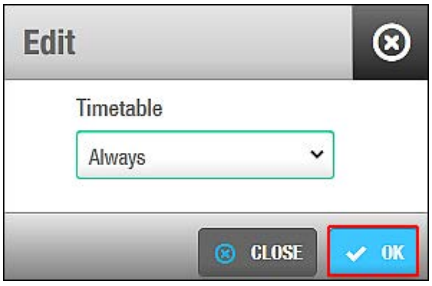


Figure 96: Edit dialog box

9. 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.

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.
2. Double-click the user name that you want to associate with a user access level. The **User** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of user access levels, is displayed.
5. 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.
6. Click **Accept**. The user access level is now associated with the user.

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.
2. Double-click the user name that you want to associate with a zone. The **User** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of zones, is displayed.
5. Select the required zone in the left-hand panel and click the chevron. The selected zone is displayed in the right-hand panel.
6. 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.

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.
2. Double-click the user name that you want to associate with an output. The **User** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of outputs, is displayed.
5. Select the required output in the left-hand panel and click the chevron. The selected output is displayed in the right-hand panel.
6. 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.
2. Double-click the user name that you want to associate with a location/function. The **User** information screen is displayed.
3. Click **Locations/Functions** in the sidebar. The **Locations/Functions** dialog box is displayed.

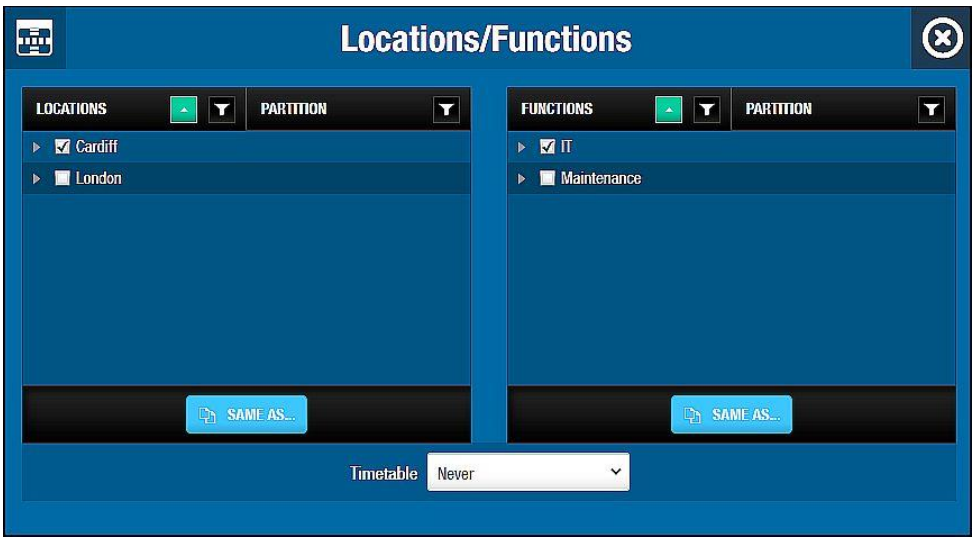


Figure 97: Locations/Functions dialog box

4. Select the checkbox for the required location in the **Locations** panel.
5. Select the checkbox for the required function in the **Functions** panel.
6. 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.

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.

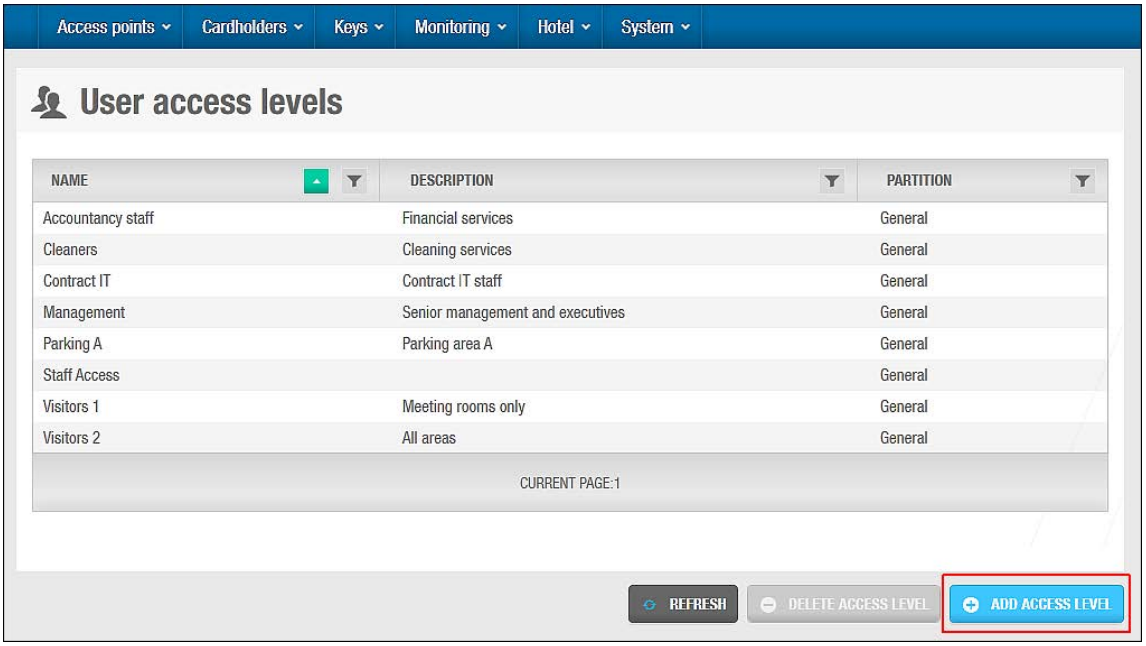


Figure 98: User access levels screen

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

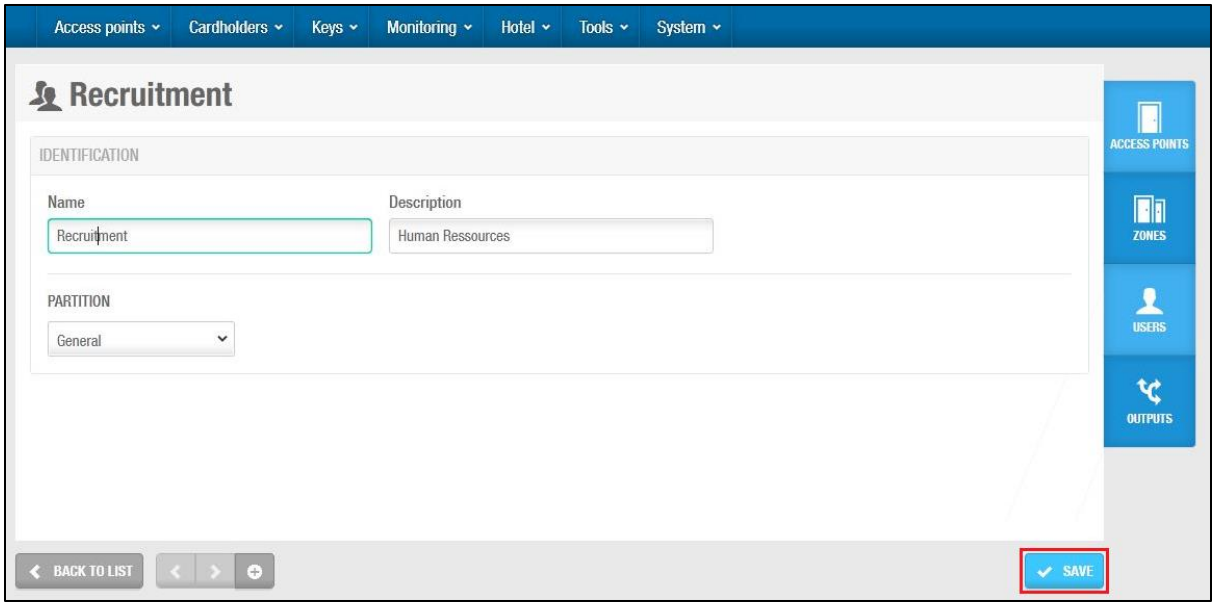


Figure 99: User access level information screen

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

   See *Partitions* for more information.
6. 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.
2. Double-click the user access level that you want to associate with an access point. The **User access level** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.
5. 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.
6. 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.
2. Double-click the user access level that you want to associate with a zone. The **User access level** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of zones, is displayed.
5. Select the required zone in the left-hand panel and click the chevron. The selected zone is displayed in the right-hand panel.
6. 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.
2. Double-click the user access level that you want to associate with a user. The **User access level** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.
5. Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right-hand panel.
6. 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.
2. Double-click the user access level that you want to associate with an output. The **User access level** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of outputs, is displayed.

5. Select the required output in the left-hand panel and click the chevron. The selected output is displayed in the right-hand panel.
6. 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.

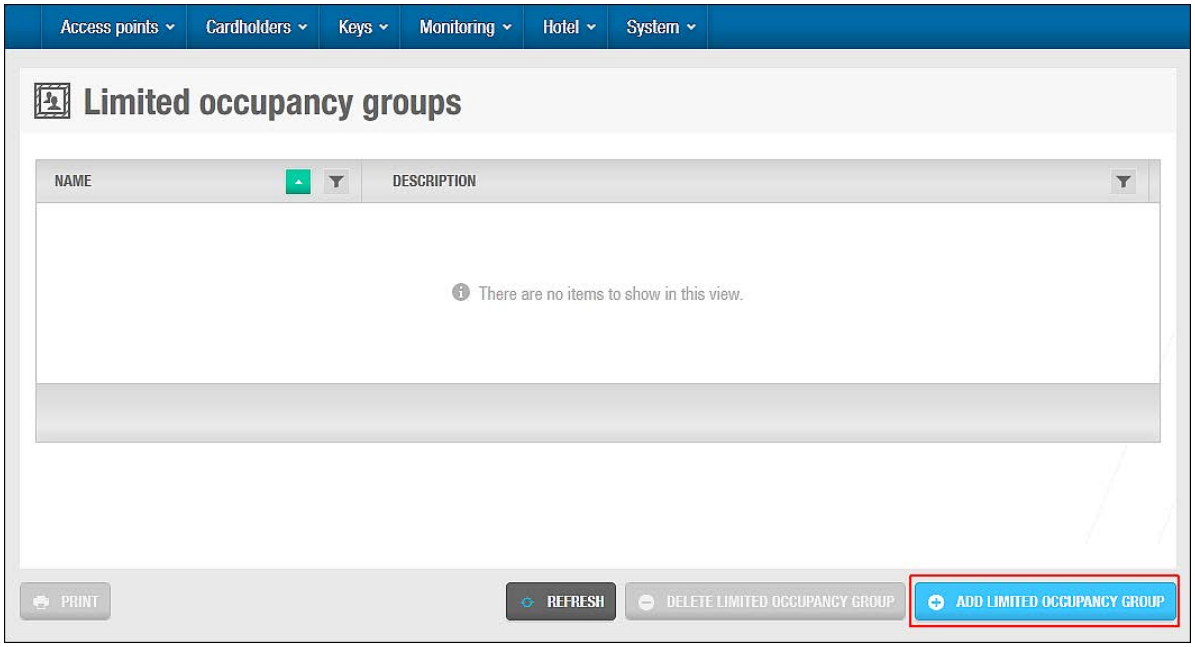


Figure 100: Limited occupancy groups screen

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

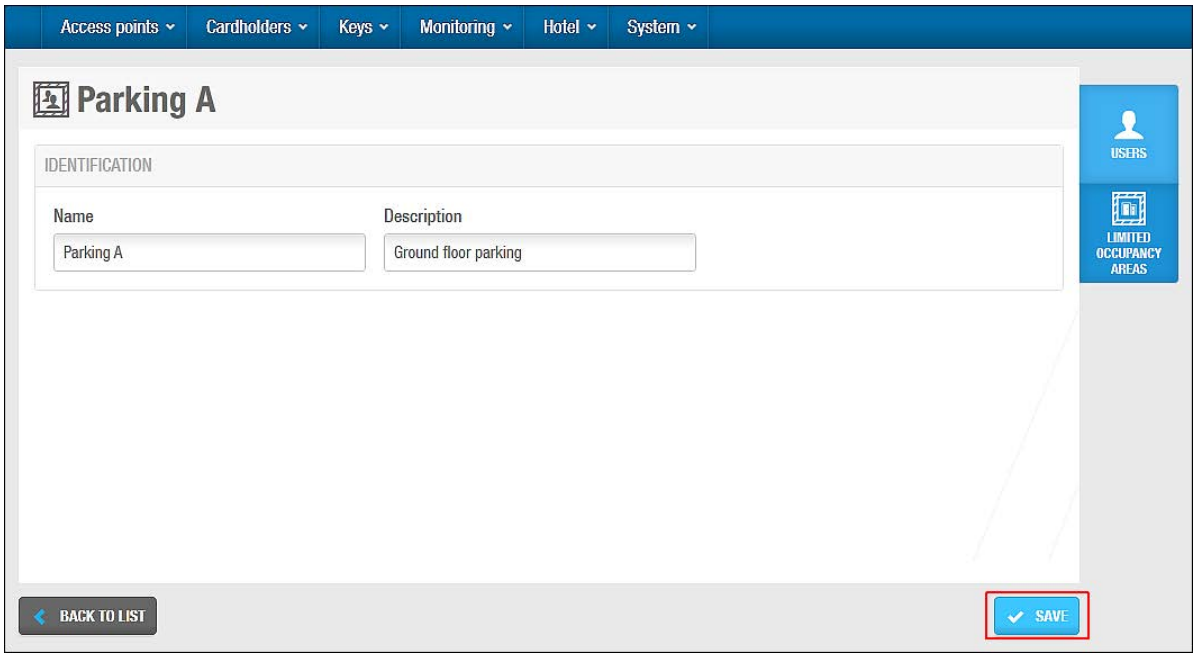


Figure 101: Limited occupancy group information screen

3. Type a name for the limited occupancy group in the **Name** field.
4. Type a description for the limited occupancy group in the **Description** field.
5. 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.
2. Double-click the limited occupancy group that you want to associate with a user. The **Limited occupancy group** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of users, is displayed.
5. Select the required user in the left-hand panel and click the chevron. The selected user is displayed in the right-hand panel.
6. 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.
2. Double-click the limited occupancy group that you want to associate with a limited occupancy area. The **Limited occupancy group** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of limited occupancy areas, is displayed.
5. 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.
6. Click **Accept**. The limited occupancy group is now associated with the limited occupancy area.
7. 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.

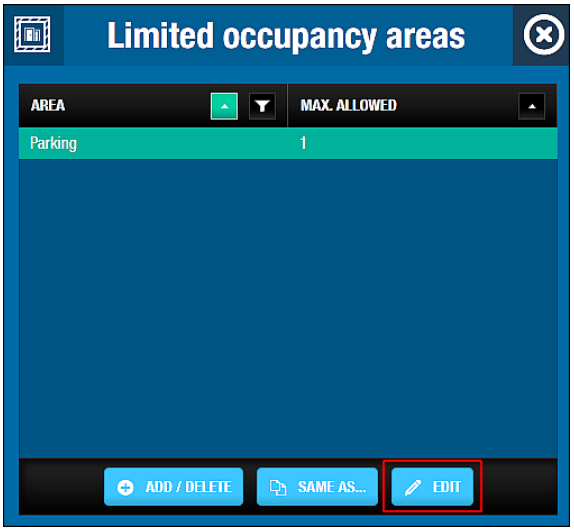


Figure 102: Limited occupancy areas dialog box

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

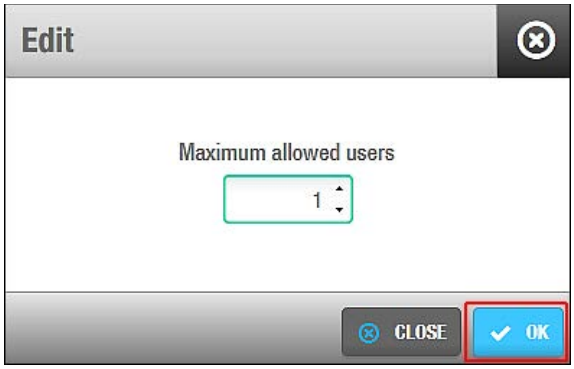


Figure 103: Edit dialog box

9. 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.
10. Click **OK**.

6. 6. Cardholder Timetables

Cardholder timetables control the time periods during which a user's key can be used with a site's access points. For example, a user who works 12-hour shifts over a four-day period could have a timetable that looks like the following example:

- 08.00 to 20.00 Monday
- 08.00 to 20.00 Tuesday
- 20.00 to 08.00 Wednesday
- 20.00 to 08.00 Thursday

A timetable can be set up so that outside of these periods the user's key is not valid and they cannot access the site.

When you create cardholder timetables, you can choose which are used with a site's access points for individual users and user access levels. This is done by selecting the required cardholder timetable in the dialog boxes for access points in the sidebar on the **User** and **User access level** information screens. See *Access Points* and *Zones* for more information and a description of the steps you should follow. You can also choose cardholder timetables to be used with a site's access points for guest access levels and visitor access levels. See *Zones*, *Access Points*, and *Zones* for more information and a description of the steps you should follow.

NOTE: You must configure the system calendar before you create cardholder timetables. The calendar determines the days or weeks that user access is granted, for example, from Monday to Friday. See *Calendar* for more information. Cardholder timetables control the time period during which user access is granted, for example, from 08:00 to 20:00.

6. 6. 1. Creating Cardholder Timetables

To create a cardholder timetable, perform the following steps:

1. Select **Cardholders** > **Cardholder timetables.** The **Cardholder timetables** screen is displayed.

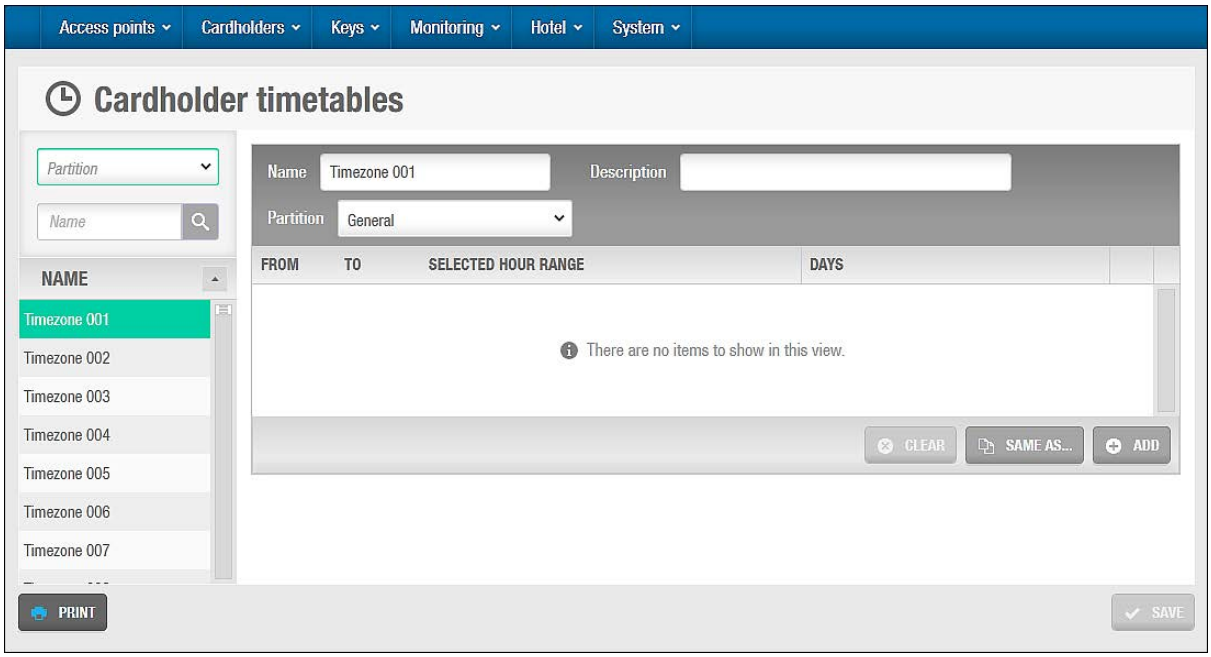


Figure 104: Cardholder timetables screen

2. Click **Add**. The **Cardholder timetables** panel is displayed.

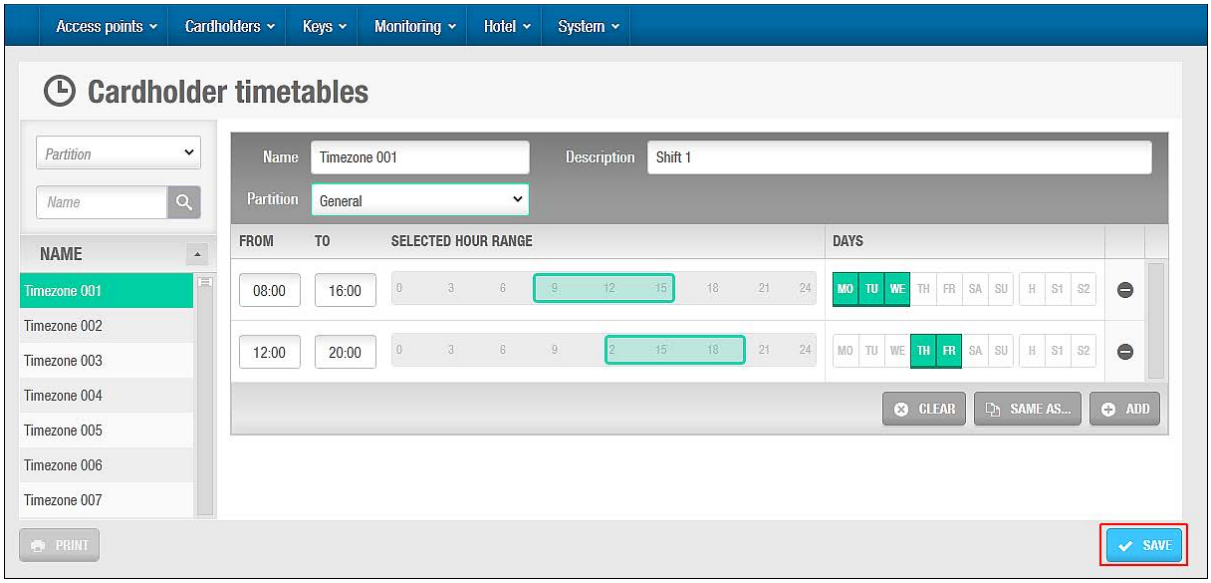


Figure 105: Cardholder timetables panel

3. Select a timezone entry from the **Name** panel.

   Timezone 001 is automatically selected. If you have already configured this timezone entry, select the next timezone entry. Up to 256 timezone entries can be created. Each timezone entry is a cardholder timetable.

4. Type a description of the timezone entry in the **Description** field.

   It is recommended that you enter a descriptive name for the timezone entry, for example Shift 1 or Shift 2. A maximum of 64 characters is allowed.

5. Select the relevant partition in the **Partition** field, if required.

   This adds the timezone entry to the selected partition. Note that you can select different partitions from the **Partition** drop-down list in the left-hand column to view a list of

timezone entries for each partition. If required, you can select timezone entries from the list and move them to a different partition by selecting the appropriate partition in the **Partition** field and clicking **Save**. See *Partitions* for more information.

6. Type a start time for the timezone entry in the **From** field.
7. Type an end time for the timezone entry in the **To** field.
8. Click the applicable days in the **Days** panel.

   If you want to deselect a day, click the applicable day again. If you want to deselect all entries, click the **Minus** icon.

   In addition to the days of the week, you can also create timed periods for holidays (H1) and special days (S1 and S2). See *Calendars* for more information about holidays and special days.
9. Click **Save**.

6. 6. 2. Copying Cardholder Timetables

You can copy saved cardholder timetables information from one specified timezone entry to another.

The following example shows how to copy all the information from one cardholder timetable to another – in this case, from Timezone 001 to Timezone 002:

1. Select **Cardholders** > **Cardholder timetables.** The **Cardholder timetables** screen is displayed.
2. Select **Timezone 002** in the **Name** panel. The details for this timetable are displayed.
3. Click **Same As…** The **Same as…** dialog box is displayed.

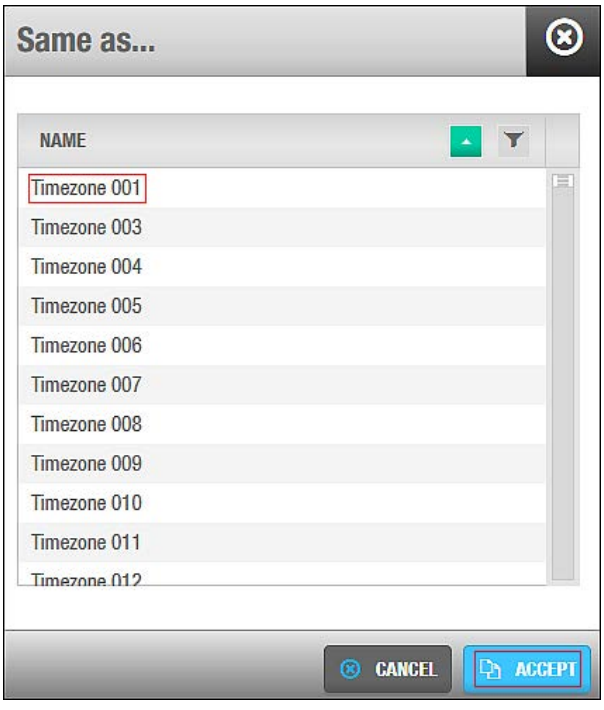


Figure 106: Same as dialog box

4. Select **Timezone 001**.
5. Click **Accept**. The Timezone 001 configuration information is copied to the Timezone 002 entry.

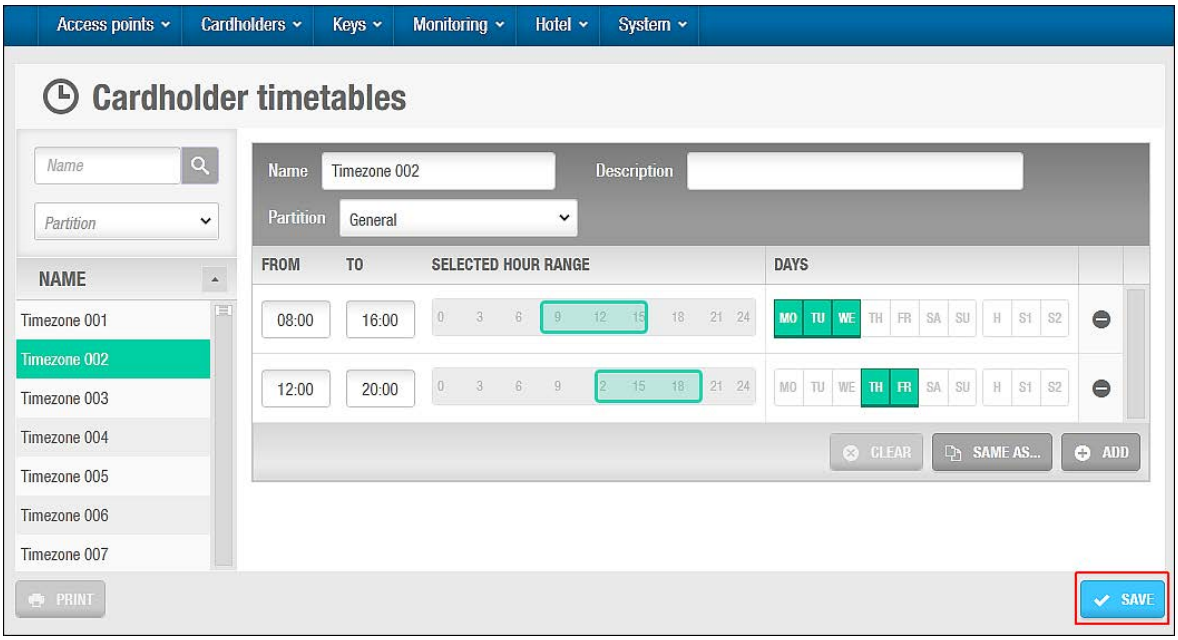


Figure 107: Save Cardholder timetable 002

6. Click **Save**.

7. VISITORS

This chapter contains the following sections:

7. 1. About Visitors

Visitors is the term used to describe cardholders who require temporary access to a site. An example of a visitor might be an engineer doing site maintenance work for a few hours. The engineer can be given access to particular areas of the site for a specified time period. When the time period expires, they can no longer access the site.

If someone regularly needs to visit the site, they can be more permanently included in the system as a visitor and an operator can check them in and out as applicable. However, they have access permissions only during the time period specified. If the appointment is a one-off visit, the operator can delete the visitor from the database once the specified check-out time has expired.

Note that the visitors functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

The information contained in this chapter applies to non-hotel sites only. Visitors should not be confused with guests – guests are applicable to hotel sites only. See *Guest Check-In* for information about guest check-in.

7. 1. 1. About Visitor Configuration

You must perform certain configuration tasks for visitors in ProAccess SPACE General options. You can activate or amend options for visitors by using the **Visitors** tab. See *Visitor Tab* for more information.

7. 2. Visitors Process

Visitors are generally created and managed by an operator with admin rights. Throughout this chapter, references are made to the admin operator. However, this can refer to any operator that has been granted admin rights.

The following example shows a simple way to complete this process:

1. **Visitor access levels created and configured**

   The admin operator creates a visitor access level and configures the visitor access level options.
2. **Visitor access levels associated**

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

3. **Visitor check-in created**

   The operator enters the check-in information.

4. **Visitor check-out created**

   The operator enters the check-out information.

5. **Visitors list managed**

   The operator views the list of visitors and deletes visitors whose visits have expired.

7. 3. Visitor Access Levels

You must define a visitor access level to group together visitors who require similar access points. For example, you can create a meeting room access level for a group of visitors who are attending the same meeting. You must define the visitor access levels before checking in visitors.

7. 3. 1. Creating Visitor Access Levels

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

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

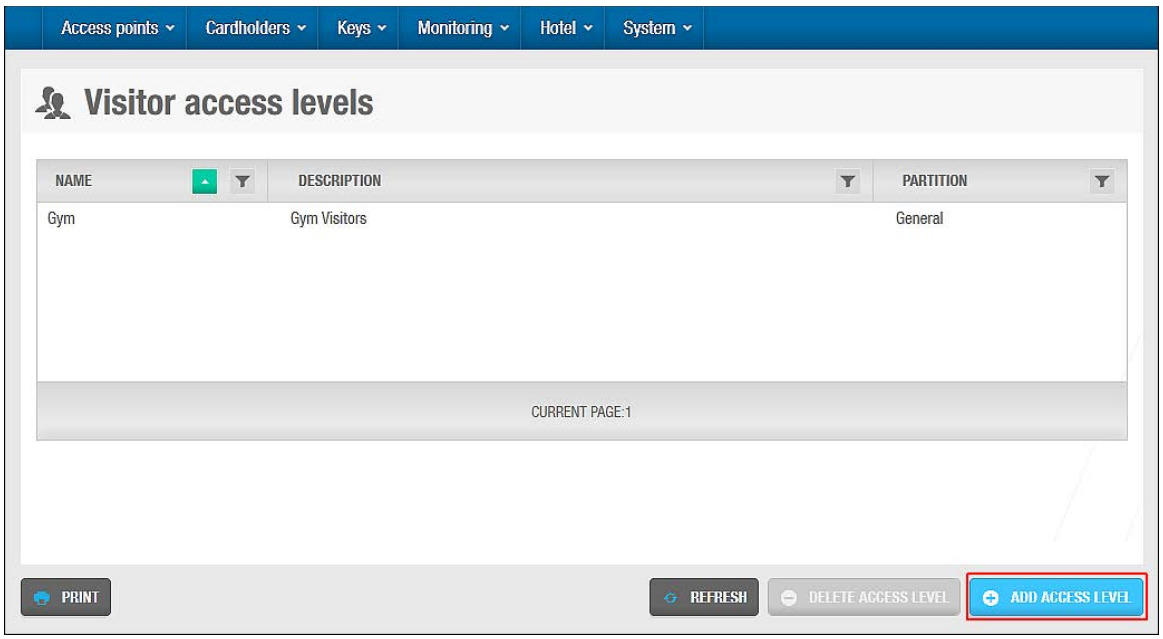


Figure 108: Visitor access levels screen

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

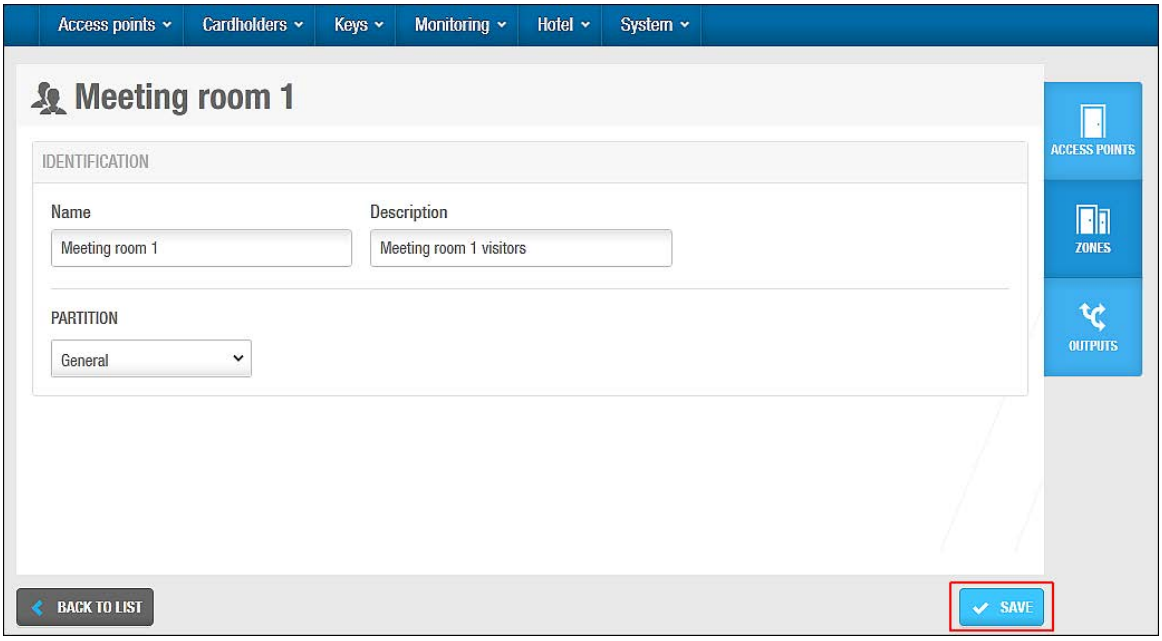


Figure 109: Visitor access level information screen

3. Type a visitor access level name in the **Name** field.
4. Type a description for the visitor access level in the **Description** field.
5. Select the relevant partition from the **Partition** drop-down list, if required.

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

7. 3. 2. Associating Visitor Access Levels

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

7. 3. 2. 1. Access Points

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

NOTE: The maximum number of doors to which a visitor can be granted access is 96.

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

1. Select **Cardholders** > **Visitor access levels**. The **Visitor access levels** screen is displayed.
2. Double-click the visitor access level that you want to associate with an access point. The **Visitor access level** information screen is displayed.
3. 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 visitor access level.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of access points, is displayed.
5. 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.
6. Click **Accept**. The visitor access level is now associated with the access point.

7. Select the access point in the **Access points** dialog box if you want to select a cardholder timetable to be used or specify whether access is optional.

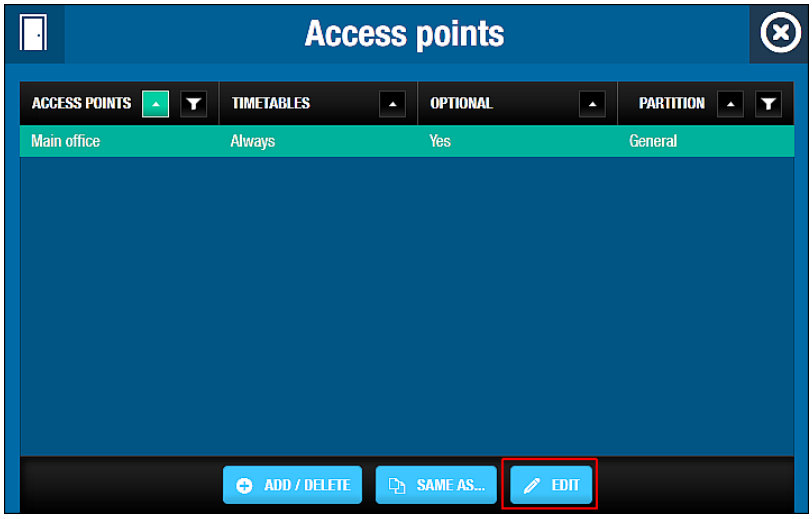


Figure 110: Access points dialog box

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

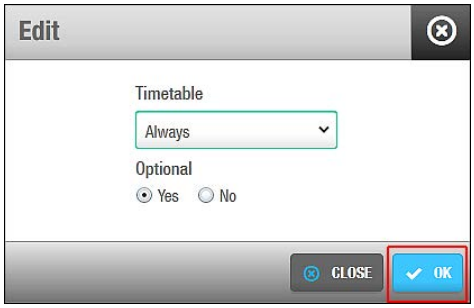


Figure 111: Edit dialog box

9. Select the appropriate cardholder 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 cardholder associated with the specified visitor access level 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**, the access point cannot be used by the visitor cardholder at any time.

10. Select **Yes** or **No** as appropriate.

    If you select **Yes**, operators can decide whether or not to grant access when they check in a visitor. If you select **No**, access is granted to visitors by default. Note that if you specify an access point as optional, it is displayed as a checkbox option on the **Visitor check-in** screen. See *Visitor Check-Ins* for more information.

11. Click **OK**.

7. 3. 2. 2. Zones

See *Zones* for a definition and information about how to create and configure a zone.

To associate a visitor access level with a zone, perform the following steps:

1. Select **Cardholders** > **Visitor access levels.** The **Visitor access levels** screen is displayed.
2. Double-click the visitor access level that you want to associate with a zone. The **Visitor access level** information screen is displayed.
3. 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 visitor access level.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of zones, is displayed.
5. Select the required zone in the left-hand panel and click the chevron. The selected zone is displayed in the right-hand panel.
6. Click **Accept**. The visitor access level is now associated with the zone.

   Note that you can select a cardholder timetable to be used and specify whether access is optional. See *Access Points* for more information and a description of the steps you should follow.

7. 3. 2. 3. Outputs

See *Outputs* for a definition and information about how to create and configure an output.

To associate a visitor access level with an output, perform the following steps:

1. Select **Cardholders** > **Visitor access levels.** The **Visitor access levels** screen is displayed.
2. Double-click the visitor access level that you want to associate with an output. The **Visitor access level** information screen is displayed.
3. 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 visitor access level.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of outputs, is displayed.
5. Select the required output in the left-hand panel and click the chevron. The selected output is displayed in the right-hand panel.
6. Click **Accept**. The visitor access level is now associated with the output.

   Note that you can specify whether access is optional. For example, you can enable elevator access so that a user can access Floor 1 and Floor 3 of a building, but not Floor 2. See *Access Points* for more information and a description of the steps you should follow.

7. 4. Visitor Check-Ins

To check in a visitor, perform the following steps:

1. Select **Keys** > **Visitor check-in**. The **Visitor check-in** screen is displayed.

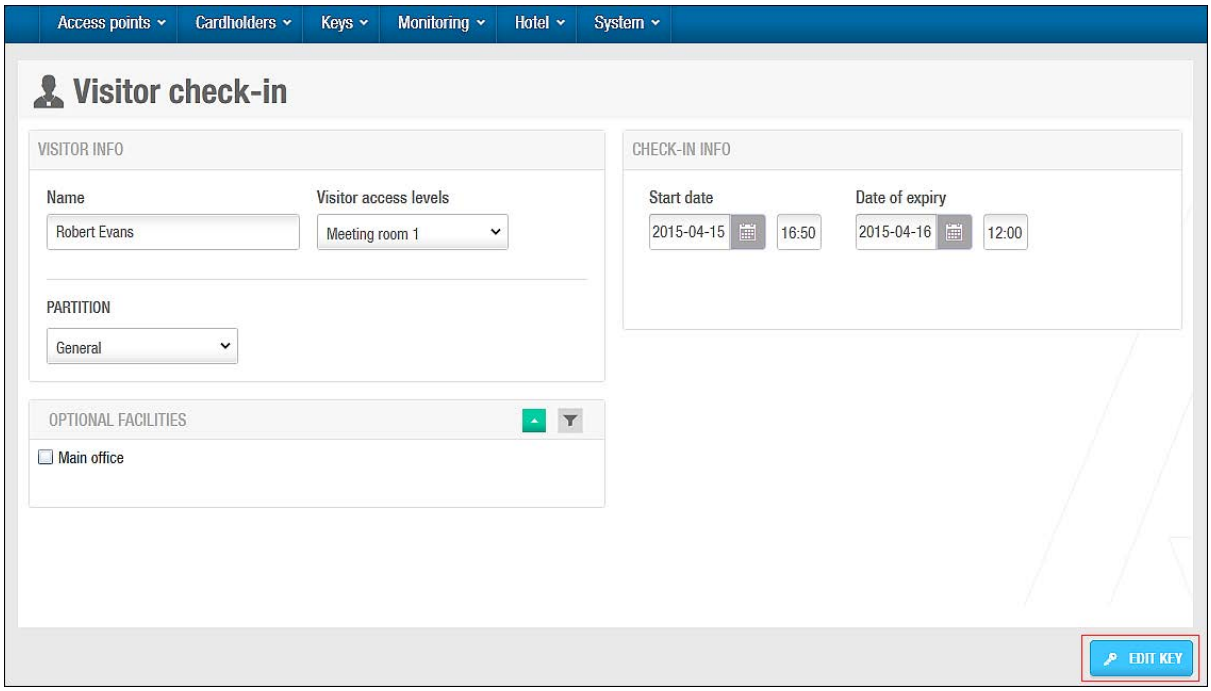


Figure 112: Visitor check-in screen

2. Type the visitor's name in the **Name** field.
3. Select the appropriate access level in the **Visitor access levels** drop-down list.

   See *Creating Visitor Access Levels* for more information about setting up visitor access levels.
4. Select the relevant partition from the **Partition** drop-down list, if required.

   See *Partitions* for more information.
5. Enter the appropriate check-in information.

   See *Visitor Check-In Information* for more information about filling in these fields.
6. Select the appropriate optional facilities if required.

   The optional facilities shown in the **Optional Facilities** panel match any access points you have set up and defined as optional.
7. Click **Edit Key**. A pop-up is displayed asking you to place the key on the encoder.
8. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed informing you that the check-in is completed.

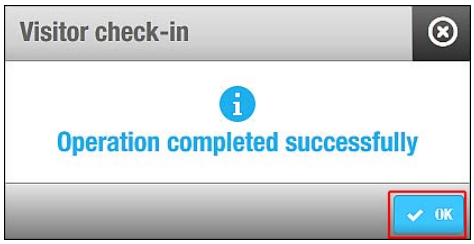


Figure 113: Visitor check-in pop-up

9. Click **OK**.

NOTE: If required, you can add an **Additional data** field to the **Visitor check-in** screen using ProAccess SPACE General options. To enable the field, you must select **Track #1**, **Track #2**, or **Track #3** from the **Save additional data on…** drop-down

list in **System** > **Configuration** > **General options** > **Visitors**. See *Visitors Tab* for more information.

7. 4. 1. Visitor Check-In Information

The visitor check-in information options are described in the following table.

Table 25: Visitor check-in information options

Option	Description
Start date	Date on which the visitor arrives on site
Date of expiry	Date on which the visitor will leave the site
Start date time	Exact time when the key becomes valid
Date of expiry time	Exact time when the key expires

NOTE: The default check-out time is 12:00. If required, you can change this in ProAccess SPACE General options in the **Default checkout time** field in **System** > **General options** > **Visitors**. See *Visitors Tab* for more information.

The default maximum number of days for which a visitor can be granted access is 30. If required, you can change this in ProAccess SPACE General options in the **Maximum number of days** field in **System** > **General options** > **Visitors**. See *Visitors Tab* for more information.

7. 5. Visitor Check-Outs

To check out a visitor, perform the following steps:

1. Select **Keys** > **Visitor check-out**. The **Visitor check-out** dialog box is displayed.

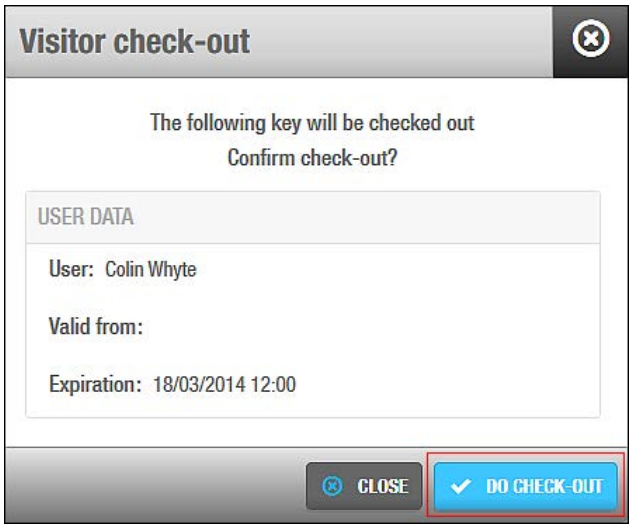


Figure 114: Visitor check-out dialog box

2. Click **Do Check-Out**. A pop-up is displayed, informing you that the check-out is completed.

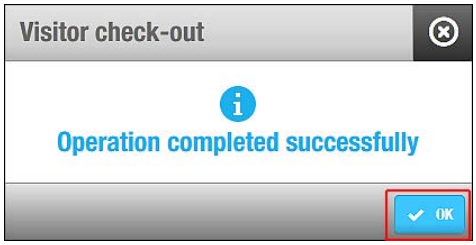


Figure 115: Visitor check-out pop-up

3. Click **OK**. The visitor key can no longer be used to access any area of the site.

7. 6. Managing Visitor Lists

It is possible to view a list of visitors and delete specific visitor entries from the list after their visit has expired.

7. 6. 1. Viewing Visitors

You can view a list of visitors by selecting **Cardholders** > **Visitors**.

By default, visitors remain on the database and are displayed in the visitors list for 120 days after the visit expires.

NOTE: To change the default display time, you can adjust the value in the **Keys expired X days ago will be removed automatically** field in **System** > **General options** > **Visitors** in ProAccess SPACE. See *Visitors Tab* for more information.

7. 6. 2. Deleting Expired Visitors

It is recommended to delete visitors as soon as their visit has ended in order to conserve system memory space.

To manually delete a visitor from the list of visitors, perform the following steps:

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

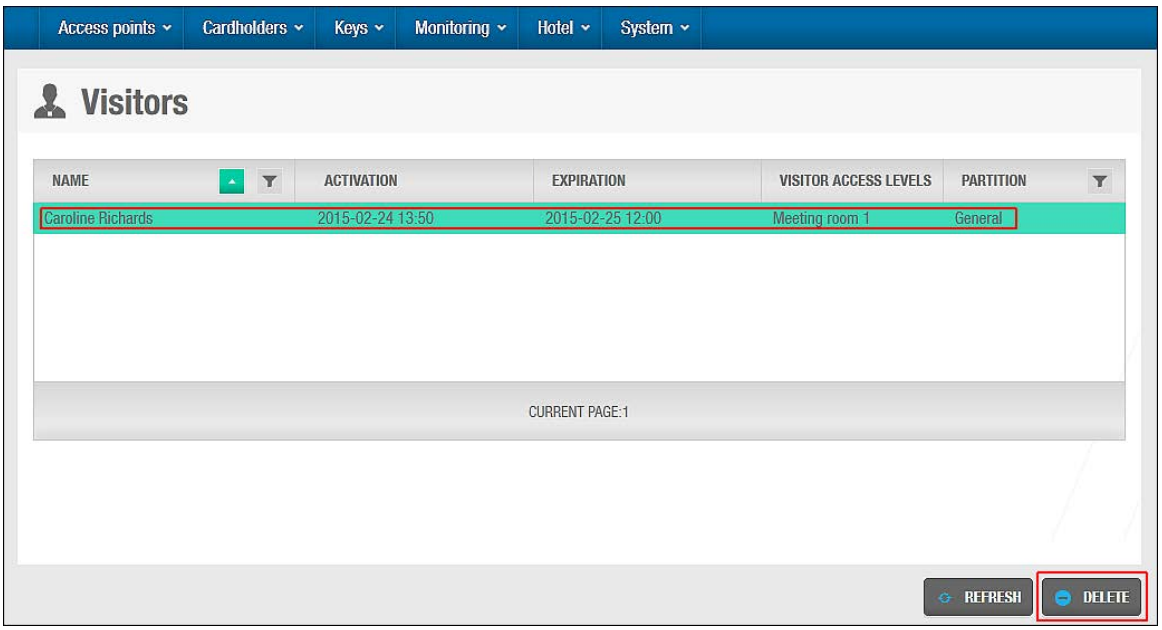


Figure 116: Visitors screen

2. Select a visitor name.
3. Click **Delete**. The visitor is removed from the visitors list.

NOTE: If you delete visitors after their visit expires, their keys are not sent to the blacklist. You can opt to select if visitor keys will be sent to the blacklist when visitors are deleted before their visit expires. To activate this option, you must enable the MORE_THAN_64K_USERS advanced parameter in ProAccess SPACE General options. See *Advanced Tab* for more information. See also *Managing Blacklists* for more information.

8. HOTELS

This chapter is relevant to hotel sites only. Operators working in non-hotel sites do not need to refer to it.

This chapter contains the following sections:

8. 1. About Hotels

Hotel sites have specific requirements that entail additional functionality not required in other SALTO installation sites. To meet these requirements, ProAccess SPACE has a Hotel interface and menu that is enabled specifically for such sites. The Hotel interface gives operators access to a restricted subset of the functionality available to an admin user. See *Admin Interface* and *Hotel Interface* for more information.

The Hotel menu options can be accessed by admin operators and any operators that have been given the appropriate permissions. These menus contain functionality relating to the access management of guests.

The admin operator (or operator with admin rights) sets up users (hotel staff) and guest access points (rooms, suites, zones, and outputs), and checks in visitors (people who require access for a fixed period, for example, to do site maintenance). They also set up hotel operator groups and hotel operators. The hotel operator can then perform tasks such as guest check-in and check-out. See *Users* for more information about users. See *Visitors* for more information about visitors.

The hotel functionality is license-dependent. Certain additional options for hotels, for example, the re-rooming and mobile guest keys functionality, are also controlled by licensing. See *Registering and Licensing SALTO Software* for more information.

NOTE: A hotel operator is generally a front-desk operator or a member of the hotel's reservations staff who has been set up with the appropriate operator permissions. They can be given access to the Hotel interface only or to additional menus and functionality; this depends on the permissions set by the admin operator. See *Operator Groups* and *Operators* for more information.

8. 1. 1. About Hotel Configuration

You must perform certain configuration tasks for hotel sites in ProAccess SPACE General options.

You can use the **Hotel** tab to do the following:

- Enable or amend options for guests
- Enable or amend options for rooms and suites
- Configure associated devices

See *Hotel Tab* for more information.

You can enable options for guest keys by using the **Hotel** tab, and configure PMS options by using the **PMS** tab if required. See *Hotel Tab* and *PMS Tab* for more information.

8. 2. Hotels Processes

Hotel access points and access levels 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. References are also made to a hotel operator. This can refer to any operator who has been given permissions particular to hotels, for example, a front-desk operator.

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

1. **Rooms created and configured**

   The admin operator creates rooms and configures the room options.
2. **Rooms associated**

   The admin operator associates automatic outputs and zones with the specified rooms.
3. **Suites created and configured**

   The admin operator creates suites and configures the suite options.
4. **Suites associated**

   The admin operator associates rooms, automatic outputs, and zones with the specified suites.
5. **Hotel keys configured**

   The admin operator configures keys for use by hotel staff and management, and the hotel operator configures keys for guests.
6. **Guest access levels created and configured**

   The admin operator creates and configures guest access levels.
7. **Guest access levels associated**

   The admin operator associates zones, outputs, and guests with the specified guest access levels.

8. **Hotel guest entries created and configured**

   a) The hotel operator selects a room and enters the guest check-in information.
   b) The hotel operator encodes the room key with the guest check-in information.
   c) The hotel operator checks the guest out when the guest is leaving.

   See *Group Check-In* for information about setting up group check-ins.

9. **Guest lists managed**

   The hotel operator views the list of guests and configures guest profiles.

8. 3. About Hotel Access Points

Hotel access points include rooms, suites, zones, and outputs. Rooms and suites are specific to hotel sites and are described in this section. Zones and outputs can be created in all SALTO installation sites. See *Zones* and *Outputs* for more information about these access points.

Guest accommodation in hotels can be configured in two ways:

- **Room**: A room assigned to one or more guests.
- **Suite**: A series of rooms containing one or more areas with individual entrance doors from the outside and a connecting door between. Guests can move between rooms without going through the hallway. These may be booked together by one guest or separately by different guests checking in as a group.

NOTE: You must initialize room and suite locks using a PPD. See *Initializing Rooms and ESDs* for more information.

8. 4. Rooms

The following sections describe how to create and configure a room.

8. 4. 1. Creating Rooms

To create a room, perform the following steps:

1. Select **Access points** > **Rooms**. The **Rooms** screen is displayed.

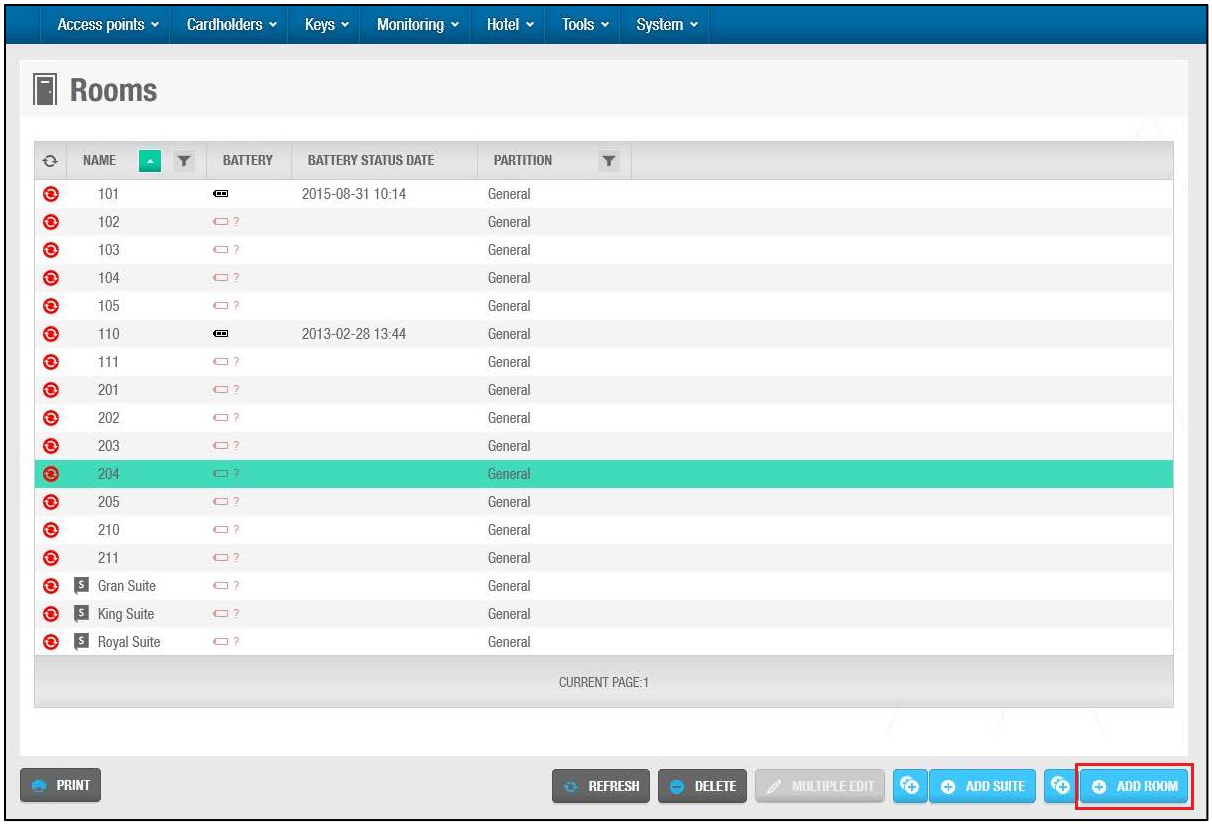


Figure 117: Rooms screen

2. Click **Add Room**. The **Room** information screen is displayed.

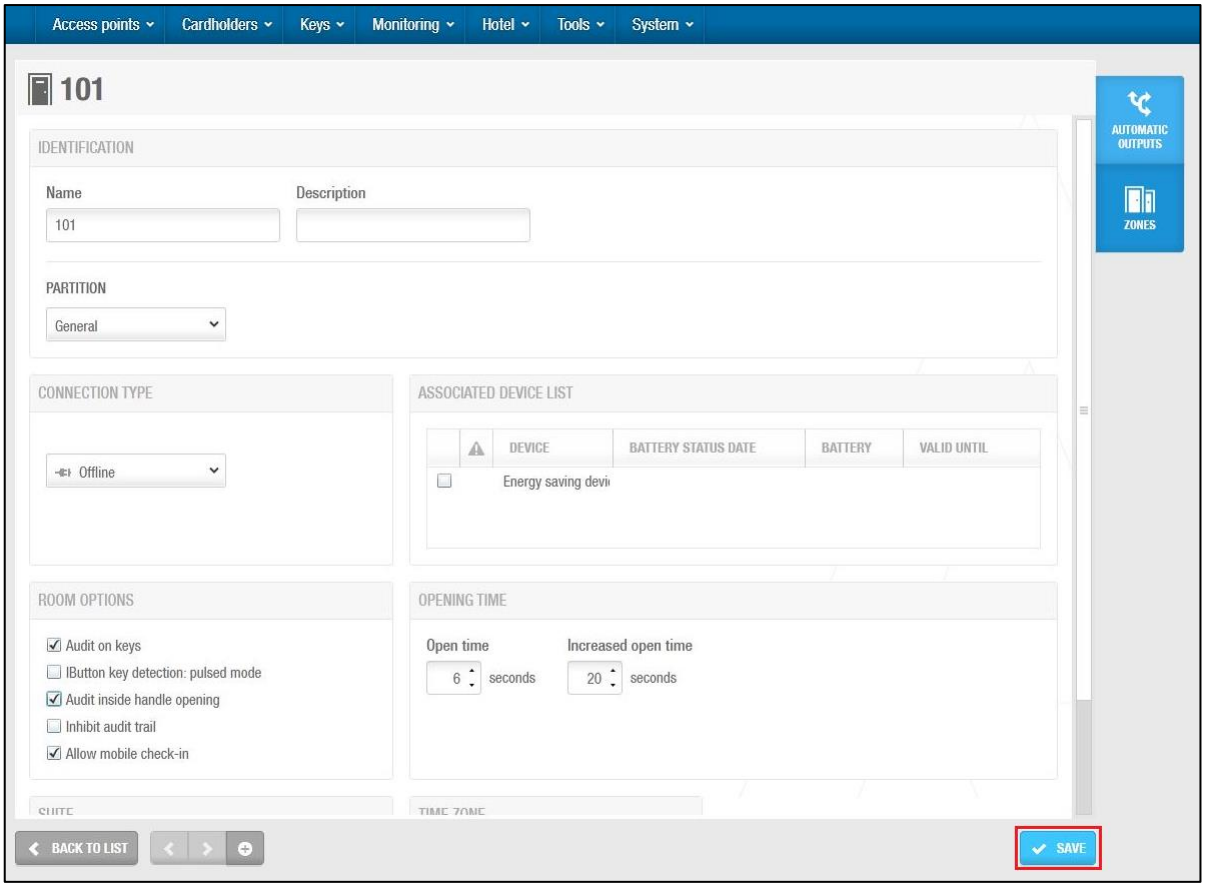


Figure 118: Room information screen

3. Type a name for the room in the **Name** field.
4. Type a description for the room in the **Description** field.
5. Select the appropriate partition from the **Partition** drop-down list if required.

   See *Partitions* for more information about partitions.
6. Select the appropriate configuration options.

   The configuration fields are described in *Configuring Rooms*.
7. Click **Save**.

You can activate up to two general purpose fields on the **Room** information screen if required. To activate a general purpose field, you must select an **Enable field** checkbox in **System** > **General options** > **Access points** in ProAccess SPACE. You can then name the field in accordance with the information that you want to capture. See *Access points Tab* for more information.

8. 4. 2. Configuring Rooms

The following sections describe the various ProAccess SPACE fields used to configure rooms.

8. 4. 2. 1. Opening Modes

The default opening mode for rooms and suites is Standard. However, you can change this to Toggle mode in ProAccess SPACE General options if required. To do so, select the **Toggle** option from the **Open mode** drop-down list in **System** > **General options** > **Hotel**. The selected opening mode applies to all external room doors in the hotel. However, it does not apply to doors in subsuites. See *Hotel Tab* and *Opening Modes and Timed Periods* for more information.

8. 4. 2. 2. Connection Types

The **Connection Type** panel defines the connection type for the room. The default option is **Offline**. When you select any of the other (online) connection types from the **Connection Type** drop-down list, a **Configure** button is displayed on the **Room** information screen. This button is activated when you click **Save**. See *Configuring Online Connection Types* for more information about configuring connection types.

Additional panels are also displayed on the **Room** information screen depending on the connection type that you select.

The connection type options are described in the following table.

Table 26: Connection type options

Option	Description
Offline	Used for doors that are not connected to the SALTO network and need to be updated using a PPD. See *PPD* for more information about PPDs.

Option	Description
Online IP (CU5000)	Used for doors that are hardwired to the SALTO network and managed using Ethernet TCP/IP protocols. See *SALTO Network* for more information. When you select this option, a **Lockdown Area** panel and a **Limited Occupancy Area** panel are displayed on the **Room** information screen. For an online CU, you can add the room to a lockdown area and/or a limited occupancy area if required. See *Lockdown Areas* and *Limited Occupancy Areas* for more information.
Online IP (CU4200)	Used for doors that are hardwired to the SALTO network and managed using Ethernet TCP/IP protocols. Same options than for the CU5000 apply to the CU4200.
Online RF (SALTO)	Used for doors that are connected to the SALTO network using RF technology. When you select this option, a **Lockdown Area** panel is displayed on the **Room** information screen. This means you can add the room to a lockdown area if required. See *Lockdown Areas* and *Limited Occupancy Areas* for more information.
Online RF (BAS integration)	Used for doors that are connected to a building automation system (BAS) that is integrated with the SALTO network. Before selecting this option, check that your BAS integration has been fully configured in ProAccess SPACE General options. See *BAS Tab* for more information. When you select this option, a **Lockdown Area** panel is displayed on the **Room** information screen. This means you can add the room to a lockdown area if required. See *Lockdown Areas* for more information.

8. 4. 2. 3. Associated Device Lists

Selecting the **Energy saving** checkbox in the **Associated Device List** panel activates the ESD in the specified room. ESDs are used to control the activation of electrical equipment in a room or area. They are used in the majority of hotel sites. See *ESDs* for more information about ESDs.

You must select the **Associated devices** checkbox on the **Hotel** tab in ProAccess SPACE General options to display the **Associated Device List** panel in SPACE if appropriate. You can also amend the configuration settings for associated devices in ProAccess SPACE General options. See *Hotel Tab* and *Configuring Associated Devices* for more information.

NOTE: When you activate a room's ESD, you must initialize it using a PPD. See *Initializing Rooms and ESDs* for more information.

ESD_#1 and ESD_#2 outputs are automatically generated by the system. These outputs activate the relays for ESDs. They cannot be deleted.

Granting Guests Access to ESDs

You must complete the following process to give guests access to ESDs:

1. Create a guest access level and associate the required guests with the guest access level.

   See *Guest Access Levels* for more information about creating guest access levels and associating guests.

2. Associate the ESD_#1 and ESD_#2 outputs with the guest access level.

   Note that, in general, the ESD_#1 output controls access to electrical lights, and the ESD_#2 output controls access to AC systems. You must associate both of these

outputs with guest access levels. See *Outputs* for more information about associating outputs with guest access levels.

3. Amend the optional access settings for the ESD_#1 and ESD_#2 outputs so access is granted to all guests by default.

   This means that when you check in a guest to a particular room, for example, room 101, their key can automatically be used to access the ESD in the room, for example, @ESD_101. Otherwise, you have to grant this access to individual guests during check-in. See *Outputs* for more information.

4. Check in the guests to the required rooms.

   Guest keys can only be used to access ESDs in rooms if a guest has been checked in to the room.

Granting Users Access to ESDs

The process for granting hotel staff (users) access to ESDs in rooms is different than for guests.

You must do the following:

1. Create a zone and associate the required ESDs with the zone.
2. Associate users (or user access levels) with the zone.
3. Associate users (or user access levels) with the ESD_#1 and ESD_#2 outputs.

   If required, you can associate users with the ESD_#1 output only. This means that they can activate electrical lights but not AC systems, which are controlled by the ESD_#2 output.

See *Zones* and *Outputs* for more information.

8. 4. 2. 4. Room Options

The **Room Options** panel controls how the door activity is audited and whether mobile guest keys can be used to access rooms.

The options are described in the following table.

Table 27: Room options

Option	Description
Audit on keys	Allows monitoring of when and where user keys, for example, hotel staff keys, are used. You must enable this feature on both the access point and the user's key. When this option is selected, the door is enabled to write or stamp the audit information on the key as long as the key's memory is not full. Also, the **Audit openings in the key** checkbox is enabled on the **User** information screen. See *Key Options* for more information. If you select an online connection type in the **Connection Type** panel, the **Audit on keys** checkbox is greyed out. This is because online doors are connected to the system, and can send audit information directly to it.
IButton key detection: pulse mode	Reduces the battery consumption and the risk of rust on the IButton reader contacts as the key detection is done in pulse mode instead of continuous. To activate this option, you must enable the SHOW_KEY_DETECT_MODE parameter in ProAccess SPACE General options. See *Advanced Tab* for more information. This option is only compatible with PPDs that have firmware version 1.02 or higher.

Option	Description
Audit inside handle opening	Allows monitoring of when a guest exits a room
Inhibit audit trail	Ensures that the lock does not memorize openings in its audit trail. However, the lock can still write information on the key. To activate this option, you must select the **Allow audit trail inhibition** checkbox in **System** > **General options** > **Access points** in ProAccess SPACE. See *Door Options* for more information.
Allow mobile guest's keys	Allows mobile guest keys to be used to access a room. Mobile guest keys allow guests to access a room by using the JustIN key app on their mobile phone (instead of a separate physical credential). When you select this option, a **Send key to guest's mobile** checkbox and a **Notification message** field are displayed on the **Hotel check-in** screen for the room. This option is currently only compatible with smartphones using iOS or Android operating systems.

8. 4. 2. 5. Opening Times

The **Opening Time** panel defines how long a door stays open after it has been unlocked.

The options are described in the following table.

Table 28: Door opening times

Option	Description
Open time	Defines how long the handle remains active. The door locks as soon as the handle is released, even if the time value is not reached. The default time value is six seconds. The value can be increased or decreased in the range 0 to 255 seconds.
Increased open time	Defines a longer opening time. This option is designed for disabled or 'hands full' users. The default time value is 20 seconds. The value can be increased or decreased in the range 0 to 255 seconds. You must enable this option in the guest's profile. See *Enabling Extended Door Opening Times* for more information.

8. 4. 2. 6. Suites

Selecting a suite from the drop-down list in the **Suite** panel adds the room to the suite.

8. 4. 2. 7. Time Zones

The **Time Zone** panel defines which one of the system time zones is used for the room. You must enable the multiple time zones functionality in ProAccess SPACE General options to display this panel in ProAccess SPACE. See *Activating Multiple Time Zones* and *Time Zones* for more information.

8. 4. 3. Associating Rooms

After you have created and configured a room, you must associate automatic outputs and zones with that room. The following sections describe how to associate rooms with those entries.

8. 4. 3. 1. Automatic Outputs

See *Automatic Outputs* for a definition and information about how to create and configure an automatic output.

To associate an automatic output with a room, perform the following steps:

1. Select **Access points** > **Rooms**. The **Rooms** screen is displayed.

2. Double-click the room that you want to associate with an automatic output. The **Room** information screen is displayed.
3. Click **Automatic Outputs** in the sidebar. The **Automatic Outputs** dialog box is displayed.

   Note that the dialog box will be blank because you have not yet associated an automatic output.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of automatic outputs, is displayed.
5. Select the required automatic output in the left-hand panel and click the chevron. The selected automatic output is displayed in the right-hand panel.
6. Click **Accept**. The room is now associated with the automatic output.
7. Select the output in the **Automatic Outputs** dialog box if you want to change the access point timed period. See *Access Point Timed Periods* for more information.

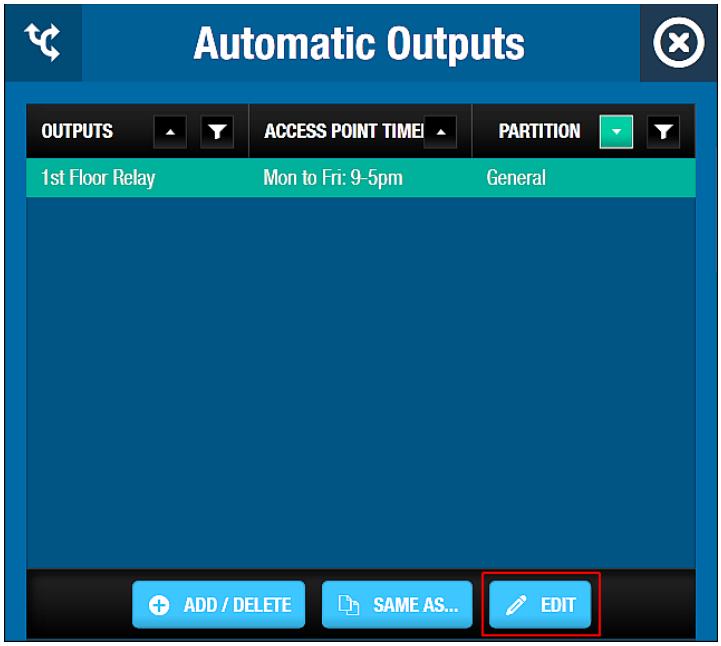


Figure 119: Automatic Outputs dialog box

8. Click **Edit**. The **Edit** dialog box is displayed. Time period 001 is selected by default.

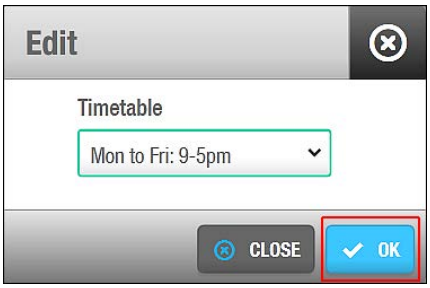


Figure 120: Edit dialog box

9. Select the appropriate access point timed period from the drop-down list.
10. Click **OK**.

8. 4. 3. 2. Zones

See *Zones* for a definition and information about how to create and configure a zone. You can associate rooms with zones by using the **Access Points** dialog box in the sidebar of the **Zone** information screen. See *Access Points* for a description of the steps that you should follow.

You can view a list of zones that are associated with each room on the system.

To view the zones associated with a room, perform the following steps:

1. Select **Access points** > **Rooms**. The **Rooms** screen is displayed.
2. Double-click the room with the zone list you want to view. The **Room** information screen is displayed.
3. Click **Zones** in the sidebar. The **Zones** dialog box, showing a list of zones, is displayed.

8. 5. Suites

The following sections describe how to create and configure a suite.

8. 5. 1. Creating Suites

To create a suite, perform the following steps:

1. Select **Access points** > **Rooms**. The **Rooms** screen is displayed.

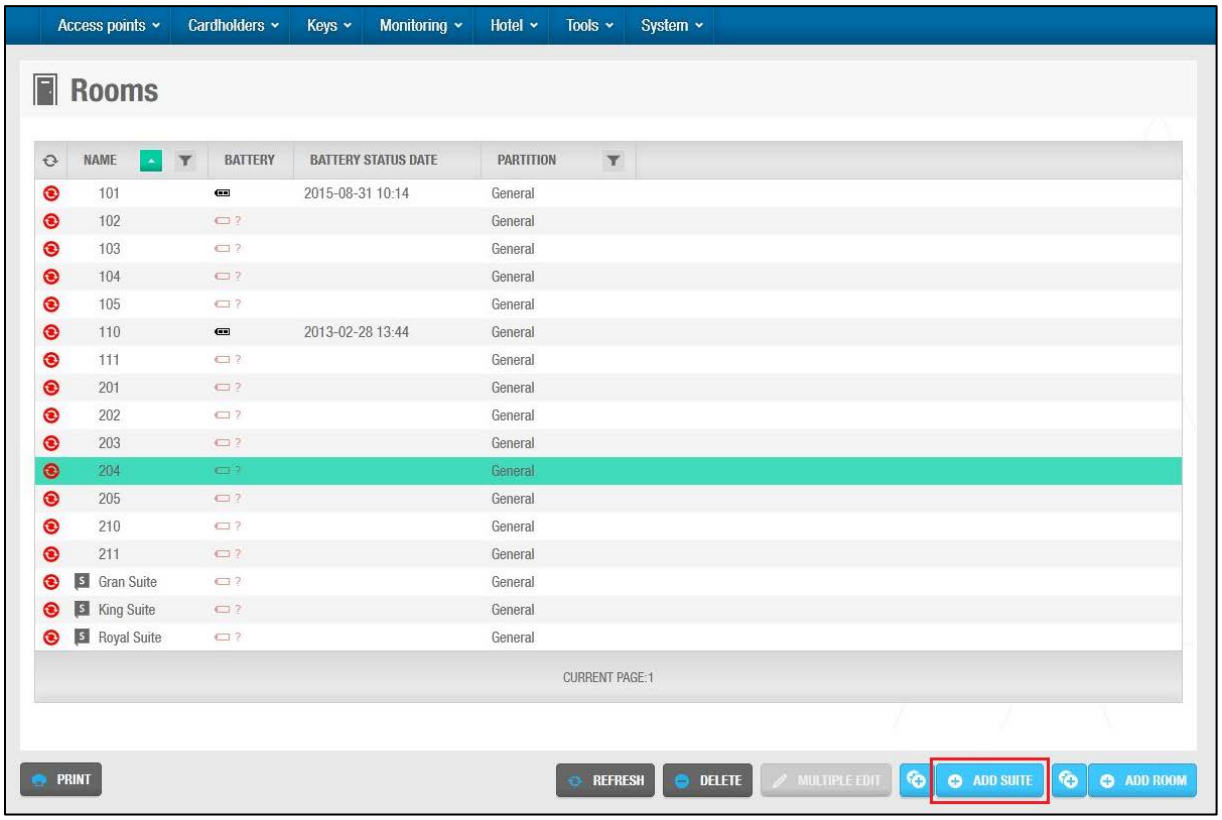


Figure 121: Rooms screen

2. Click **Add Suite**. The **Suite** information screen is displayed.

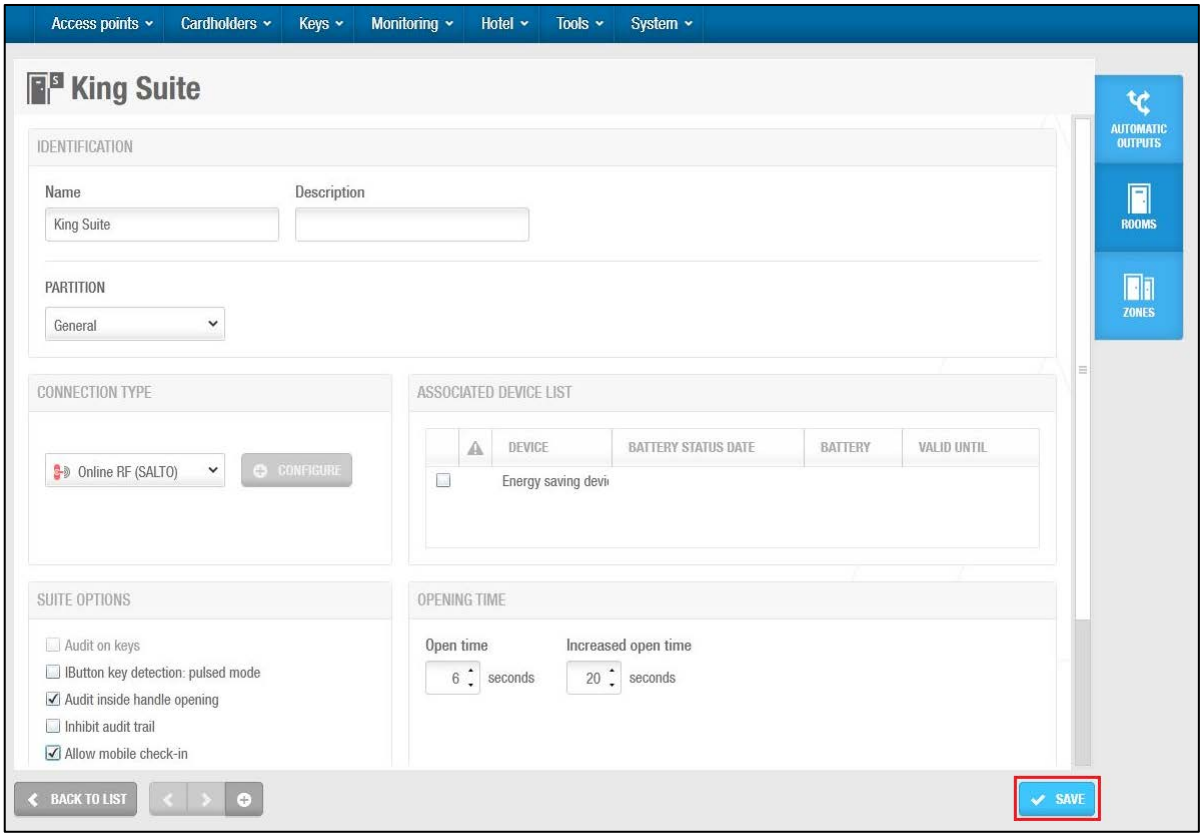


Figure 122: Suite information screen

3. Type a name for the suite in the **Name** field.
4. Type a description for the suite in the **Description** field.
5. Select the appropriate partition from the **Partition** drop-down list if required.

   See *Partitions* for more information about partitions.
6. Select the appropriate configuration options.

   The configuration fields are described in *Configuring Suites*.
7. Click **Save**.

NOTE: Once a suite is created, it is displayed on the **Rooms** screen. A **Suite** icon is displayed on the left-hand side of each suite name.

8. 5. 2. Configuring Suites

The following sections describe the various ProAccess SPACE fields used to configure suites.

8. 5. 2. 1. Opening Modes

The default opening mode for rooms and suites is Standard. However, you can change this to Toggle mode in ProAccess SPACE General options if required. To enter Toggle mode, select the **Toggle** option from the **Open mode** drop-down list in **System** > **General options** > **Hotel**. The selected opening mode applies to all external suite doors in the hotel. However, it does not apply to doors in subsuites. See *Hotel Tab* for more information.

You can enable Office mode for subsuite doors by activating the SUBSUITE_OFFICE and SUBSUITE OFFICE_GUESTS parameters in **System** > **General options** > **Advanced** in

ProAccess SPACE. See *Advanced Tab* and *Opening Modes and Timed Periods* for more information.

8. 5. 2. 2. Connection Types

The connection types are the same for suites and rooms. See *Connection Types* for more information.

8. 5. 2. 3. Associated Device Lists

The associated device list is the same for suites and rooms. See *Associated Device Lists* for more information.

8. 5. 2. 4. Suite Options

The suite options are the same as the room options for rooms. See *Room Options* for more information.

8. 5. 2. 5. Opening Times

The opening time options are the same for suites and rooms. See *Opening Times* for more information.

8. 5. 2. 6. Time Zones

The time zone options are the same for suites and rooms. See *Time Zones* for more information.

8. 5. 3. Associating Suites

When you have created and configured a suite, you must associate automatic outputs, rooms, and zones with that suite. The following sections describe how to associate suites with those entries.

8. 5. 3. 1. Automatic Outputs

See *Automatic Outputs* for a definition and information about how to create and configure an automatic output.

To associate an automatic output with a suite, perform the following steps:

1. Select **Access points** > **Rooms**. The **Rooms** screen is displayed.

   The **Rooms** screen shows a list of rooms and suites.
2. Double-click the suite that will be associated with an automatic output. The **Suite** information screen is displayed.
3. Click **Automatic Outputs** in the sidebar. The **Automatic Outputs** dialog box is displayed.

   Note that the dialog box will be blank because you have not yet associated an automatic output.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of automatic outputs is displayed.
5. Select the required automatic output in the left-hand panel and click the chevron. The selected automatic output is displayed in the right-hand panel.
6. Click **Accept**. The suite is now associated with the automatic output.

   You can specify which access point timed period is used. See *Automatic Outputs* for more information and a description of the steps that you should follow.

8. 5. 3. 2. Rooms

See *About Hotel Access Points* and *Rooms* for a definition and information about how to create and configure a room.

To associate a room with a suite, perform the following steps:

1. Select **Access Points** > **Rooms**. The **Rooms** screen is displayed.
   The **Rooms** screen shows a list of rooms and suites.
2. Double-click the suite that you want to associate with a room. The **Suite** information screen is displayed.
3. Click **Rooms** in the sidebar. The **Rooms** dialog box is displayed.
   Note that the dialog box will be blank because you have not yet associated a room.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of rooms, is displayed.
5. Select the required room in the left-hand panel and click the chevron. The selected room is displayed in the right-hand panel.
6. Click **Accept**. The suite is now associated with the room.

8. 5. 3. 3. Zones

See *Zones* for a definition and information about how to create and configure a zone. You can associate suites with zones by using the **Access Points** dialog box in the sidebar of the **Zone** information screen. See *Access Points* for a description of the steps that you should follow.

You can view a list of zones that are associated with each suite in the system.

To view the zones associated with a suite, perform the following steps:

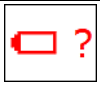
1. Select **Access points** > **Rooms**. The **Rooms** screen is displayed.
   The **Rooms** screen shows a list of rooms and suites.
2. Double-click the suite with the zone list you want to view. The **Suite** information screen is displayed.
3. Click **Zones** in the sidebar. The **Zones** dialog box, showing a list of zones, is displayed.

8. 6. Room and Suite Icons

When you create rooms and suites, different icons are displayed on the **Rooms** screen. These icons vary, depending on the battery status of room and suite doors and whether they need to be updated.

The icons are described in the following table.

Table 29: Room and suite icons

Icon	Description
 Update required	Indicates that a door needs to be updated. This icon is displayed in the **Update required** column.
 Unknown	Indicates that the battery status of a door is unknown. This icon is displayed in the **Battery** column.

Icon	Description
 Battery status	Indicates the battery status of a door. This can be normal, low, or run-out.

NOTE: Icons are displayed on the **Room status** information screen to indicate if rooms or suites are occupied. See *Checking Room and Suite Status* for more information.

8. 7. Creating Multiple Rooms and Suites

You can create multiple rooms or suites at once if required.

8. 7. 1. Creating Multiple Rooms

To create multiple rooms, perform the following steps:

1. Select **Access points** > **Rooms**. The **Rooms** screen is displayed.

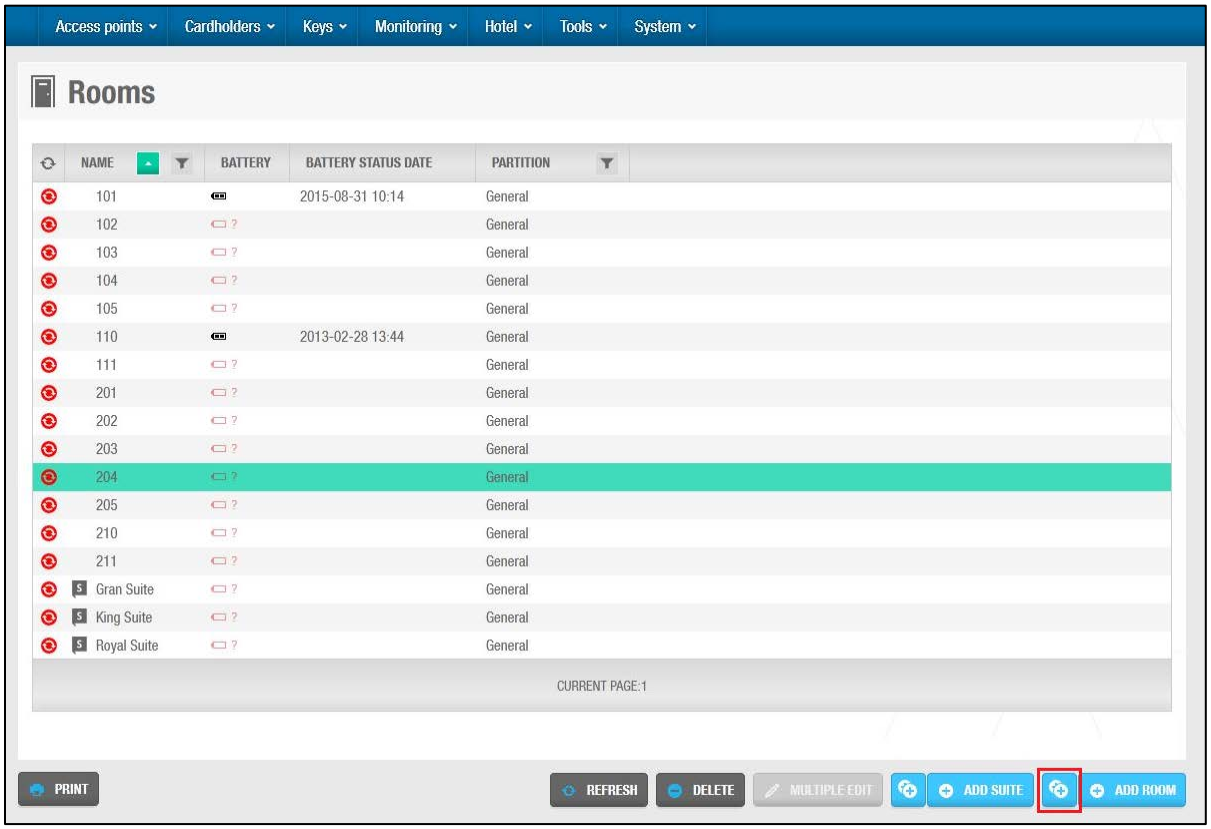


Figure 123: Rooms screen

2. Click **Multiple Add**. The **Multiple add** dialog box is displayed.

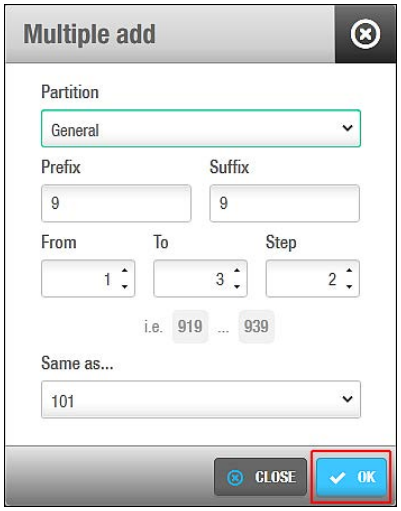


Figure 124: Multiple add dialog box

3. Select the appropriate partition from the **Partition** drop-down list if required.

   See *Partitions* for more information about partitions.

4. Type a prefix in the **Prefix** field if required.

   This is included at the beginning of the new room names. For example, if you type 9 in the **Prefix** field, and create two rooms, the rooms are named 91 and 92 respectively. You can change individual room names by amending the text in the **Name** field on the **Room** information screen if required.

5. Type a suffix in the **Suffix** field if required.

   This is included at the end of the new room names. For example, if you type 9 in the **Suffix** field, and create two rooms, the rooms are named 19 and 29 respectively.

6. Select the required numbers by using the up and down arrows in the **From** and **To** fields.

   The numbers in these fields define the number of rooms that are created. For example, if you select **1** in the **From** field and **3** in the **To** field, three rooms are created. The number of each room is included in the room name by default. In this example, if you have not entered a prefix or a suffix, the rooms are named 1, 2, and 3 respectively.

7. Select the appropriate number by using the up and down arrows in the **Step** field if required.

   This allows you to more accurately define what rooms are created within the number range you have selected in the **From** and **To** fields. For example, if you select **2** in the **Step** field, rooms are created for every second number within the specified range.

8. Select the appropriate room from the **Same as** drop-down list if required.

   If you select a room from the drop-down list, the configuration settings of the new rooms are the same as the room you select. However, if you select a suite, multiple suites with the same configuration settings are created. You must associate rooms with each of the new suites individually if required. See *Rooms* for more information and a description of the steps you should follow. The default option is **None**. In this case, multiple rooms are created, but you must define the configuration settings for each one.

9. Click **OK**.

8. 7. 2. Creating Multiple Suites

The process for creating multiple suites is the same as for creating multiple rooms. See *Creating Multiple Rooms* for a description of the steps you should follow.

NOTE: You can edit multiple rooms or suites at once by using the **Multiple Edit** button. This button is enabled when you select more than one entry on the **Rooms** screen. This allows you to enter the appropriate identification and configuration details on the **Multiple edit** screen. The details are then applied to all of the selected entries. See *Configuring Rooms* and *Configuring Suites* for more information about the configuration settings for rooms and suites.

8. 8. Checking Room and Suite Status

You can view whether a room or suite is available or occupied by selecting **Hotel** > **Room status**.

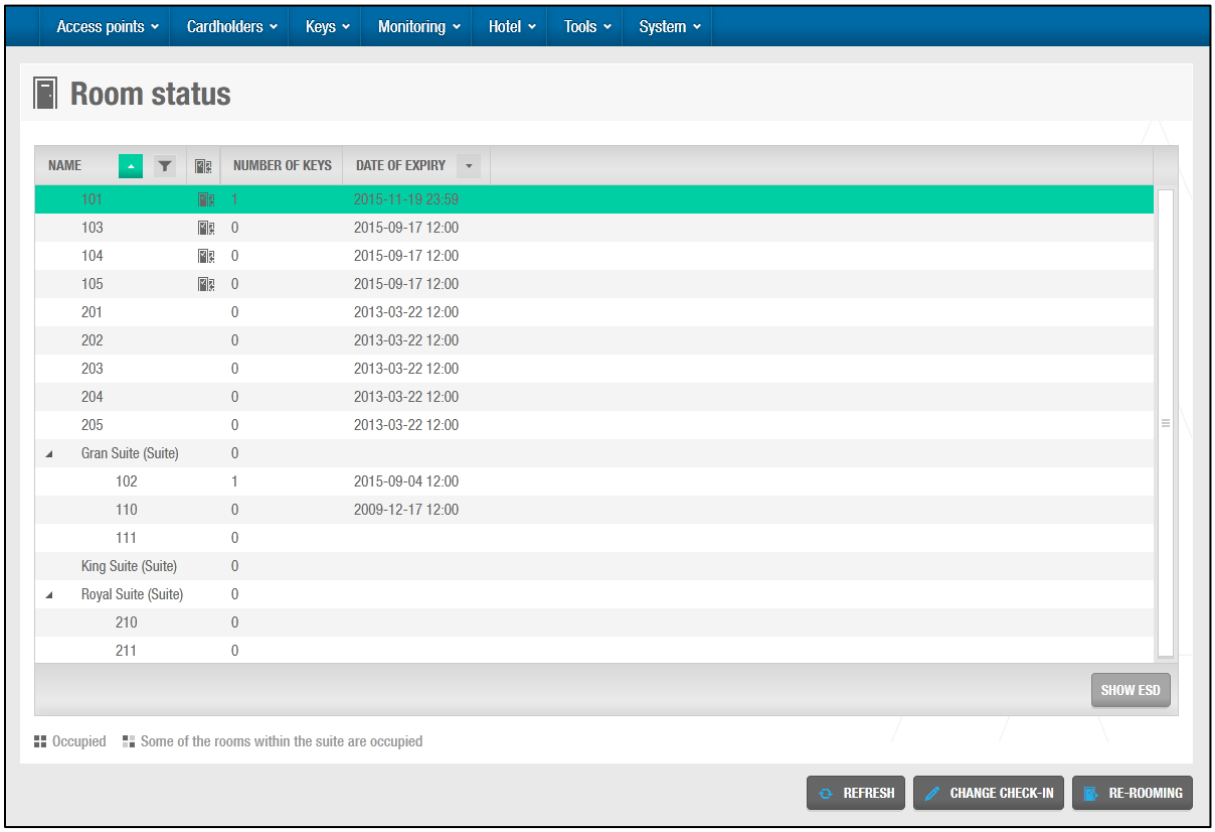


Figure 125: Room status information screen

The **Room status** information screen shows all of the rooms and suites in the hotel. Different icons are displayed, depending on the status of each room and suite.

These are described in the following table.

Table 30: Room and suite status icons

Icon	Description

Icon	Description
 Occupied	Indicates that a room or suite is occupied by guests. This icon is displayed on the left-hand side of the room or suite name. If a room or suite is occupied, the expiration date is also shown in the **Date of Expiry** column.
 Some of the rooms within the suite are occupied	Indicates that some of the rooms in a suite are occupied by guests. This icon is displayed on the left-hand side of the suite name. In this case, you cannot perform a check-in for the suite.
 Belongs to a check-in group	Indicates that a room or suite is reserved for a check-in group. This icon is displayed in the **Belongs to a check-in group** column.

8. 8. 1. Checking ESD Status

You can click the **Show ESD** button to see the ESD status on the **Room status** information screen. Click the **Hide ESD** button to hide the **ESD** column. A green dot is displayed in the **ESD** column if the ESD is online and communicating correctly with its CU. If a communication issue occurs, a red dot is displayed. When a user or guest activates an ESD using their key, a **Key** icon and the name of the user or guest are also displayed in the column. See *ESDs* and *Associated Device Lists* for more information about ESDs.

8. 9. Configuring Hotel Keys

You can perform a number of special key configurations for hotels. These are as follows:

- **Copy guest key**: You can make up to 10 copies of a guest key at a time. This is useful if the room is occupied by more than one guest.
- **Cancellation of guest lost keys**: You can cancel guest keys if the guest has lost the key or if the guest leaves before the check-out date, taking the key with them. This sends the key to the blacklist, and prevents the key being used by someone other than the original guest. See *About Blacklists* for more information. If the guest has only been given access to their room, a guest cancelling key can be used to prevent unauthorized access. However, if the guest has access to optional facilities such as the hotel leisure centre, it is recommended that you use the **Cancellation of guest lost keys** option.
- **One shot key**: You can configure a key to be used only once. A one shot key can be valid for up to four rooms at any one time. This is useful if a guest wants to view a number of rooms before checking in.
- **Programming/Spare keys**: You can pre-program a programming key and edit spare keys for use in case a hotel power failure occurs or an encoder failure.
- **Edit guest cancelling key**: You can configure a key to be used by hotel staff to deny a guest with a valid key access to a room. This is useful if hotel management need to speak with the guest before they re-enter their room for example. Once a guest cancelling key is used, a new guest check-in is required to allow the guest to access the room. However, the guest's key is not sent to the blacklist. See *About Blacklists* for more information.
- **Room cleaner keys**: You can configure keys to be used by room cleaning staff to let front-desk operators know that the room is ready for occupancy.

The following sections describe these key configurations.

8. 9. 1. Copying Guest Keys

To copy a guest key, perform the following steps:

1. Select **Hotel** > **Copy guest key**. The **Copy guest key** information screen is displayed.

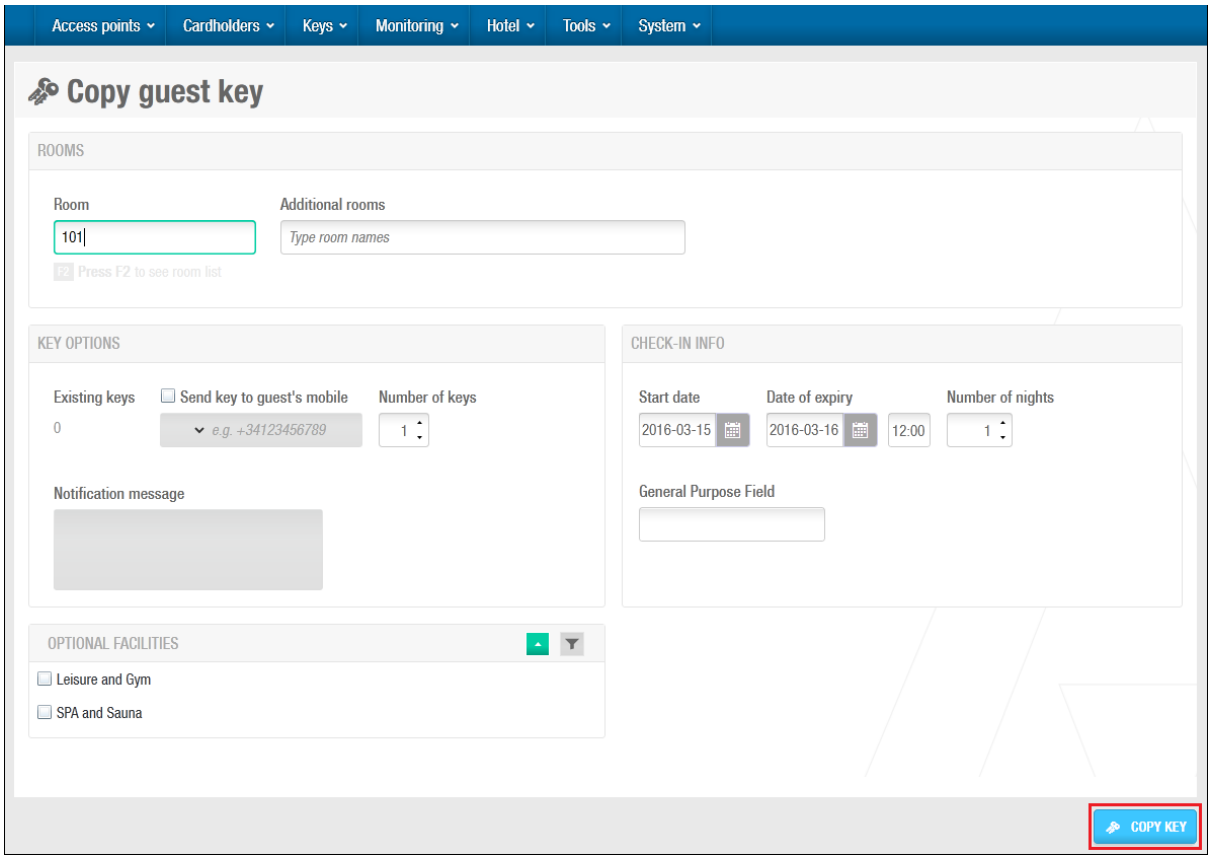


Figure 126: Copy guest key information screen

2. Type the room for the key you want to copy.

   If the room is part of a suite, ensure that you copy the suite and not just an individual room. Copying a room within the suite cancels the original key. You can also use the **Additional rooms** field to copy more rooms. Type the name of the room or press F2 to display the **Select room** dialog box and select a room from the list.

   If the room is assigned to a guest who is using a mobile key, on the screen you will see the option to make the copy of the key to another mobile number. Alternatively, you can make a copy as a traditional credential. If you want to make another mobile key, click on Send key to guest mobile and include the new mobile number which will receive a copy of the key. Note that you can only add one mobile number at a time.

3. Type the number of keys required in the **Number of keys** field.

   The fields in the **Check-In Info** panel automatically update with the information from the original key.

NOTE: You can only make up to 10 copies of a guest key at a time. However, you can repeat the operation as many times as you want.

4. Click **Copy Key**. A pop-up is displayed asking you to place a key on the encoder.

5. Place the key on the encoder when the LED light begins to flash. The room information is transferred to the key. A pop-up is displayed confirming the operation was successful.
6. Remove the key and click **OK**.
7. Repeat Steps 4, 5, and 6 to continue copying keys.

8. 9. 2. Cancelling Guest Lost Keys

To cancel a guest lost key, perform the following steps:

1. Select **Hotel** > **Cancellation of guest lost keys**. The **Cancellation of guest lost keys** dialog box is displayed.

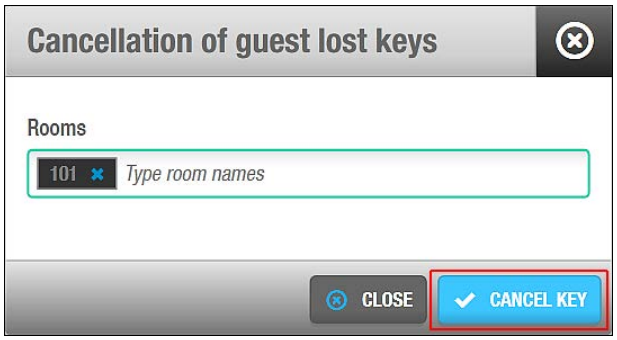


Figure 127: Cancellation of guest lost keys dialog box

2. Type the room for the key you want to cancel.
   You can press F2 to display the **Select rooms** dialog box and select a room from the list.
3. Click **Cancel Key**. The key is cancelled. A pop-up is displayed confirming that the operation was successful.
4. Click **OK**.

8. 9. 3. Creating One Shot Keys

To create a one shot key, perform the following steps:

1. Select **Hotel** > **One shot key**. The **One shot key** dialog box is displayed.

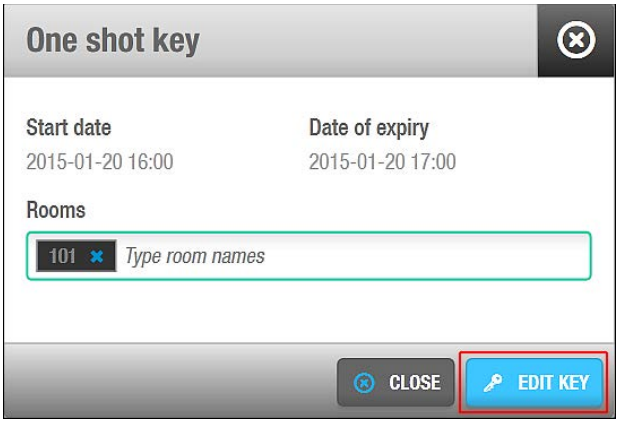


Figure 128: One shot key dialog box

2. Type the room for the one shot key.
   You can press F2 to display the **Select rooms** dialog box and select a room from the list. By default, the expiration data for a one shot key is one hour from the moment of encoding. The default cannot be changed.

3. Click **Edit Key**. A pop-up is displayed asking you to place the key on the encoder.
4. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming the operation was successful.
5. Remove the key and click **OK**.

8. 9. 4. Creating Programming/Spare Keys

You can create programming keys, copy programming keys, and edit spare keys.

NOTE: Operators can only create programming keys, copy programming keys, and edit spare keys for their own partitions. See *Partitions* for more information about partitions. The partition options that are displayed when performing these tasks depend on operator permissions.

8. 9. 4. 1. Creating Programming Keys

Programming keys are used with spare keys in the case of a power failure or an encoder failure. Programming keys allow you to continue check-ins without interruption so that guests can access their rooms. The programming key is presented to the room lock, and a spare key is then subsequently presented. The programming key updates the lock to allow the spare key to be used. The guest can use the spare key, which does not have an expiration date, to access their room until normal operation resumes and a new guest key is encoded. See *Editing Spare Keys* for more information about spare keys.

NOTE: It is highly recommended that after you create your programming key, you make multiple copies of it. Store these keys in a safe place for use by hotel staff in an emergency situation. Copies of programming keys can be used with spare keys. However, if a new programming key is created, this invalidates any existing spare keys. You should always create copies of the programming key unless it is lost or damaged. In this case, you need to create a new programming key.

To create a programming key, perform the following steps:

1. Select **Hotel** > **Programming & spare keys**. The **Programming & spare keys** screen is displayed.

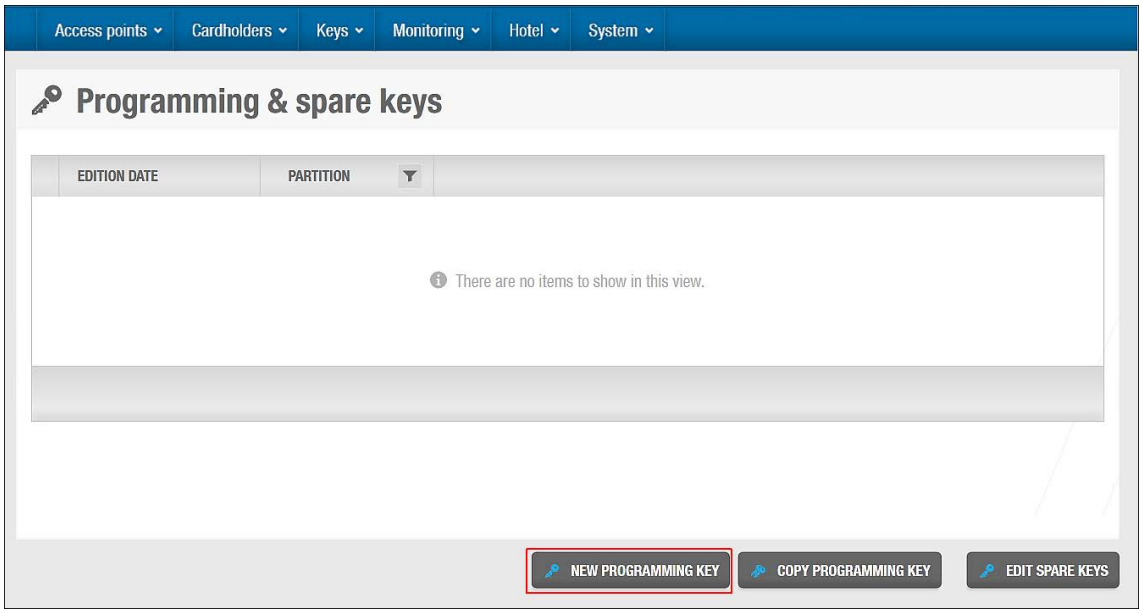


Figure 129: Programming & spare keys screen

2. Click **New Programming Key**. The **Partition** dialog box is displayed.

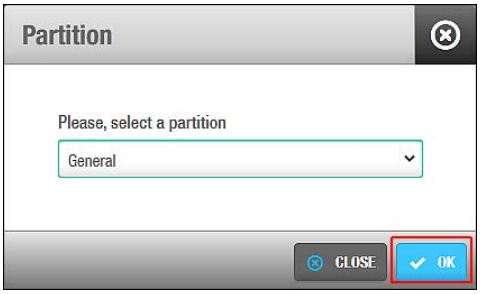


Figure 130: Partition dialog box

The partitions functionality is license-dependent. If you do not have access to this in your licensing options, the **Partition** dialog box is not displayed. See *Partitions* for more information about partitions.

3. Select a partition from the drop-down list if required.
4. Click **OK**. A pop-up is displayed asking you to place the key on the encoder.
5. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming the operation was successful.
6. Click **OK**.

After you create a programming key, the date and time it was programmed are displayed on the **Programming & spare keys** screen.

NOTE: Copies of programming keys can be used with spare keys. See *Copying Programming Keys* and *Editing Spare Keys* for more information. However, if a new programming key is created, this invalidates any existing spare keys. If guests do not return spare keys, or they are damaged, you can create new spare keys for use with the existing programming key after normal operation resumes.

8. 9. 4. 2. Copying Programming Keys

Copies of programming keys can be made. These can be specially useful for hotels with a large number of rooms for example.

To copy a programming key, perform the following steps:

1. Select **Hotel** > **Programming & spare keys**. The **Programming & spare keys** screen is displayed.

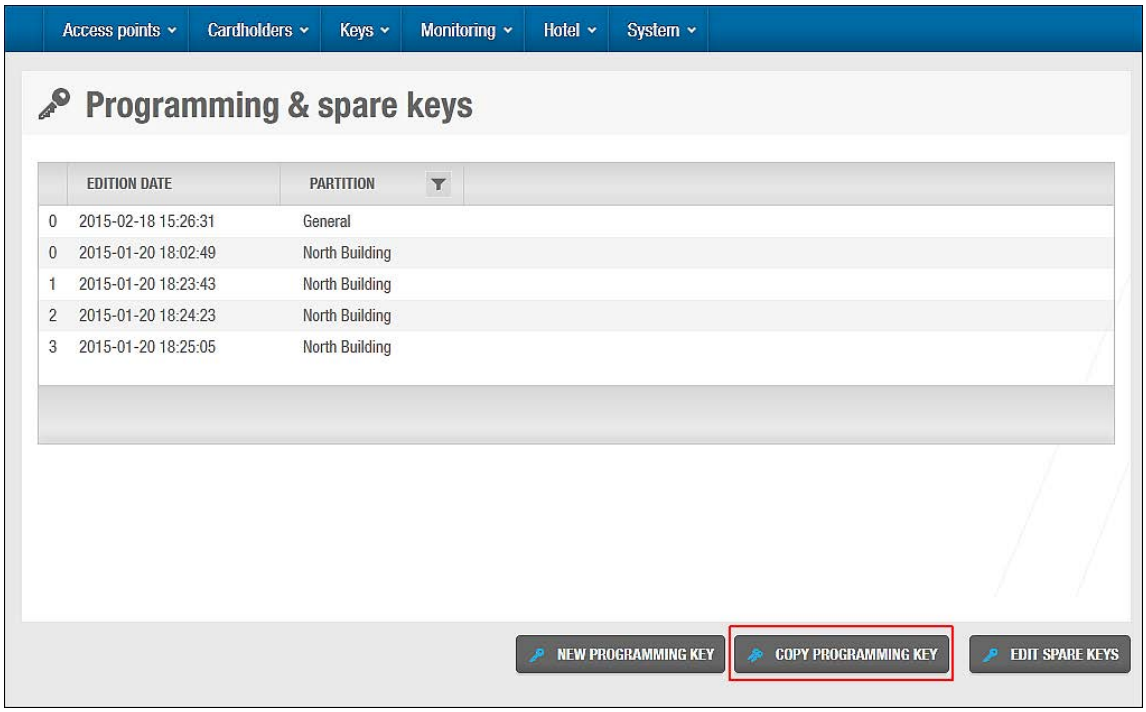


Figure 131: Programming & spare keys screen

2. Click **Copy Programming Key**. The **Partition** dialog box is displayed.

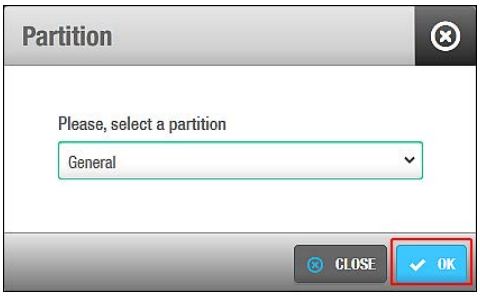


Figure 132: Partition dialog box

3. Select a partition from the drop-down list if required.

   The partitions functionality is license-dependent. If you do not have access to this in your licensing options, the **Partition** dialog box is not displayed. See *Partitions* for more information about partitions.
4. Click **OK**. A pop-up is displayed asking you to place the key on the encoder.
5. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming that the operation was successful.
6. Remove the key and click **OK**.

After you copy a programming key, the date and time it was copied are displayed on the **Programming & spare keys** screen.

8. 9. 4. 3. Editing Spare Keys

Spare keys are used with programming keys to allow guests to access rooms in the case of a power failure or an encoder failure. See *Creating Programming Keys* for more information about programming keys.

When a spare key is used, it automatically cancels any other keys for the room, except those of hotel staff (users). A spare key is automatically cancelled when a new guest key or a new spare key is used to access the room.

It is recommended that you edit a higher number of spare keys than hotel rooms. For example, if a hotel has 300 rooms, you should edit approximately 450 spare keys.

NOTE: Copies of programming keys can be used with the spare keys you create. See *Copying Programming Keys* for more information. However, if a new programming key is created, this invalidates any existing spare keys.

To edit a spare key, perform the following steps:

1. Select **Hotel** > **Programming & spare keys**. The **Programming & spare keys** screen is displayed.

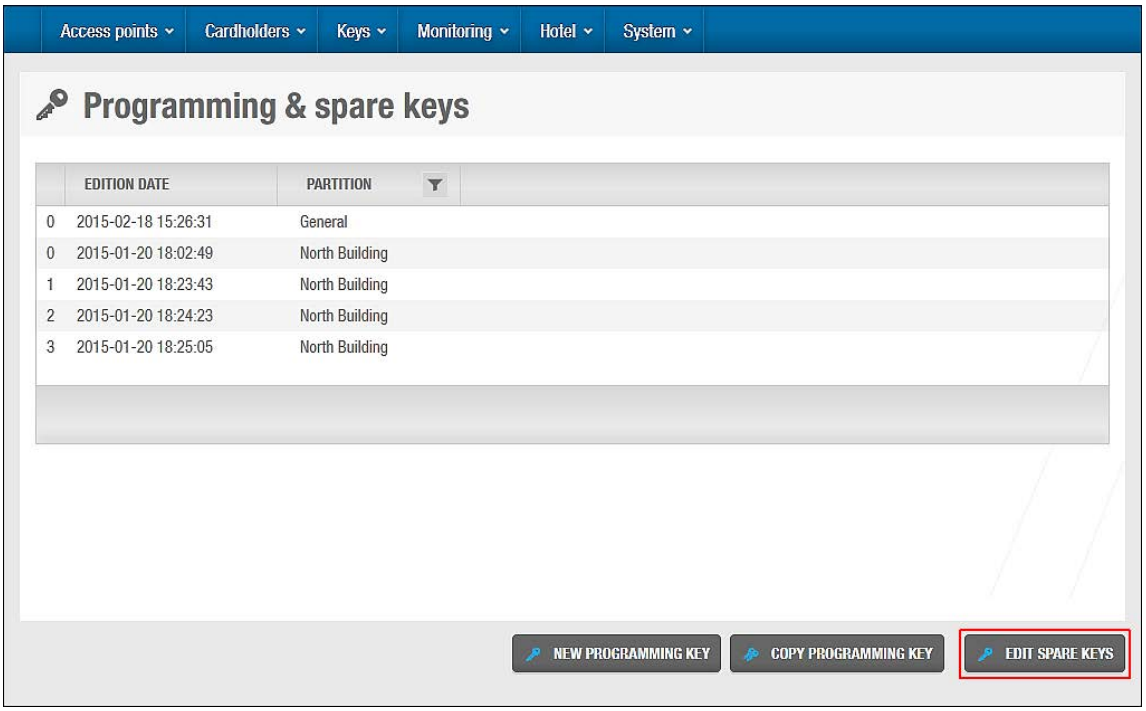


Figure 133: Programming & spare keys screen

2. Click **Edit Spare Keys**. A pop-up is displayed asking you to place the key on the encoder.
3. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming that the operation was successful.
4. Remove the key and click **Close**.

   You can click **Edit Another Spare Key** to continue editing keys.

8. 9. 4. 4. Editing Spare Key Copies

You can make copies of spare keys if you have enabled this functionality in ProAccess SPACE General options. To activate this option, you must select the **Allow copies of spare keys checkbox** in **System** > **General options** > **Hotel**. When you select this option, an **Edit Spare Keys Copies** button is displayed on the **Programming & spare keys** screen. See *Hotel Tab* and *Editing Spare Keys* for more information.

To edit spare key copies, perform the following steps:

1. Select **Hotel** > **Programming & spare keys**. The **Programming & spare keys** screen is displayed.

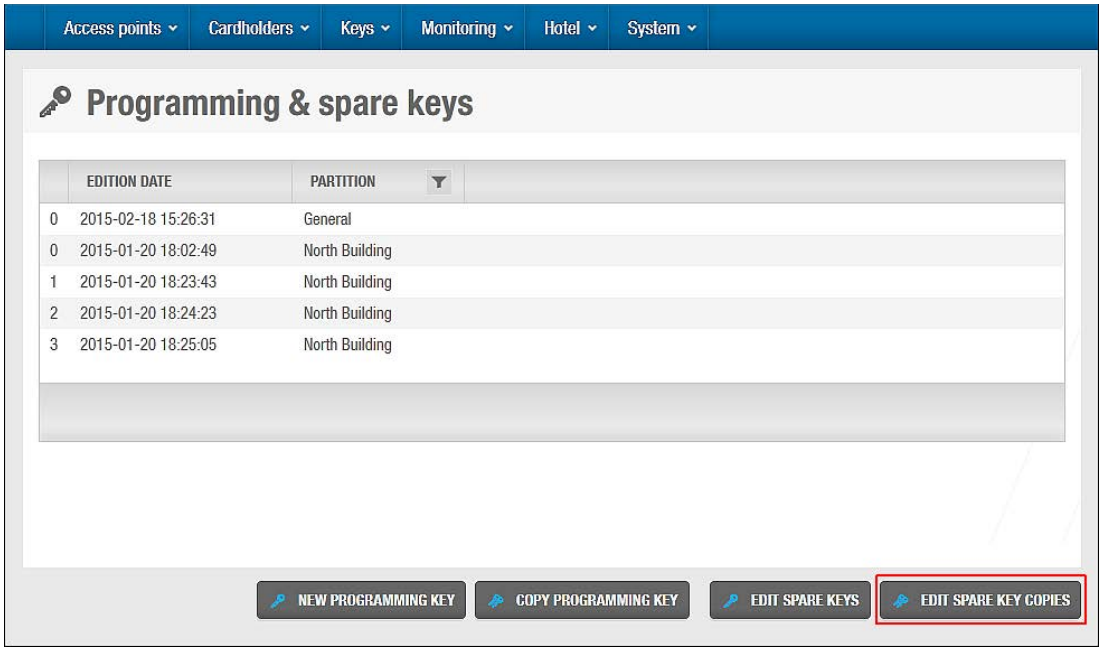


Figure 134: Programming & spare keys screen

2. Click **Edit Spare Key Copies**. The **Copy spare key** dialog box is displayed.

Figure 135: Copy spare key dialog box

3. Select the number of keys you want to copy by using the up and down arrows in the **Number of keys** field.

NOTE: You can only edit up to 10 spare key copies at a time. However, you can repeat the operation as many times as you want.

4. Click **OK**. A pop-up is displayed asking you to place the key on the encoder.
5. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming that the key has been edited and asking you to place the next key on the encoder.
6. Place the next key on the encoder and click **Accept**.
7. Repeat the process for all the required keys. A pop-up is displayed confirming that the operation was completed successfully.
8. Click **OK**.

8. 9. 5. Editing Guest Cancelling Keys

To edit a guest cancelling key, perform the following steps:

1. Select **Hotel** > **Edit guest cancelling key**. The **Guest cancelling key** dialog box is displayed.

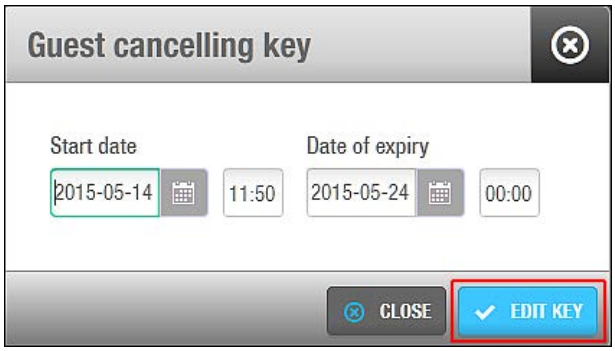


Figure 136: Guest cancelling key dialog box

2. Select the start date using the calendar and type the time in the **Start date** fields.
3. Select the date of expiry using the calendar and type the time in the **Date of expiry** fields.
4. Click **Edit Key**. A pop-up is displayed asking you to place the key on the encoder.
5. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming that the operation was successful.
6. Remove the key and click **OK**.

8. 9. 6. Editing Room Cleaner Keys

Room cleaner keys are used to inform hotel front-desk staff that rooms are ready for occupancy. They are not used to access rooms or other hotel access points, or to activate ESDs. When a room has been cleaned, cleaning staff insert the room cleaner key in the room's ESD and then remove it. Alternatively, they can present the key at an RF door after they have exited the room. This creates an audit trail entry that shows the room door and indicates the room has been cleaned. For example, the audit trail entry can contain the text 'room cleaned'. Front-desk staff can check whether rooms are ready by viewing the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

To create a room cleaner key, perform the following steps:

1. Select **Hotel** > **Room cleaner**. A pop-up is displayed asking you to place the key on the encoder.
2. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming that the operation was successful.
3. Remove the key and click **OK**.

8. 10. Hotel Guests

A guest can be described as someone who is staying temporarily at a hotel and requires access to an assigned room for a fixed period of time. Hotel guests should not be confused with users, who are members of the hotel staff.

The following sections describe the two types of guests and the associated configuration options:

- **Guest**: An individual requiring one room or a suite
- **Group**: A number of guests requiring multiple rooms

8. 11. Guest Access Levels

Guest access levels are used to group together guests and access points for access to a specific area. For example, you can create a first floor access level for all guests staying on the first floor or a leisure access level for guests to access the gym. You must define the guest access levels before checking in guests.

The following sections describe how to create and associate a guest access level.

8. 11. 1. Creating Guest Access Levels

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

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

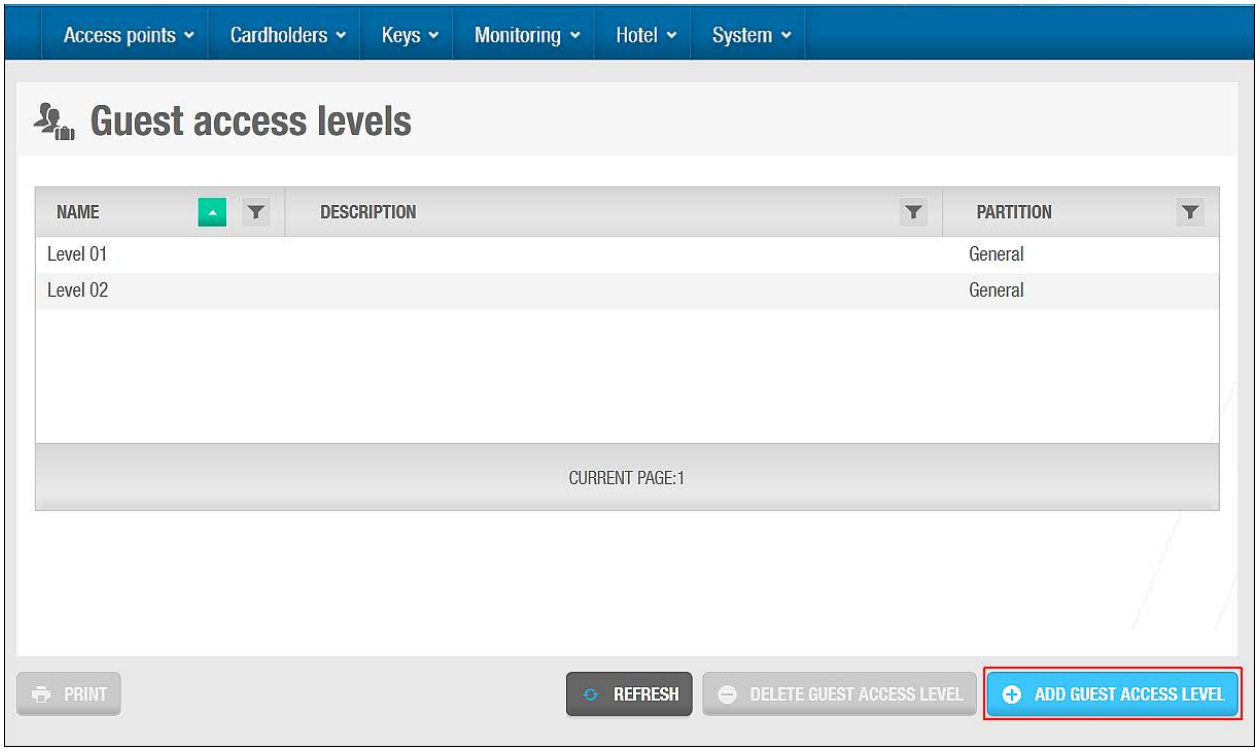


Figure 137: Guest access levels screen

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

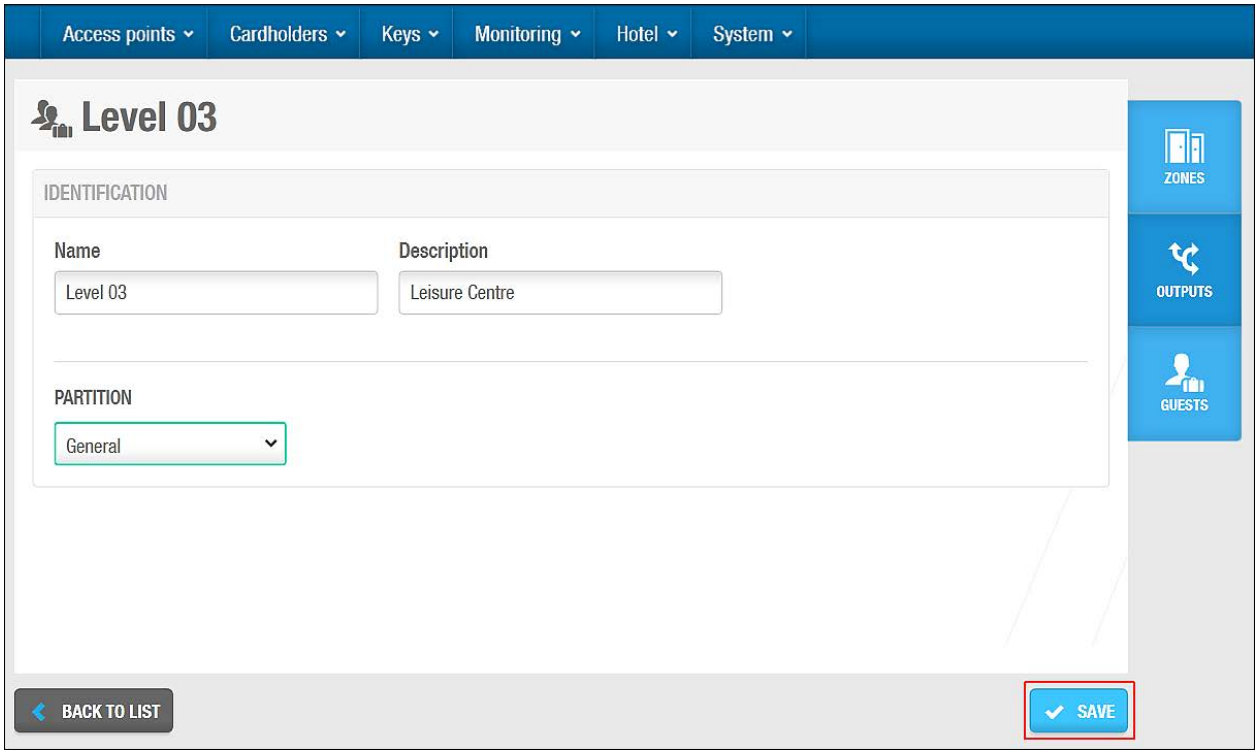


Figure 138: Guest access level information screen

3. Type a name for the guest access level in the **Name** field.
4. Type a description for the guest access level in the **Description** field.
5. Select the appropriate partition from the **Partition** drop-down list if required.

   See *Partitions* for more information about partitions.
6. Click **Save**.

8. 11. 2. Associating Guest Access Levels

After you have created a guest access level, you must associate zones, outputs, and guests with that guest access level. The following sections describe how to associate guest access levels with those entries.

8. 11. 2. 1. Zones

To associate a zone with a guest access level, perform the following steps:

1. Select **Cardholders** > **Guest access levels**. The **Guest access levels** screen is displayed.
2. Double-click the guest access level that you want to associate with a zone. The **Guest access level** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of zones, is displayed.
5. Select the required zone in the left-hand panel and click the chevron. The selected zone is displayed in the right-hand panel.
6. Click **Accept**. The guest access level is now associated with the zone.
7. Select the zone in the **Zones** dialog box if you want to select a cardholder timetable to be used or specify whether access is optional. See *Cardholder Timetables* for more information.

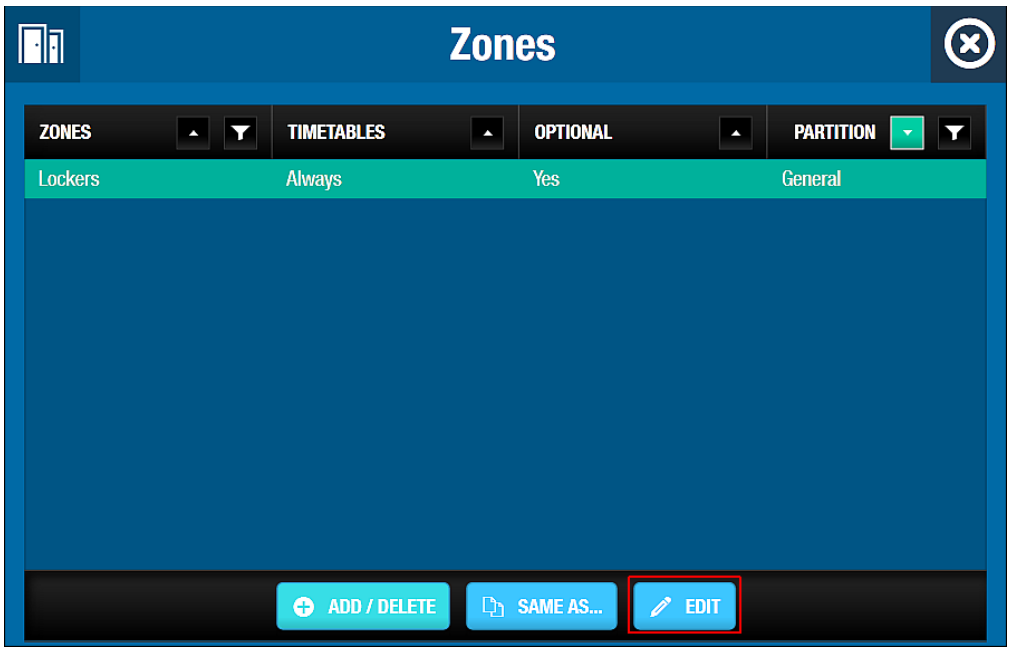


Figure 139: Zones dialog box

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

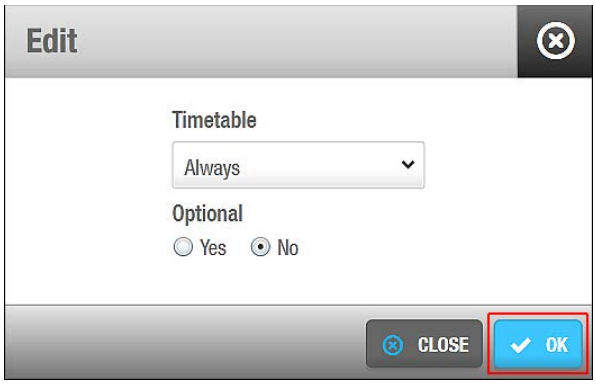


Figure 140: Edit dialog box

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

   The **Always** option is selected by default. This means that guests associated with the specified guest access level always have access to the zone, 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 zone at any time.

10. Select **Yes** or **No** as appropriate.

    If you select **Yes**, the hotel operator can decide whether or not to grant access when they check in a guest. If you select **No**, access is granted to all guests in the guest access level by default. Note that if you specify an access point as optional, it is displayed as a checkbox option in the **Optional Facilities** panel on the **Hotel check-in** screen. Optional access is useful for hotels offering various accommodation packages and rates to guests, for example, accommodation with or without spa access.

11. Click **OK**.

NOTE: For security purposes, a guest access level cannot be associated with a zone that contains a room. Guests can only be given access to their own rooms or specific additional rooms at check-in.

8. 11. 2. 2. Outputs

To associate an output with a guest access level, perform the following steps:

1. Select **Cardholders** > **Guest access levels**. The **Guest access levels** screen is displayed.
2. Double-click the guest access level that you want to associate with an output. The **Guest access level** information screen is displayed.
3. 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.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of outputs, is displayed.
5. Select the required output in the left-hand panel and click the chevron. The selected output is displayed in the right-hand panel.
6. Click **Accept**. The guest access level is now associated with the output.

   You can specify whether access is optional. For example, you can give all guests in the guest access level access to the penthouse floor by default or opt to grant guests access to this floor during check-in. See *Zones* for more information and a description of the steps that you should follow.

NOTE: It is recommended that you select **No** in the **Optional** column for the ESD_#1 and ESD_#2 outputs that are generated by the system. This ensures that guests automatically receive access to the ESD in their room when their key is encoded, and hotel operators do not have to grant this access to individual guests during check-in. See *Associated Device Lists* and *Zones* for more information.

8. 11. 2. 3. Guests

To associate a guest with a guest access level, perform the following steps:

1. Select **Cardholders** > **Guest access levels**. The **Guest access levels** screen is displayed.
2. Double-click the guest access level that you want to associate with a guest. The **Guest access level** information screen is displayed.
3. Click **Guests** in the sidebar. The **Guests** dialog box is displayed.

   Note that the dialog box will be blank because you have not yet associated a guest.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of guests, is displayed.
5. Select the required guest in the left-hand panel and click the chevron. The selected guest is displayed in the right-hand panel.
6. Click **Accept**. The guest access level is now associated with the guest.

8. 12. Guest Check-In

A guest check-in es generally performed by the front-desk operator when a guest arrives at the hotel.

A guest check-in is performed in the following order:

1. **Room is selected and check-in information is entered**

The hotel operator selects a room and enters the check-in information, for example, the dates of the guest's stay and any additional rooms required.

2. **Key is edited**

   The hotel operator edits the key for the guest using an encoder. See *Encoders* for more information about encoders.

8. 12. 1. Selecting Rooms

When a guest arrives at the hotel, the hotel operator selects a room and enters the guest check-in information.

To select a room, perform the following steps:

3. Select **Hotel** > **Check-in**. The **Hotel check-in** screen is displayed.

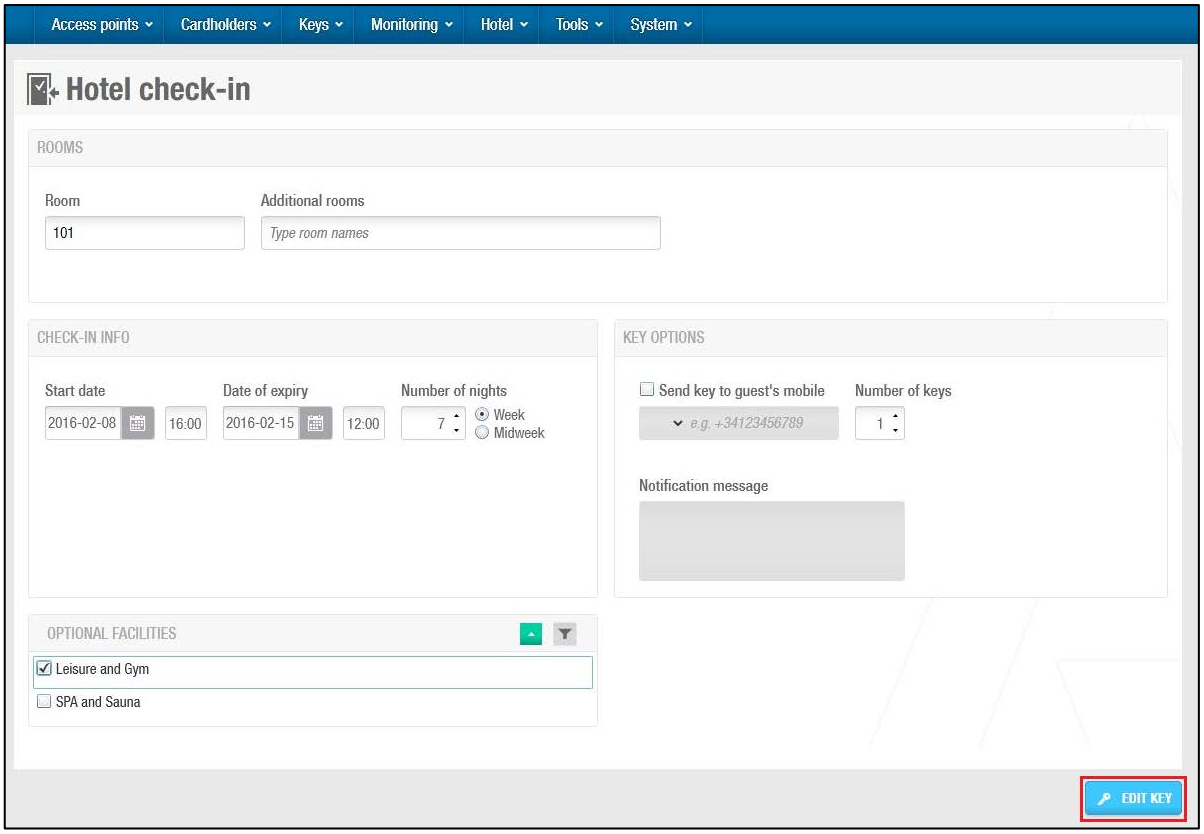


Figure 141: Hotel check-in screen

4. Type the name of the room or, alternatively, press F2 to display the **Select room** dialog box.

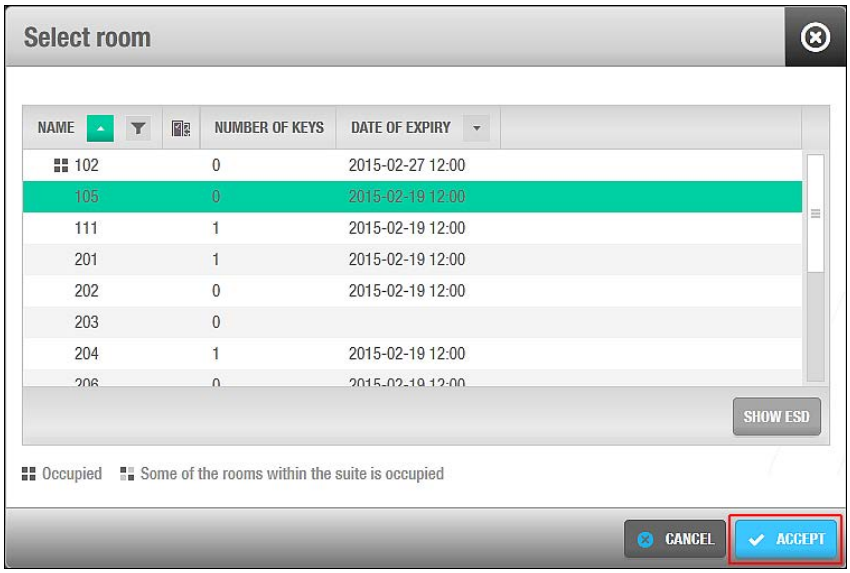


Figure 142: Select room dialog box

5. Select an available room.
6. Click **Accept**. The selected room is added to the **Room** field in the **Hotel check-in** screen.

   You can use the **Additional rooms** field to give the guest access to other rooms. For example, parents may be staying in Room 101 and their children may be staying in Room 102. You can give the parents access to both Room 101 and Room 102. If a suite is selected, access is granted to all of the rooms within the suite. Additional rooms outside of the suite can also be added.

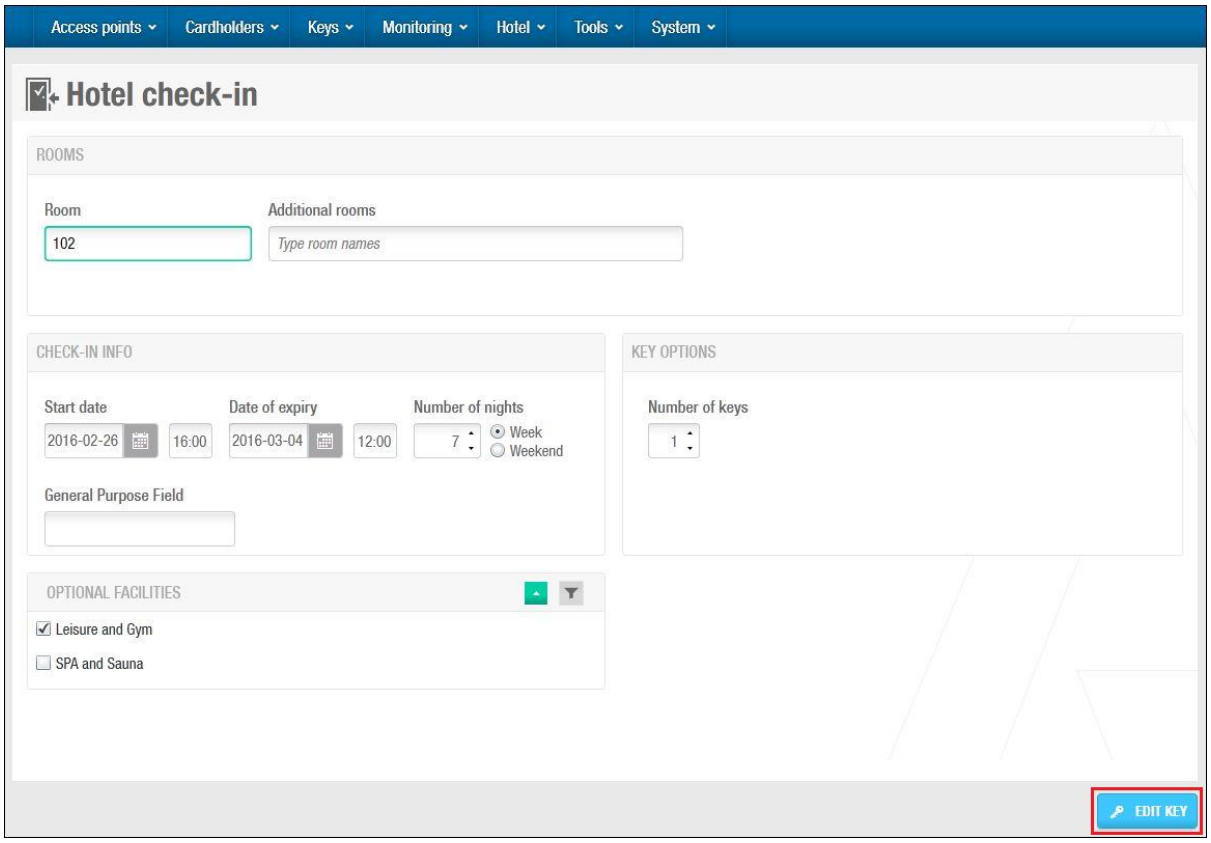


Figure 143: Hotel check-in screen

7. Select the applicable check-in information in the **Check-In Info** panel.

   The check-in information fields are described in *Adding Check-In Information*.
   You can also add a **General purpose field** in the check-in window. See *Hotel Tab* for more information about guests general purpose fields. The content of the General purpose field can be added to a track in the guest key. For example, the guest car tag is added to the General purpose field, this data in turn is written in the key track so it can be sent to a third party application when the key is read.
8. Select the appropriate optional facilities if required.

   The optional facilities shown in the **Optional Facilities** panel match any access points you have set up and defined as optional. See *Zones* for more information about defining guest access points as optional. You can control whether guests can access optional facilities before their specified room start time in ProAccess SPACE General options. You can also define the time when guest access to optional facilities expires on their check-out day. See *Hotel Tab* for more information.
9. Select the number of keys required in the **Number of keys** field.

NOTE: Up to 10 keys can be issued per room during a check-in. Only the original key and the first three copies are named differently by the system. For example, for Room 101, the first four keys are named as follows: @101, @101#1, @101#2, and @101#3.The remaining six keys are all named @101 #3. If more keys are required, additional copies can also be made. See *Copying Guest Keys* for more information.

10. Click **Edit Key**. A pop-up is displayed asking you to place the key on the encoder.
11. Place the key on the encoder when the LED light begins to flash. The check-in information is transferred to the key. A pop-up is displayed confirming that the operation was successful.
12. Remove the key and click **OK**.

8. 12. 1. 1. JustIN Mobile check-in

When a guest arrives at the hotel or does an online check-in, the hotel operator can select to send the key data to a **Bluetooth Low Energy** (BLE) enabled smartphone. Please note that this option of using a BLE-enabled smartphone as a credential can only be used with locks that have been equipped with BLE readers.

This mobile check-in feature is license-dependent. This means that the functionality will not be enabled in your SALTO installation unless it is covered by your selected license options.

Please note that a guest must download SALTO's **JustIN Mobile** application from the AppStore for iOS operating systems, or the Play Store for smartphones using Android prior to being able to use JustIN Mobile to receive a room key.

NOTE: The **JustIN Mobile** key does not share the same characteristics as traditional credentials such as cards, bracelets and fobs. For example, the smartphone-based credential does not support data on tracks, Wiegand applications, free assignment lockers, anti-passback, last rejection data or audit on key. Also Wall Readers (update points) cannot write data on a smartphone-based credential.

Once the guest has downloaded the **JustIN Mobile** application, a guest need only follow the instructions on the application to complete registration.

To select a room, perform the following steps:

1. Select **Hotel** > **Check-in**. The **Hotel check-in** screen is displayed.

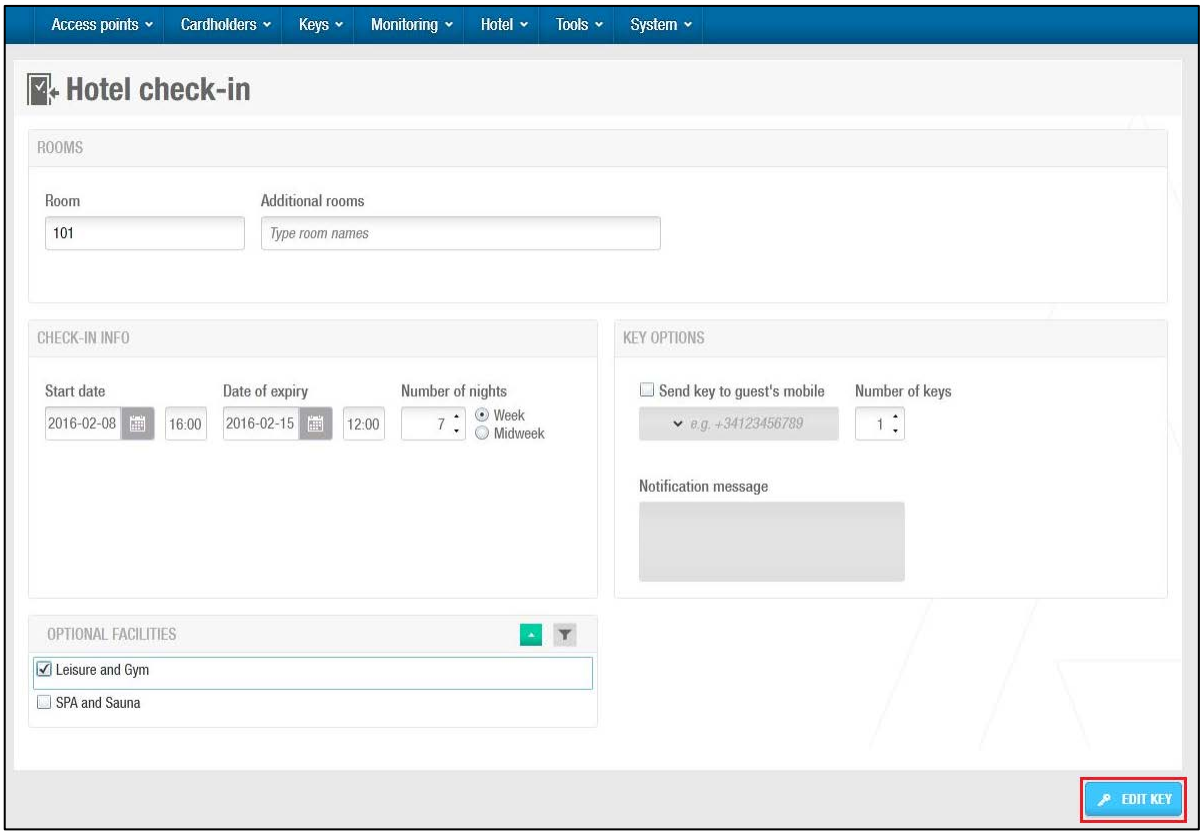


Figure 144: Hotel check-in screen

2. Type the name of the room or, alternatively, press F2 to display the **Select room** dialog box.

NOTE: To see the **Send key to guest's mobile** in **Key options** during the Check-in, you must enable **Allow mobile guest's keys** in the room. See *Room options* for more information. If **Allow mobile guest's keys** is not checked in rooms, the **Send key to guest's mobile** will not be shown during the check-in process.

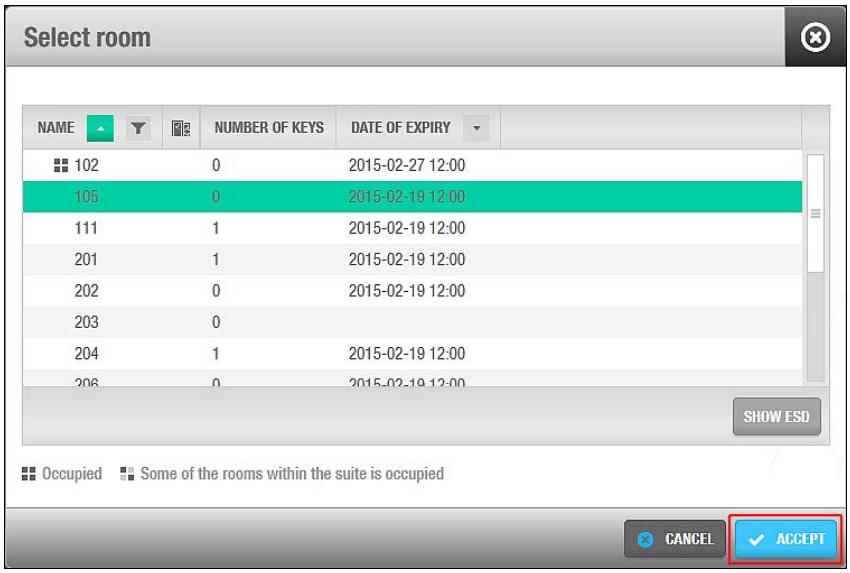


Figure 145: Select room dialog box

3. Select an available room.
4. Click **Accept**. The selected room is added to the **Room** field in the **Hotel check-in** screen.

   You can use the **Additional rooms** field to give the guest access to other rooms. For example, parents may be staying in Room 101 and their children may be staying in Room 102. You can give the parents access to both Room 101 and Room 102. If a suite is selected, access is granted to all of the rooms within the suite. Additional rooms outside of the suite can also be added.

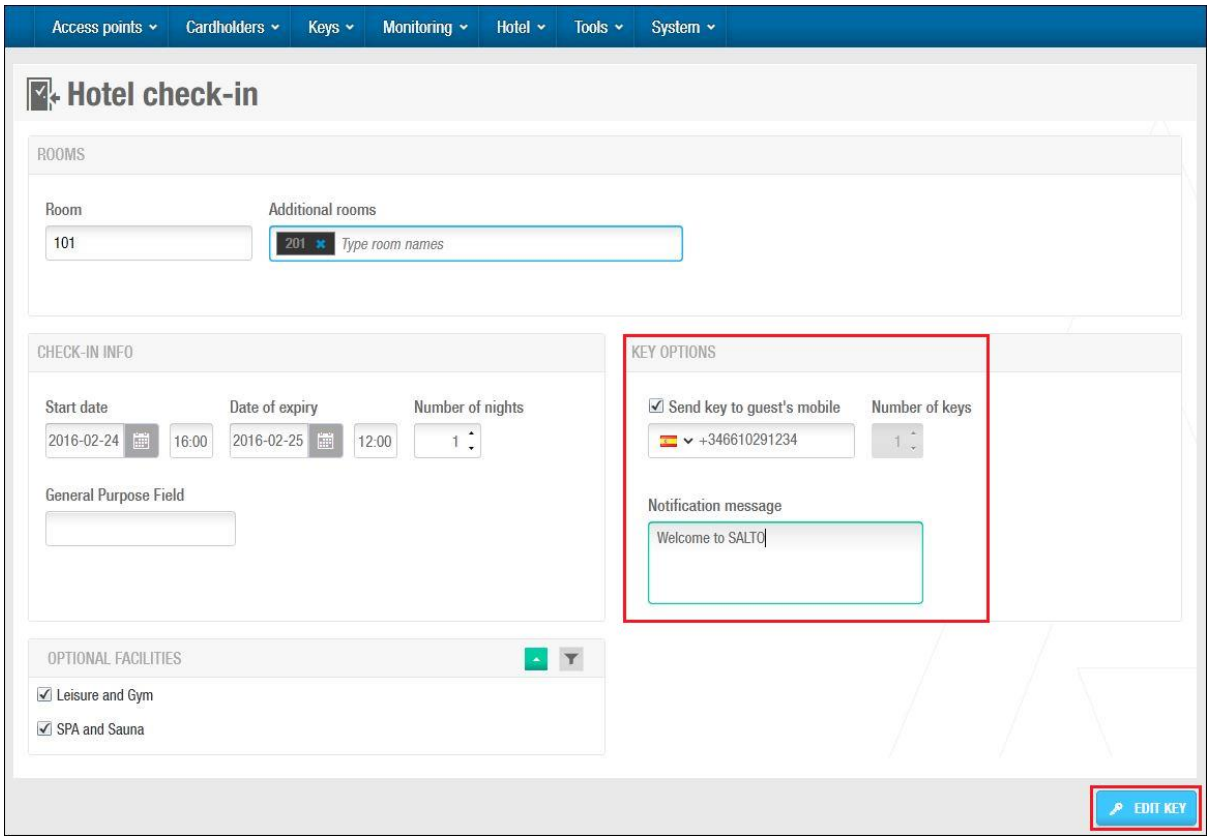


Figure 146: Hotel check-in screen

5. Select **Send key to guest's mobile** in the **Key option** panel.
   You can add a message in the Notification message box and this message will be shown in the guest mobile. For example, "Welcome to Hotel Paradise"

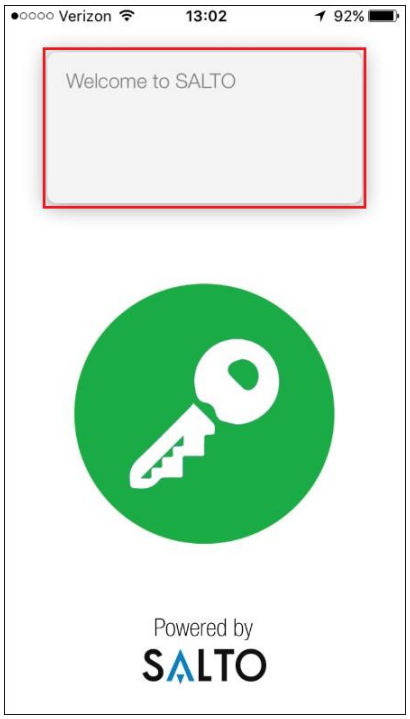


Figure 147: Hotel Mobile check-in screen

6. Select the appropriate optional facilities if required.
   The optional facilities shown in the **Optional Facilities** panel match any access points you have set up and defined as optional. See *Zones* for more information about defining guest access points as optional. You can control whether guests can access optional facilities before their specified room start time in ProAccess SPACE General options. You can also define the time when guest access to optional facilities expires on their check-out day. See *Hotel Tab* for more information.
7. Only one mobile key can be created during the guest check-in. Additional copies of a mobile key can be issued through the *Copy guest key* screen.
8. Click **Edit Key**. A pop-up is displayed telling you that the operation was completed successfully.

NOTE: The data sent Over The Air (OTA) to your mobile phone is encrypted and this happens by using the SALTO Ethernet encoder as a Dongle. See *Devices Tab* in **System** > **General options** for more information.

The mobile phone must be online in order to receive the check-in information.

9. Tap the green key button on the application and present the mobile phone to the lock.

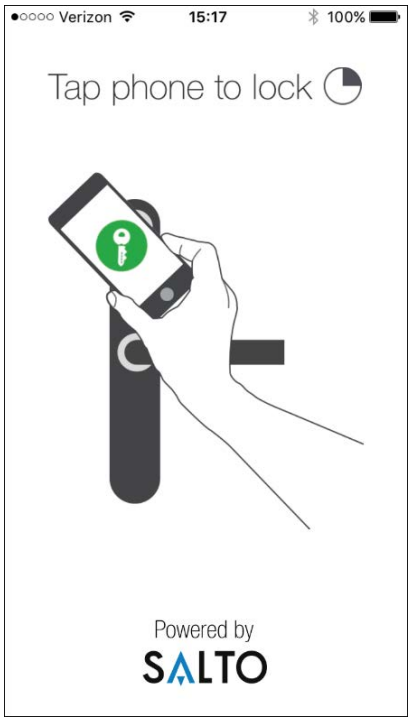


Figure 148: Mobile opening screen

NOTE: Make sure Bluetooth is activated on the mobile phone. A message will appear if Bluetooth has not beed activated.

8. 12. 2. Adding Check-In Information

The check-in information options are described in the following table.

Table 31: Check-in information options

Option	Description
Start date	Date on which the guest checks in to the hotel
Number of nights	Number of nights the guest is staying
Date of expiry	Date on which the key expires and the key is no longer valid. This automatically updates when the number of nights is entered.
Start date time	Time when the key becomes valid. The **Start date time** field is displayed when the **Rooms activation time** drop-down list is enabled on the **Hotel** tab in ProAccess SPACE General options. The default start time is 16.00. If required, you can amend this by changing the value in the **Rooms activation time** drop-down list. See *Hotel Tab* for more information.
Date of expiry time	Latest check-out time. After this time, the key is no longer valid. The default expiry time is 12.00. If required, you can change the default expiry time by amending the value in the **Room expiration time** field in **System** > **General options** > **Hotel** in ProAccess SPACE. See *Hotel Tab* for more information.

Option	Description
Number of nights	Pre-set amount of check-in days for the guest stay. According to the guest arrival day various options will be shown: • Weekend: from Friday to Sunday, • Week: from Monday to Sunday, • Midweek: from Monday to Friday. By selecting one of these options you will automatically set the departure date. To activate this option, you must select the **Enable predefined packages at check-in checkbox** in **System** > **General options** > **Hotel**. See *Hotel Tab* for more information.
General Purpose Field	You can have up to 5 General Purpose Fields for guests. In the general purpose field you can add information related with the guest such as his car tag, an ID number or a zip code for example. See the *Hotel Tab* in **General options** for more information. This information can also be added into *key tracks* if required. See Tracks of guest keys in **General options** > *Hotel Tab* for more information.

8. 12. 3. Changing Stay Duration

After arrival, a guest may decide to extend or shorten the duration of his stay.

To change the stay duration or a guest who is already checked-in, perform the following steps:

1. Select **Hotel** > **Room status**. The **Room status** information screen is displayed.

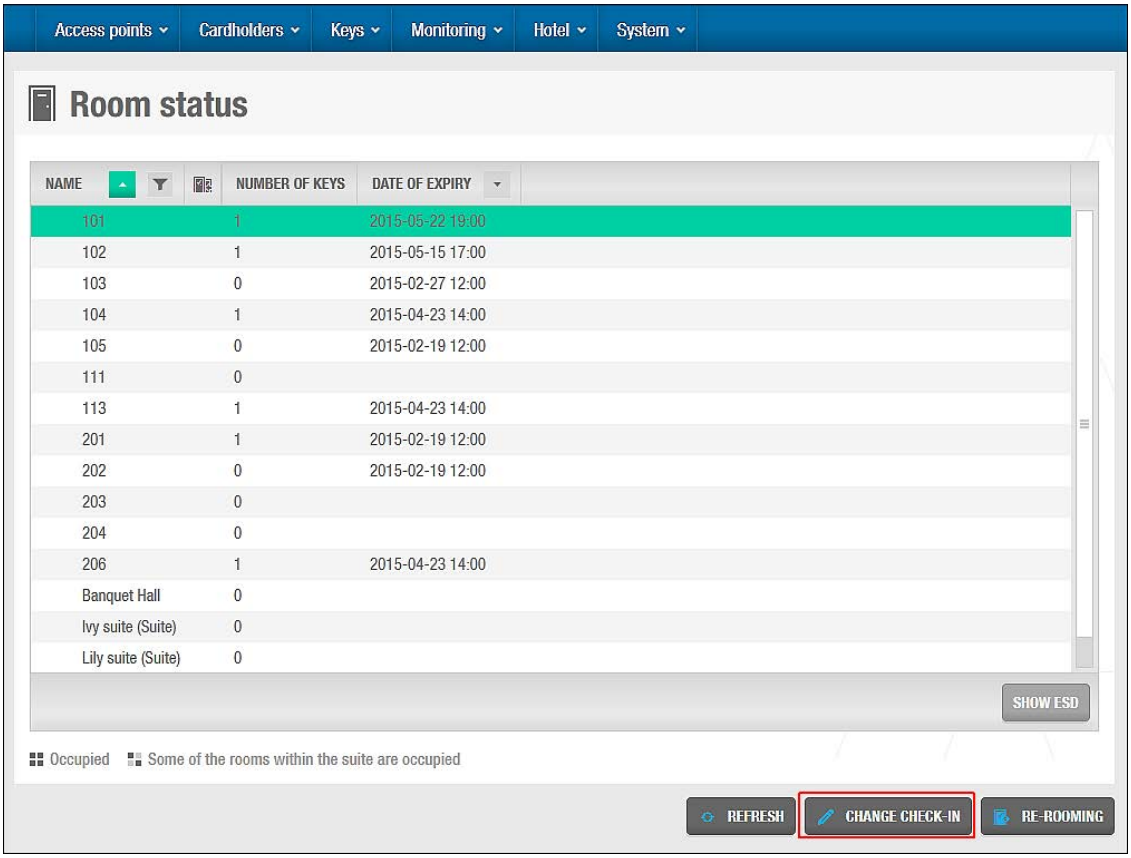


Figure 149: Room status information screen

2. Select the room for which you want to change the stay duration.

3. Click **Change Check-In**. The **Hotel check-in** information screen is displayed.

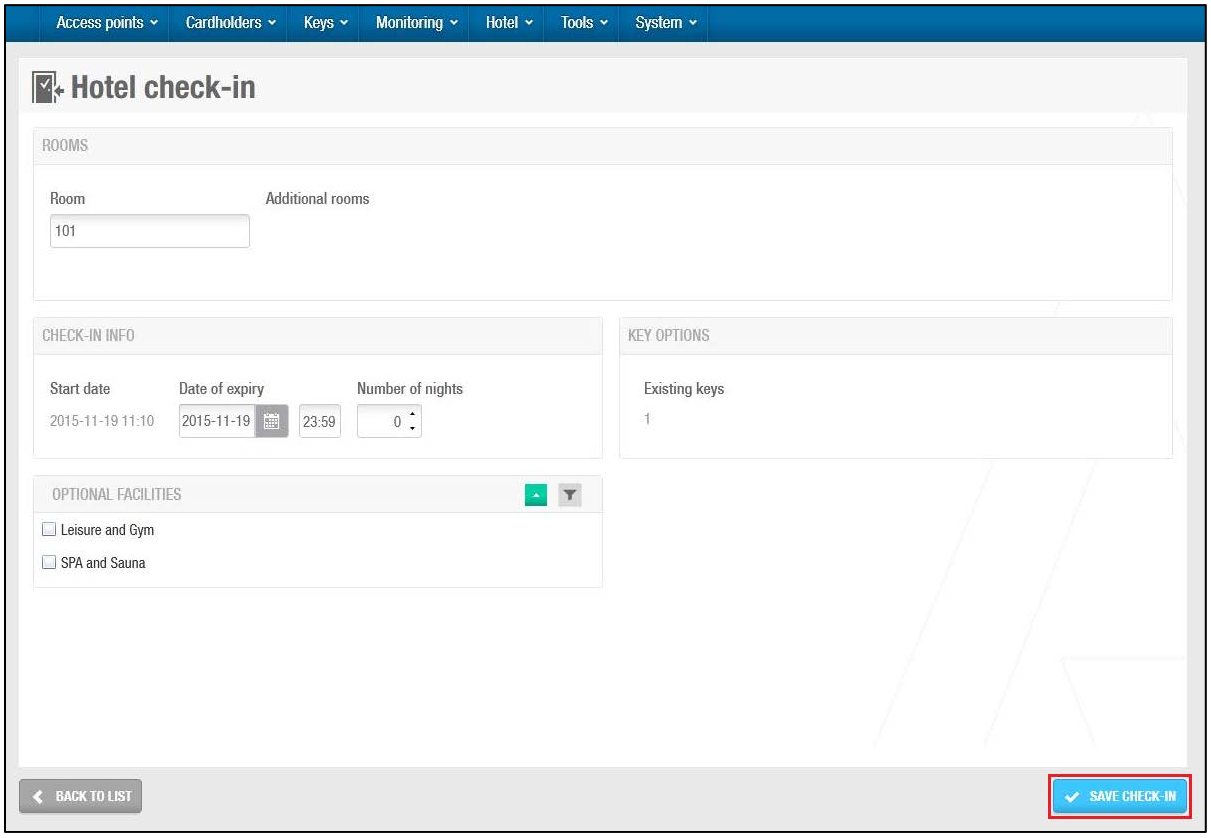


Figure 150: Hotel check-in information screen

4. Select the required number of nights by using the up and down arrows or, alternatively, type the number in the **Number of nights** field.

   The **Date of expiry** field updates automatically.

5. Click **Save Check-In**. The stay duration is changed.

NOTE: The new check-in data is sent automatically to RF doors so that the guest is granted access until the new check-out date. The guest's key is automatically updated when they present it to an SVN wall reader. The new check-in data is not sent to non-RF doors automatically. Instead, the key must be updated at an SVN wall reader or at an encoder in reception.

To allow guest key updates, you must enable this functionality in ProAccess SPACE General options. This is done by selecting the **Enable guest keys update** checkbox in **System** > **General options** > **Hotel**. See *Hotel Tab* for more information.

8. 13. Guest Check-Out

All guests should be checked out when they complete their stay and depart the hotel.

To check out a guest, perform the following steps:

1. Select **Hotel** > **Check-out**. The **Hotel check-out** dialog box is displayed.

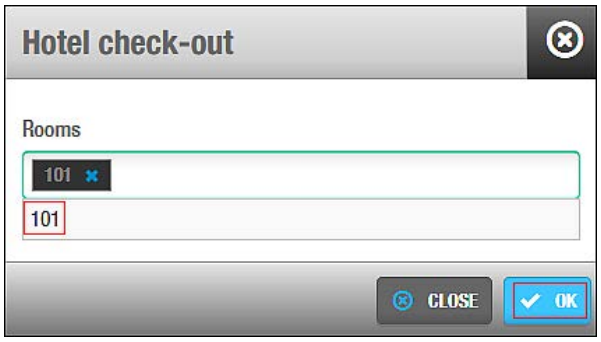


Figure 151: Hotel check-out dialog box

2. Type the room from which the guest is checking out.

   You can also press F2 to display the **Select rooms** dialog box and select a room from the list.
3. Click **OK**. A pop-up is displayed informing you that the check-out was completed.
4. Click **OK** again. The guest is now checked out.

NOTE: When you check out a guest, the check-in list is updated. However, this does not invalidate the key. The key remains valid until it reaches its expiration date or a new check-in is performed. When the new guest uses their key to access the room, this invalidates the previous key.

8. 14. Group Check-In

Group check-in is a feature that is generally performed by the front-desk operator. A group check-in can be done in advance of the arrival of a large group so as to avoid long check-in wait times when the group does arrive to the hotel.

A group check-in is performed as follows:

1. **Group check-in information is entered**

   The hotel operator enters the group check-in information.
2. **Pre-edit guest key information is added**

   The key is pre-edited and the room is reserved for the arrival date. The hotel operator adds the pre-edit guest key information using the key encoder.

NOTE: A new guest can occupy the reserved rooms before the group arrives. This does not affect the encoded keys for the group.

3. **Group is checked in**

   The hotel operator checks in the group when they arrive at the hotel.

8. 14. 1. Entering Group Check-In Information

Hotel operators such as reservation staff can enter the group check-in information at the time of booking.

To enter the group check-in information, perform the following steps:

1. Select **Hotel** > **Check-in groups**. The **Check-in groups** screen is displayed.

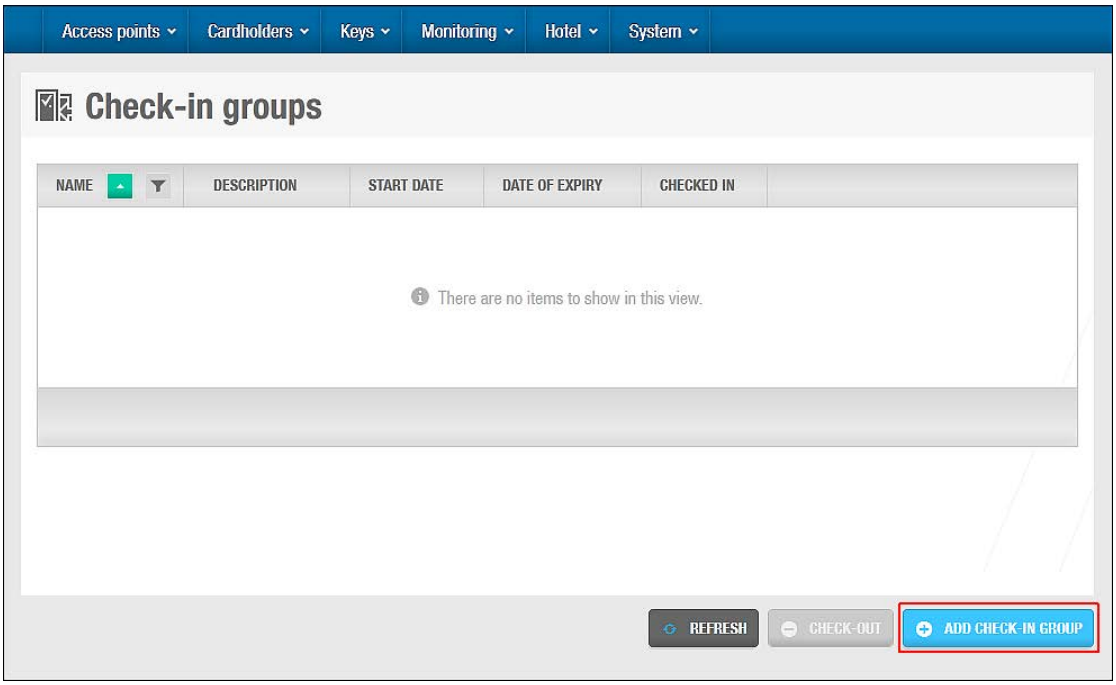


Figure 152: Check-in groups screen

2. Click **Add Check-In Group**. The **Check-in group** information screen is displayed.

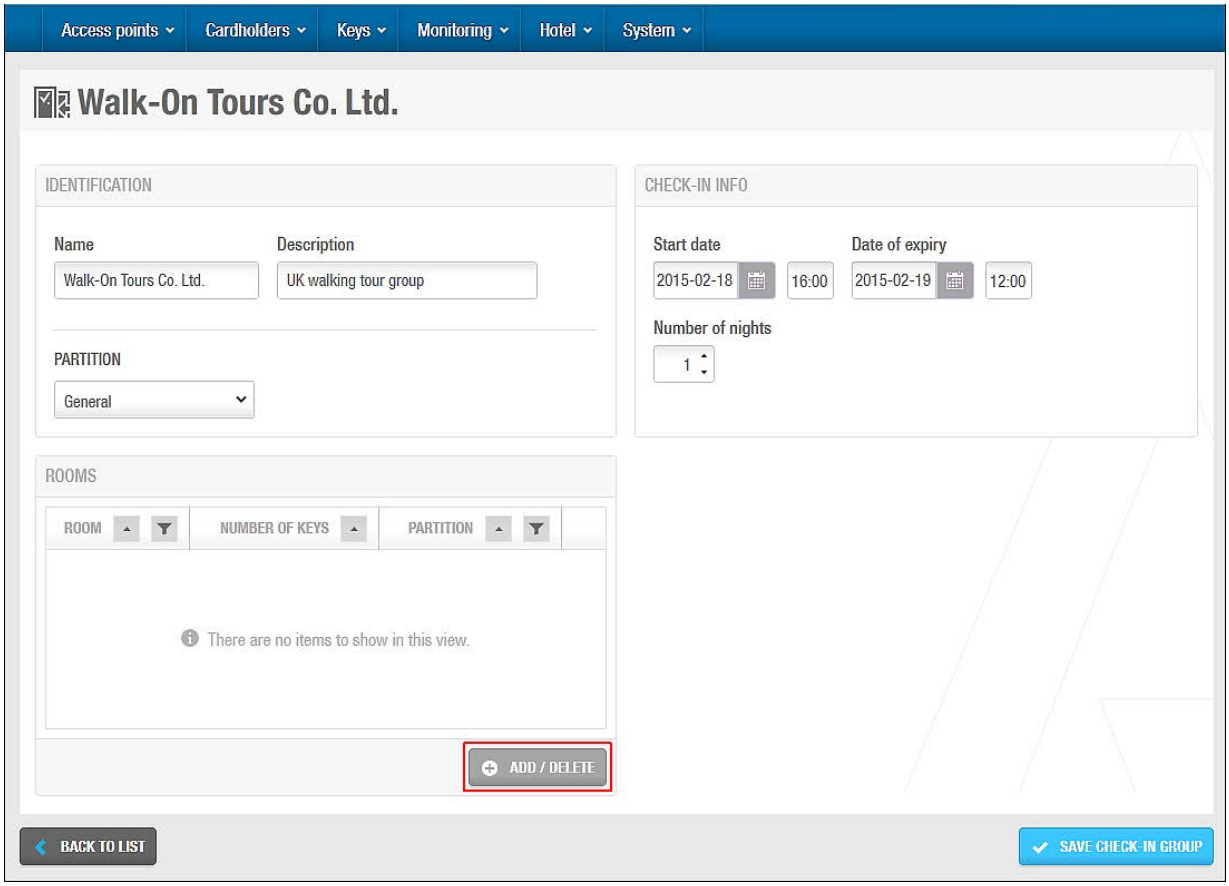


Figure 153: Check-in group information screen

3. Type the name of the group in the **Name** field.
4. Type a description of the group in the **Description** field.

5. Select the applicable check-in information in the **Check-In Info** panel.
   The check-in information fields are described in *Adding Check-In Information*.
6. Select the appropriate partition from the **Partition** drop-down list if required.
   See *Partitions* for more information about partitions.
7. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of room names, is displayed.
8. Select the available rooms from the left-hand panel and click the chevron. The selected rooms are now displayed in the right-hand panel.
   You can hold down the Ctrl key while clicking the rooms to make multiple selections.
9. Click **Accept**. The selected rooms are displayed in the **Check-in groups** information screen.

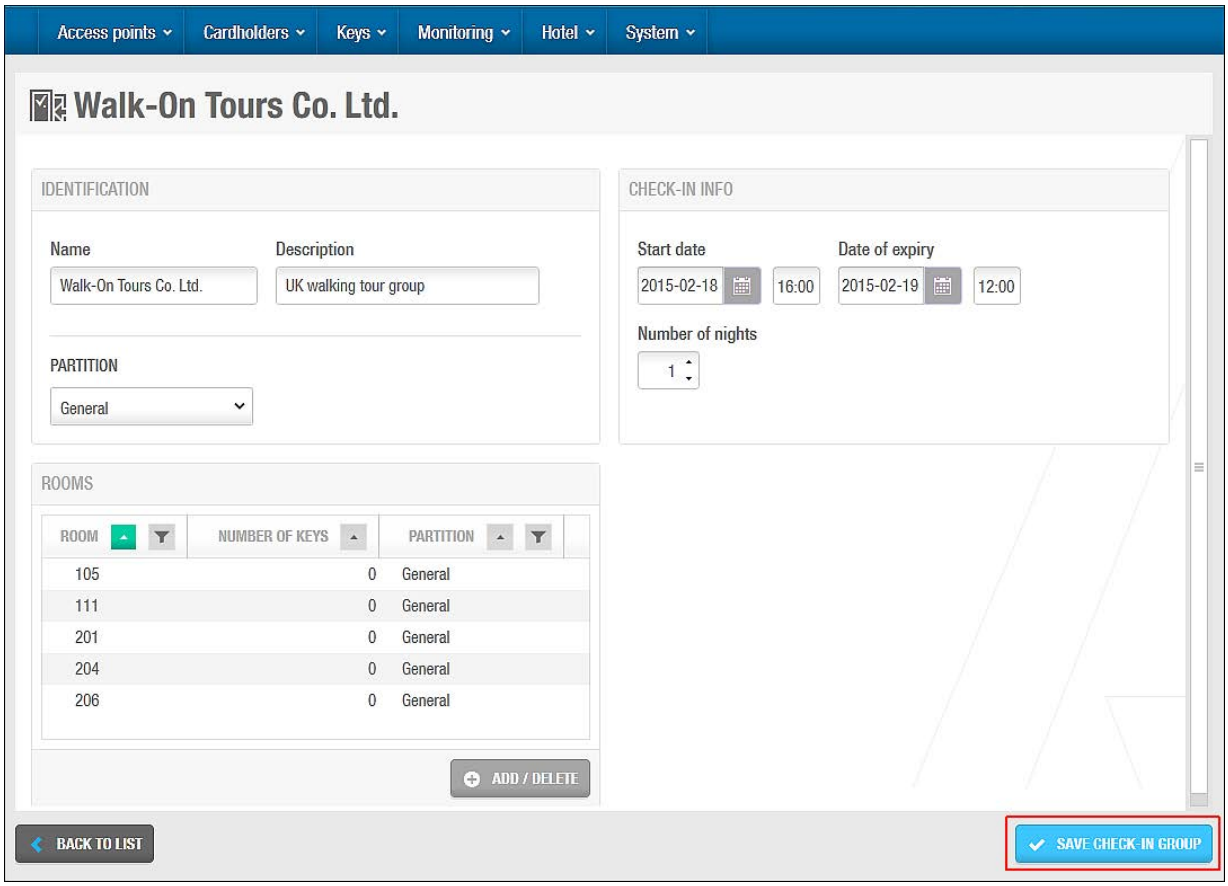


Figure 154: Check-in group information screen

10. Click **Save Check-In Group**. The group check-in information is saved.

8. 14. 1. 1. Check-In Group Icons

When you add check-in groups to the system, different icons are displayed in the **Checked In** column on the **Check-in groups** screen. These icons vary depending on the status of each group and are described in the following table.

Table 32: Check-in group icons

Icon	Description
 Checked in	Indicates that a group has been checked in
 Check-in pending	Indicates that a group needs to be checked in

8. 14. 2. Pre-Editing Guest Keys

You must pre-edit guest keys before performing a group check-in. This allows you to assign the number of keys per room and encode the keys in advance of the group arriving which speeds up the check-in process when a big group arrives.

To pre-edit guest keys, perform the following steps:

1. Select **Hotel** > **Check-in groups**. The **Check-in groups** screen is displayed.

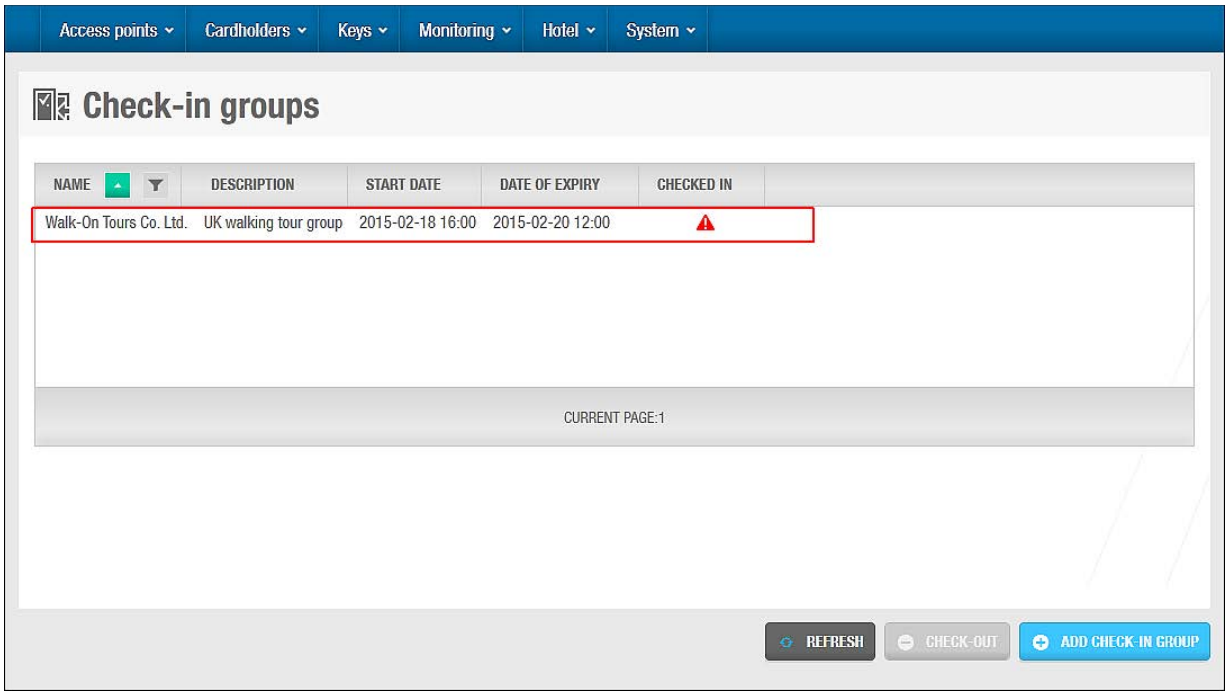


Figure 155: Check-in groups screen

2. Double-click the check-in group. The **Check-in group** information screen is displayed.

   The **Rooms with Pre-Edited Keys** information field (shown in grey at the top of the **Check-in group** information screen) displays how many rooms have had pre-edited keys added.

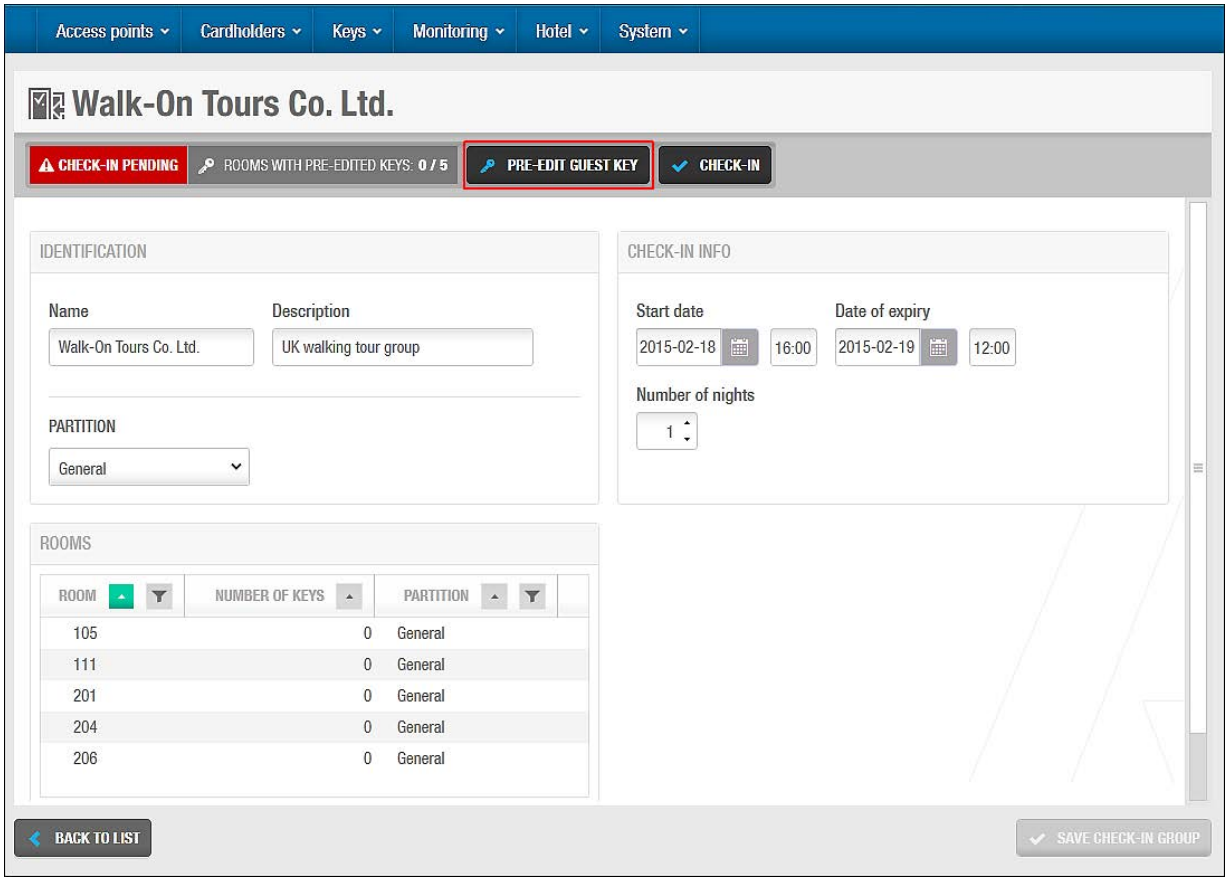


Figure 156: Check-in group information screen

3. Click **Pre-Edit Guest Key**. The **Guest Key pre-edition** dialog box is displayed.

Figure 157: Guest key pre-edition dialog box

4. Select the room in the **Room** drop-down list.
5. Select the number of keys in the **Number of keys** drop-down list.
6. Click **Edit Key**. A pop-up is displayed asking you to place the key on the encoder.
7. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming that the operation was successful.

   If you have selected more than one key in the **Number of keys** field, a pop-up is displayed asking you to place the next key on the encoder and click **Accept**. You must do this for each required key.
8. Remove the key and click **OK**.
9. Repeat the process for each room.

8. 14. 3. Performing a Group Check-In

To check in a group, perform the following steps:

1. Select **Hotel** > **Check-in group**. A list of check-in groups is displayed.
2. Double-click the check-in group. The **Check-in group** information screen is displayed.

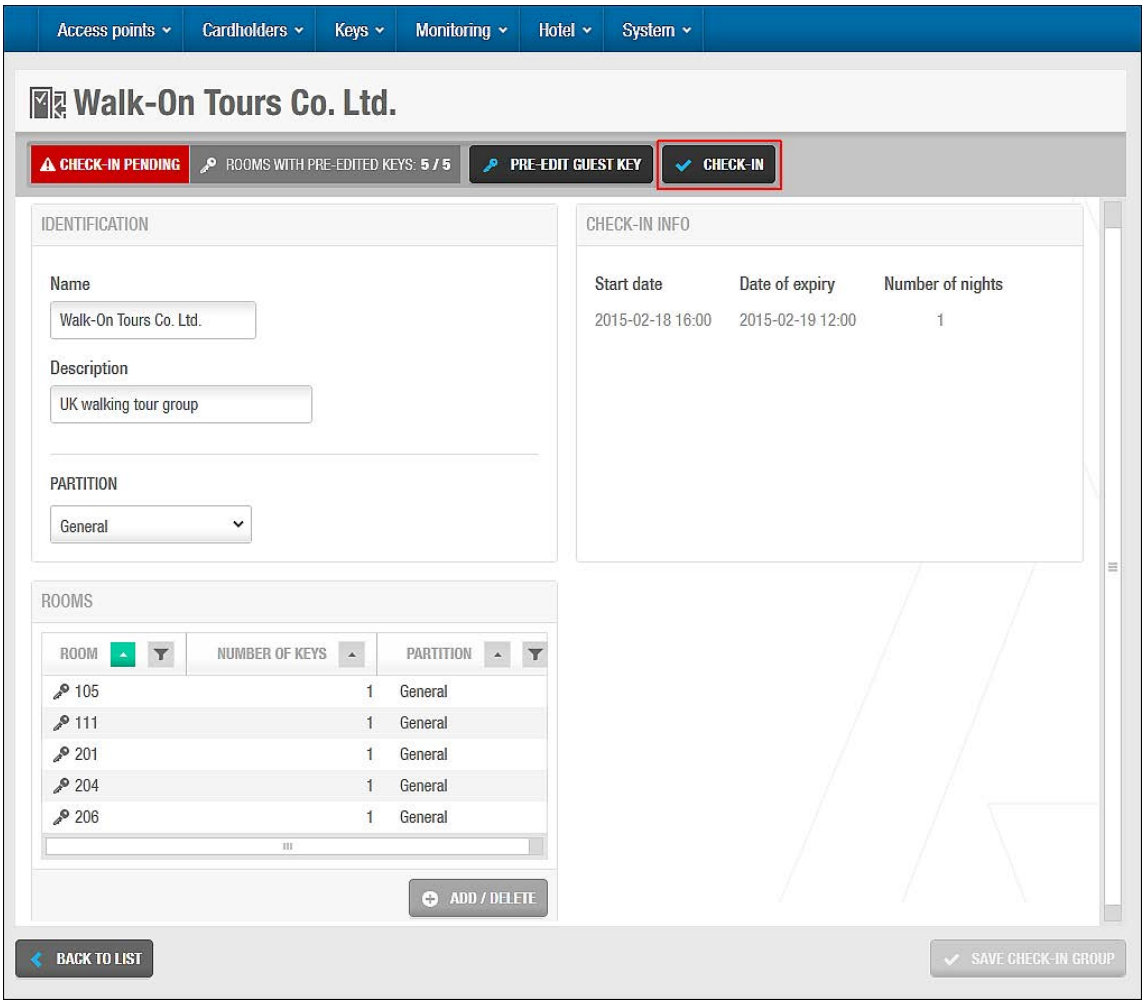


Figure 158: Check-in group information screen

3. Click **Check-In**. The group is checked in.

   This operation is important as it informs the system that the group has arrived.

NOTE: You must pre-edit guest keys before performing a group check-in. See *Pre-Editing Guest Keys* for more information about pre-editing guest keys.

8. 15. Group Check-Out

A group check-out is generally performed by the front-desk operator. Groups must be checked out after departure to make the rooms available in the system and delete the group.

To check out a group, perform the following steps:

1. Select **Hotel** > **Check-in groups**. A list of check-in groups is displayed.

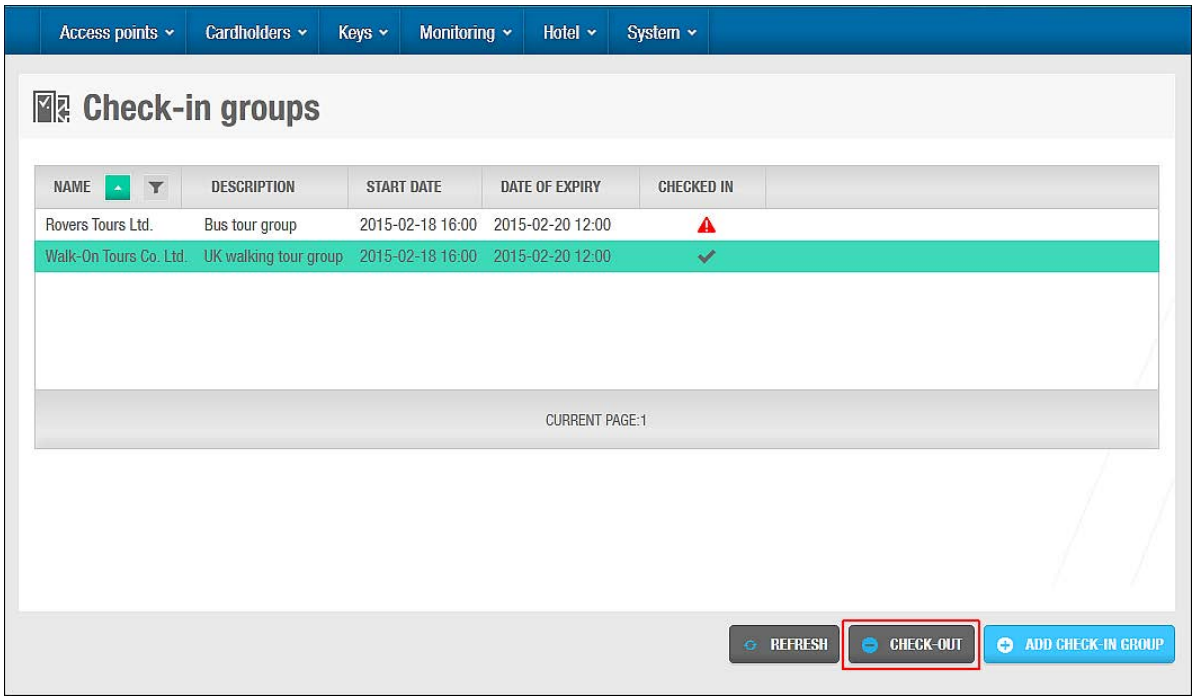


Figure 159: Check-in groups screen

2. Select the group that you want to check out.
3. Click **Check-Out**. A pop-up is displayed asking you to confirm that you want to check out the selected group.

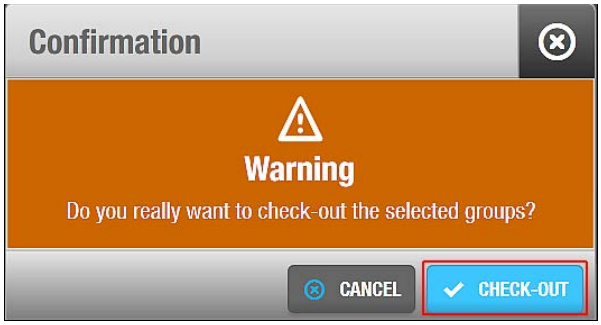


Figure 160: Check-out group confirmation pop-up

4. Click **Check-Out**. The group is now checked out.

8. 16. Managing Guest Lists

When you create rooms and suites, guest profiles are automatically added to the **Guests** information screen. These profiles show system-generated names that associate the guest with their room and check-in group (rather than individual guest names). Each profile corresponds to the name of a particular room or suite, for example, @104 or @Ivy suite. It also shows a check-in group name, for example, &101 or &Ivy suite. This allows you to view a list of guests, configure guest profiles, and associate guests with guest access levels.

8. 16. 1. Viewing Guest Lists

You can view a list of guests by selecting **Cardholders** > **Guests**. Note that you can access the most up to date list by clicking **Refresh**.

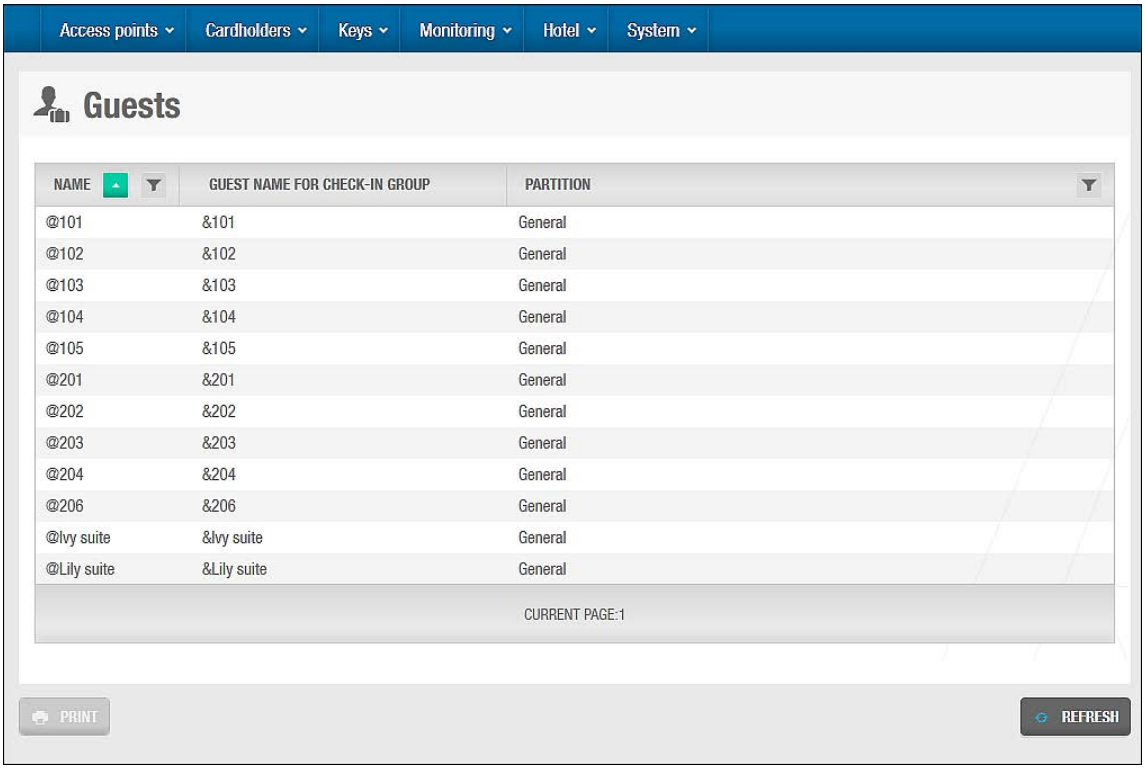


Figure 161: Guests screen

8. 16. 2. Configuring Guests

You can add specific information to guest profiles and enable extended door opening times.

8. 16. 2. 1. Adding Additional Information

By default, the **Guest** information screen only displays the guest name, the guest name for check-in groups, the partition (if enabled in the installation's license options), and the extended opening time option.

However, if required, you can also activate up to five general purpose fields on the **Guest** information screen. To activate a general purpose field, you must select an **Enable field** checkbox in **System** > **General options** > **Hotel**. You can then name the field in accordance with the information that you want to capture, for example, special requirements. See *Hotel Tab* for more information.

8. 16. 2. 2. Enabling Extended Door Opening Times

To enable an extended door opening time for a guest, perform the following steps:

1. Select **Cardholders** > **Guests**. The **Guests** screen is displayed.
2. Double-click the name of the relevant guest. The **Guest** information screen is displayed.

   You can also access the **Guest** information screen by clicking **Show Guest** on the **Room** or **Suite** information screen.

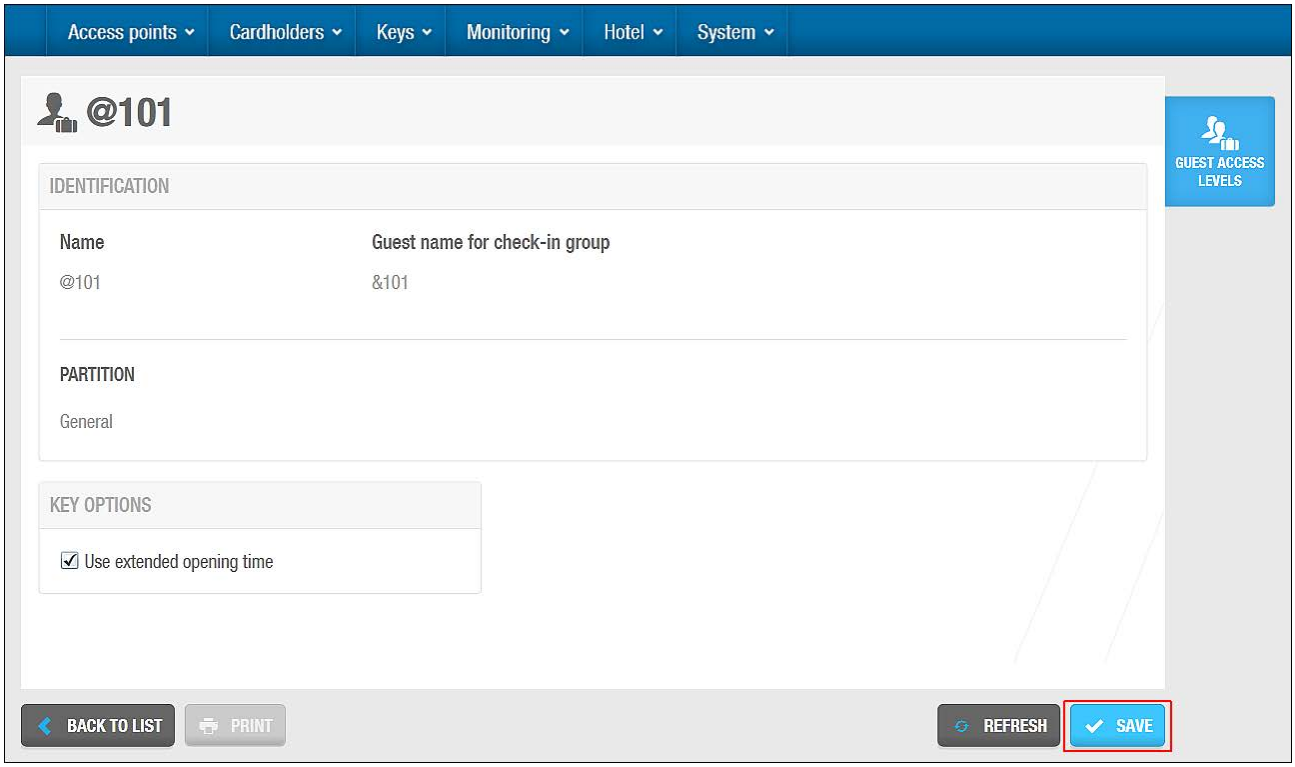


Figure 162: Guest information screen

3. Select the **Use extended opening time** checkbox.
4. Click **Save**.

NOTE: You must set the value of the extended door opening time in the **Increased open time** field on the **Room** information screen.

8. 16. 3. Associating Guests

Guest access levels are associated with access points. See *Guest Access Levels* for more information. In order for the guest to use those access points, their guest profile must be associated with a guest access level.

8. 16. 3. 1. Guest Access Levels

To associate a guest access level with a guest, perform the following steps:

1. Select **Cardholders** > **Guests**. The **Guests** screen is displayed.
2. Double-click the guest that you want to associate with a guest access level. The **Guest** information screen is displayed.
3. Click **Guest Access Levels** in the sidebar. The **Guest access levels** dialog box is displayed.

   Note that the dialog box will be blank because you have not yet associated a guest access level.
4. Click **Add/Delete**. The **Add/Delete** dialog box, showing a list of guest access levels, is displayed.
5. Select the required guest access level in the left-hand panel and click the chevron. The selected guest access level is displayed in the right-hand panel.
6. Click **Accept**. The guest is now associated with the guest access level.

8. 17. Re-Rooming

The re-rooming functionality allows the hotel operator to assign a different room to a guest without the guest having to return to the front desk. For example, a guest arrives to his room but doesn't like the view and then calls the reception desk to ask for a room change. The front-desk operator can use the re-rooming function to assign the guest to a new room without the guest having to go to reception for a new room key.

The following sections describe how to re-room a guest.

NOTE: The new check-in data is sent automatically to RF doors, and the new access information is automatically transferred to the guest's key when they present it to an SVN wall reader. In the case of non-RF doors, the key must be updated at an SVN wall reader or at an encoder in reception. To allow guest key updates, you must enable this functionality in ProAccess SPACE General options. See *Changing Stay Duration* for more information about this process.

8. 17. 1. Re-Rooming Guests

To re-room a guest, perform the following steps:

1. Select **Hotel** > **Room status**. The **Room status** information screen is displayed.

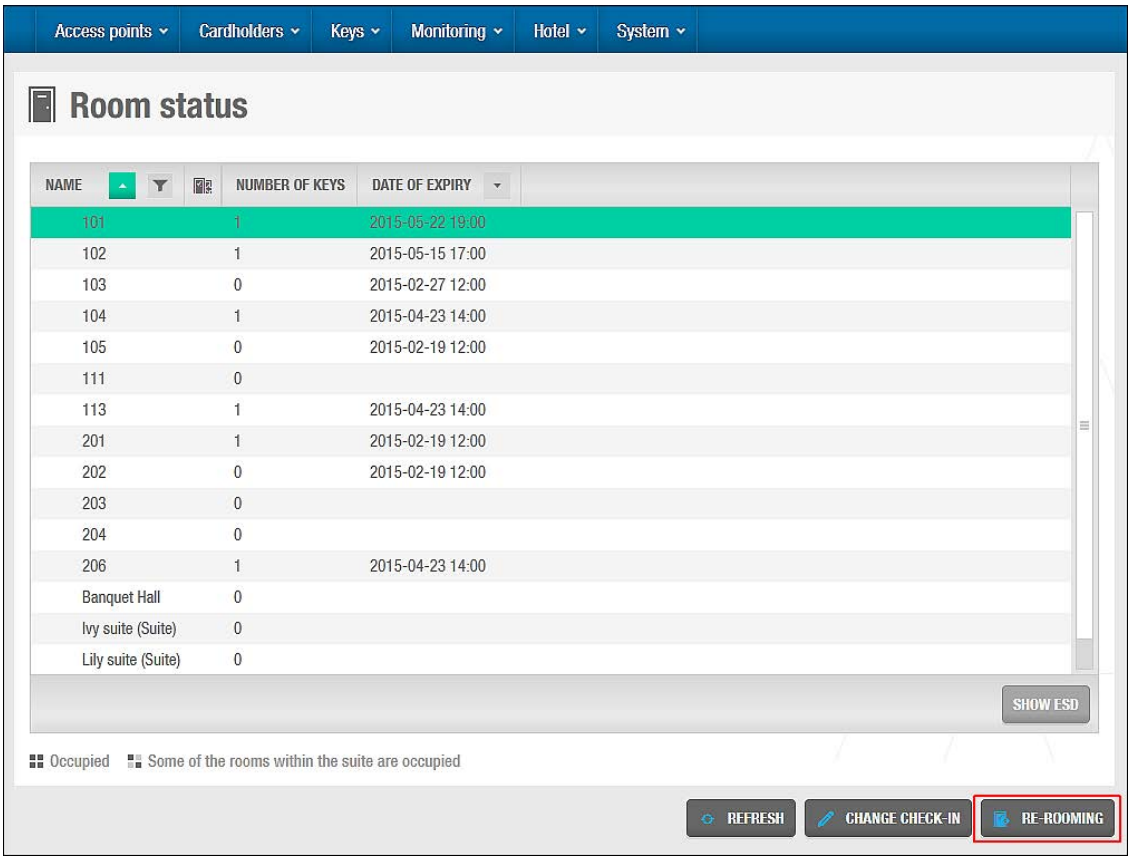


Figure 163: Room status information screen

2. Select the room in which the guest is currently staying.
3. Click **Re-Rooming**. The **Re-rooming** dialog box is displayed.

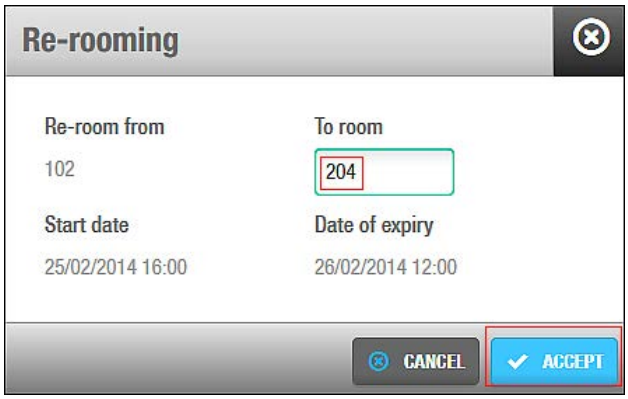


Figure 164: Re-rooming dialog box

4. Type the room to which you want to re-room the guest in the **To room** field.
5. Click **Accept**. A pop-up is displayed informing you that the re-rooming was successful.
6. Click **OK**. The guest's key is now valid for the new room and can no longer be used to access their previous room.

9. KEYS

This chapter contains the following sections:

9. 1. About Keys

In the SALTO system, a key (also known as a carrier) controls access to an area, building, and/or site asset (for example, a cupboard or locker). SALTO keys are encoded with the access data that controls who can enter, as well as when and where they can enter. This is why the technology is called SALTO data-on-card. See *SALTO Data-on-Card* for more information. For example, all staff can be given access to a company's main building entrance but access to certain internal areas can be restricted to specific members of staff and to specific times.

This chapter describes the various types of keys that can be used with the SALTO system. It also describes how to assign, read, delete, update, and cancel user keys.

NOTE: You must install the Local IO Bridge to use a USB encoder when assigning, reading, deleting, and updating keys. See *Local IO Bridge* for more information about the Local IO Bridge.

9. 1. 1. About Key Configuration

You must perform certain configuration tasks for keys in ProAccess SPACE General options.

You can use the **Users** tab to do the following:

- Enable or amend options for user keys
- Configure tracks content
- Configure Wiegand codes

See Users Tab for more information.

You can use the **Hotel** tab to do the following:

- Enable or amend options for guest keys
- Configure tracks content

See Hotel Tab ***Error! Reference source not found.*** for more information.

You can use the **Visitors** tab to do the following:

- Enable options for visitor keys

- Amend options for visitor keys

See *Visitors Tab* for more information.

You can also select particular key configuration settings on the **Access points** and **Users** tabs. See *Access Points Tab* and *User Tab* for more information.

9. 1. 2. Types of Keys

Key is a generic term in the SALTO system as keys are available in a wide range of formats, for example, bracelets, fobs, or keycards. These formats are described in the following table.

Table 33: Key types

Key Type	Description
Keycard	Access data is stored on a credit-card sized plastic card.
Bracelet	Access data is stored on a bracelet worn on the wrist.
Fob	Access data is stored on a small device that can be attached to a key ring.
Watch	Access data is stored on a watch-type device worn on the wrist. This device is similar to a bracelet.
Sticker	Access data is stored on a sticker. Stickers can, for example, be used for access to and from shared car parks.

9. 1. 3. Key Status Icons

Different icons are displayed in the **Key status** column on the **Users** screen when keys have been assigned to users. These icons vary depending on the status of keys. The key status is also shown on the **User** information screen. See *Assigning User Keys* for more information about assigning keys to users.

The icons are described in the following table.

Table 34: Key status icons

Icon	Description
 No update required	Indicates that a key has been assigned to a user and no updates are required
 Key expired	Indicates that a user's key has expired. This icon is displayed when the long-term expiration date of a user's data and access permissions has passed. In this case, the user must update their key by presenting it to an SVN wall reader. Alternatively, an encoder can be used to update it. See *User and Key Expiration* for more information.
 Re-edition required	Indicates that a user's key needs to be re-edited using an encoder. This icon is displayed if you make changes that affect the structure of the key. Such changes include system edits or amendments to the user's profile. For example, the icon is displayed if you select the antipasspack option for a user. See *Enabling Anti-passback* for more information. Note that the lights displayed by SVN wall readers indicate whether keys need to be re-edited. For example, when you present IButton and proximity cards to an SVN wall reader, a flashing blue light is displayed when they are being updated, and a green or red light is displayed when the door is opened or closed respectively. If the light changes to a solid blue light, the key needs to be re-edited. For

Icon	Description
	smart cards, a solid orange light is displayed to indicate that they need to be re-edited.
 Update required	Indicates that a user's key needs to be updated at an SVN wall reader or on an encoder. This icon is displayed if you make changes to a user's access data. It is also shown if a user's key is due to expire within a period of seven to fifteen days and needs to be revalidated. This depends on when the key was edited. If the key was edited between seven to fifteen days ago, the system recommends an update seven days before its expiration date. If it was edited more than fifteen days ago, the system recommends an update 15 days before the expiration date. Note that if you encode keys for a period of less than seven days, the icon is not displayed.

9. 2. Reading Keys

In the case of keys that are found and the owner is unknown, you can read the key details by placing the key on the encoder.

To read a key, perform the following steps:

1. Select **Keys** > **Read key**. A pop-up is displayed asking you to place the key on the encoder.
2. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed showing the key data – for example, the owner, expiry date, and the key access points. If you have enabled and configured specific tracks for keys, this information is also shown with other relevant technical data. See *Configuring Tracks* for more information about tracks.

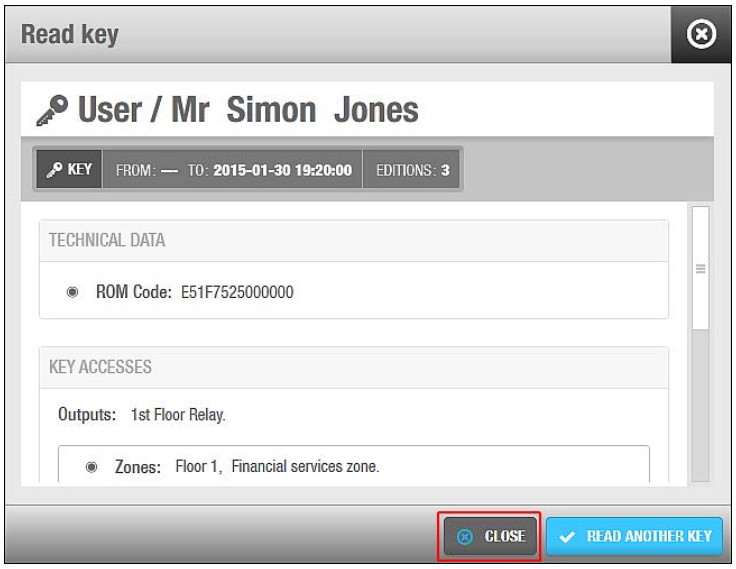


Figure 165: Read key pop-up

3. Click **Close**.

You can click **Read Another Key** if you want to continue reading keys.

9. 3. Assigning User Keys

Keys assigned to users are encoded with the access information relevant to the specific user. For this reason, you must set up and configure user profiles before assigning keys to these users. See *Users* for more information.

When you assign a key to a user, the **Update Key** and **Cancel Key** buttons are added to the **User** information screen, and you can use them to update or cancel the assigned key. See *Updating Keys* and *Cancelling Keys* for more information. The period for which the key is valid is displayed in the **Valid Until** information field. The key status is also shown. For example, you can see if a key update is required or if the key has expired.

NOTE: The status of keys is also displayed in the **Key status** column on the **Users** screen. See *Key Status Icons* for more information. The period for which keys are valid is also displayed in the **Key Expiration** column on the **Users** screen.

9. 3. 1. Assigning a user key

To assign user keys, perform the following steps:

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

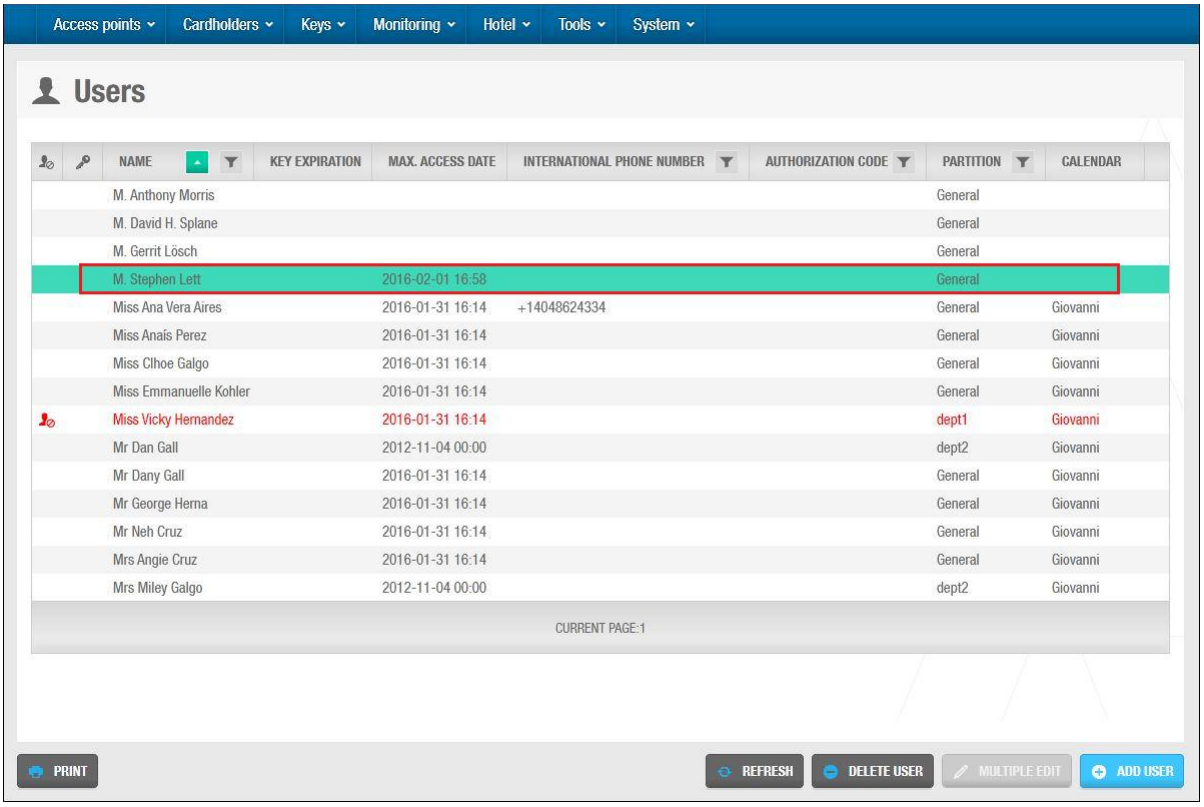


Figure 166: Users screen

2. Double-click the name of the user to whom you want to assign a key. The **User** information screen is displayed.

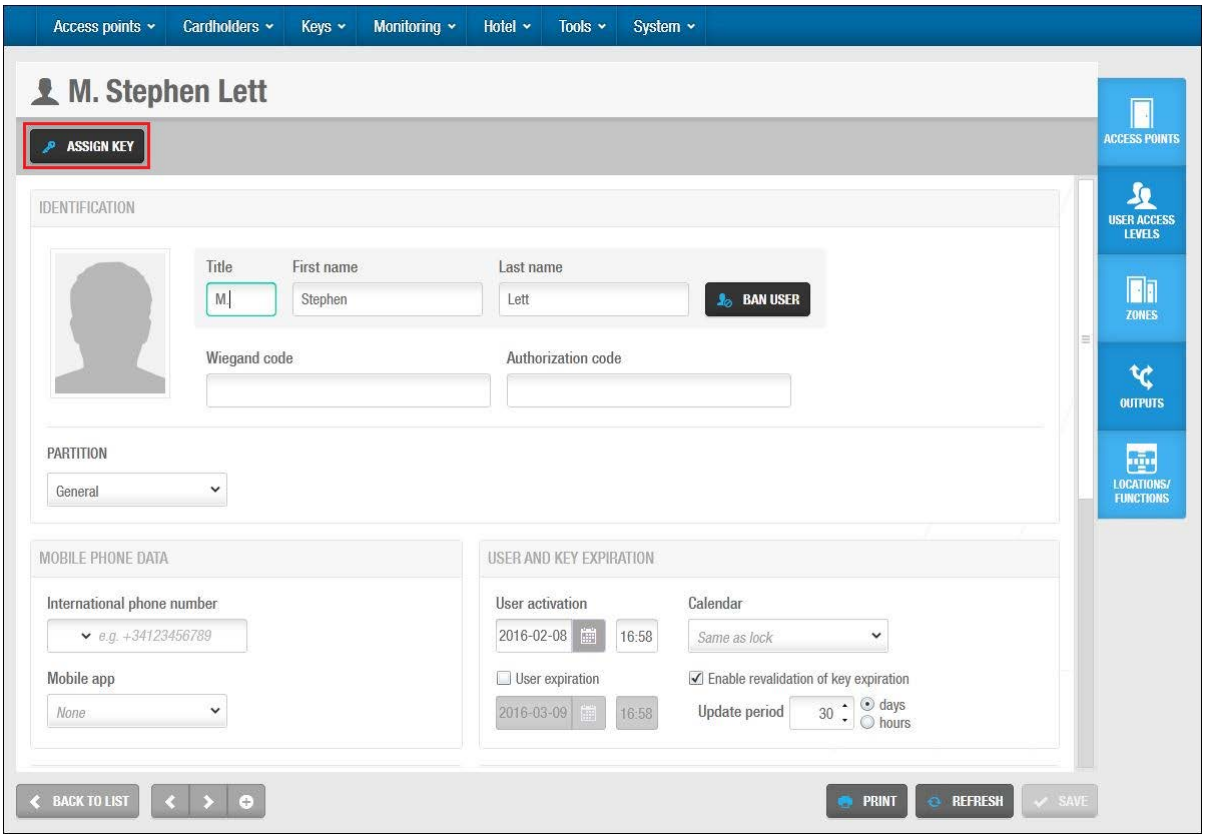


Figure 167: User information screen

3. Click **Assign Key**. The **Assign key** dialog box is displayed.

   The start date and date of expiry of the key are displayed in this dialog box.

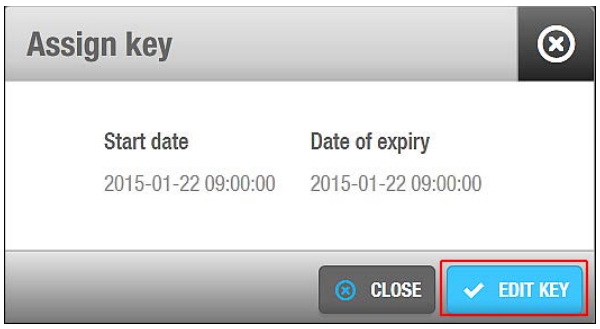


Figure 168: Assign key dialog box

4. Click **Edit Key**. A pop-up is displayed asking you to place the key on the encoder.
5. Place the key on the encoder when the LED light begins to flash. The user access information is transferred to the key. A pop-up is displayed confirming that the operation was successful.
6. Remove the key and click **OK**.

9. 3. 2. Assigning a user key for JustIN mSVN application

The **JustIN mSVN** mobile application is used to update existing user keys using **NFC** (Near Field Communication). Only **Android** phones are compatible with this feature at the moment. The cards can only be Desfire Evolution 1 and have to be formatted with specific requirements in order to be updatable by the **JustIN mSVN** application.

When **JustIN Mobile** application is downloaded, follow your phone instructions for registration.

To format the Desfire key perform the following steps;

1. Go to **System** > **SAM & Issuing options**. In **Active keys**, select **Desfire,** click the pencil. See *Configuring Desfire keys settings* for more information about SAMing Desfire cards. **SAM & Issuing options** functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.
2. Click the **Read SAM card** button to read the SALTO SAM key (SALTO Application Media). The SAM keys will be represented by dots and won't be shown for security reasons.
3. Ensure the emission type is **AES**.
4. Ensure **Updateable by NFC** is checked.
5. Click **Save**.

Once the SAM keys are in the system, you can now assign the card to the user.

1. Go to **Cardholders** > **User**. In Mobile phone data, type the phone number in the **International phone number** field. Click on the down arrow and select the country the mobile phone line is from. Alternatively, you can type the sign **+**, the country code and then the phone number.
2. In mobile app, select **JustIN mSVN** from the dropdown menu. **JustIN mSVN** must be selected before the key is assigned. If the user key was assigned before, you have to **Cancel key** and re-assign after selecting **JustIN mSVN**. See *Cancelling keys* for more information about how to cancel a user key.

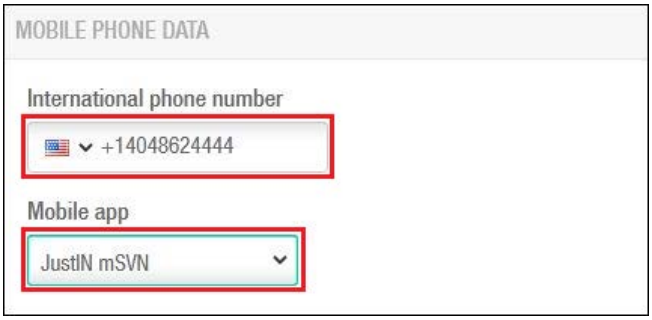


Figure 169: JustIN mSVN selection dialog box

3. Make sure the key expiration is 7 days or less. The system won't allow a key expiration higher than 7 days.

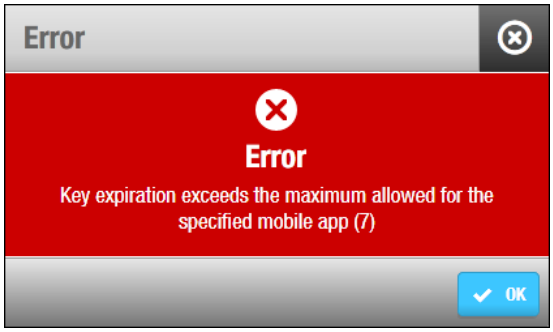


Figure 170: JustIN mSVN key expiration dialog box

4. **Assign** the user key. See *Assigning a user key* for more information.
5. The system will send updates directly to the mobile phone. **JustIN mSVN** can then be used to update the user key. Tap the white key on the blue background circle and present the key on the back of the mobile phone.

NOTE: The updates sent over the air (OTA) to your mobile phone have to be encrypted. To do so, a SALTO Ethernet encoder is used as **Dongle**. See *Devices tab* in **System** > **General options** for more information.

The mobile phone has to be online in order to receive the access data information and NFC feature has to be enabled.

9. 3. 3. Assigning a user JustIN Mobile key

In case the user prefers a mobile key instead of a standard one, the data can be sent OTA (Over the air) to the mobile phone.

The locks have to be equipped with **SALTO BLE (Bluetooth Low Energy) readers**.

This feature is license-dependent. This means that the functionality will not be enabled in your SALTO installation unless it is covered by your selected license options.

The SALTO **JustIN Mobile** application must be downloaded from Apple Store for iPhones or Play Store for Android smart phones.

NOTE: The mobile key has some limitations comparing to standard keys. Mobile key do not support data on Tracks, Wiegand application, Free assignment lockers, Antipassback, Last rejection or Audit on key. The readers are not capable to write any data in the mobile key.

When you downloaded the **JustIN Mobile** application, follow your phone instructions for registration.

To assign a mobile key perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.
2. Double-click the name of the user to whom you want to assign a key. The **User** information screen is displayed.
3. Type the phone number in the **International phone number** field. Click on the down arrow and select the country the mobile phone line is from. Alternatively, you can type the sign **+**, the country code and then the phone number.
4. In mobile app, select **JustIN Mobile** from the dropdown menu.

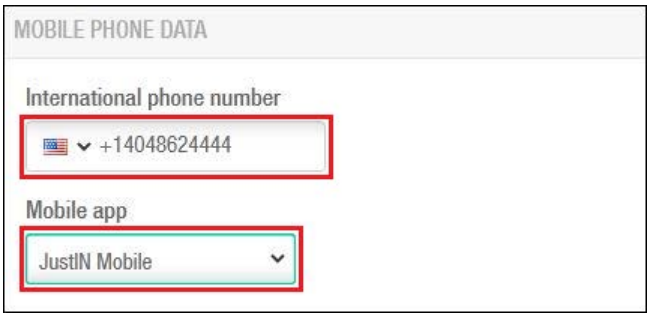


Figure 171: JustIN Mobile selection dialog box

5. Click **Assign key.** The data is sent to the user mobile phone.

NOTE: The data sent over the air (OTA) to your mobile phone has to be encrypted. To do so, a SALTO Ethernet encoder is used as **Dongle**. See *Devices tab* in **System** > **General options** for more information.

The mobile phone has to be online in order to receive the access data information.

6. Tap the white key on the green background circle and present the mobile phone to the lock.

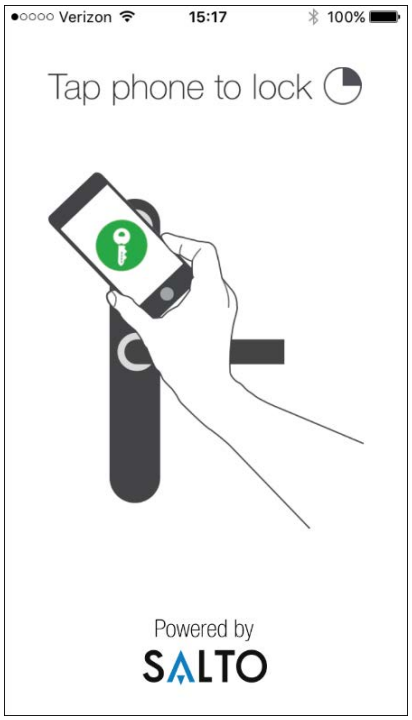


Figure 172: Mobile opening screen

NOTE: Make sure **Bluetooth** is ON in the mobile phone. A message will pop up in case it is not.

9. 3. 4. Cancelling Keys

You can cancel a user's key at any time, for example, if a user loses their key. This means that the key can no longer be used to access the site.

When you cancel a valid user key before it has expired, it is sent to the blacklist by default. See *About Blacklists* for more information. However, keys that are cancelled after they have expired are not sent to the blacklist.

NOTE: You can choose to select if user keys will be sent to the blacklist when cancelled. To activate this option, you must enable the MORE_THAN_64K_USERS advanced parameter in ProAccess SPACE General options. See *Advanced Tab* and *Managing Blacklists* for more information.

To cancel a key, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.
2. Double-click the name of the user whose key you want to cancel. The **User** information screen is displayed.

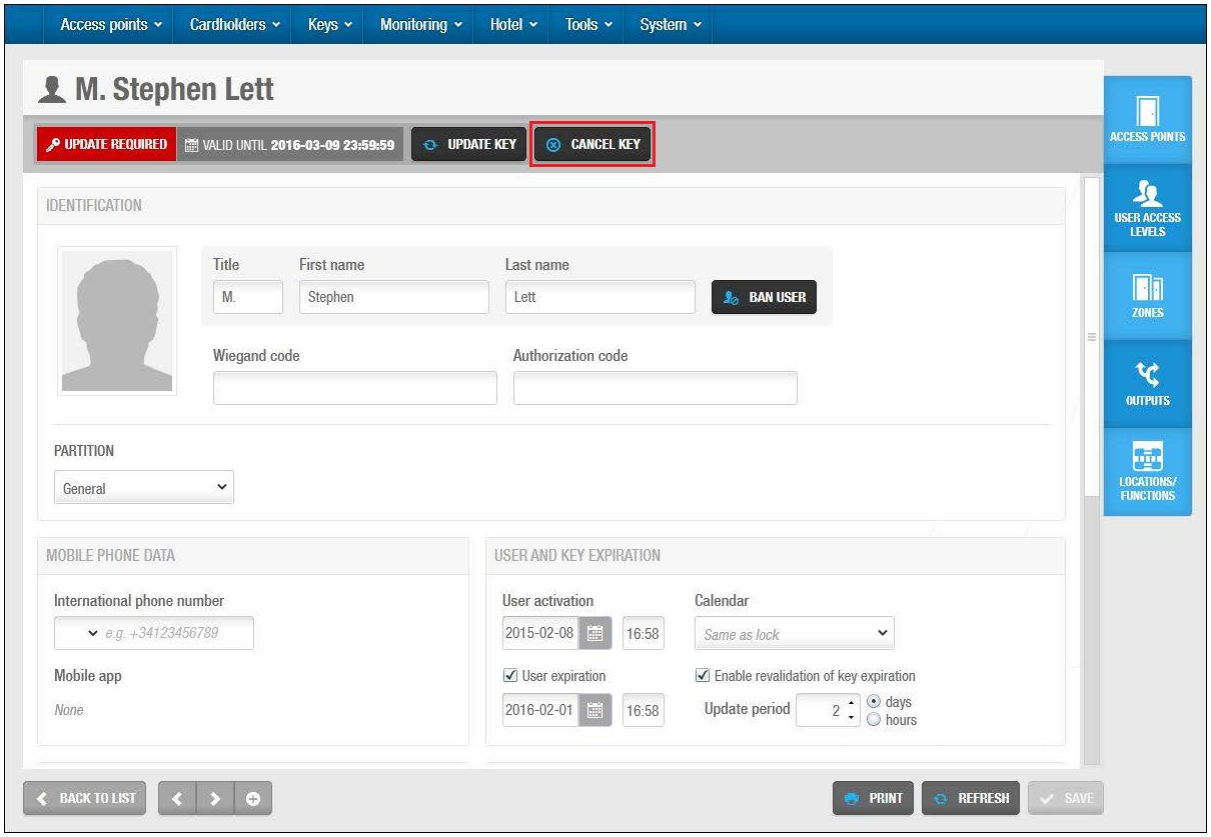


Figure 173: User information screen

3. Click **Cancel Key**. A pop-up is displayed asking you to confirm that you want to cancel the key.

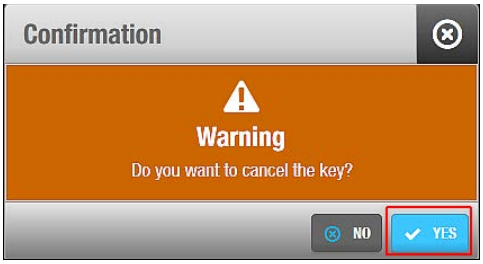


Figure 174: Cancel key confirmation pop-up

Click **Yes**. The key is cancelled.

9. 4. Deleting Keys

You can remove a user's access to a site by deleting all their access data from their key. When all information has been removed from their key, the user may still exist on the system, but they can no longer use their key with any of the access points.

NOTE: When you delete a valid user key, it is sent to the blacklist by default. See *About Blacklists* for more information about blacklists.

To delete a key, perform the following steps:

1. Select **Keys** > **Delete key**. A pop-up is displayed asking you to place the key on the encoder.

2. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming that the operation was successful.
3. Remove the key and click **Close**.

   You can click **Delete Another Key** if you want to continue deleting keys.

9. 5. Reset Locker data

You can reset a user's key in the event that the key becomes corrupted or the key cannot open the user's locker.

To reset the key, perform the following steps:

1. Go to **Keys** > **Reset locker data**. The reset locker data screen is displayed.
2. Present the key to the encoder. The key is now reset and can capture another locker.

9. 6. Updating Keys

Users can update their keys at any SVN wall reader in your site. You can also update user keys using an encoder. Like SVN wall readers, encoders update keys with new access point data. However, only encoders can re-edit keys. This modifies the structure of keys.

When you make changes to access point data, an **Update required** icon is displayed in the **Key status** column on the **Users** screen. In this case, the key can be updated when the user presents it to an SVN wall reader. If the **Re-edition required** icon is displayed, however, this means that an encoder is required to re-edit the key. See *Key Status Icons* for more information.

NOTE: You can configure Ethernet encoders to update keys automatically when users present their keys to them. In this case, the encoders run continuously but can only be used to update keys and modify their structure. They cannot be used to encode keys with access data. These encoders are usually located in areas of a site where there is no reception desk. Users can update their keys at the encoder as they pass through the area. See *Adding Ethernet Encoders* for more information.

To update a key using an encoder, perform the following steps:

1. Select **Cardholders** > **Users**. The **Users** screen is displayed.
2. Double-click the name of the user whose key you want to update. The **User** information screen is displayed.

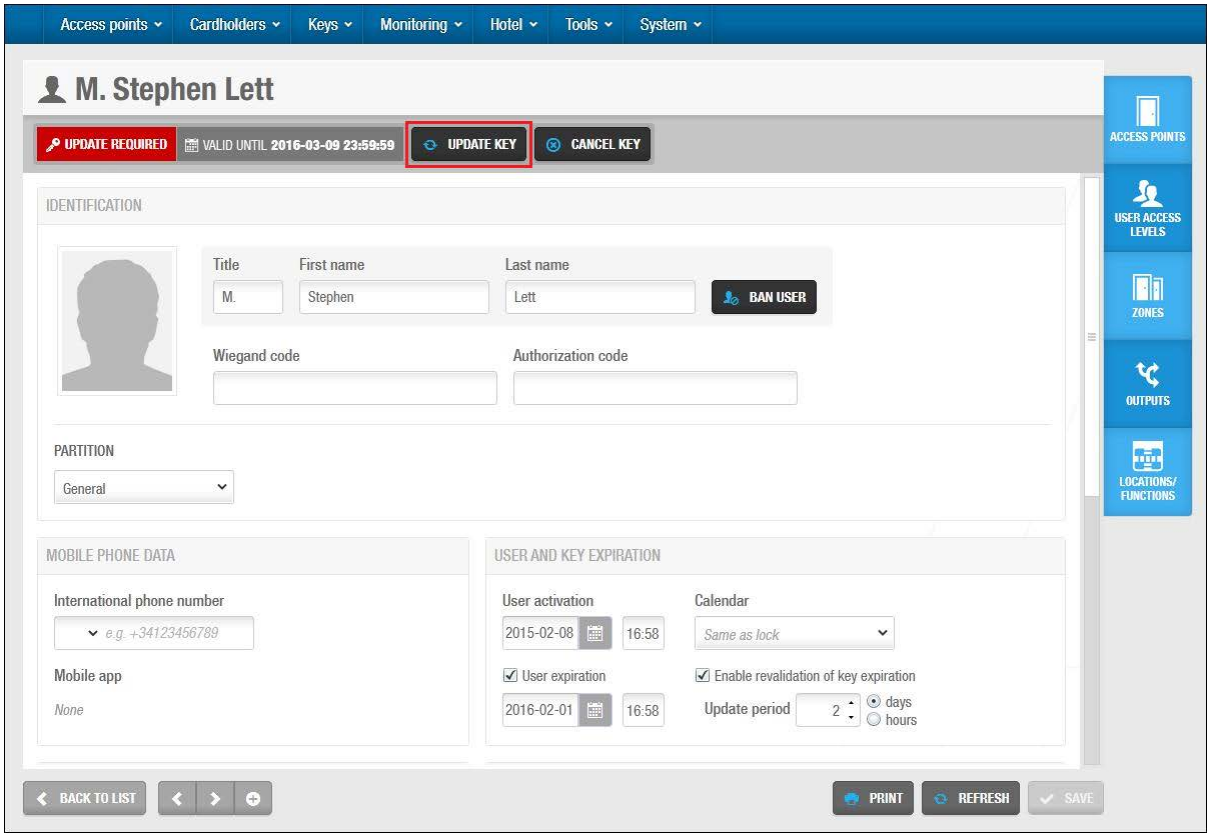


Figure 175: User information screen

3. Click **Update Key**. The **Update key** dialog box is displayed.

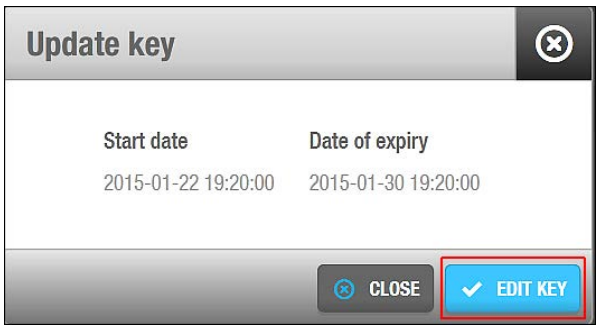


Figure 176: Update key dialog box

4. Click **Edit Key**. A pop-up is displayed asking you to place the key on the encoder.

   You must place the key that belongs to the selected user on the encoder. If you place a different user key on the encoder, an **Invalid user key** pop-up message is displayed.

5. Place the key on the encoder when the LED light begins to flash. A pop-up is displayed confirming that the operation was successful.
6. Remove the key and click **OK**.

9. 7. Assigning Keys Automatically

You can configure the system to assign keys to users automatically by using the **User** tab in ProAccess SPACE General options. See *Automatic Key Assignment* for more information. This option is particularly useful in university sites, for example, where thousands of new users (students) arrive at the start of each academic year. The automatic key assignment functionality means that users do not have to wait in line to have their key encoded. Instead, their key is assigned automatically when it is presented to an SVN wall reader, or an encoder with a running update reader. See *Adding Ethernet Encoders* for more information.

The automatic key assignment functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

NOTE: For security purposes, when you cancel keys that have been assigned automatically, you cannot use them for automatic key assignment again. Instead, you must assign these keys manually. See *Assigning User Keys* for more information.

9. 8. About Blacklists

The blacklist is a record of cancelled keys. See *Cancelling Keys* for more information about cancelling keys. When a cancelled key is sent to the blacklist, the information is communicated throughout the system. As users update their keys at SVN wall readers and present their keys to locks, the new blacklist information is circulated to all access points.

If you delete valid user keys, they are sent to the blacklist by default. See *Deleting Keys* for more information about deleting keys.

An unlimited amount of users and four million keys can be created, but a maximum of 65,535 keys can be cancelled through the blacklist. If the blacklist is full, you cannot create any new users on the system, and you cannot edit new keys for users. This can be avoided by monitoring the blacklist. You can view the blacklist status on the **System resources** screen. See *System Resources* for more information about viewing the blacklist status.

NOTE: If the blacklist is full, you can perform a blacklist recovery. You should consult your SALTO technical support contact for more information about this process.

9. 8. 1. Managing Blacklists

You can choose to select if user keys will be sent to the blacklist when cancelled by enabling the MORE_THAN_64K_USERS advanced parameter in ProAccess SPACE General options. This parameter also allows you to control whether visitor and guest keys are sent to the blacklist. See *Advanced Tab* for more information.

The process is different for user, visitor, and guest keys.

9. 8. 1. 1. Sending User Keys to the Blacklist

When you enable the MORE_THAN_64K_USERS advanced parameter in ProAccess SPACE General options, a **New key can be cancelled through blacklist** checkbox is displayed in the **Key Options** panel on the **User** information screen in ProAccess SPACE. This checkbox is selected by default. If you clear the checkbox, the cancelled key is not sent

to the blacklist. Instead, it is invalidated when it expires or when it is presented to an SVN wall reader.

By default, the maximum expiration period for keys that cannot be cancelled through the blacklist is three days. You can change this value by using the **User** tab in ProAccess SPACE General options if required. However, it cannot be higher than seven days for security reasons. See *Users Tab* for more information.

9. 8. 1. 2. Sending Visitor Keys to the Blacklist

When you enable the MORE_THAN_64K_USERS advanced parameter in ProAccess SPACE General options, a **Visitors keys are cancellable through blacklist** checkbox is displayed on the **Visitors** tab in ProAccess SPACE General options. This checkbox is selected by default. The option applies to all the visitor keys in the system. This means that visitor keys are sent to the blacklist if you delete visitors in ProAccess SPACE before their visit has expired.

Note that if you delete visitors after their visit has expired, their keys are not sent to the blacklist. If you clear the **Visitors keys are cancellable through blacklist** checkbox, valid visitor keys are not sent to the blacklist when you delete them. Instead, the keys are invalidated when they expire, or when they are presented to an SVN wall reader. See *Deleting Expired Visitors* for more information about deleting visitors.

9. 8. 1. 3. Sending Guest Keys to the Blacklist

When you enable the MORE_THAN_64K_USERS advanced parameter in ProAccess SPACE General options, guest keys are sent to the blacklist when you cancel them. This applies to all guest keys in the system. See *Configuring Hotel Keys* for more information.

10. MONITORING

This chapter contains the following sections:

10. 1. About Monitoring

SALTO ProAccess SPACE monitoring permits users to track what happen in the property. It allows consulting the audit trail and see WHO, WHERE and WHAT was made in the property. It also allows real time monitoring in online doors or manage the parking occupancy for example.

10. 2. Audit Trails

The **Audit trail** information screen shows a list of events for each access point. Each event has a date and time stamp. By default, it shows events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering Audit Trail Data* for more information.

NOTE: The audit trail and system auditor track different system information. The **System auditor** information screen shows system and operator events. The **Audit trail** information screen shows access point events only.

See *Collecting Audit Trail Data from Offline Doors* for information about how to collect audit trail data from offline doors.

You can view the audit trail information by selecting **Monitoring** > **Audit trail**.

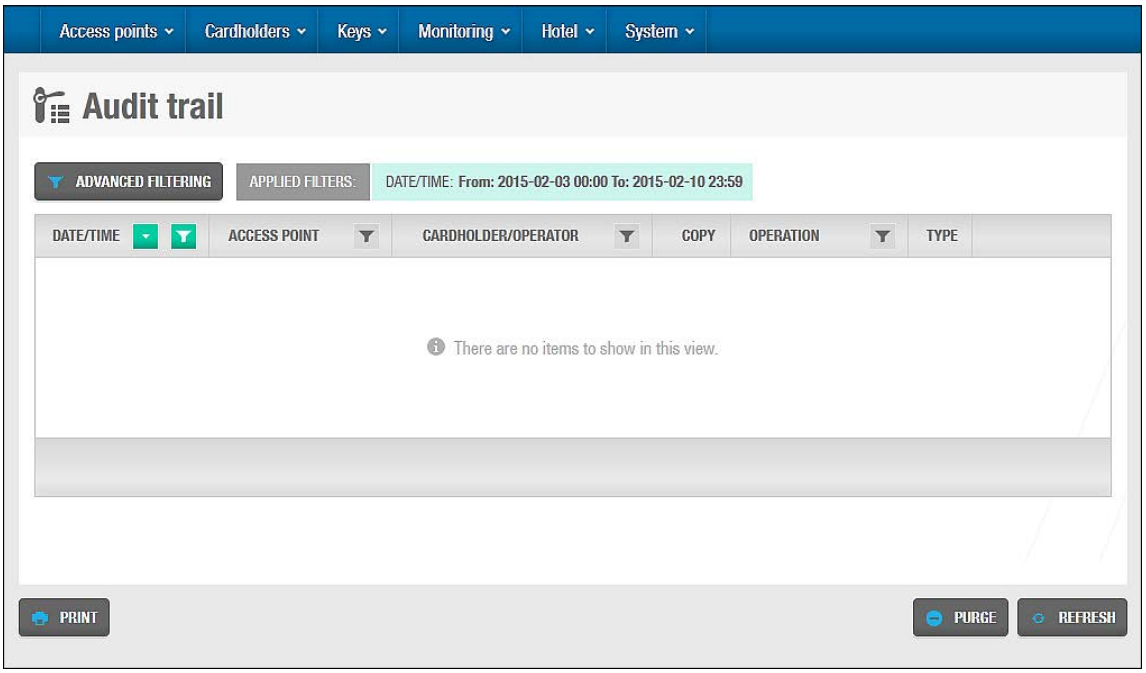


Figure 177: Audit trail information screen

10. 2. 1. Restricting Audit Trail Data

You can restrict the type of data that is displayed in the audit trail by selecting the **Disable collection of personal registries on audit trail** checkbox in **System** > **General options** ProAccess SPACE. When you select this option, operators can view entries for lock and key updates but not opening and closing events, or failed access attempts. See *General Tab* ***Error! Reference source not found.*** for more information.

10. 2. 2. Printing and Exporting Audit Trail Lists

You can select **Monitoring** > **Audit trail** and click **Print** on the **Audit trail** information screen to print a hard copy of the audit trail list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

10. 2. 3. Filtering Audit Trail Data

You can filter the audit trail data by event date/time, access point, cardholder/operator, operation, and/or type. See *Audit Trail Filters* for more information.

To filter the audit trail data, perform the following steps:

1. Select **Monitoring** > **Audit trail**. The **Audit trail** information screen is displayed.

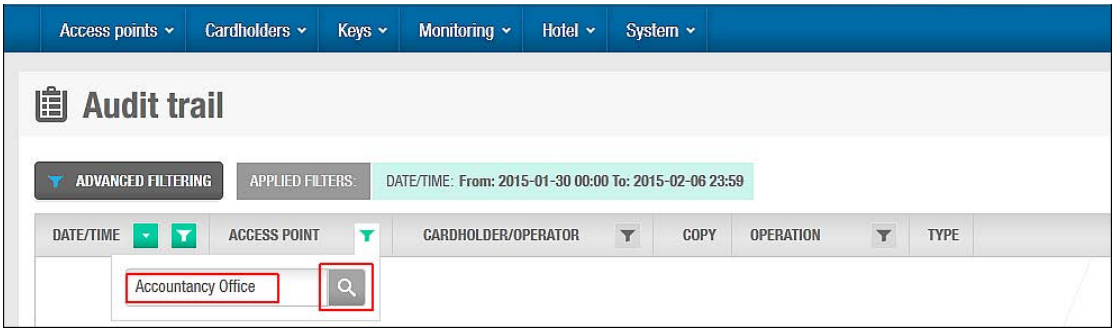


Figure 178: Audit trail information screen

2. Click the **Funnel** icon above the filter item. A search dialog box is displayed.

   For example, if you want to filter by access point name, click the **Funnel** icon at the top of the **Access Point** column.
   For the **Operation** and **Type** filters, you can see a predefined drop-down list of search terms by clicking on the down arrow in the dialog box.
   For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.

3. Type your search term.

   Or
   Select a predefined search term from the drop-down list.
   Or
   Select a date range.
   You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.
   However, you cannot remove the **Date/Time** filter.

4. Click the **Search** icon. A filtered audit trail list is displayed.

10. 2. 3. 1. Audit Trail Filters

You can use the **Audit trail** information screen filters to display only certain events. The options are described in the following table.

Table 35: Audit trail filters

Audit Data Filter	Description
Event Date/Time	Date and time when the event took place
Access Point	Access point name where the event took place, for example, which door was opened
Cardholder/Operator	User name of the person who caused the event, for example, the name of the user who opened the Financial Services office door
Operation	Details of the event, for example, door opened, CU updated
Type	Predefined category type of the event. For example, a door left open is defined under the Alarms and warnings type.

10. 2. 4. Advanced Filtering

You can configure advanced filters and apply them to audit trail data. You can also save any advanced filters that you create.

You can filter audit trail events by the following:

- Cardholders, and/or operators, and/ or access levels
- Access points and/or zones
- Operations and/ or operation groups
- Date and time period

The sections below describe how to complete each step in this process.

10. 2. 4. 1. Step One: Adding Filter Details

To complete Step one:

1. Select **Monitoring** > **Audit trail**. The **Audit trail** information screen is displayed.

2. Click **Advanced Filtering**. The **Advanced filtering** screen is displayed.

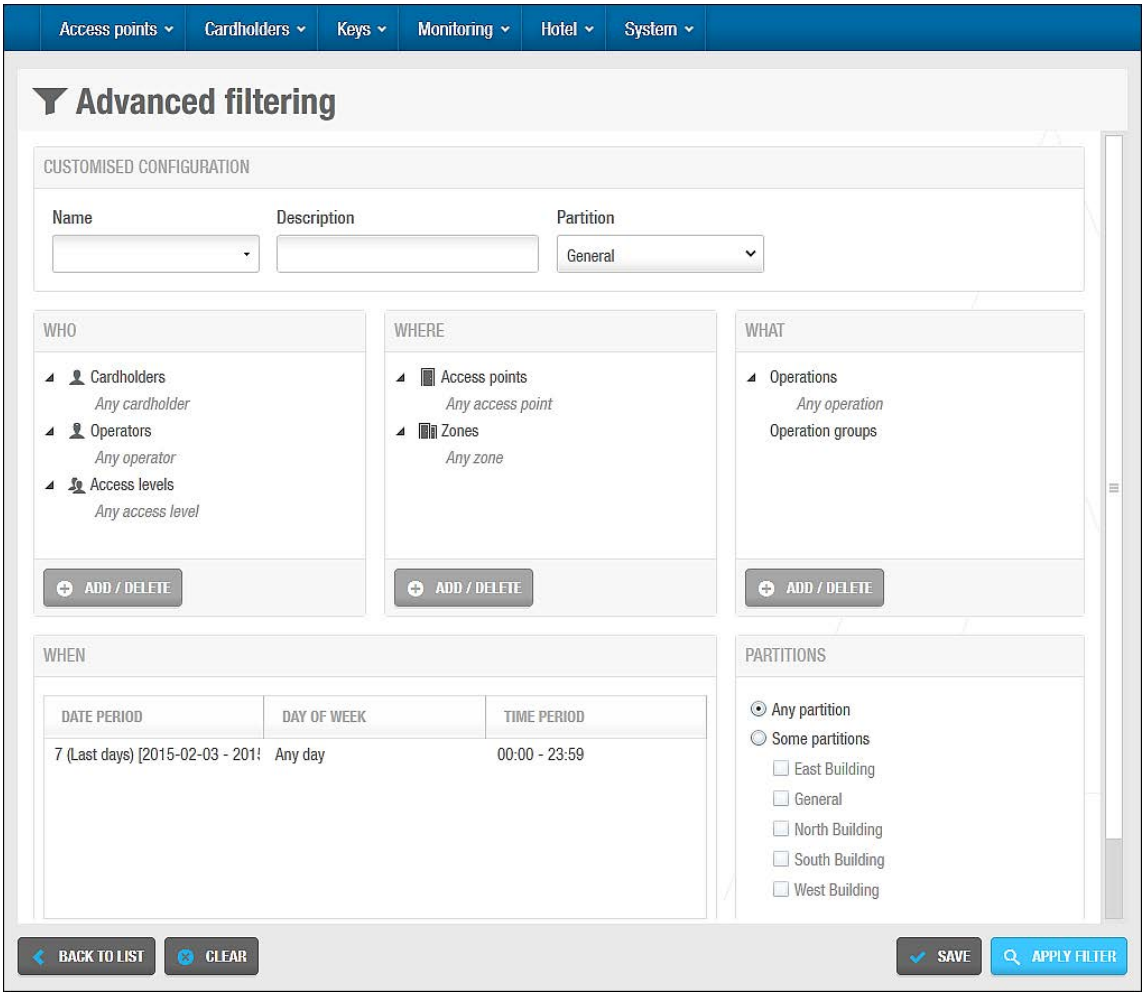


Figure 179: Advanced filtering screen

3. Type a name for the filter in the **Name** field.
4. Type a description for the filter in the **Description** field.
5. Select a partition from the **Partition** drop-down list if required.

   See *Partitions* for more information about partitions. The filter is only applied to the partition you select.

10. 2. 4. 2. Step Two: Selecting Filter Parameters

To complete Step two:

1. Click **Add/Delete** in the **Who** panel. The **Add/Delete** dialog box, which contains a list of cardholders, operators, and access levels on three tabs, is displayed.
2. Select the required cardholders in the left-hand panel and click the chevron. The selected cardholders are displayed in the right-hand panel.

   You can hold down the Ctrl key while clicking the fields to make multiple selections. As soon as you select a cardholder, the default **Any cardholder** option is automatically moved to the left-hand panel. You can use the default option if you want to view audit trail data for all the cardholders in the system.
3. Click the **Operators** tab if you also want to filter by operator. A list of operators is displayed.

4. Select the required operators in the left-hand panel and click the chevron. The selected operators are displayed in the right-hand panel.
5. Click the **Access levels** tab if you also want to filter by access levels. A list of access levels is displayed.
6. Select the required access levels in the left-hand panel and click the chevron. The selected access levels are displayed in the right-hand panel.
7. Click **Accept**. The selected cardholders, operators, and access levels are displayed in the **Who** panel.
8. Follow the procedure described in Steps 1 to 7 to add the access points and zones you want to filter to the **Where** panel.
9. Follow the procedure described in Steps 1 to 7 to add the operations and operation groups you want to filter to the **What** panel.

10. 2. 4. 3. Step Three: Specifying Filter Date Periods

To complete Step three:

1. Click **Add/Delete** in the **When** panel. The **Add/delete** periods dialog box, showing the default period, is displayed.

   The default period is any time in the previous seven days.

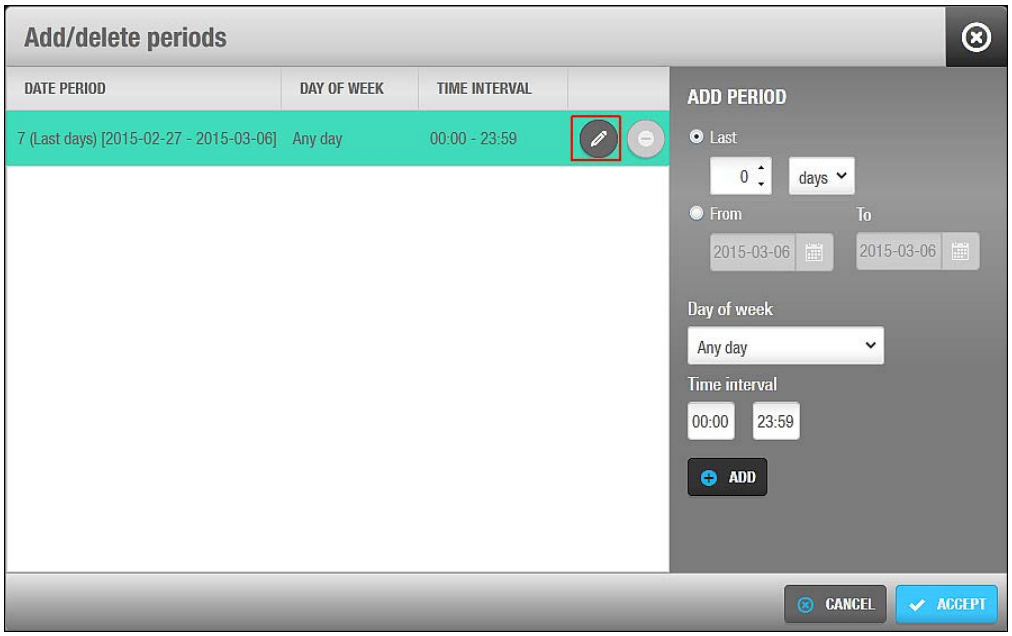


Figure 180: Add/delete periods

2. Click the **Edit** icon to change the date period and time interval if required.

   You can also click **Add** to add additional periods. For example, you can add a period to filter the audit trail data between 09:00 and 11:00 each day within a specified date period, and add another period to filter the audit trail data between 14:00 and 17:00 each day within the same date period.
3. Click **Accept** when you have finished editing or adding periods. The changes are displayed in the **When** panel.
4. Select the **Any partition** or **Some partitions** option in the **Partitions** panel.

   See *Partitions* for more information about partitions. If you select the **Some partitions** option, you must select the appropriate partitions from the list.

5. Click **Apply Filter**. The **Audit trail** information screen, showing the relevant entries and the name of the advanced filter, is displayed.

   Alternatively, you can click **Save** to save the filter you have created. You can click **Advanced Filtering** or the name of the advanced filter on the **Audit trail** information screen to return to the **Advanced filtering** screen and change the filter configuration or save the filter. When you save a filter, it is automatically added to the drop-down list in the **Name** field on the **Advanced Filtering** screen. To view a saved filter, select it from the drop-down list.

NOTE: You can also filter audit trail data by using the events stream functionality in ProAccess SPACE Tools. See *Events Streams* for more information.

10. 2. 5. Purging Audit Trail Data

Purging the audit trail removes all audit trail data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the audit trail are scheduled by default. See *Automatic Audit Trail Purging* for more information.

To purge the audit trail, perform the following steps:

1. Select **Monitoring** > **Audit trail**. The **Audit trail** information screen is displayed.
2. Click **Purge**. The **Audit trail purging** dialog box is displayed.

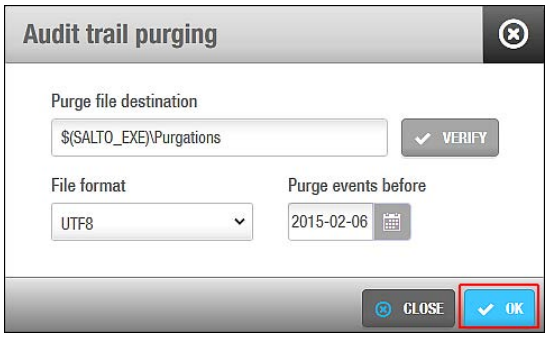


Figure 181: Audit trail purging dialog box

3. Type the appropriate destination folder name in the **Purge file destination** field.

   You can click **Verify** to verify the file directory exists and is correct.
4. Select a format from the **File format** drop-down list.

   This specifies the format of the file containing the purged events.
5. Select the required date by using the calendar in the **Purge events before** field.

   All events prior to the date you select are purged.
6. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
7. Click **OK**.

10. 3. Online Monitoring

The online lock monitoring functionality allows you to view and control the status of online control units (CUs) in real-time. It also allows you to perform actions on doors like setting the

emergency open or emergency close mode. Online CUs also enable the blacklist to be transmitted automatically to doors without the need to visit each door with an updated key.

To access the monitoring functionality, select **Monitoring** > **Online monitoring**. The **Online monitoring** screen is displayed.

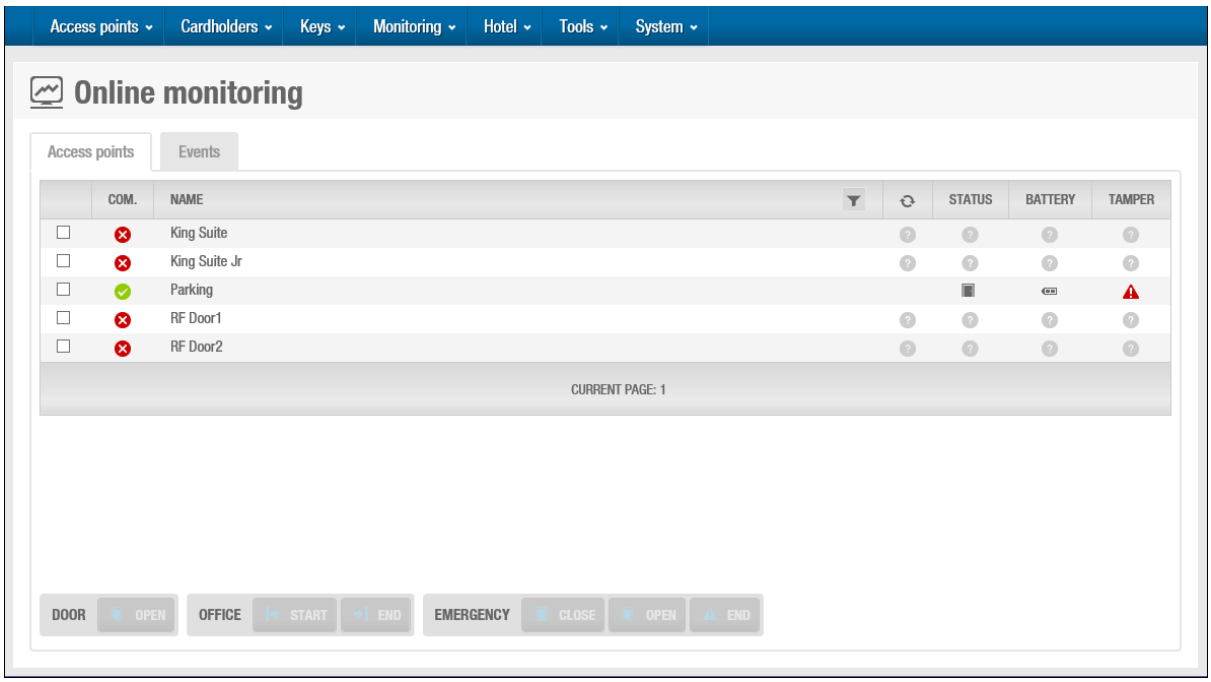


Figure 182: Online Monitoring screen

Two tabs are displayed on this screen: **Access points** and **Events**. While **Access points** shows online peripheral status, **Events** shows real-time events from all the connected doors.

10. 3. 1. Access points

The **Access points** tab allows you to control doors in emergency situations. Select a peripheral on the **Access point** tab to enable the buttons underneath.

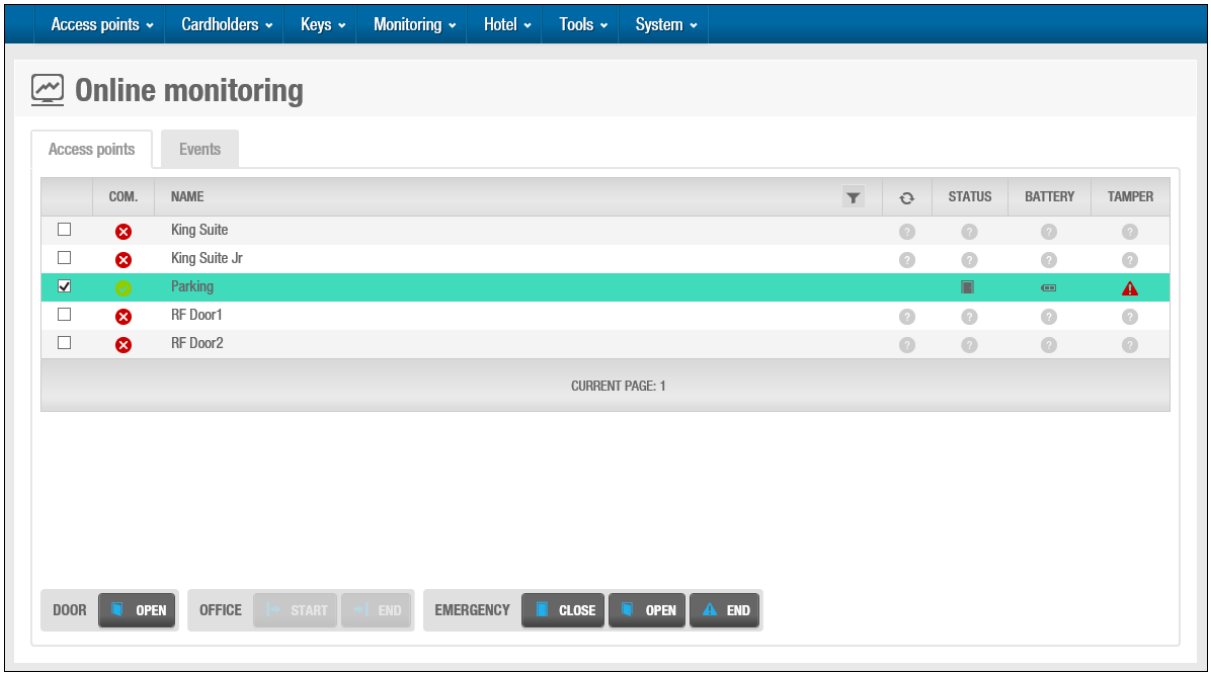


Figure 183: Access point tab

The **Online monitoring** tab buttons are described in the following table.

Table 36: Online monitoring buttons

Button	Functionality
Open	Allows remote doors to be opened
Start office	Enables the Office mode for doors
End office	Disables the Office mode for doors
Emergency Close	Closes any doors to any user, visitor, or guest, regardless of their access permissions, until the end of the emergency
Emergency Open	Opens any doors to any user, visitor, or guest, regardless of their access permissions, until the end of the emergency
Emergency End	Returns doors to their normal working mode

The columns at the top of the **Access point** tab are described in the following table.

Table 37: Monitoring columns

Column	Functionality
Com.	Indicates the communication status of the door: a green circle means the door is communicating correctly; a red circle means there is a communication error.
Name	Specifies the name of the door
Update status	Indicates the action required: a white escutcheon icon means the door must be addressed; a red escutcheon icon means an update is required. If no escutcheon icon is shown, this means no update is required. Note that this column does not have a title on the screen.
Status	Indicates the status of the door: an open door icon means the door is open; a closed door icon means the door is closed; an exclamation mark indicates an emergency door opening or closing. Note that a door detector is required to provide these status updates to the SALTO system.

Column	Functionality
Battery	Indicates the battery status of the door
Tamper	Indicates whether the door has been altered. The tamper is a connection in the online CU that can be used for different purposes. For example, you can connect a switch in SALTO power boxes (where CUs are installed) to indicate that a door was opened.

10. 3. 2. Events

The **Events** tab displays a real-time record of every event involving the door, including the particular action, the name of the door, the user, the user picture and the time and date. Click **Clear events** to remove all events from this panel. Note that events removed from this panel are still listed in the audit trail. See *Audit Trail* for more information about audit trails. The **Pause events notification** button stops new events from showing momentarily. This is useful in case an important event is shown and you don't want new events to replace it. The picture of the user is also show at the top of the Events screen if the feature is enabled. See *General tab* in the ProAccess SPACE General options for more information.

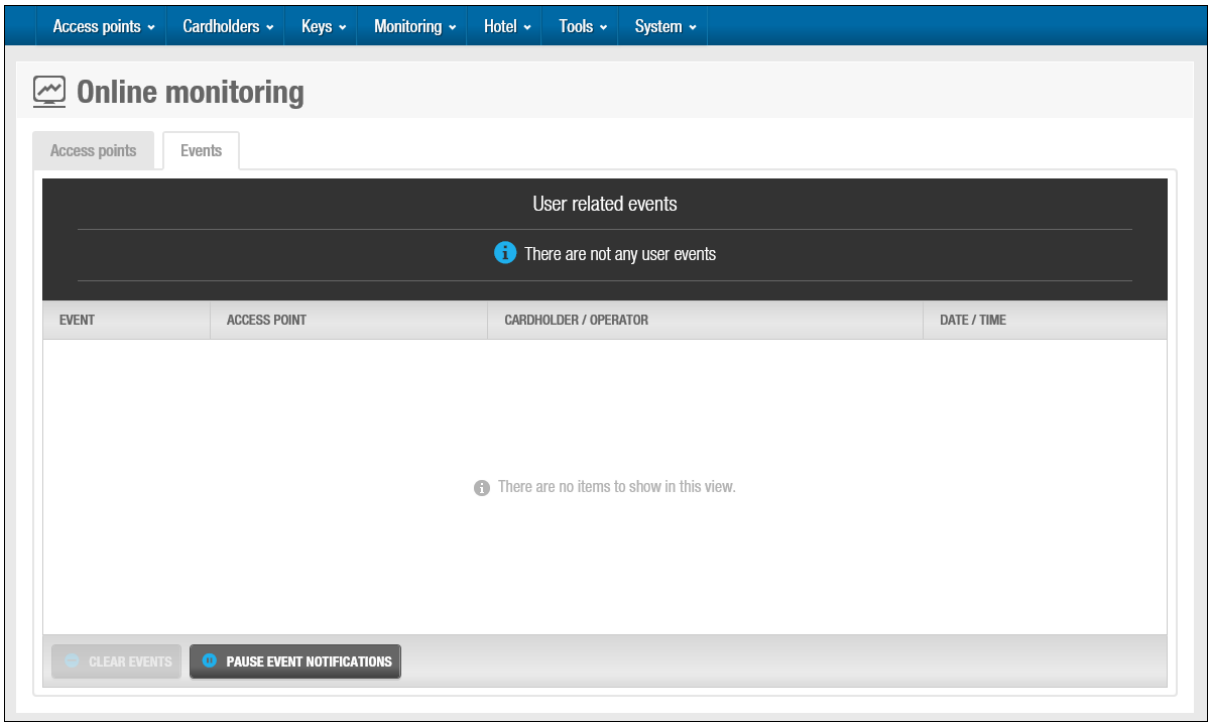


Figure 184: Online monitoring Events tab

The columns at the top of the **Events** tab are described in the following table.

Table 38: Events columns

Column	Functionality
Event	Specifies the event occurred at the door. It can also show the reason of the key rejection.
Access point	Specifies the name of the door.

Column	Functionality
Cardholder / Operator	Shows the name of the cardholder or of the operator if the operation was done remotely for example.
Date / Time	Date and time of the event.

In the upper part of the window, in **User related events**, you can see the user picture icon. Click on the picture icon to see the event data.

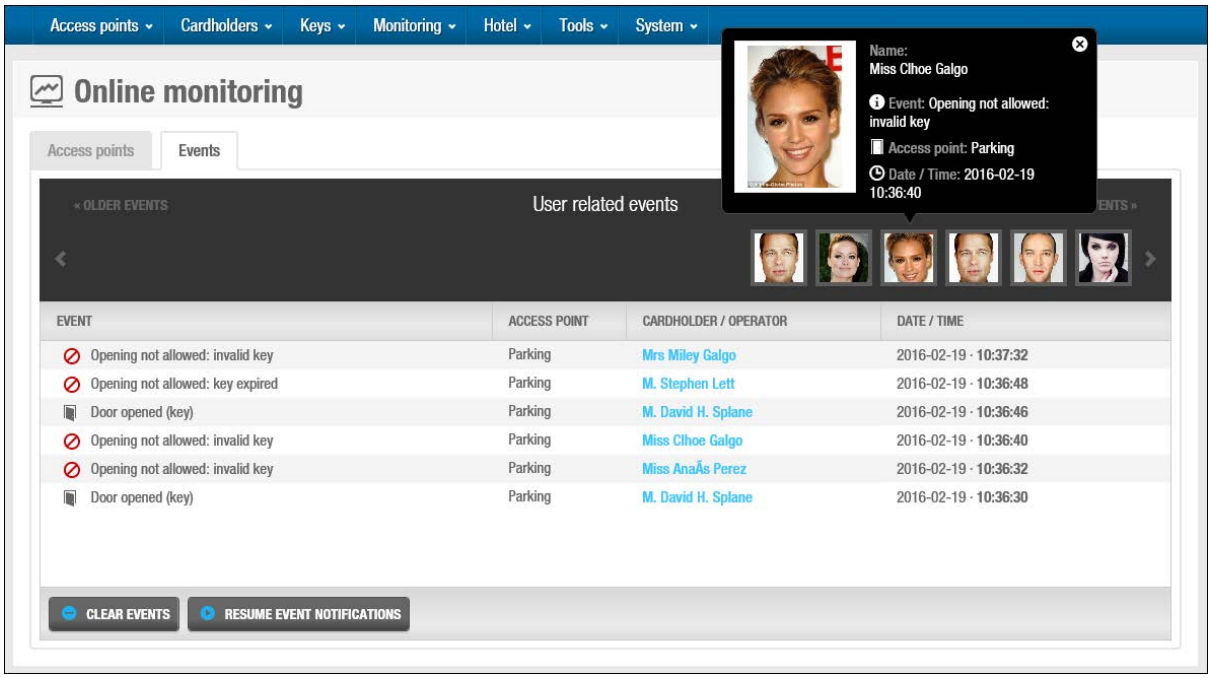


Figure 185: Online monitoring Events tab

You can also click the user name under the Cardholder / Operator column shown in blue, and the user event data will pop up.

10. 4. Lockdown Monitoring

A lockdown area is a defined area where all access points can be closed or opened in an emergency situation. See *Lockdown Areas* for more information. Select the checkbox next to a lockdown area on the **Lockdown** tab to enable the buttons on the right-hand side.

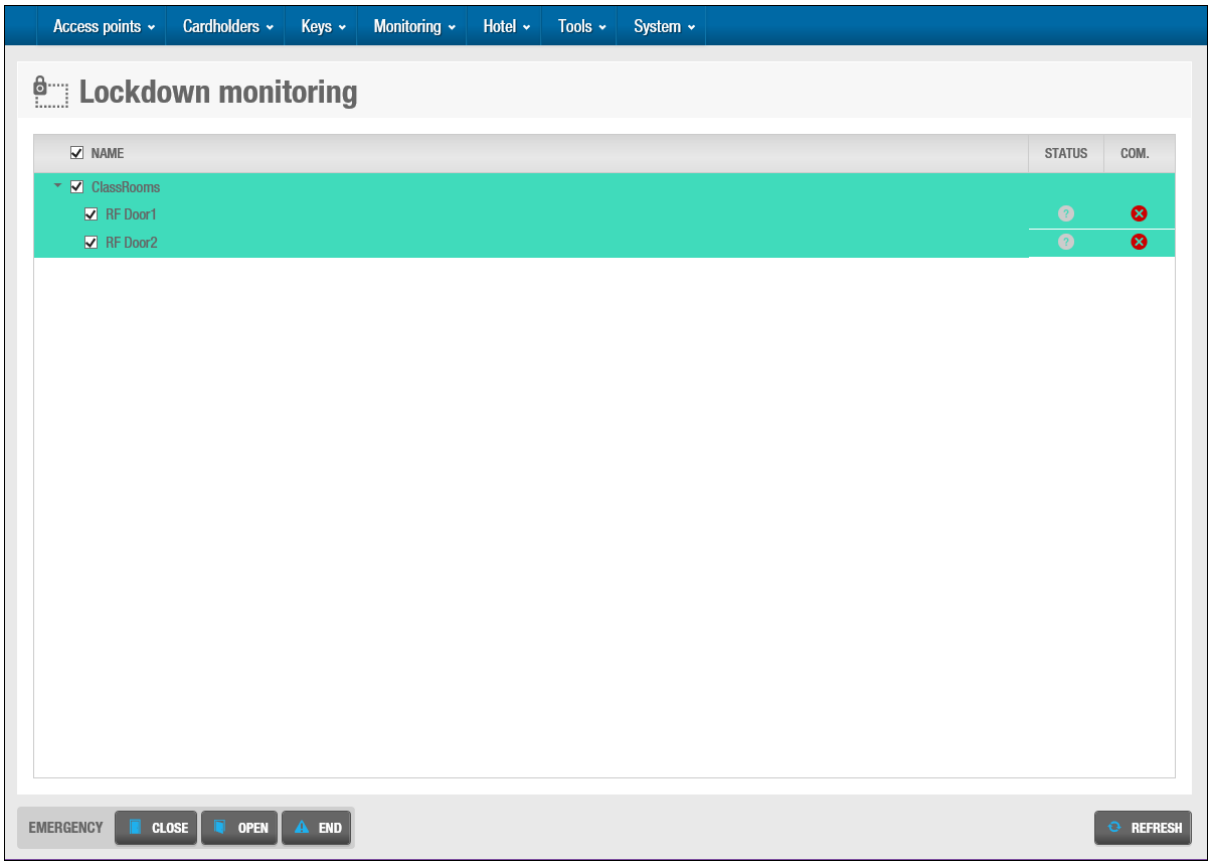


Figure 186: Lockdown tab

Click the **Expand** button next to a lockdown area to show the doors associated with that area. Click the **Collapse** button next to a lockdown area to hide the doors.

The **Lockdown** tab buttons are described in the following table.

Table 39: Lockdown buttons

Button	Functionality
Emergency Close	Closes all selected doors in the lockdown area to any user, visitor, or guest, regardless of their access permissions, until the end of the emergency
Emergency Open	Opens all selected doors in the lockdown area to any user, visitor, or guest, regardless of their access permissions, until the end of the emergency
End emergency	Returns doors in the lockdown area to their normal working mode

NOTE: Only users with the override lockdown functionality enabled on their profile can open a door closed by lockdown. The **Override lockdown** checkbox is located in the **Key Options** panel on the **User** information screen. See *Key Options* for more information.

10. 5. Limited Occupancy Monitoring

In ProAccess SPACE, the limited occupancy areas functionality allows you to designate an area, for example a car park, and specify the maximum number of permitted users within that area. The limited occupancy group is a grouping of users who require access to a

specified limited occupancy area. See *Limited Occupancy Areas* and *Limited Occupancy Groups* for more information.

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

In ProAccess SPACE, the limited occupancy monitoring functionality allows you to control limited occupancy groups.

To add or remove a user from a limited occupancy group, perform the following steps:

1. Select **Monitoring** > **Limited occupancy monitoring**. The **Limited occupancy monitoring** screen is displayed.
2. Select the limited occupancy group from which you want to add or remove a user.

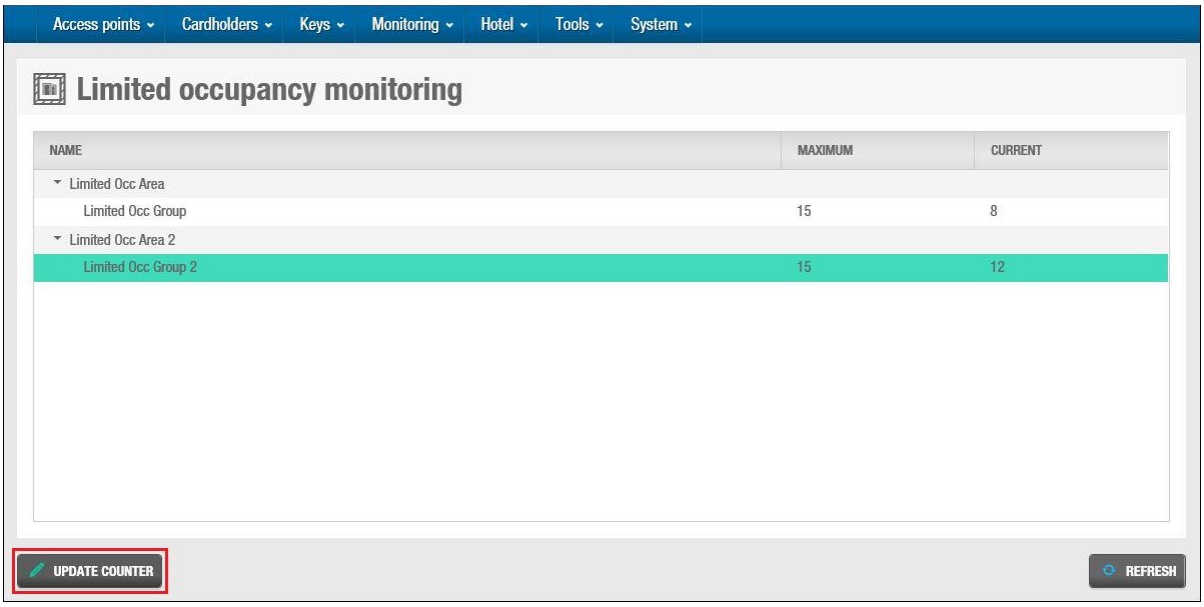


Figure 187: Selected limited occupancy group

3. Click **Update counter**. The **Current users in** dialog box, showing the number of users in the limited occupancy group, is displayed.

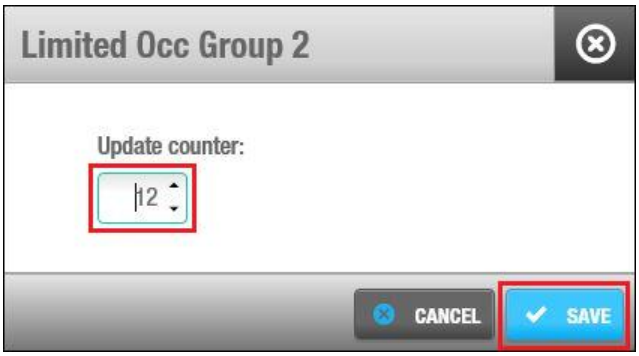


Figure 188: Current users in dialog box

4. Enter the appropriate number in the **Current users in** field.

Click **Save.** The updated number of users in the limited occupancy group is displayed.

10. 6. Roll-Call Monitoring

The roll-call functionality identifies whether users are inside or outside a specific location in a site. You can use it to list the individual users in a specified area, for example, a canteen, at a particular time. A roll-call area in the SALTO system tracks the time and date individual users entered that area. See *Roll-Call Areas* for information about how to create a roll-call area.

Note that the roll-call functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

10. 6. 1. Searching for Users

If a user needs to be located, you can search all roll-call areas for that user.

To search all roll-call areas, perform the following steps:

1. Select **Monitoring** > **Roll-call monitoring**. The **Roll-call** screen is displayed.
2. Select the user's name from the **Search user** drop-down list.
3. Click the **Search** button (binoculars). The user is displayed within the appropriate roll-call area.

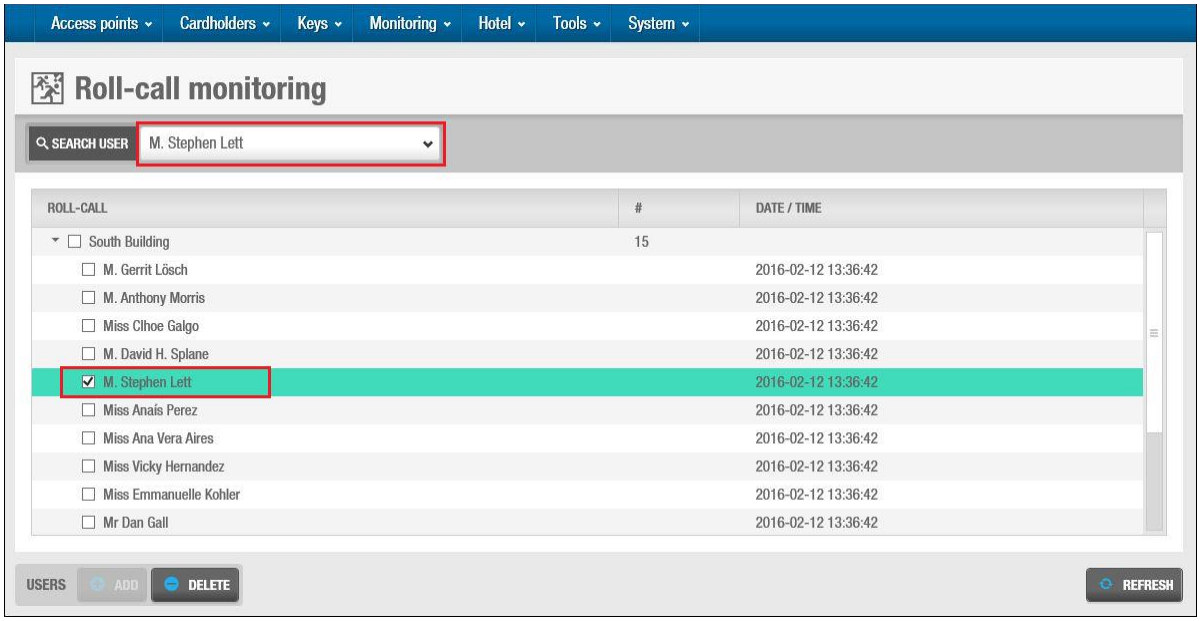


Figure 189: Locating a user in a roll-call area

10. 6. 2. Adding Users

You can manually add users to a roll-call area. Typically, this is only done when you need to amend the number of users recorded in a roll-call area. For example, if five users enter the canteen roll-call area together but only the first user presents a key, the system only records that one user has entered the area. To correct this, you can manually add the additional four users to that roll-call area.

To add a user to a roll-call area, perform the following steps:

1. Select **Monitoring** > **Roll-call monitoring**. The **Roll-call** screen is displayed.
2. Select the roll-call area to which you want to add the user.

3. Click **Add user**. The **Selection dialog** box, showing a list of users, is displayed.
4. Select the required user in the left-hand panel and click the arrow. The selected user is displayed in the right-hand panel.

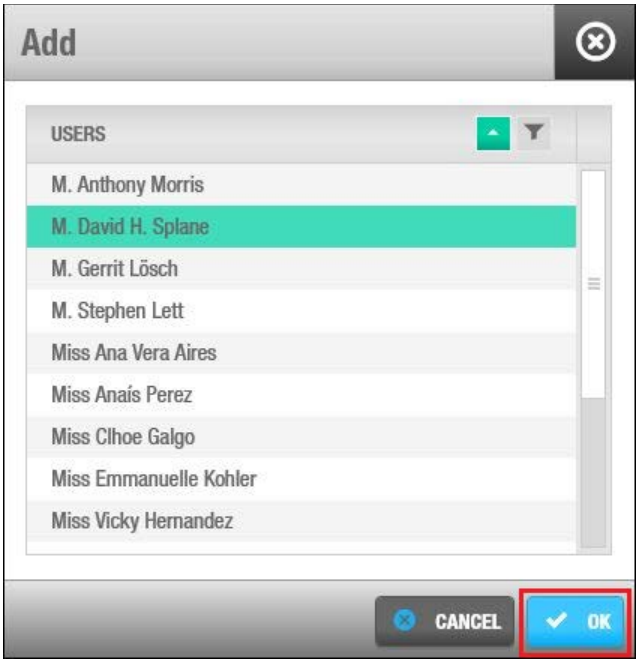


Figure 190: Selected user

5. Click **Ok**. The selected user is now added to the roll-call area.

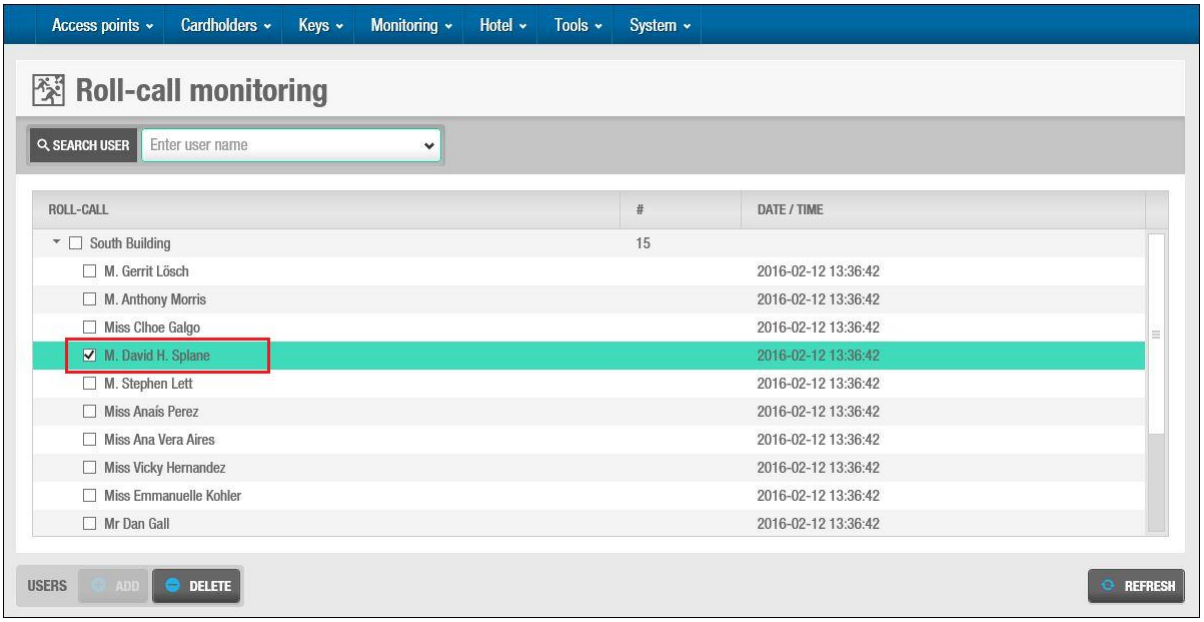


Figure 191: Selected user added to the roll-call area

6. Click **Close**.

10. 6. 3. Removing Users

You can manually remove users from a roll-call area. For example, if, at the end of a working day, all users have physically exited a roll-call area but the system shows users still in that area, you can remove users accordingly.

To remove a user from a roll-call area, perform the following steps:

1. Select **Monitoring** > **Roll-call monitoring**. The **Roll-call** screen is displayed.
2. Select the user's name in the roll-call area.
3. Click **Remove user**. The user is removed from the roll-call area.

10. 6. 4. Printing User Names

You can print a report listing all user names, their roll-call area, and the time and date each user entered the roll-call area.

To print a report, perform the following steps:

1. Select **Monitoring** > **Roll-call monitoring**. The **Roll-call** screen is displayed.
2. Click **Print**. The report is then printed.

11. PROACCESS SPACE TOOLS

This chapter contains the following sections:

11. 1. About ProAccess SPACE Tools

System tools in ProAccess SPACE allow you to conduct tasks such as automatically scheduling data synchronization jobs, and purging and exporting system data. You can also view all tasks performed by each operator, as well as an audit trail of access point opening and closing events.

This chapter describes how to schedule system jobs, view and filter audit events, and view the status of system resources.

11. 2. Scheduling Jobs

Scheduled jobs are system tasks that are set up to be performed automatically. You can view the scheduled jobs on the system by selecting **System** > **Scheduled jobs**.

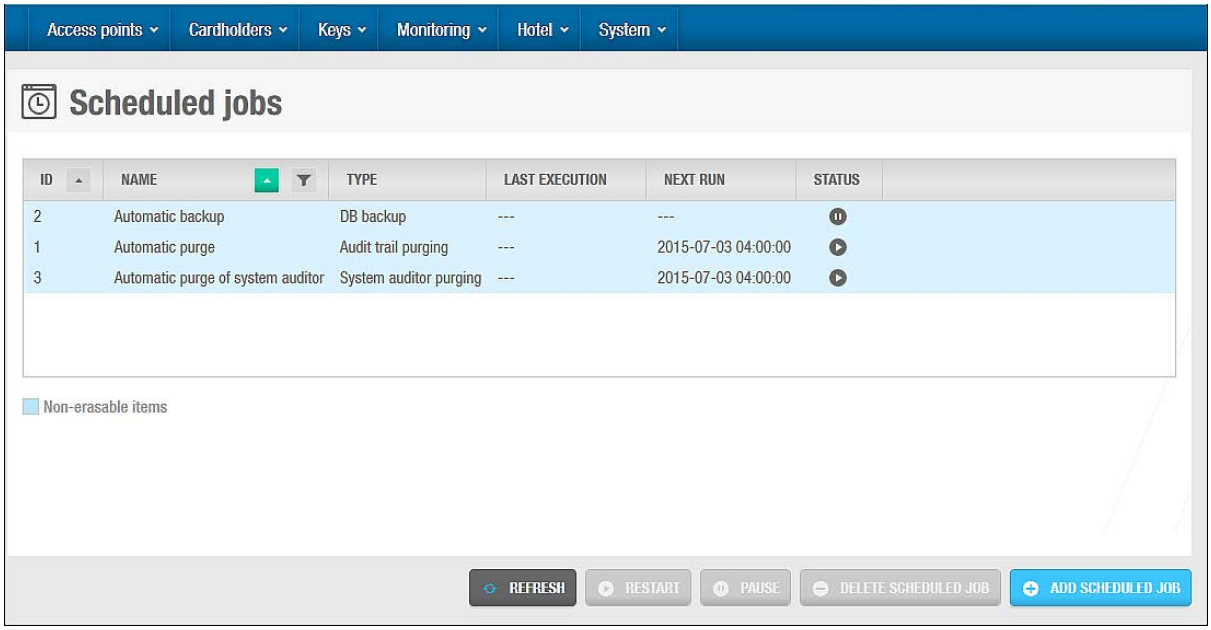


Figure 192: Scheduled jobs screen

The following three job types are scheduled on the system by default:

- Database backup

- Audit trail purging
- System auditor purging

Different icons are displayed in the **Status** column on the **Scheduled jobs** screen, depending on the status of each job. These icons are described in the following table.

Table 40: Scheduled job icons

Icon	Description
 Paused	Shows when a job is paused. You can select the job and click **Restart** to restart it.
 Running	Shows when a job is running. You can select the job and click **Pause** to pause it.

You can change the configuration and scheduling options for the default jobs, or create additional scheduled jobs. If you create an additional scheduled job, you have the option to delete the entry. However, you cannot delete any of the default job types.

NOTE: Scheduled jobs are not performed when the SALTO Service is not running.

11. 2. 1. Automatic Audit Trail Purging

Audit trail purging removes all audit trail data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location. See *Audit Trail* for more information about audit trails. Automatic purges of the audit trail are scheduled to be performed every 60 days by default but you can change the configuration and scheduling options for this job.

NOTE: It is strongly recommended that you purge the audit trail at least once a month. This is because system communication can slow down if the audit trail is very full. Regular audit trail purges also allow you to perform more efficient searches on audit trail entries.

The sections below describe how to complete each step in this process.

11. 2. 1. 1. Step One: Job Configuration

To complete Step one:

1. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
2. Double-click the audit trail purging entry. The **Job Configuration** screen is displayed.

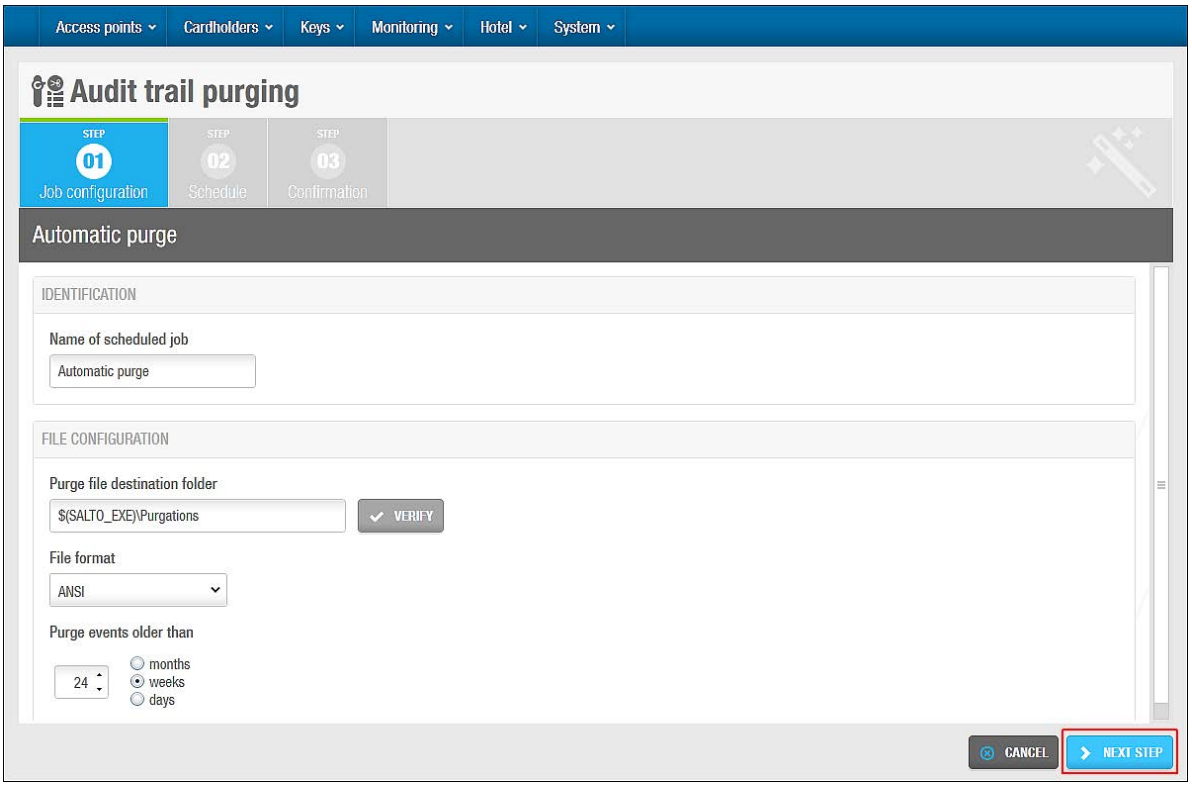


Figure 193: Job configuration screen

The **Name of scheduled job** and **Purge file destination folder** fields are automatically populated but you can change the text in these fields if required. It is recommended that you click **Verify** to verify the file directory exists and is correct.

3. Select a format from the **File format** drop-down list.

   This specifies the format of the file containing the purged events. The appropriate format depends on the alphabet you are using. In general, the system selects the required format by default. However, you can amend this if required.

4. Select the required time parameters using the up and down arrows and the options in the **Purge events older than** field.

   All events prior to the time you select are purged.

5. Click **Next Step**. The **Schedule** screen is displayed.

11. 2. 1. 2. Step Two: Schedule

To complete Step two:

1. Select the required number of days by using the up and down arrows in the **Frequency (days)** field on the **Schedule** screen.

   If you select **50**, for example, the job is performed every 50 days.

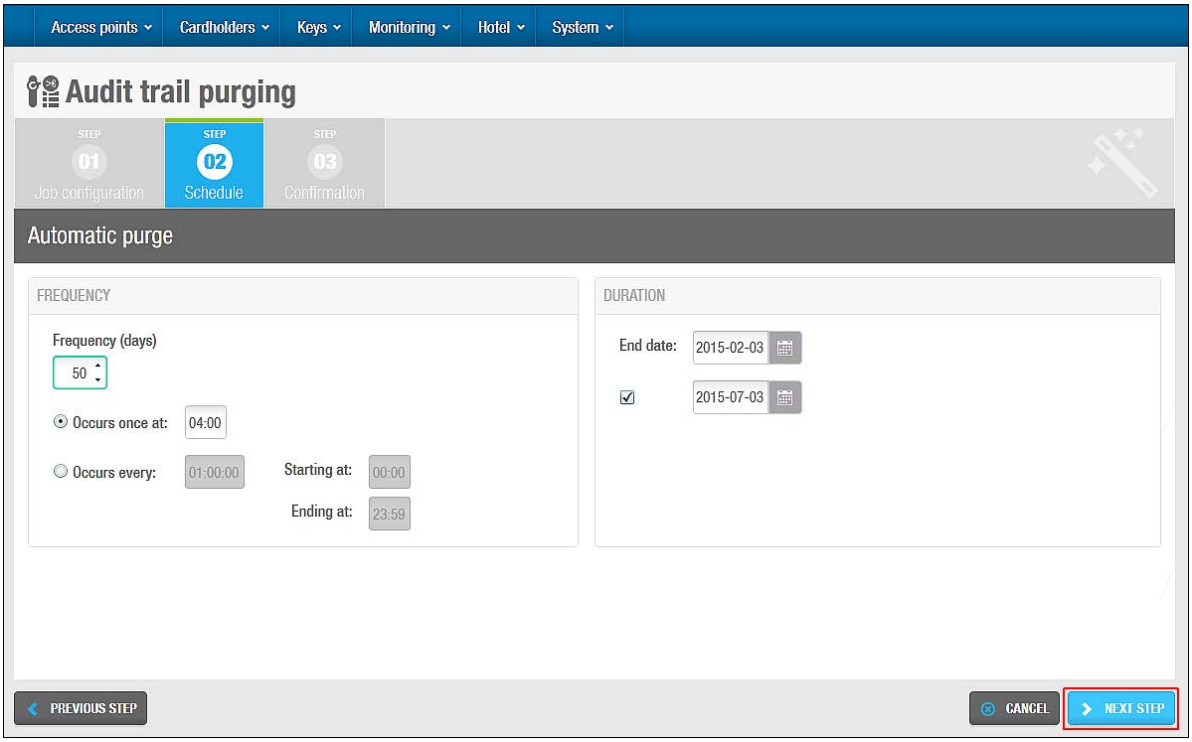


Figure 194: Schedule screen

2. Select either the **Occurs once at** or the **Occurs every** option and type the required time parameters for the selected option.

   These options allow you to specify whether the job occurs once on the scheduled day or at specific intervals during that day.
3. Select a start date for the job using the calendar in the **Start date** field in the **Duration** panel.
4. Select the **End date** checkbox and select an end date for the job using the calendar if required.

   If you do not select an end date the job is performed indefinitely.
5. Click **Next Step**. The **Confirmation** screen is displayed.

11. 2. 1. 3. Step Three: Confirmation

To complete Step three:

1. Review the job configuration and scheduling details on the **Confirmation** screen.

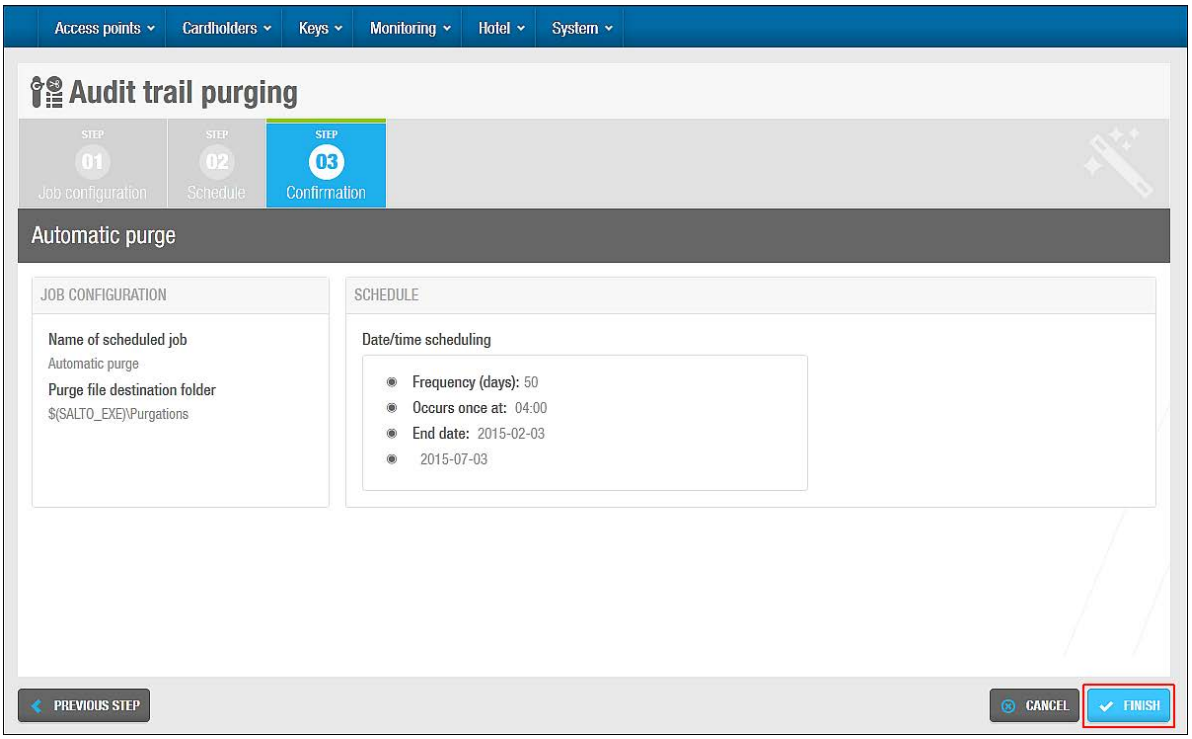


Figure 195: Confirmation screen

You can click **Previous Step** to amend the job configuration and scheduling details or click **Cancel** to discard all your configuration changes.

2. Click **Finish** if all your configuration is complete and correct.

11. 2. 2. Automatic System Auditor Purging

System auditor purging removes all system auditor data within a selected time frame from the system. See *System Auditor* for more information. The purged data is saved to a text file in a specified folder location. Automatic purges of the system auditor are scheduled to be performed every 60 days by default but you can change the configuration and scheduling options for this job.

NOTE: It is strongly recommended that you purge the system auditor at least once a month. They system auditor expands quickly as all system operator events are saved, and system communication can slow down if this is very full. It is particularly important to purge the system auditor regularly if you schedule automatic synchronization jobs. See *Automatic CSV File Synchronization* and *Automatic Database Table Synchronization* for more information.

The sections below describe how to complete each step in this process.

11. 2. 2. 1. Step One: Job Configuration

To complete Step one:

1. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
2. Double-click the system auditor purging entry. The **Job configuration** screen is displayed.

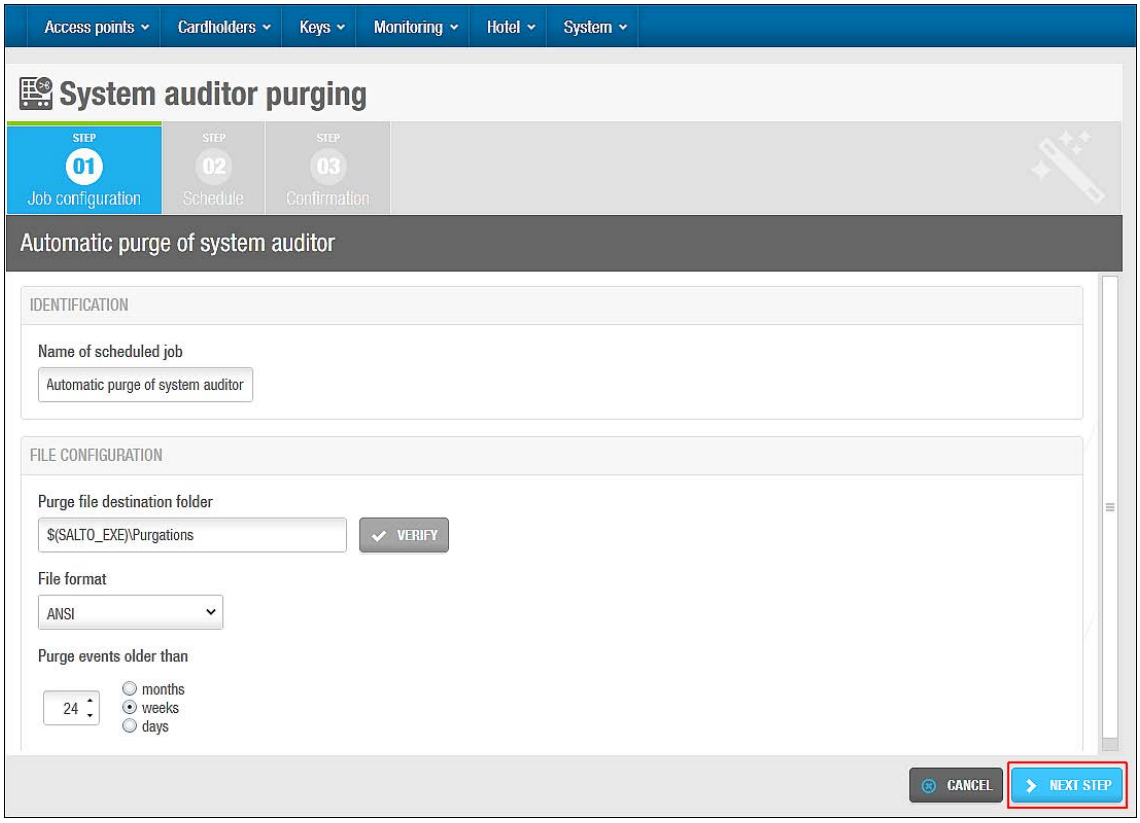


Figure 196: Job configuration screen

The **Name of scheduled job** and **Purge file destination folder** fields are automatically populated but you can change the text in these fields if required. It is recommended that you click **Verify** to verify the file directory exists and is correct.

3. Select a format from the **File format** drop-down list.

   This specifies the format of the file containing the purged events. The appropriate format depends on the alphabet you are using. In general, the system selects the required format by default. However, you can amend this if required.

4. Select the required time parameters by using the up and down arrows and the options in the **Purge events older than** field.

   All events prior to the time you select are purged.

5. Click **Next Step**. The **Schedule** screen is displayed.

11. 2. 2. 2. Step Two: Schedule

All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

11. 2. 2. 3. Step Three: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

11. 2. 3. Automatic Database Backups

Automatic database backups are scheduled to be performed every seven days by default but you can change the configuration and scheduling options for this job.

You can also make database backups by using the appropriate menu option in ProAccess SPACE. See *Making Database Backups* for more information.

NOTE: It is recommended that you perform database backups once a week. This ensures data is up to date if you need to restore system backups. Large sites may opt to perform database backups daily. You should not allow more than a month to elapse between backups. System backups are the only means of restoring the system in the event of a total system crash.

The sections below describe how to complete each step in this process.

11. 2. 3. 1. Step One: Job Configuration

To complete Step one:

1. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
2. Double-click the database backup entry. The **Job configuration** screen is displayed.

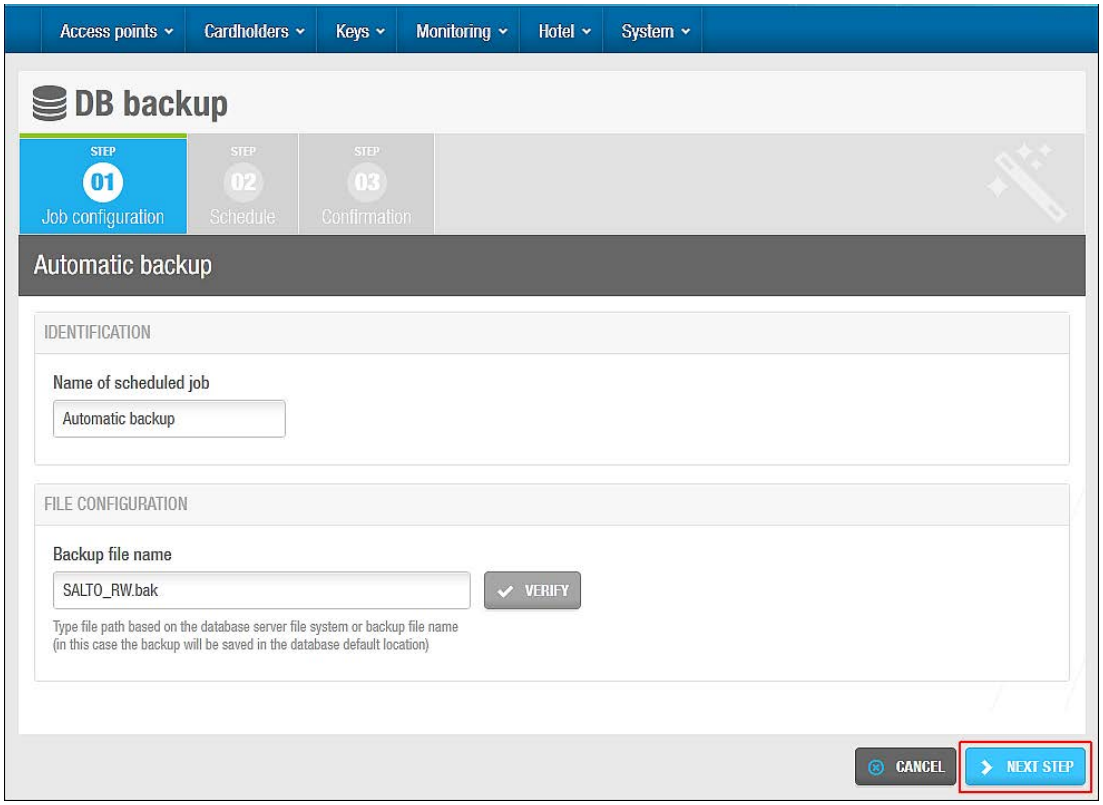


Figure 197: Job configuration screen

The **Name of scheduled job** and **Backup file name** fields are automatically populated but you can change the text in these fields if required. It is recommended that you click **Verify** to verify the file directory exists and is correct.

3. Click **Next Step**. The **Schedule** screen is displayed.

11. 2. 3. 2. Step Two: Schedule

All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

11. 2. 3. 3. Step Three: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

11. 3. Creating Scheduled Jobs

You can create the following types of scheduled job on the system:

- Comma-separated values (CSV) file synchronization
- Database table synchronization
- Audit trail export

When you create a job, it is displayed on the **Scheduled Jobs** screen. The following sections describe how to create these jobs.

The synchronization functionality is license-dependent. The export functionality is also controlled by your licensing options. See *Registering and Licensing SALTO Software* for more information.

11. 3. 1. Automatic CSV File Synchronization

CSV file synchronization allows you to synchronize user data from external system files with ProAccess SPACE. For example, in a university site, you can synchronize with the data in a student record system. You use data from a CSV or a text file to create entries and populate specified fields in ProAccess SPACE. This means you can automatically transfer data from other systems (rather than entering the same data manually in ProAccess SPACE).

NOTE: See the *SALTO_Data_Sync* document for more information about CSV file synchronization.

The sections below describe how to complete each step in this process.

11. 3. 1. 1. Step One: Job Configuration

To complete Step one:

1. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
2. Click **Add Scheduled Job**. The **Add scheduled job** dialog box is displayed.
3. Select **CSV file synchronization** from the drop-down list.
4. Click **OK**. The **Job Configuration** screen is displayed.

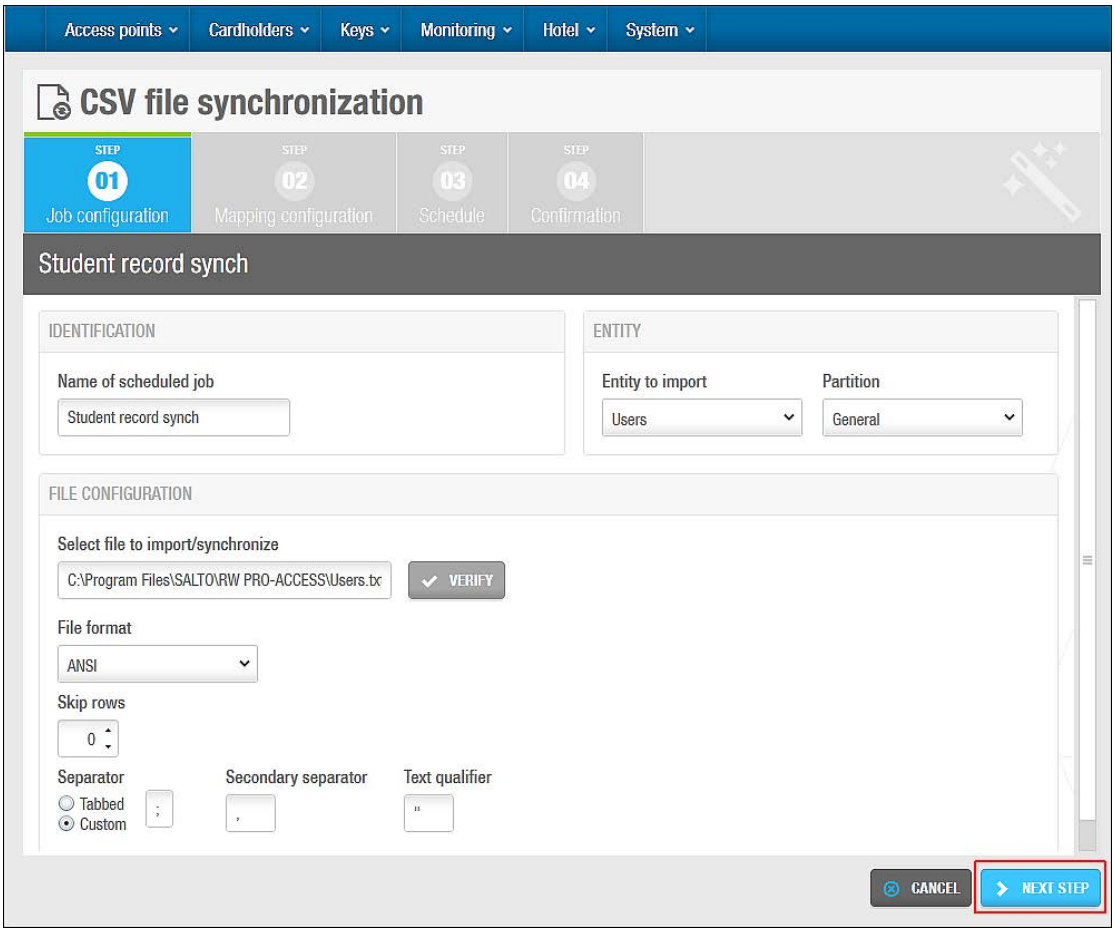


Figure 198: Job configuration screen

5. Type a name for the job in the **Name of scheduled job** field.
6. Type the name of the file that you want to import in the **Select file to import/synchronize** field.

   You can click **Verify** to verify the file directory exists and is correct.
7. Select the appropriate format from the **File format** drop-down list.
8. Select the required number of rows by using the up and down arrows in the **Skip rows** field.

   This specifies the row in the file where you want to begin importing data.
9. Select either the **Tabbed** or **Custom** option.

   The **Secondary separator** and **Text qualifier** fields are automatically populated but you can change the characters in these fields if required. The secondary separator is used to separate each access level ID in the file. The text qualifier is used for text fields that contain spaces.
10. Select the **Entity to import**. Two entities can be selected, **Users** and **Operators**.
11. Select a partition from the **Partition** drop-down list if required.

11. 4. See *Partitions* System Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows

events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

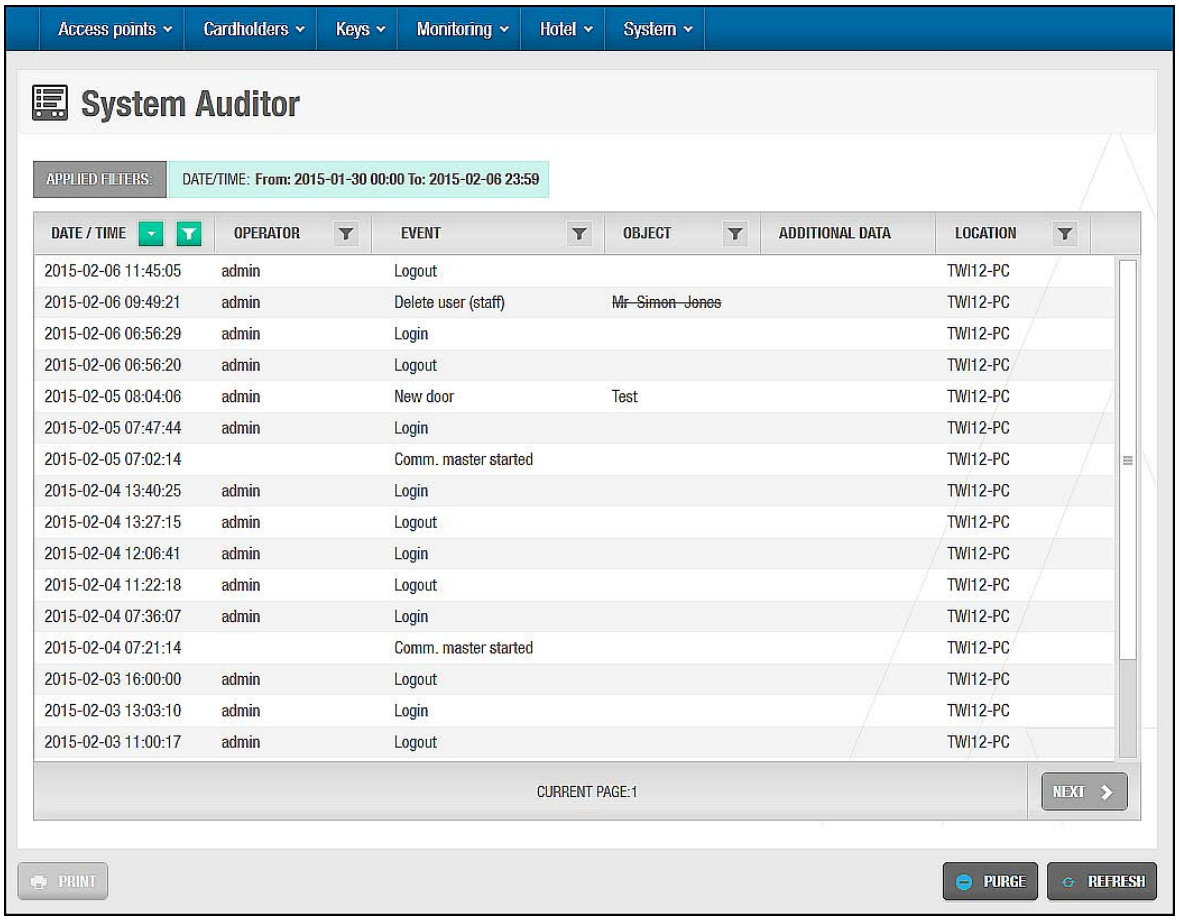


Figure 228: System Auditor information screen

11. 4. 1. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

11. 4. 2. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

12. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

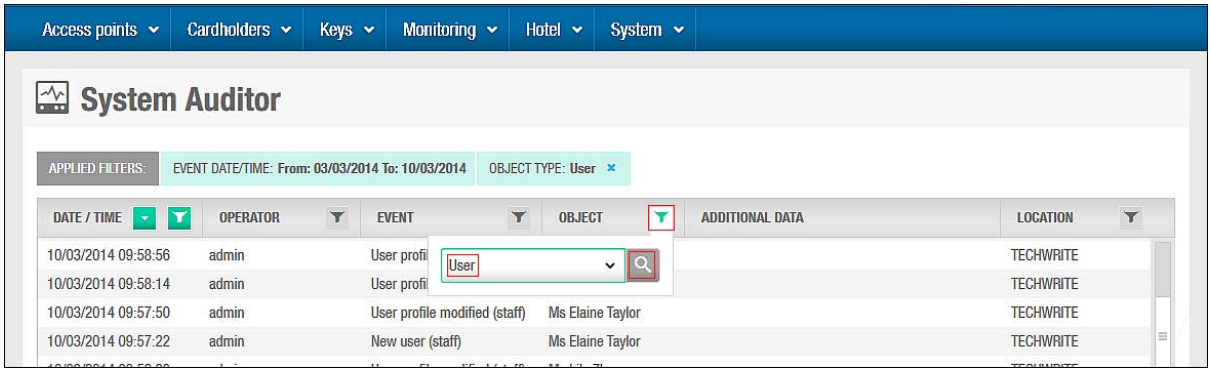


Figure 229: System Auditor information screen

13. Click the **Funnel** icon above the filter item. A search dialog box is displayed.

    For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.

    For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.

    For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.

14. Type your search term.

    Or

    Select a predefined search term from the drop-down list.

    Or

    Select a date range.

    You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.

    However, you cannot remove the **Date/Time** filter.

15. Click the **Search** icon. A filtered audit trail list is displayed.

11. 4. 2. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

11. 4. 3. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic*

System Auditor Purging for more information.

To purge the system auditor, perform the following steps:

16. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
17. Click **Purge**. The **Purge system auditor** dialog box is displayed.

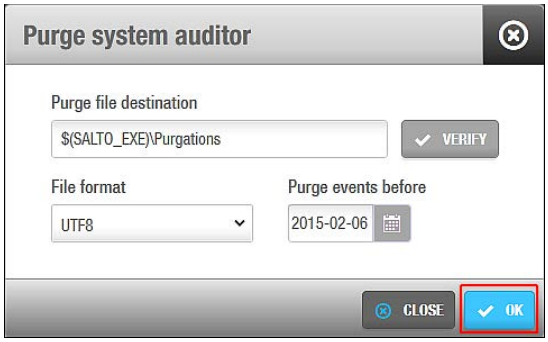


Figure 230: Purge system auditor dialog box

18. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
19. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
20. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
21. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
22. Click **OK**.

11. 5. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

11. 5. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

23. Select **System** > **Operators**. The **Operators** screen is displayed.

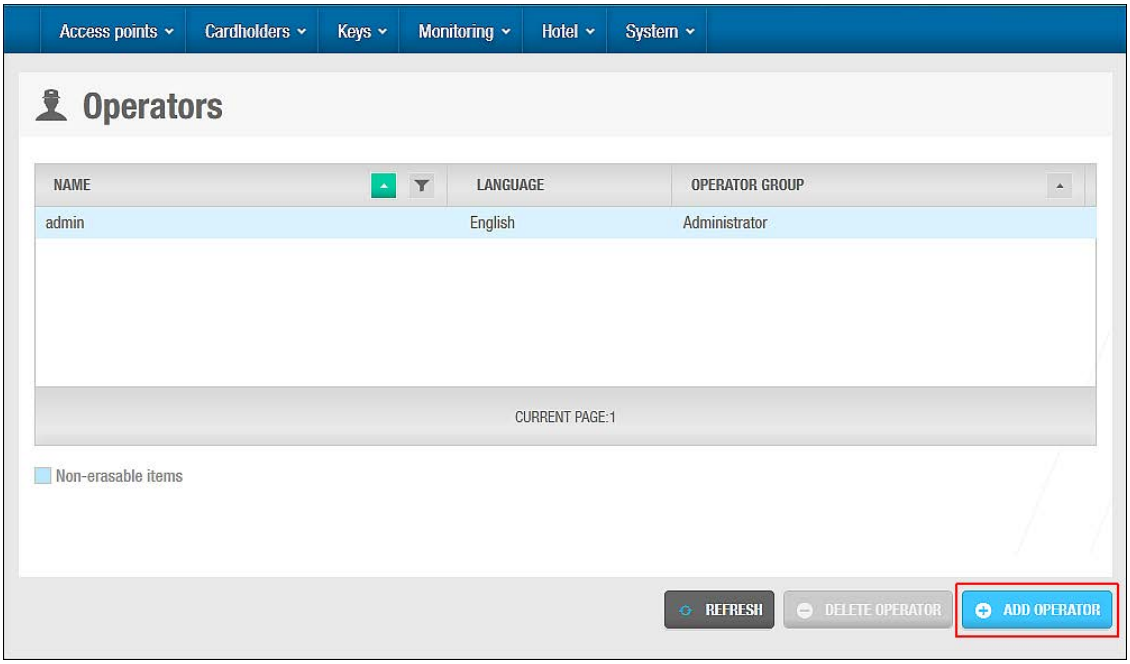


Figure 231: Operators screen

24. Click **Add Operator**. The **Operator** information screen is displayed.

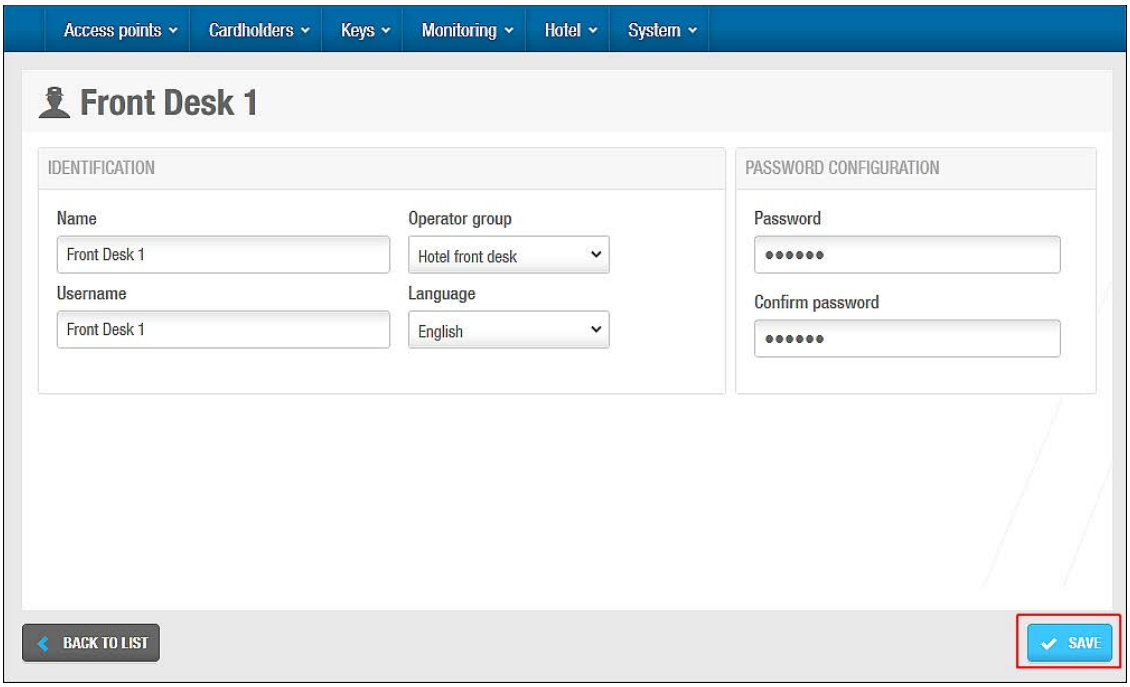


Figure 232: Operator information screen

25. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

26. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

    A maximum of 64 characters can be entered. The user name is not case sensitive.

27. Select the appropriate operator group from the **Operator group** drop-down list.
28. Select the display language for the operator in the **Language** drop-down list.

29. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.

30. Confirm the password.
31. Click **Save**.

11. 6. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

11. 6. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

32. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

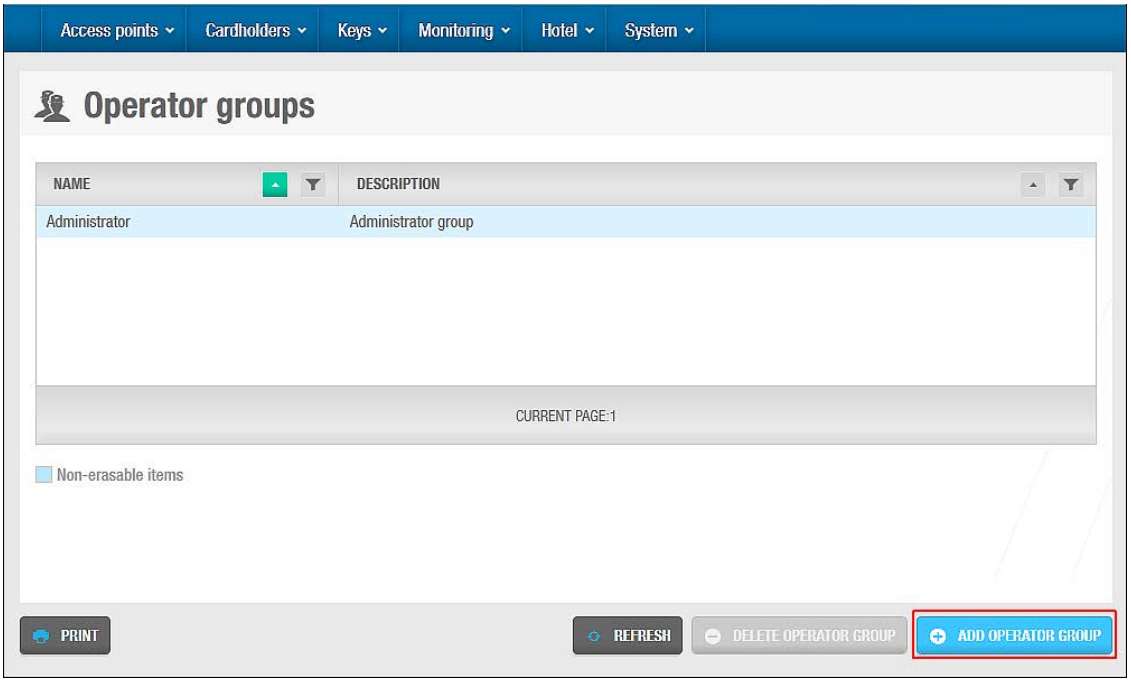


Figure 233: Operator groups screen

33. Click **Add Operator Group**. The **Operator group** information screen is displayed.

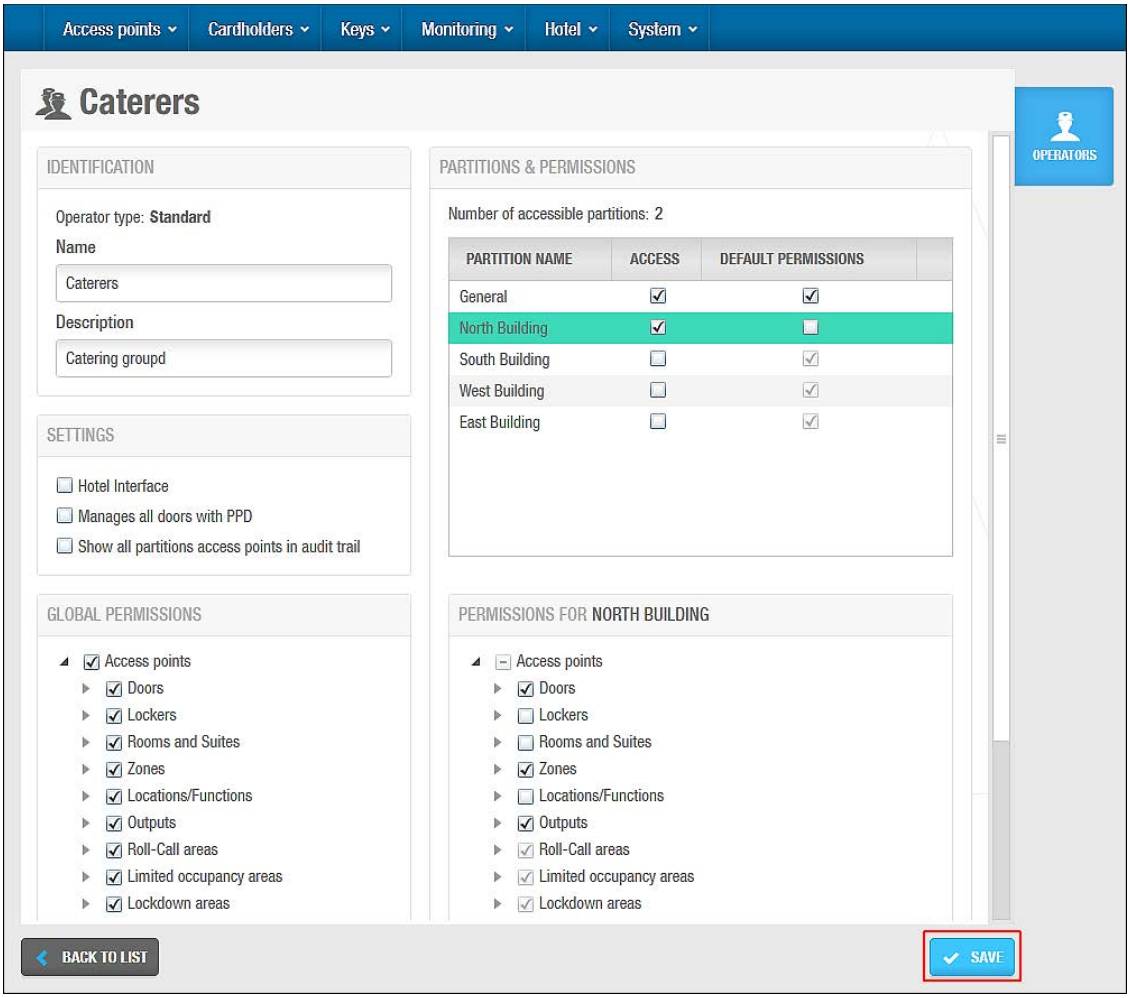


Figure 234: Operator group information screen

34. Type the name of the operator group in the **Name** field.
35. Type a description for the group in the **Description** field.
36. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.
37. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.
38. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes

in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.

39. Click **Save**.

11. 6. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

11. 6. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level **Monitoring** checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors

Permission	Description
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas

Permission	Description
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

11. 6. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

40. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
41. Double-click the operator group with the operator list you want to view.
42. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

    Partitionsfor more information about partitions. The file data is only imported to the partition you select.
43. Click **Next Step**. The **Mapping Configuration** screen is displayed.

11. 6. 2. 1. Step Two: Mapping Configuration

To complete Step two:

1. Click **Add** on the **Mapping configuration** screen. The number **1** is displayed in the **Source Fields** column.
2. Click the arrow on the right-hand side of the entry to view the **Destination Fields** drop-down list.

   The **[Do not import]** option is selected by default. The destination fields are the targeted ProAccess SPACE options. See the *SALTO_Data_Sync* document for a description of these fields.
3. Select the destination field to which you want to map the data from the source field. The selected option is displayed in the **Destination Fields** column.

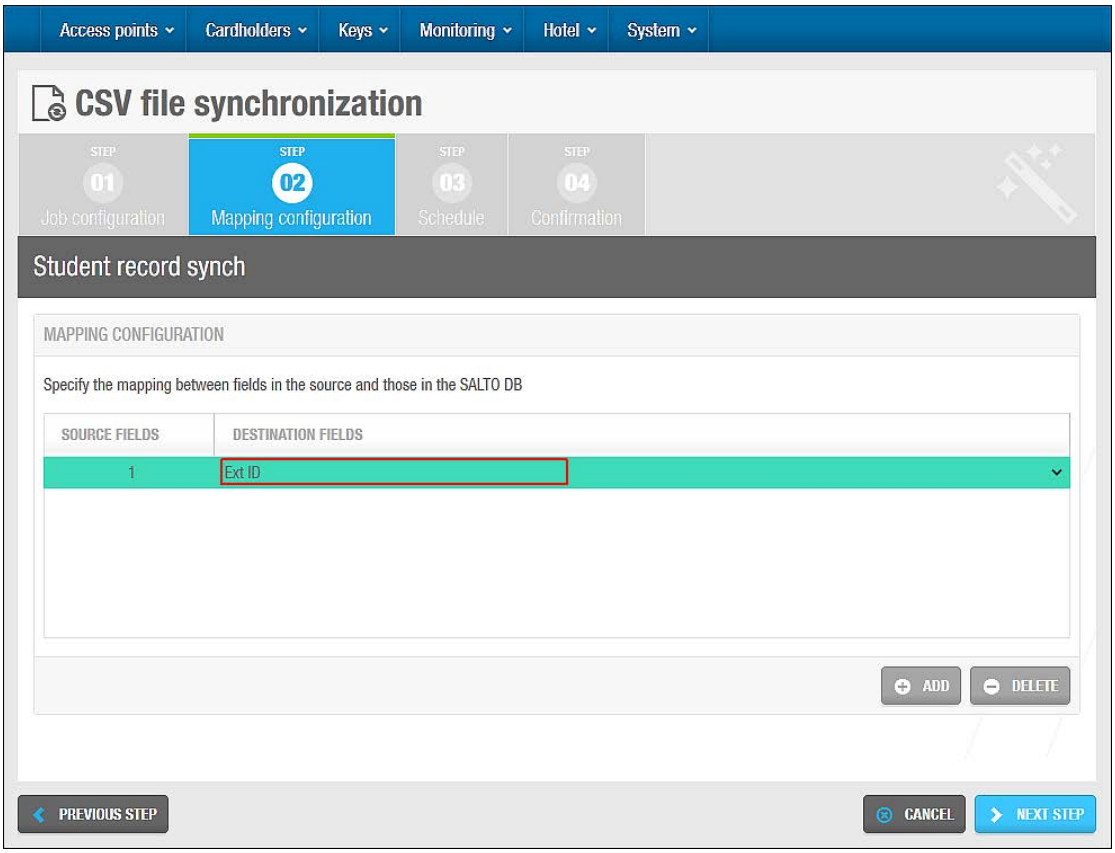


Figure 199: Select destination field

4. Repeat Steps 1, 2, and 3 until you have specified the mapping between all the appropriate source and destination fields and the order of the fields.

NOTE: You must select the **Ext ID** option as one of the destination fields to proceed to the next step. The extension ID is a unique ID that is used to identify users in the system. Selecting this option ensures that the file data is associated with the appropriate users.

5. Click **Next Step**. The **Schedule** screen is displayed.

11. 6. 2. 2. Step Three: Schedule

You can schedule CSV file synchronization to occur as frequently as required, for example, every 24 hours or every second. All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

11. 6. 2. 3. Step Four: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

11. 6. 3. Automatic Database Table Synchronization

Database table synchronization allows you to synchronize user data from external databases with the SALTO database. For example, in a university site, you can synchronize with the data in a human resources database. You can access data stored in an external database and use it to create entries and populate specified fields in ProAccess SPACE.

This means you can automatically transfer data from other databases (rather than entering the same data manually in ProAccess SPACE).

NOTE: See the *Salto_User_Sync_Staging_Table* document for more information about database table synchronization.

The sections below describe how to complete each step in this process.

11. 6. 3. 1. Step One: Job Configuration

To complete Step one:

1. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
2. Click **Add Scheduled Job**. The **Add scheduled job** dialog box is displayed.
3. Select **DB table synchronization** from the drop-down list.
4. Click **OK**. The **Job Configuration** screen is displayed.

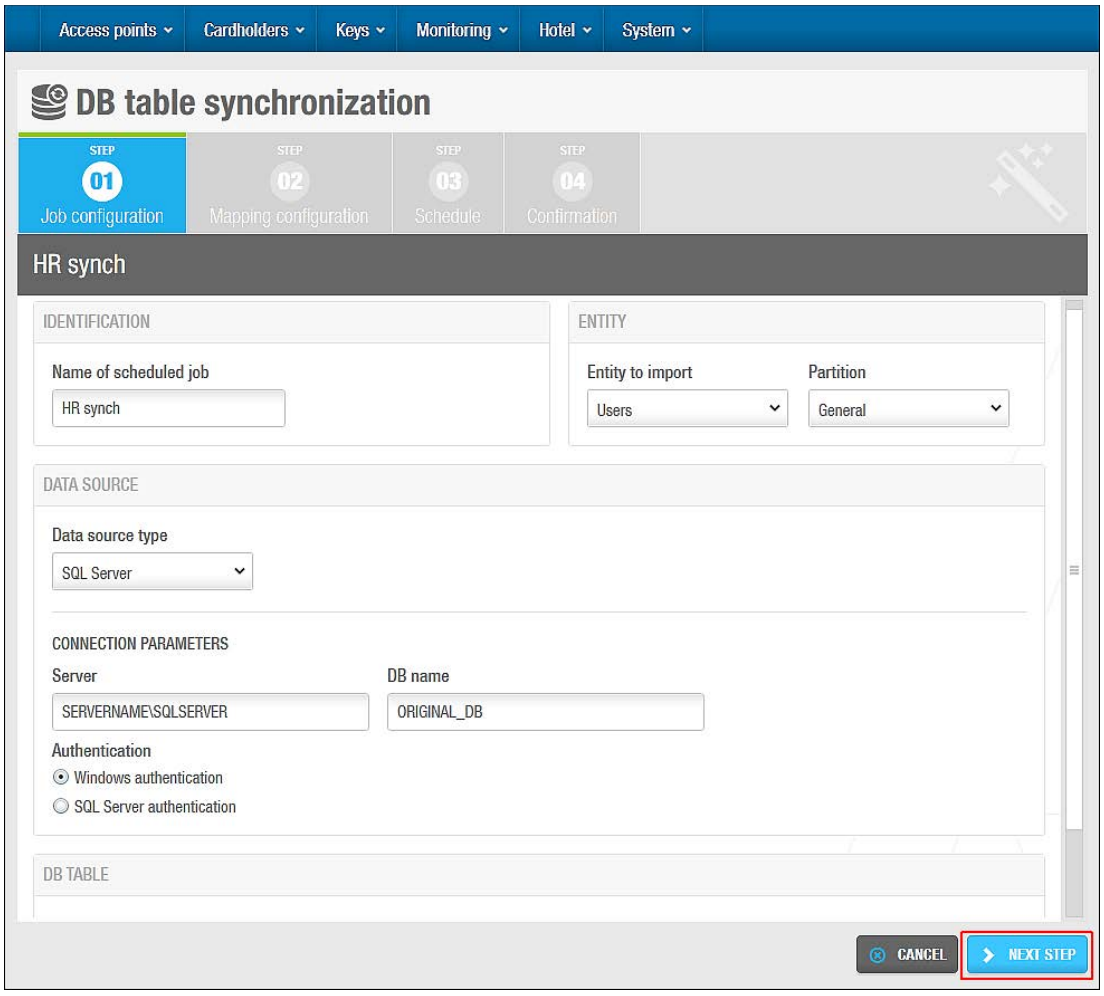


Figure 200: Job configuration screen

5. Type a name for the job in the **Name of scheduled job** field.
6. Select the appropriate data source type from the **Data source type** drop-down list.

   The following options are available:

   - SQL server
   - Oracle
   - ODBC data sources

7. Enter the required information in the fields in the **Connection Parameters** panel.

   The information you must enter in the **Connection Parameters** panel varies depending on which option you select from the **Data source type** drop-down list.
8. Type the name of the database table in the **Table name** field.

   The **Separator** field is automatically populated but you can change the character in this field if required.
9. Select the **Entity to import**. Two entities can be selected, **Users** and **Operators**.
10. Select a partition from the **Partition** drop-down list if required.

    See *Partitions* for more information about partitions. The data is only imported to the partition you select.
11. Click **Next Step**. The **Mapping configuration** screen is displayed.

11. 6. 3. 2. Step Two: Mapping Configuration

To complete Step two:

1. Click **Add** on the **Mapping configuration** screen. The number **1** is displayed in the **Source Fields** column.
2. Click the arrow on the right-hand side of the entry to view the **Destination Fields** drop-down list.

   The **[Do not import]** option is selected by default. The destination fields are the available SALTO database fields to which you can import data. Once imported into the SALTO database, the information is then displayed in the appropriate field in ProAccess SPACE. See the *Salto_User_Sync_Staging_Table* document for a description of these fields.
3. Select the destination field to which you want to map the data from the source field. The selected option is displayed in the **Destination Fields** column.

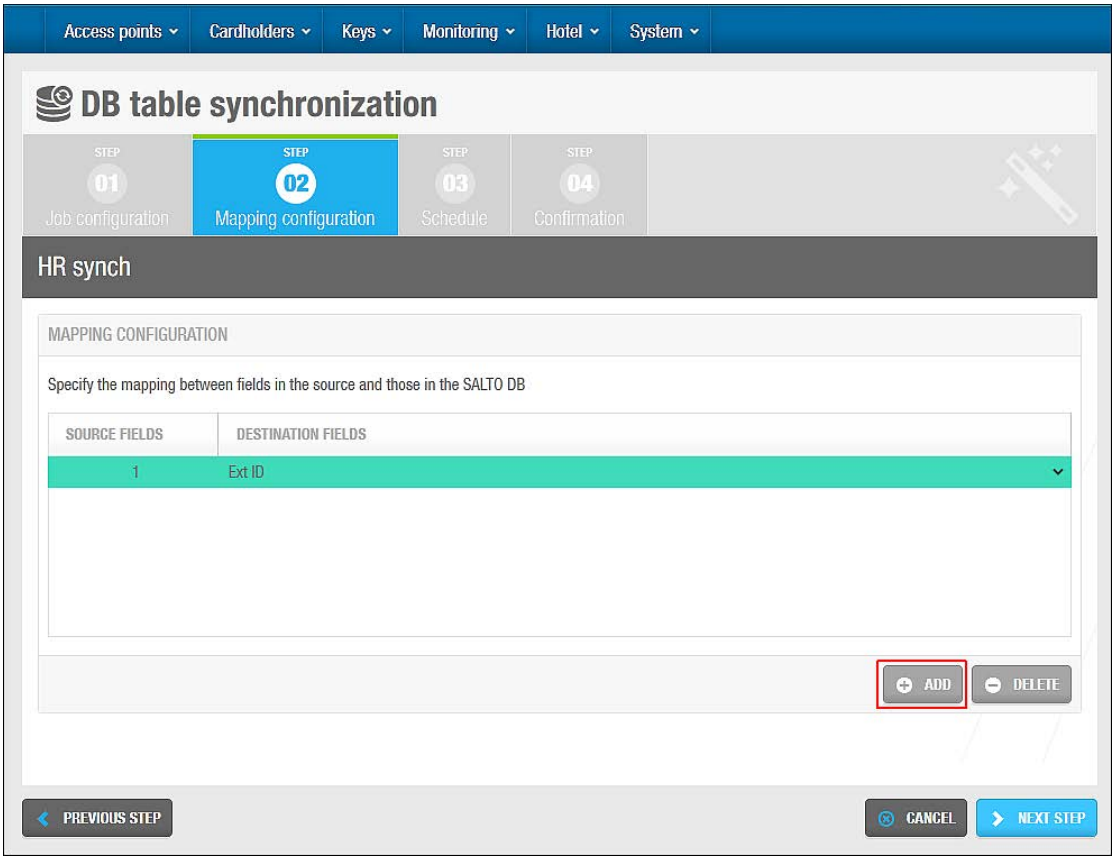


Figure 201: Select destination field

4. Repeat Steps 1, 2, and 3 until you have specified the mapping between all the appropriate source and destination fields and the order of the fields.

   You must select the following options as destination fields to proceed to the next step:

   - Ext ID
   - Control field (to be processed by SALTO)
   - Control field (processed date/time)
   - Control field (error code)
   - Control field (error message)

   The system uses these fields to write a report after database table synchronization occurs. If all of these options are not selected, the synchronization job cannot be performed.
5. Click **Next Step**. The **Schedule** screen is displayed.

11. 6. 3. 3. Step Three: Schedule

All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

11. 6. 3. 4. Step Four: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

11. 6. 4. Automatic Audit Trail Exports

You can export audit trail data from the SALTO database as a CSV file. This allows you to use the data in another system, for example, a time recording system.

NOTE: When you export audit trail data, you can still access the data in ProAccess SPACE as it is not removed. However, when you purge the audit trail, the data is permanently removed from the audit trail and the database. See *Automatic Audit Trail Purging* for more information.

See also the S*altoAutomaticExportOfAuditTrail* document for more information about exporting audit trail data.

The sections below describe how to complete each step in this process.

11. 6. 4. 1. Step One: Job Configuration

To complete Step one:

1. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
2. Click **Add Scheduled Job**. The **Add scheduled job** dialog box is displayed.
3. Select **Audit trail export** from the drop-down list.
4. Click **OK**. The **Job Configuration** screen is displayed.

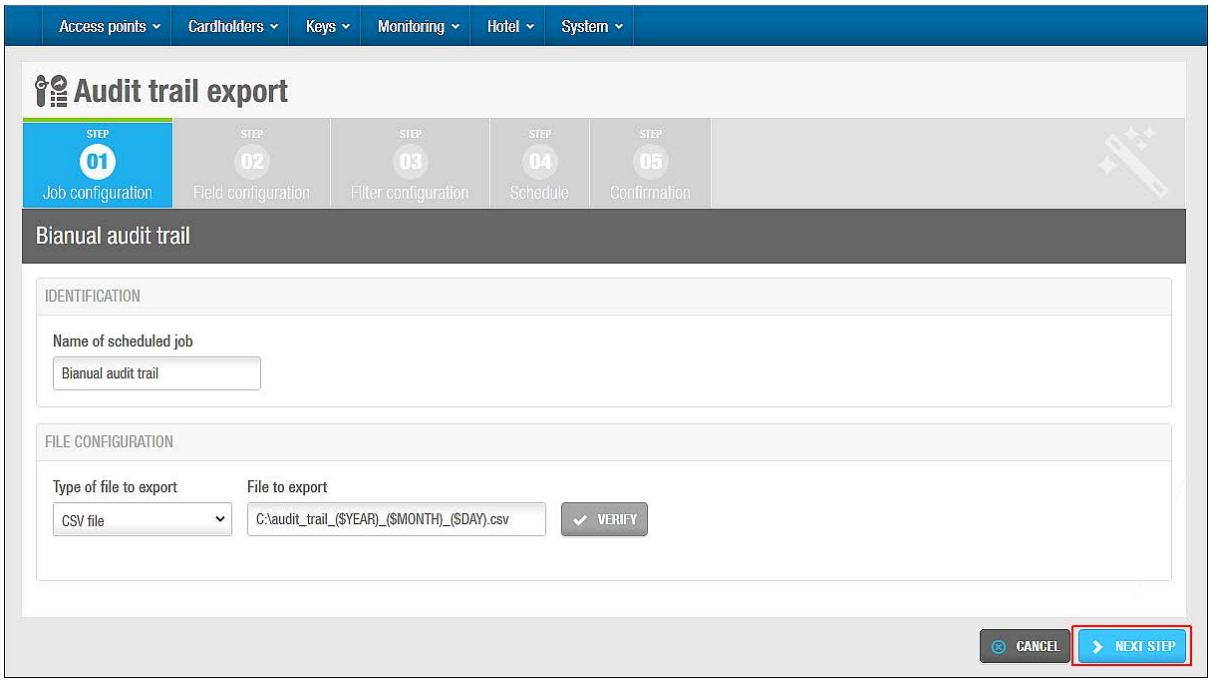


Figure 202: Job configuration screen

5. Type a name for the job in the **Name of scheduled job** field.

   The default option in the **Type of file to export** field is a CSV file. This option cannot be changed.
6. Type a name for the file that you want to export in the **File to export** field.
7. Press F2 to display the **File path** dialog box and insert macros in the file name if required.

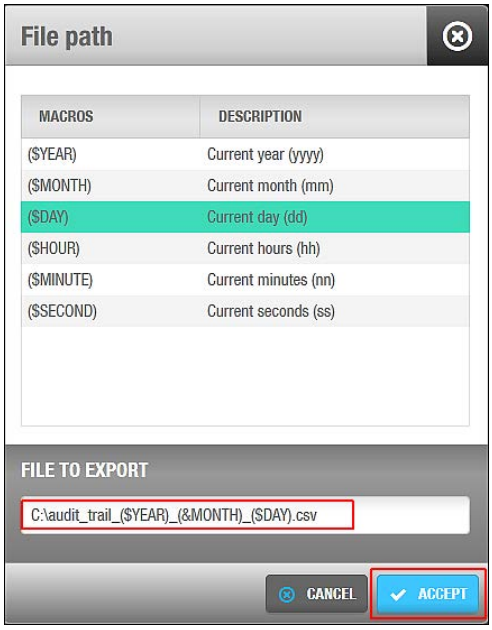


Figure 203: File path dialog box

Using macros, for example, ($YEAR), allows you to save the file with a unique name so it is not overwritten by the next file that is created.

8. Double-click the appropriate macro to insert it in the file name.

   Each macro you insert is displayed in the file name in the **File To Export** field.

9. Click **Accept** when you have finished inserting macros and the appropriate file name is displayed in the **File To Export** field.

   You can click **Verify** on the **Job configuration** screen to verify the file directory exists and is correct.

10. Click **Next Step**. The **Field configuration** screen is displayed.

11. 6. 4. 2. Step Two: Field Configuration

To complete Step two:

1. Select a format from the **File format** drop-down list on the **Field configuration** screen.

   This specifies the format of the file containing the exported audit trail data.

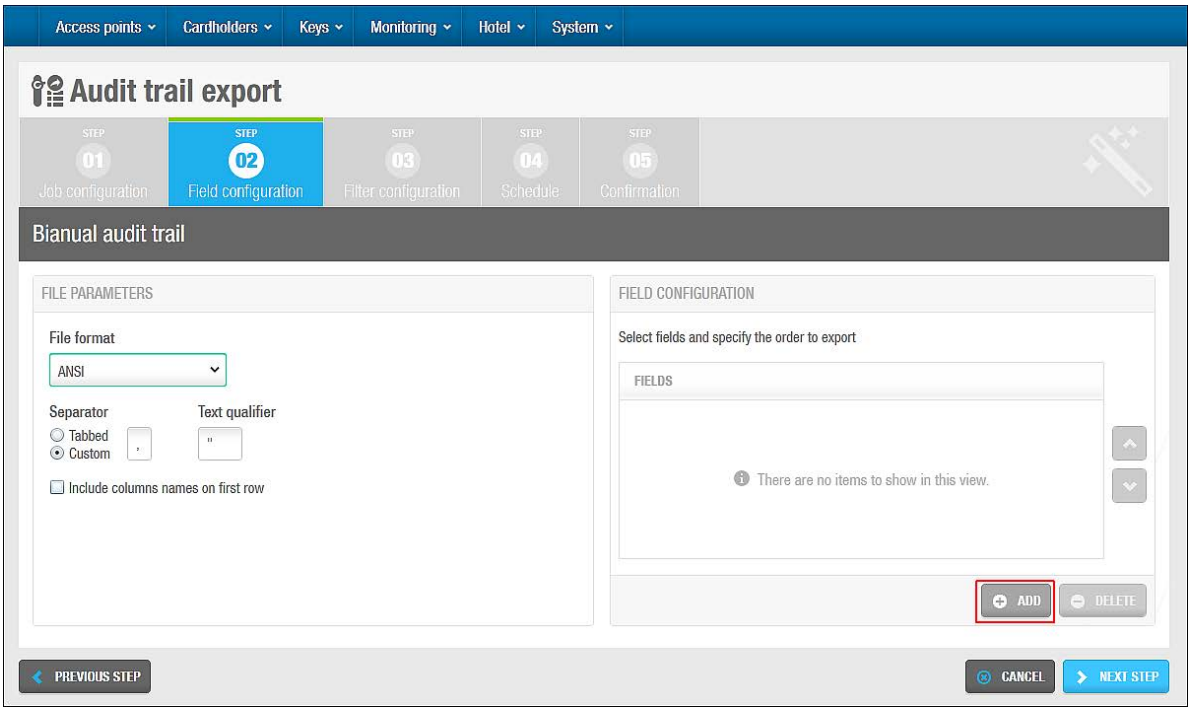


Figure 204: Field configuration screen

2. Select either the **Tabbed** or **Custom** option.

   This specifies how the audit trail data is stored in the file. The **Separator** and **Text qualifier** fields are automatically populated but you can change the characters in these fields if required.
3. Select the **Include column names on first row** checkbox if required.

   If you select this, the column names are included in the first row of the file.
4. Click **Add** in the **Field configuration** panel. The **Select fields** dialog box, showing a list of fields, is displayed.

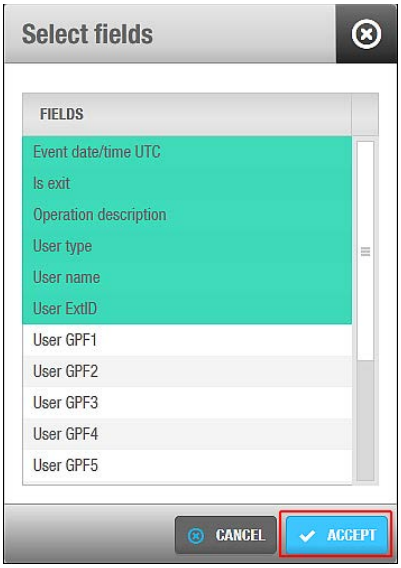


Figure 205: Select fields dialog box

   See the *SaltoAutomaticExportOfAuditTrail* document for a description of these fields.
5. Select the required fields.

You can hold down the Ctrl key while clicking the fields to make multiple selections.

6. Click **Accept**. The selected fields are displayed in the **Fields** list on the **Field configuration** screen.

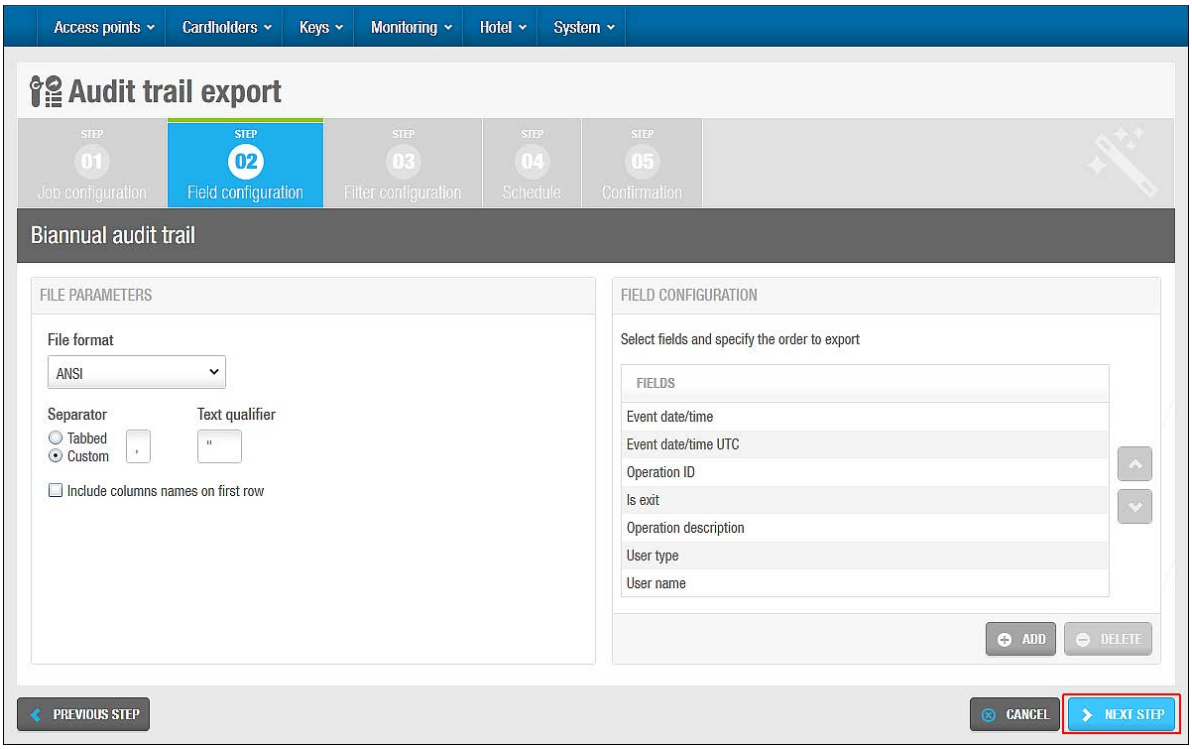


Figure 206: Select field

The order of the fields in the **Fields** list determines the order in which the fields are exported. You can select fields and click the up and down chevrons to change the order of the fields if required.

7. Click **Next Step**. The **Filter configuration** screen is displayed.

11. 6. 4. 3. Step Three: Filter Configuration

The filter configuration step allows you to filter the type of audit trail data that is exported within a specified time period. The default option is to export all of the audit trail data within the previous 12-month period.

You can filter audit trail events by the following:

- Cardholders and/or operators
- Access points
- Operations
- Date and time period

To complete Step three:

1. Click **Add/Delete** in the **Who** panel on the **Filter configuration** screen. The **Add/Delete** dialog box, which contains a list of cardholders and operators on two tabs, is displayed.

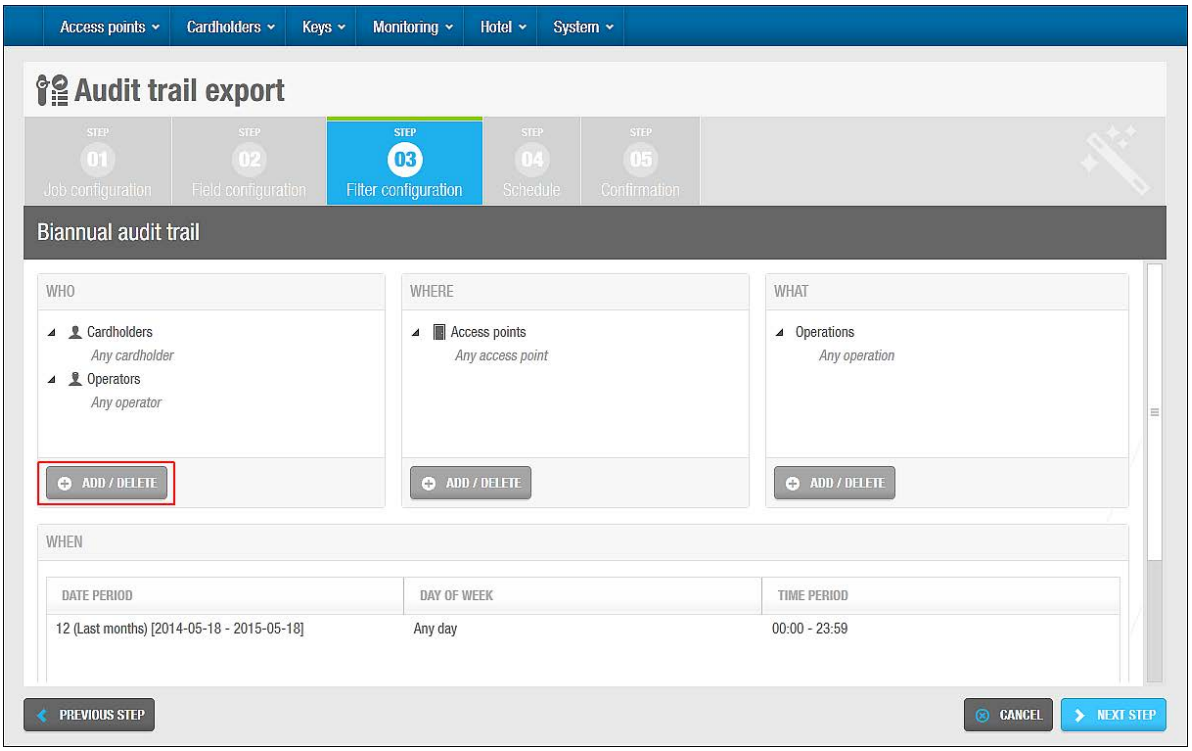


Figure 207: Filter configuration screen

2. Select the required cardholders in the left-hand panel and click the chevron. The selected cardholders are displayed in the right-hand panel.

   You can hold down the Ctrl key while clicking the fields to make multiple selections. As soon as you select a cardholder, the default **Any cardholder** option is automatically moved to the left-hand panel. You can use the default option if you want to export audit trail data for all the cardholders in the system.
3. Click the **Operators** tab if you also want to filter by operator. A list of operators is displayed.
4. Select the required operators in the left-hand panel and click the chevron. The selected operators are displayed in the right-hand panel.
5. Click **Accept**. The selected cardholders and operators are displayed in the **Who** panel.
6. Follow the procedure described in Steps 1, 2, and 5 to add the access points you want to filter to the **Where** panel.
7. Follow the procedure described in Steps 1, 2, and 5 to add the operations you want to filter to the **What** panel.
8. Click **Add/Delete** in the **When** panel. The **Add/delete periods** dialog box, showing the default period, is displayed.

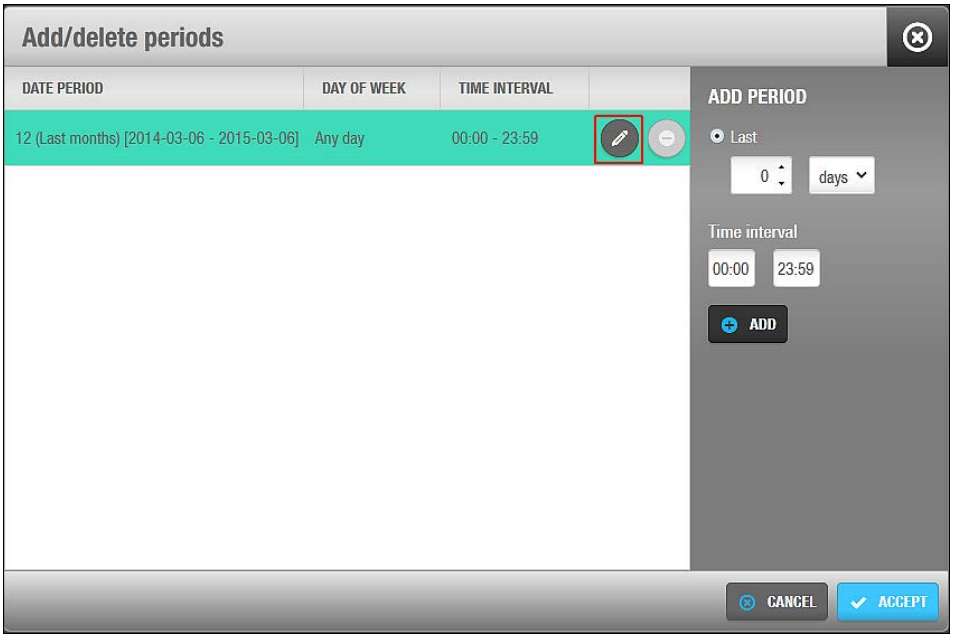


Figure 208: Add/delete periods dialog box

9. Click the **Edit** icon to change the date period and time interval if required.

   You can also click **Add** to add additional periods. For example, you can add a period to export the audit trail data between 09:00 and 11:00 each day within a specified date period, and add another period to export the audit trail data between 14:00 and 17:00 each day within the same date period.
10. Click **Accept** when you have finished editing or adding periods. The changes are displayed in the **When** panel.

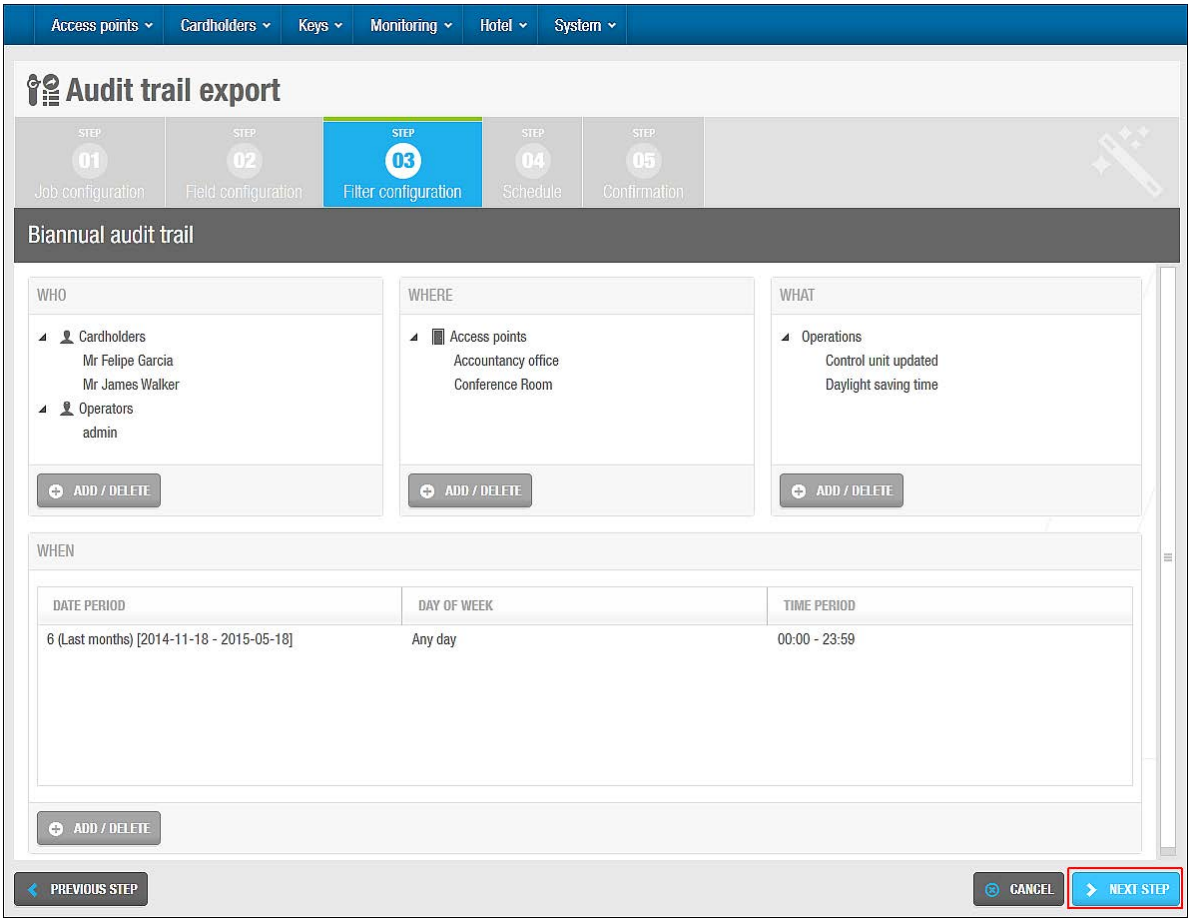


Figure 209: Edit period

11. Click **Next Step**. The **Schedule** screen is displayed.

11. 6. 4. 4. Step Four: Schedule

All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

11. 6. 4. 5. Step Five: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

11. 7. Manual Synchronization

You can manually perform the following synchronization jobs on the system:

- CSV file synchronization
- Database table synchronization

You can start these jobs by selecting **System** > **Synchronization** and completing each step in the configuration process. Alternatively, you can schedule either of these jobs to be performed automatically on the **Scheduled jobs** screen. See *Automatic CSV File Synchronization* and *Automatic Database Table Synchronization* for a description of how to complete the required steps for each job.

NOTE: The scheduling steps in the sections referenced above are not relevant when you are manually performing CSV file synchronization or database table synchronization jobs.

11. 8. Making Database Backups

Database backups can be made from the SALTO system:

- Using ProAccess SPACE's **System** > **Make DB Backup** option

By default, system backups are stored in an SQL backup folder. For example:

C:\Program Files\Microsoft SQL Server\MSSQL12.SQLEXPRESS\MSSQL\Backup

Note that the SQL folder name may vary slightly depending on which SQL version is installed. It is recommended to create all SQL backups in this folder. The backup file is saved with a .bak extension.

NOTE: Automatic database backups are scheduled on the system by default. See *Automatic Database Backups* for more information.

To make a database backup in ProAccess SPACE, perform the following steps:

1. Select **System** > **Make DB Backup**. The **Make DB Backup** dialog box is displayed.

Figure 210: Make DB Backup dialog box

2. Type a file path based on the database server file system or backup file name.
3. Click **OK**. The database backup is performed. A pop-up is displayed confirming that the operation was completed successfully.
4. Click **OK**.

11. 8. 1. Restoring Database Backups

You cannot restore a backup while ProAccess SPACE is connected to an existing backup. The database backup can be restored using **Microsoft Management Studio** or the SALTO **DB Utils for RW-ProAccess Space** tool. For more info, please contact your SALTO technical support.

11. 9. Events Streams

The events stream functionality allows third parties to receive real-time notifications about events that occur (for example, a door opened by a particular cardholder) within the SALTO system. See the *Stream of events from the Salto software* document for more information.

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

An events stream conveys the following information about an event:

- Who produced it (for example, the cardholder)
- When it was produced (for example, the date/time)
- Where it was produced (for example, the location of the door)
- What type of event was produced (for example, the door was opened)

The aim of the events stream is to filter the audit trail. See *Audit Trails* for more information about audit trails. Sending selected events in the appropriate order to the system enables it to process the received information and perform real-time actions.

You must complete these steps within the wizard to create an events stream:

1. Configure the general settings.
2. Select the data fields.
3. Specify the parameters.
4. Confirm the configuration settings.

11. 9. 1. Step 1: Configuring the General Settings

The first step of creating an events stream is to provide general information such as the formatting and encoding of the events stream.

To provide the general information, perform the following steps:

1. Select **Tools** > **Events streams**. The **Events streams list** dialog box is displayed.
2. Click **New**. The **Events stream configuration** dialog box is displayed.

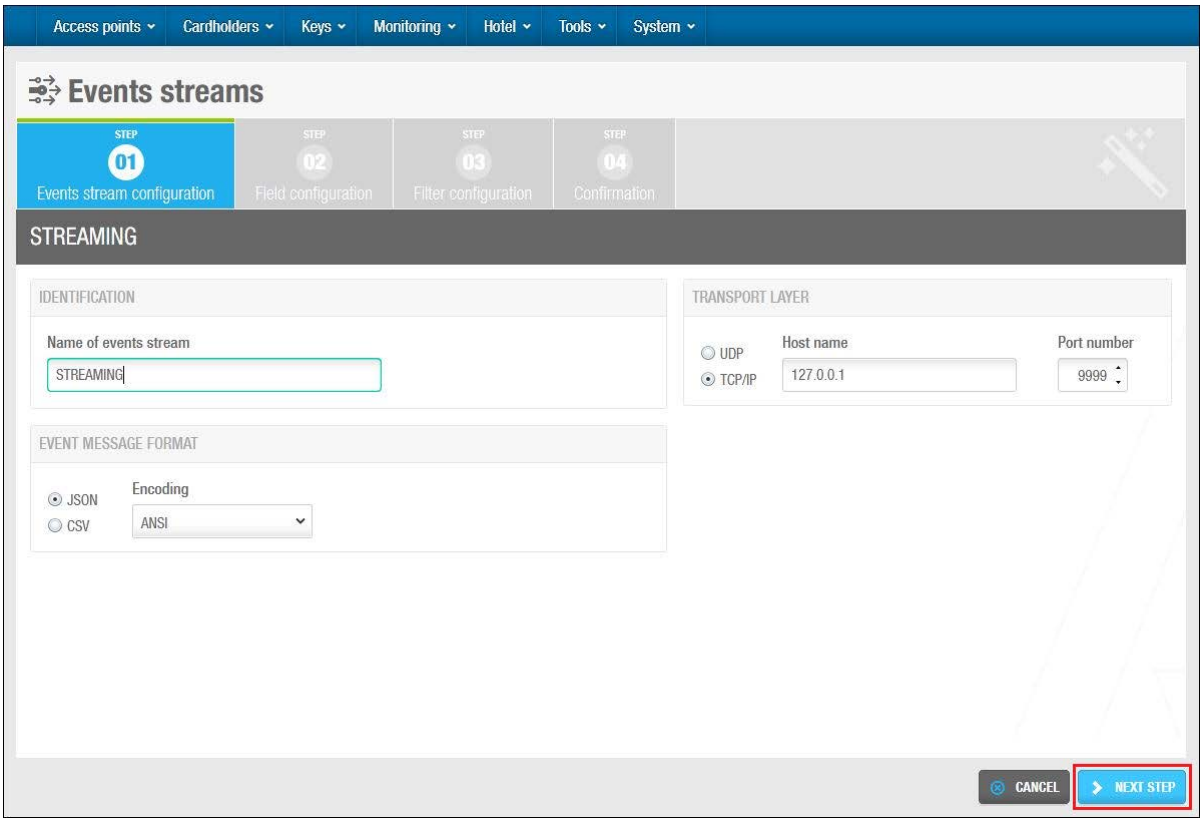


Figure 211: Events stream configuration dialog box

3. Click **Next**.
4. Type the events stream name in the **Name of events stream configuration** field.
5. Select either **UDP** or **TCP/IP** in the **Transport layer** panel.

   Event streams can be received through UDP or TCP/IP protocols.
6. Type the machine name in the **Host name** field and the port number in the **Port number** field.

   Event streams will be notified through the machine name and port number of the listening socket you specify.
7. Select either **JSON** or **CSV** in the **Event message format** panel.

   JSON uses a string format. CSV uses a list format where a list of field values is separated by a semi-colon. See examples of each below.


```
[
{
"EventID" : "11223344556677889900",
"EventDateTime" : "2012-04-14T13:03:20",
SALTO HAMS……p.321
"EventTime" : "13:03:20",
"EventDateTimeUTC" : "2012-04-14T11:03:20Z",
"OperationID" : 17,
"OperationDescription": "Door opened: key",
"IsExit" : false,
"UserType" : 0,
"UserName" : "John Smith",
"UserGPF3" : "Marketing department",
"DoorName" : "Gym",
"DoorGPF1" : "Leisure area",
}
]
```


Figure 212: JSON format


```
EVENT_START "11223344556677889900"; 2012-04-14T13:03:20;
13:03:20; 2012-04-14T13:03:20z; 17; "Door opened: key"; false; 0;
"John Smith"; "Marketing department"; "Gym"; "Leisure area"
EVENT_END
```


Figure 213: CSV format

8. Select the applicable character encoding from the **Encoding** drop-down list.

   You can select ANSI, UTF-8, Unicode, or Unicode Big Endian.
9. Click **Next**. The dialog box to select the data fields is displayed.

   You can also click **Back** on any step to return to the previous dialog box.

11. 9. 2. Step 2: Selecting the Data Fields

After you provide the general information about the events stream, you need to select the data fields for the events stream.

To select the data, perform the following steps:

1. Click **Add/ Delete**. The **Select fields** dialog box is displayed.

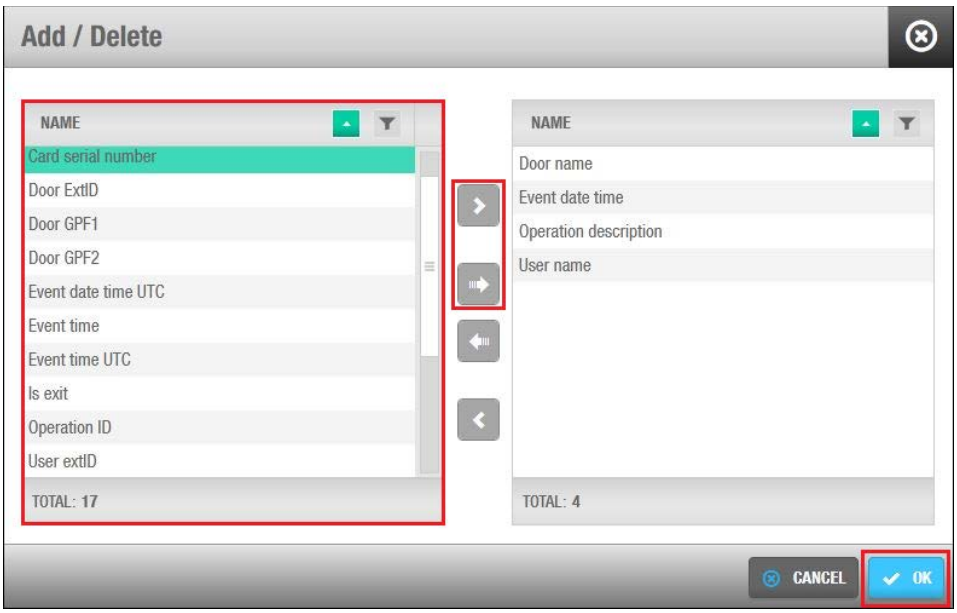


Figure 214: Select fields dialog box

2. Select the data fields that will be sent as part of the events stream.

   The fields listed here match the information passed by keys to the SALTO SQL DB and to the third-party systems.
3. Click the chevron to transfer the selected fields to the right side of the dialog box.
4. Click **Ok**. The fields you selected are displayed. Note that if you want to have a specific order in the list, you must select them one at a time. When the fields are added to the list, you cannot change the order.

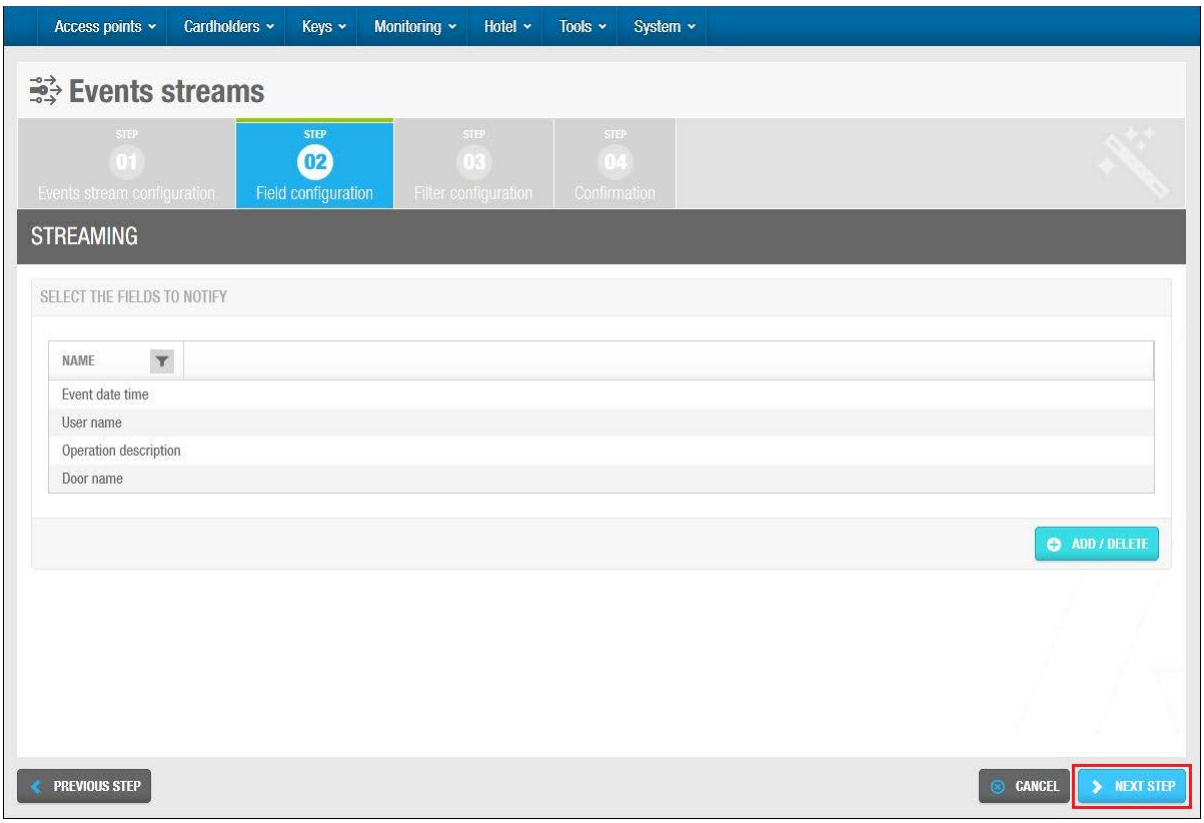


Figure 215: Selected fields displayed

5. Click **Delete** if you want to remove entries from this field.

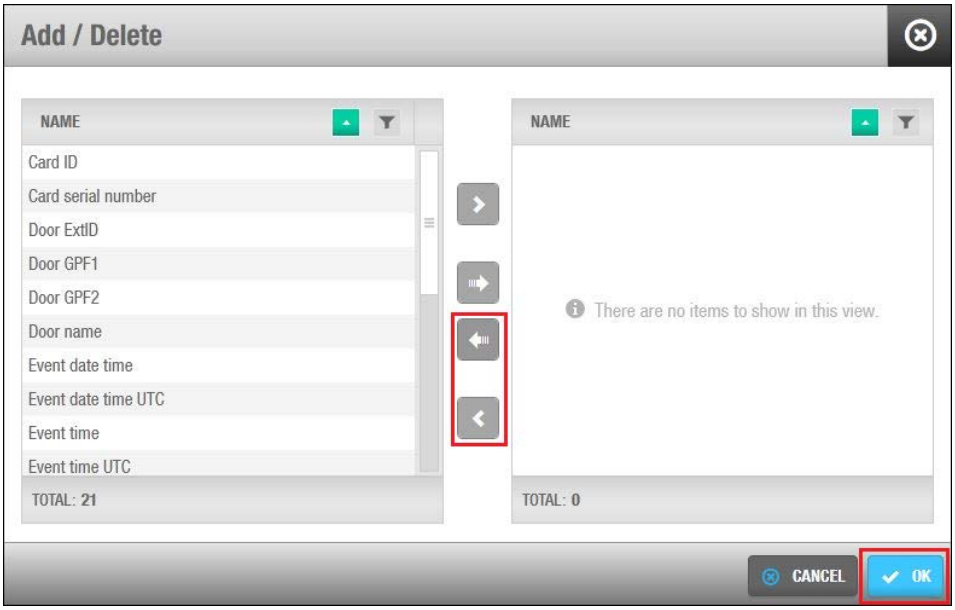


Figure 216: Deselecting fields displayed

6. Click **Next**. The **Who**, **Where**, **What**, and **When** panels and the **Real time window** fields are displayed.

11. 9. 3. Step 3: Specifying the Parameters

After you select the data fields for the events stream, you need to specify the parameters, for example, the location and type of event, for the events stream.

To specify the parameters, perform the following steps:

1. Select **Users** in the **Who** panel.

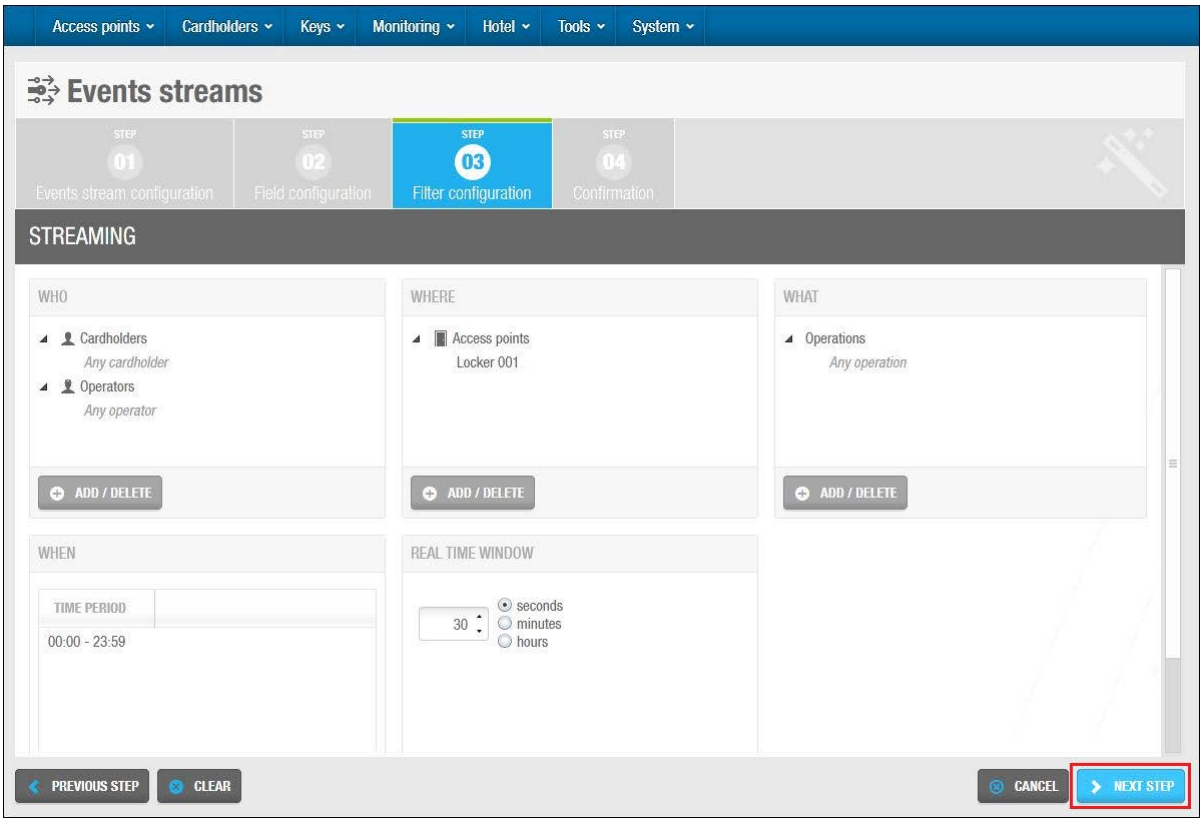


Figure 217: Panels and the Real time window

2. Click the **Add/remove items** button below the **Who** panel. The **Who** dialog box, showing a list of cardholders, is displayed.

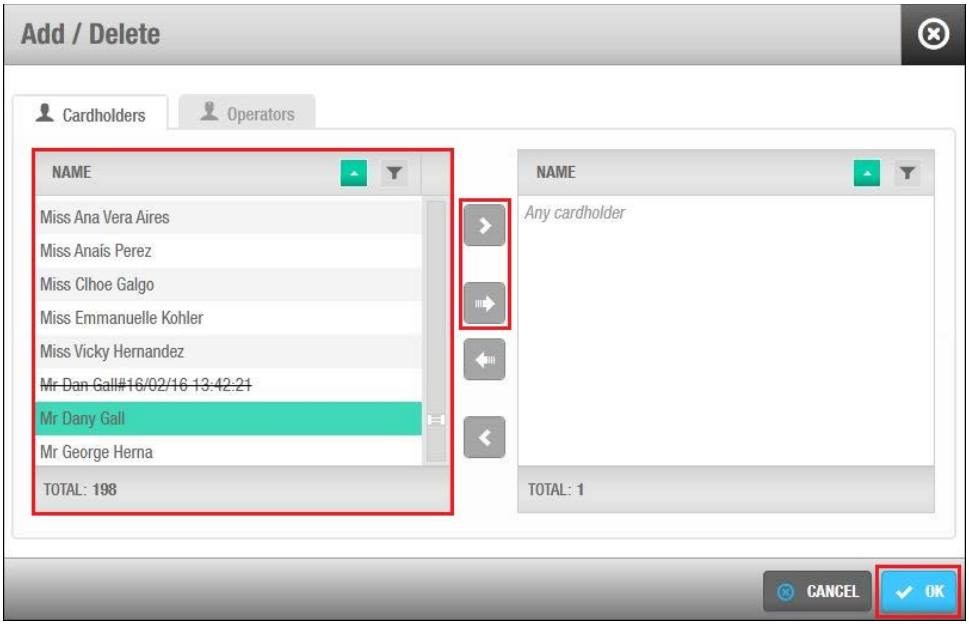


Figure 218: Who dialog box

3. Select the required user in the **Non-selected items** panel and click the arrow. The selected user is displayed in the **Selected items** panel.

   By default, **Any cardholder** is displayed in the **Selected items** panel. This means that all users are included in the events stream. To remove this value, select **Any cardholder**

in the **Selected items** panel and click the inverted arrow. **Any cardholder** is displayed in the **Non-selected items** panel. You must repeat these steps if you want to remove **Any operator** from **Operators**, **Any door** from **Doors**, and **Any operation** from **Operations**, as applicable.

4. Click **Ok**.
5. Click the **Operators** tab.
6. Repeat the above steps for operators.
7. Click **Ok**.

   The selected users and operators are displayed in the **Who** panel.

8. Repeat the above steps to select the required doors in the **Where** panel.
9. Repeat the above steps to select the required operations in the **What** panel.
10. Click **Add** below the **When** panel. The **Select period** dialog box is displayed.

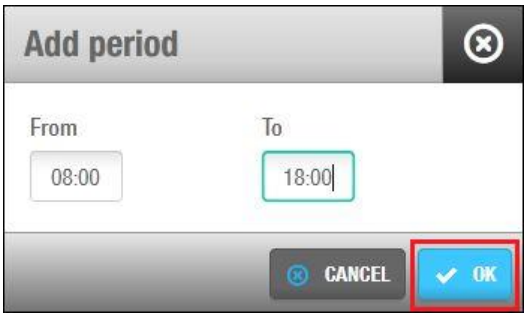


Figure 219: Select period dialog box

11. Select the applicable time interval using the arrows in the **From** and **To** fields.

    This specifies the active period for the events stream. In the above example, the system only sends events during the period 08:00 to 18:00.

12. Click **Ok**. The selected time interval is displayed in the **When** panel.
13. Specify the frequency of events stream notifications by typing the applicable number in the **Real time window** field and selecting either **seconds**, **minutes**, or **hours**, as applicable.

    For example, if you specify 30 seconds, the system only sends events created 30 seconds ago or less.

11. 9. 4. Confirming the Configuration Settings

After you specify the parameters for the events stream, you need to confirm the configuration settings.

To do this, perform the following steps:

1. Click **Next**. The events stream configuration settings are displayed.

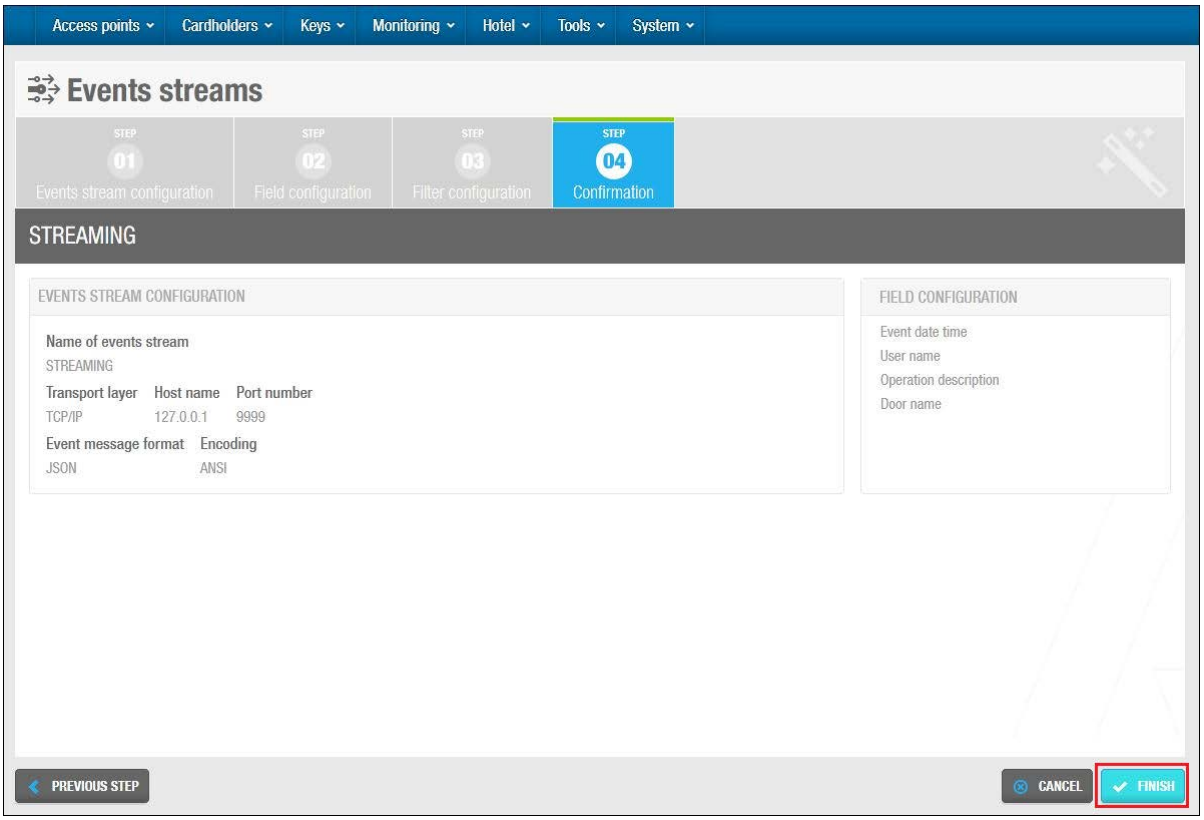


Figure 220: Select period dialog box

2. Click **Finish**. A message is displayed confirming that the changes will not take effect until you restart the SALTO Service.

   The events stream you created is displayed in the **Events streams list** dialog box.

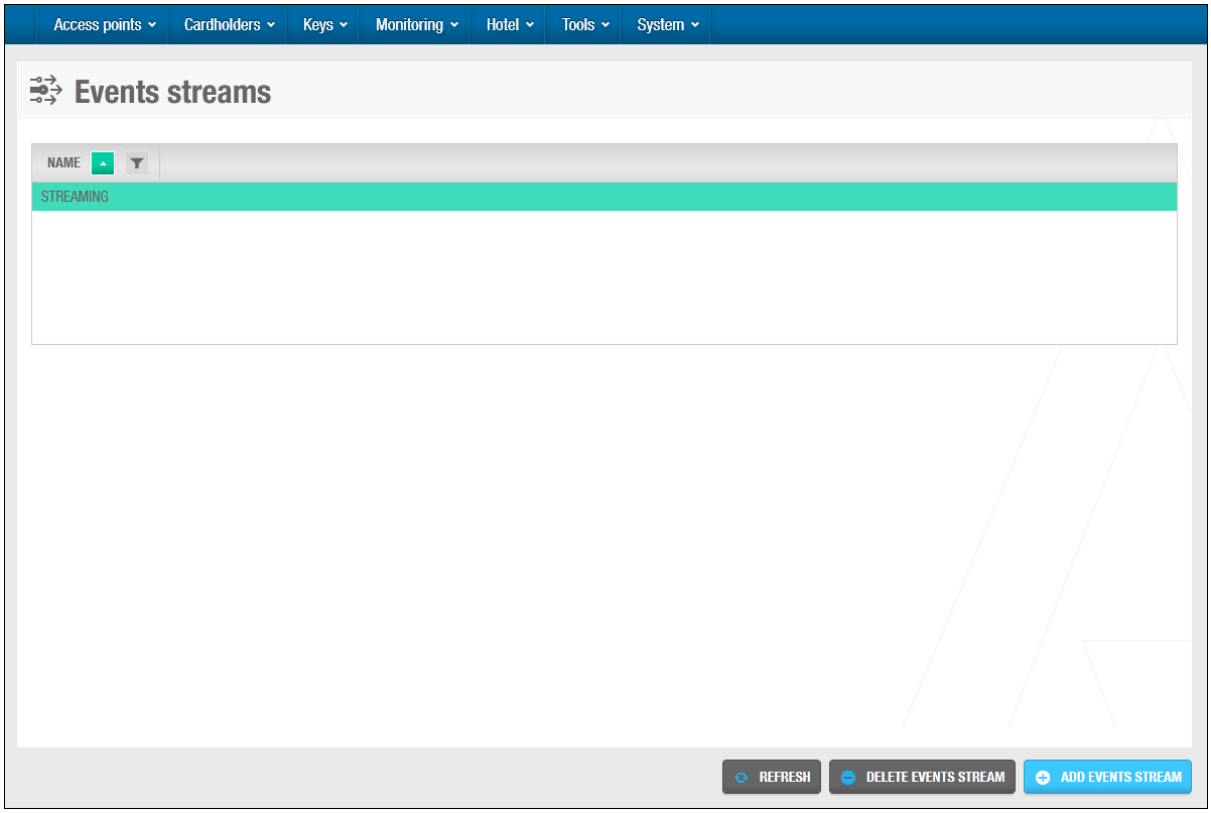


Figure 221: Created event stream

3. Click **Close**.

11. 10. Card printing

You can create badge templates within ProAccess SPACE and print these templates as user cards (keys). You can create card templates for different users in your organization. For example, you can create one template for day staff and a different template for night staff.

To create a badge template, perform the following steps:

1. Select **Tools** > **Card template list**. The **Card template list** screen is displayed.

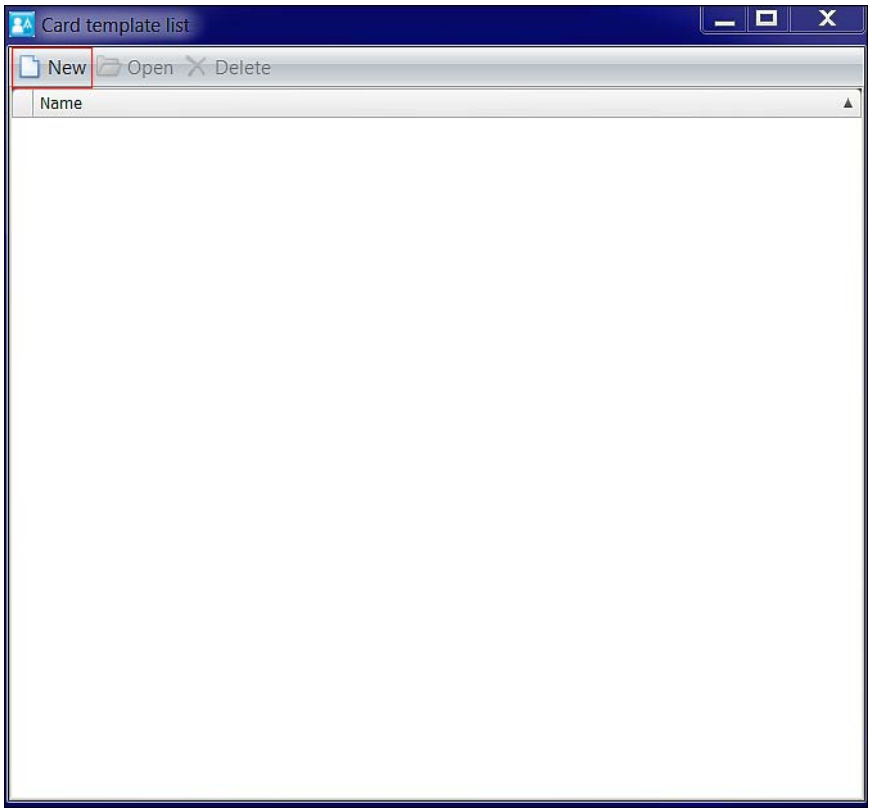


Figure 222: Card template list screen

2. Click **New**. The **New** dialog box is displayed.

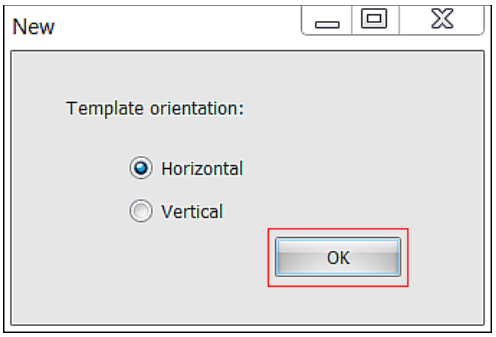


Figure 223: New dialog box

3. Select either **Horizontal** or **Vertical** as your template orientation and click **OK**. The **Card template design** screen is displayed.

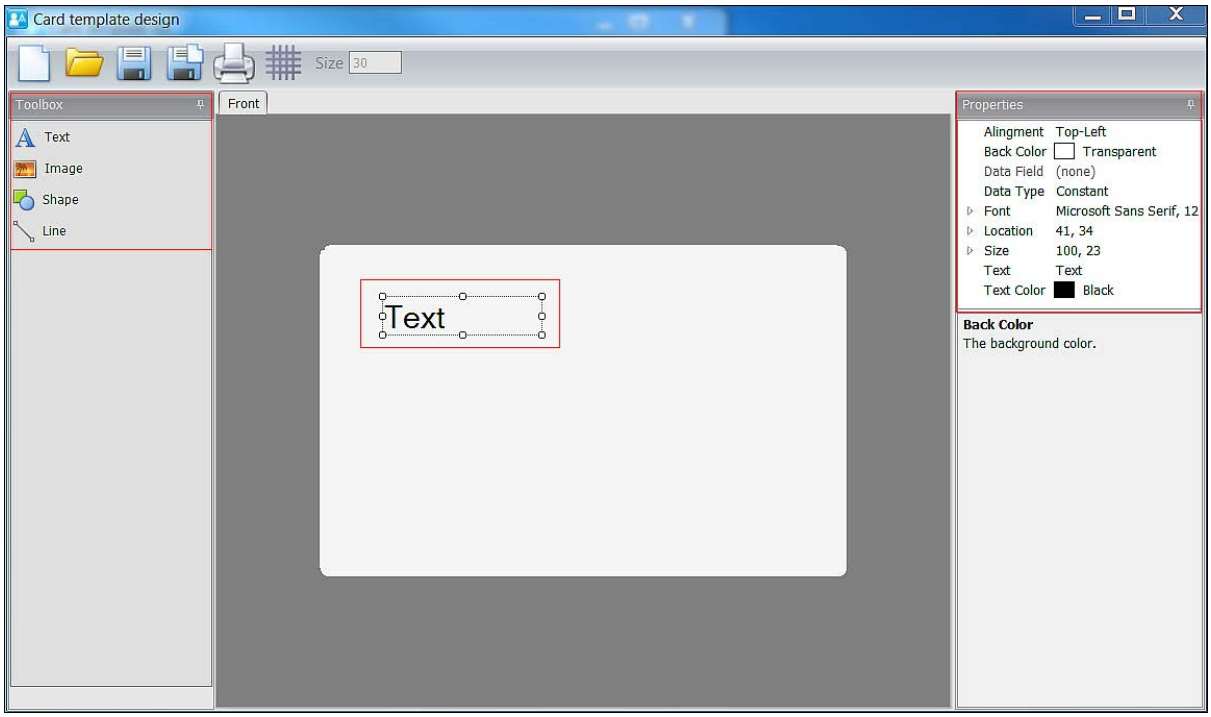


Figure 224: Card template design screen

The **Toolbox** section within the **Card template design** screen is comprised of four features:

- Text
- Image
- Shape
- Line

After you select any of the **Toolbox** features, you can customize it on the blank template in the centre of the screen. When you select the feature on the template, a **Properties** menu, specific to the feature, is displayed in the top right of the screen.

The four **Toolbox** feature menus are described in the following sections.

11. 10. 1. Text

The **Text** menu allows you to customize the text used in the template.

The options are described in the following table.

Table 41: Text menu options

Option	Description
Alignment	Arrangement of the text on the template, for example, **Top-Center**
Back Color	Background colour for the template
Data Field	Text field to include in the template, for example, **Title**, **First Name**, **User ID**, or **Passport**. This field is only enabled when **Dynamic** is selected for **Data Type**.
Data Type	Allows the text to be defined as **Constant** (static text) or **Dynamic** (variable text). If you want the fields in the printed card template to be automatically completed with user data, select **Dynamic**. When **Dynamic** is selected, the **Data Field** is activated.
Font	Text font on the template

Option	Description
Location	Location of the text on the template. You can specify the X and Y coordinates.
Size	Height and width of the text
Text	Text that appears on the template
Text Color	Colour of the text on the template

11. 10. 2. Image

The **Image** menu allows you to customize images imported into the template.

The options are described in the following table.

Table 42: Image menu options

Option	Description
Back Color	Background colour for the image
Data Field	Allows the selection of an image from the specific **User** information screen (in ProAccess SPACE). This field is only enabled when **Dynamic** is selected for **Data Type**.
Data Type	Allows the image to be defined as **Constant** (static image) or **Dynamic** (variable image). When **Dynamic** is selected, the **Data Field** is activated.
Image	Image for the template. Click the ellipsis icon to browse for an image to import.
Image Mode	Arrangement of the image on the template, for example, **Scaled**
Location	Location of the image on the template. You can specify the X and Y coordinates.
Size	Size of the image on the template. You can specify the height and width.

After you create a badge template, you can associate it with an individual user in ProAccess SPACE. See *Card Printing Templates* for more information.

11. 10. 3. Shape

The **Shape** menu allows you to customize shapes on the template.

The options are described in the following table.

Table 43: Shape menu options

Option	Description
Back Color	Background colour for the shape
Line Color	Line colour for the shape
Line Width	Line width of the shape
Location	Location of the shape on the template. You can specify the X and Y coordinates.
Size	Size of the shape on the template. You can specify the height and width.
Type	Shape can be a rectangle or an ellipse

11. 10. 4. Line

The **Line** menu allows you to customize lines on the template.

The options are described in the following table.

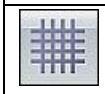
Table 44: Line menu options

Option	Description
Back Color	Background colour of the line
Direction	Direction of the line
Line Color	Colour of the line
Line Width	Width of the line
Location	Location of the line on the template. You can specify the X and Y coordinates.
Size	Size of the line on the template. You can specify the height and width.

11. 10. 5. Design Icons

There are six design icons on the top left of the **Card template design** screen. These icons are described in the following table.

Table 45: Design icons

Icon	Description
 New	Allows you to create a new card template
 Open	Allows you to select any templates you previously created
 Save	Allows you to save a card template
 Save As	Allows to you save card templates with different names, for example, in case you need to use the current design as a basis for another template design
 Print	Allows you to print your template
 Grid	Allows you to use a grid reference to place design elements accurately

11. 10. 6. Back Design

You can design the front and back of a card template.

To add information for the back of the card template, perform the following steps:

1. Right-click the **Front** tab. The **Add back side** option is displayed.

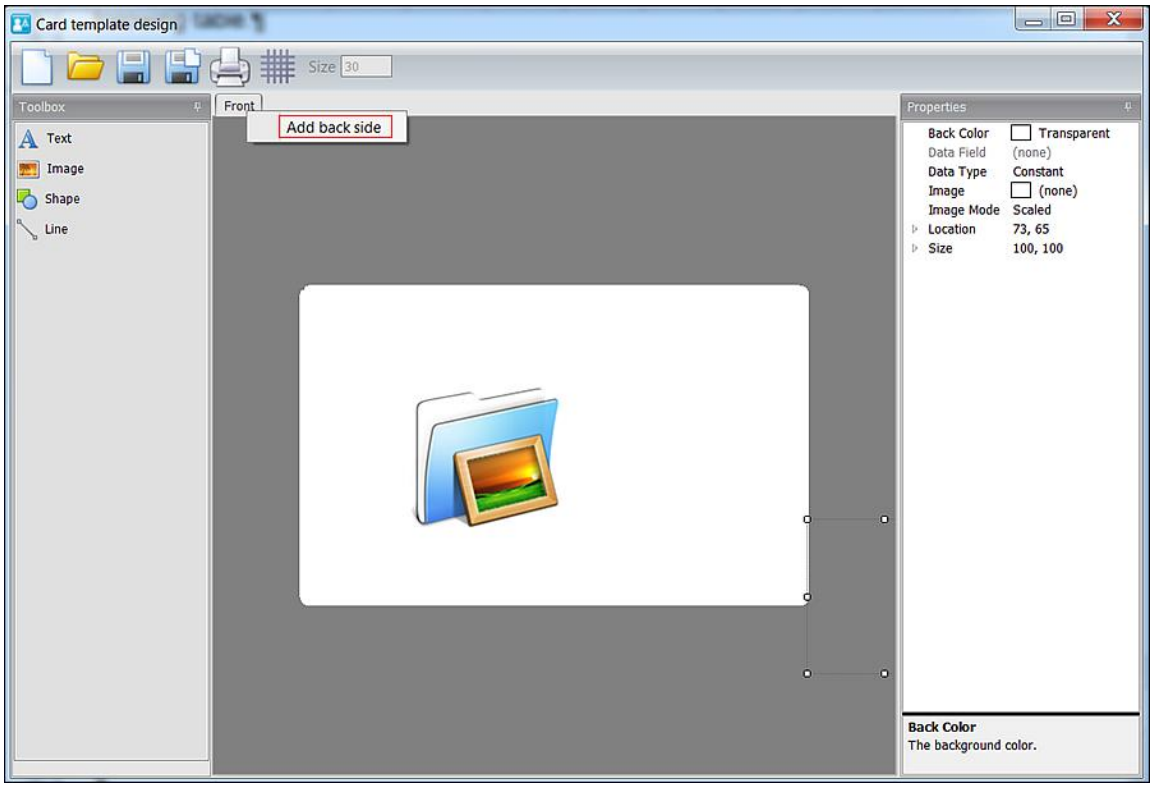


Figure 225: Add back side option

2. Click **Add back side**. A new **Back** tab is displayed.

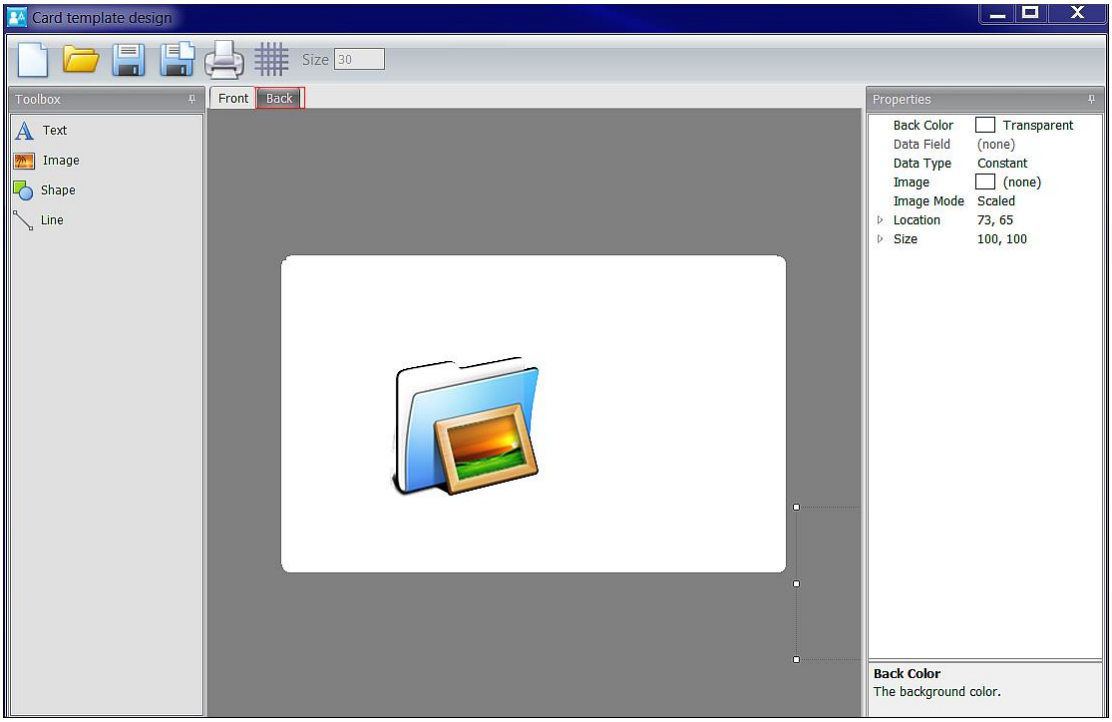


Figure 226: New Back tab

3. Click the **Back** tab to design the back of the card template.

11. 11. Using Card Printing Templates

After you create your badge templates, you can print these as user cards (keys) in ProAccess SPACE. The card printing functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

NOTE: To print card templates, the template must contain dynamic fields with a specific data field in the user list.

To print card templates perform the following steps:

1. Select **Cardholders** > **Users**. Select the user associated with the card template to print. The **Print** button is visible in **Card Printing Template**.

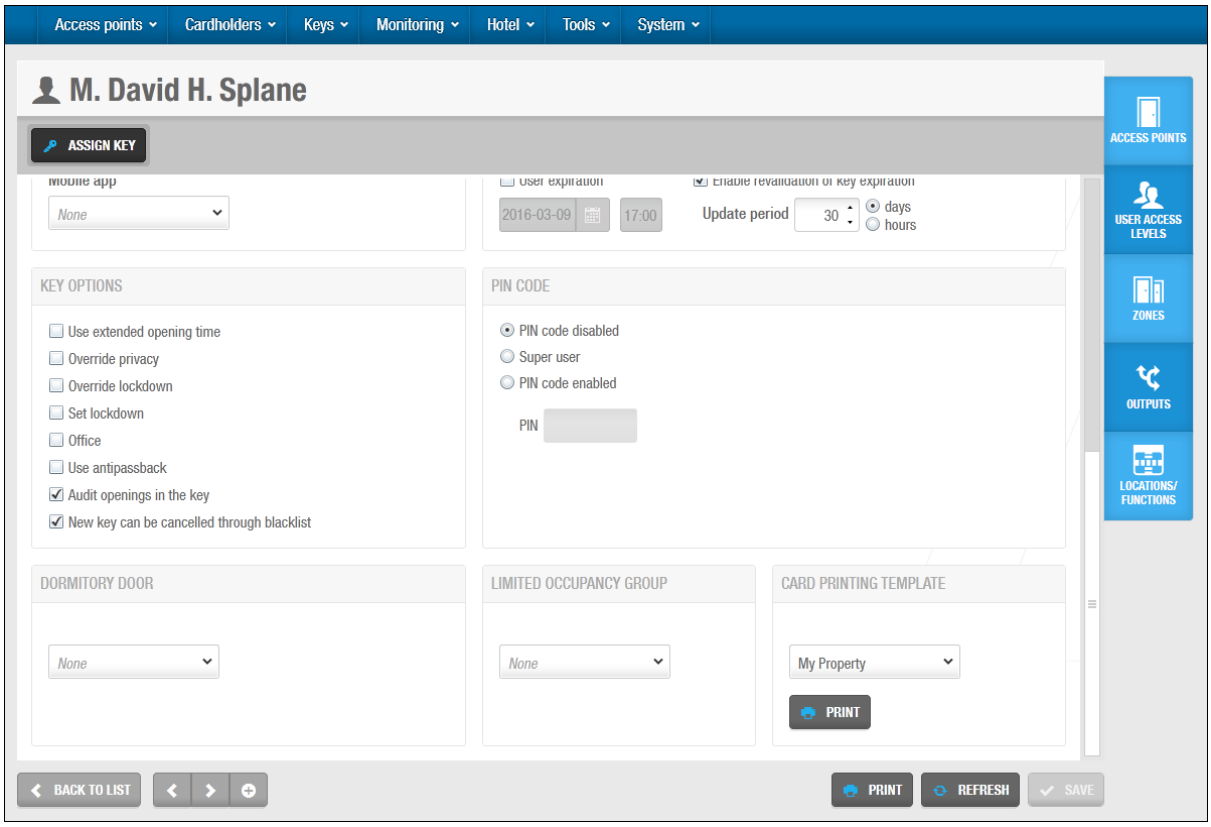


Figure 227: Print users cards screen

2. Click **Print**. The **Card Preview** screen is displayed.
3. Select the **Print** icon on the top left-hand side of the screen. The templates are then printed.

12. PROACCESS SPACE SYSTEM CONFIGURATION

This chapter contains the following sections:

12. 1. About ProAccess SPACE System

This chapter describes the various system configuration options that control the advanced features of ProAccess SPACE. Currently, calendars, daylight saving time (DST), multiple time zones, operators, operator groups, and partitions can be set up in ProAccess SPACE. Network devices such as encoders, control units (CUs), and gateways can also be configured.

The following sections describe how to create and configure your organization's calendars and manage DST and multiple time zones. They also describe how to add partitions, operator groups and operators, and manage network devices.

12. 2. ProAccess SPACE System Process

System configuration tasks are generally managed by an operator with admin rights. Throughout this chapter, references are made to the admin operator. However, this can refer to any operator who has been granted admin rights.

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

1. **System auditor**
   The admin operator creates reports of what was done in the SALTO System. For example, what operator created a key, a backup or lost and re-established communication with the SALTO database.
2. **Operators created and configured**
   The admin operator creates operator profiles and configures the operator options.
3. **Operators associated**

The admin operator associates operator groups with the specified operators.

4. **Operator groups created and configured**

   The admin operator creates operator groups and configures the operator group options.

5. **Operator groups associated**

   The admin operator associates operators with the specified operator groups.

6. **Partitions created**

   The admin operator creates partitions and adds items to partitions.

7. **Partitions associated**

   The admin operator associates operator groups with the specified partitions.

8. **PPD**

   The admin operator loads the PPD and operators on doors.

9. **SALTO network devices added and configured**

   a) The admin operator adds encoders, RF gateways, RF nodes, CU42E0 gateways, and CU4200 nodes to the system.

   b) The admin operator configures online connection types. These are as follows:

   - Online IP (CU5000)
   - Online IP (CU42E0)
   - Online RF (SALTO)
   - Online RF (BAS integration)

   See *Adding Network Devices* and *Configuring Online Connection Types* for more information about these tasks.

10. **Calendars created and configured**

    The admin operator creates calendars and configures the calendar options.

11. **Multiple time zones added and configured**

    The admin operator adds additional time zones to the system and configures the time zone options if required. The admin operator configures the DST options for the default system time zone. Note that you must enable the multiple time zones functionality in ProAccess SPACE General options. See *Time Zones* for more information.

12. **General options**

    The admin operator configures all the general options in the system. Many of the options in the general options will enable features in ProAccess SPACE.

13. **SAM & Issuing options**

    The admin operator configures the system to use third-party keys.

14. **PMS authorizations**

    The admin operator configures the Property Management System (PMS)

15. **System resources**

    The admin operator manages the blacklist status and recovery.

12. 3. System Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows

events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

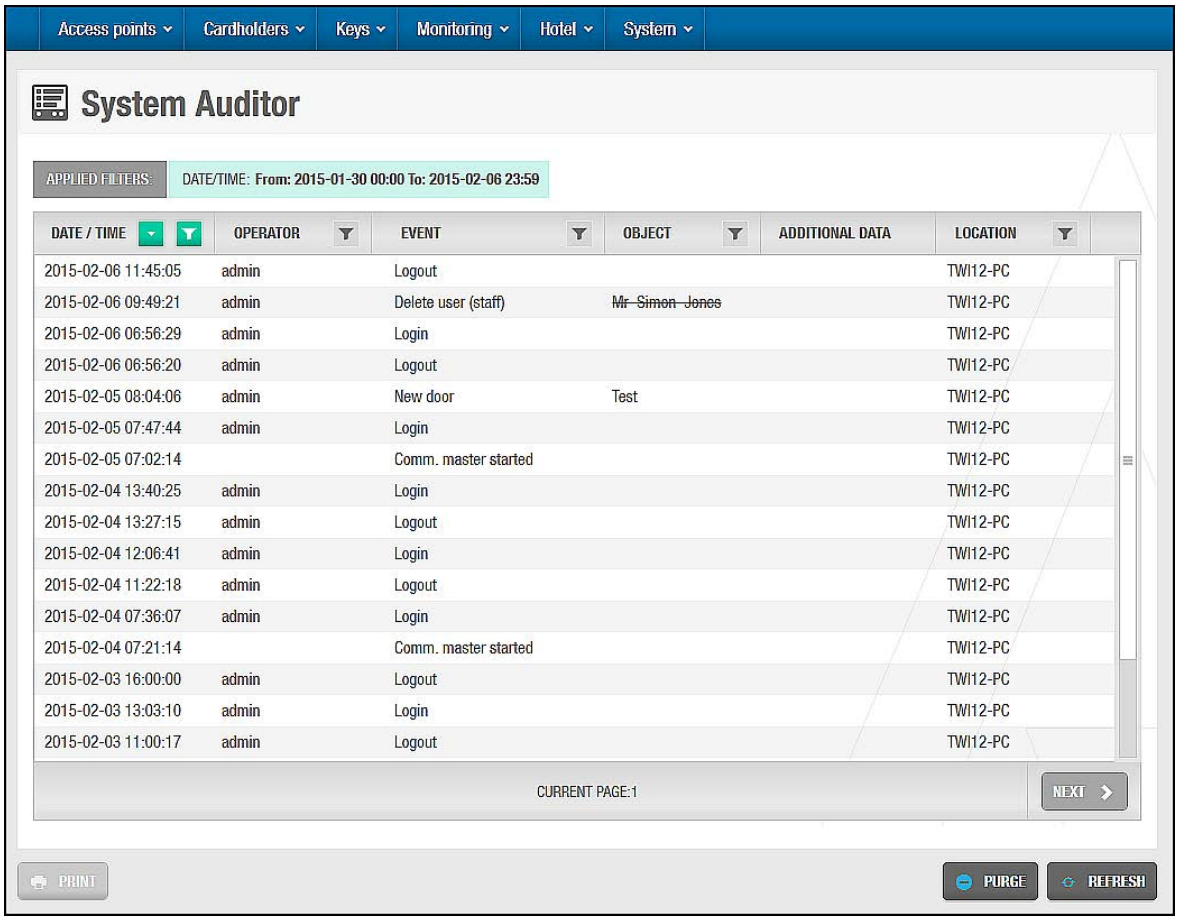


Figure 228: System Auditor information screen

12. 3. 1. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

12. 3. 2. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

16. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

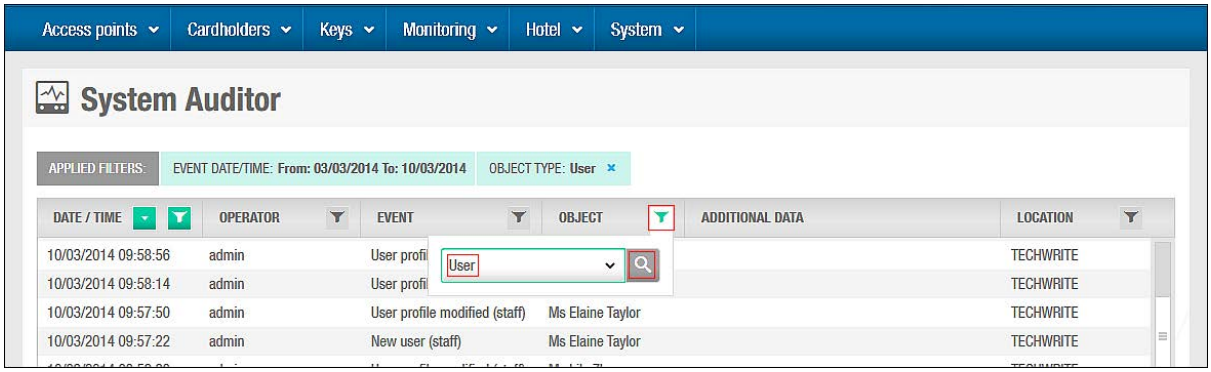


Figure 229: System Auditor information screen

17. Click the **Funnel** icon above the filter item. A search dialog box is displayed.

    For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.

    For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.

    For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.

18. Type your search term.

    Or

    Select a predefined search term from the drop-down list.

    Or

    Select a date range.

    You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.

    However, you cannot remove the **Date/Time** filter.

19. Click the **Search** icon. A filtered audit trail list is displayed.

12. 3. 2. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

12. 3. 3. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic*

System Auditor Purging for more information.

To purge the system auditor, perform the following steps:

20. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
21. Click **Purge**. The **Purge system auditor** dialog box is displayed.

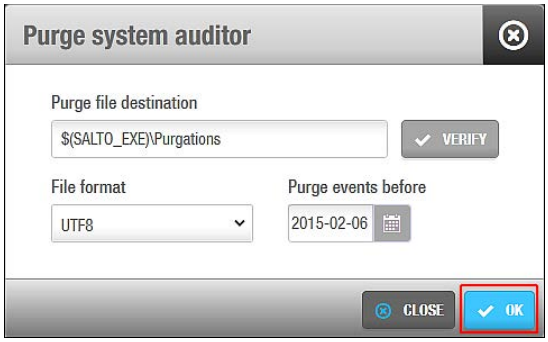


Figure 230: Purge system auditor dialog box

22. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
23. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
24. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
25. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
26. Click **OK**.

12. 4. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

12. 4. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

27. Select **System** > **Operators**. The **Operators** screen is displayed.

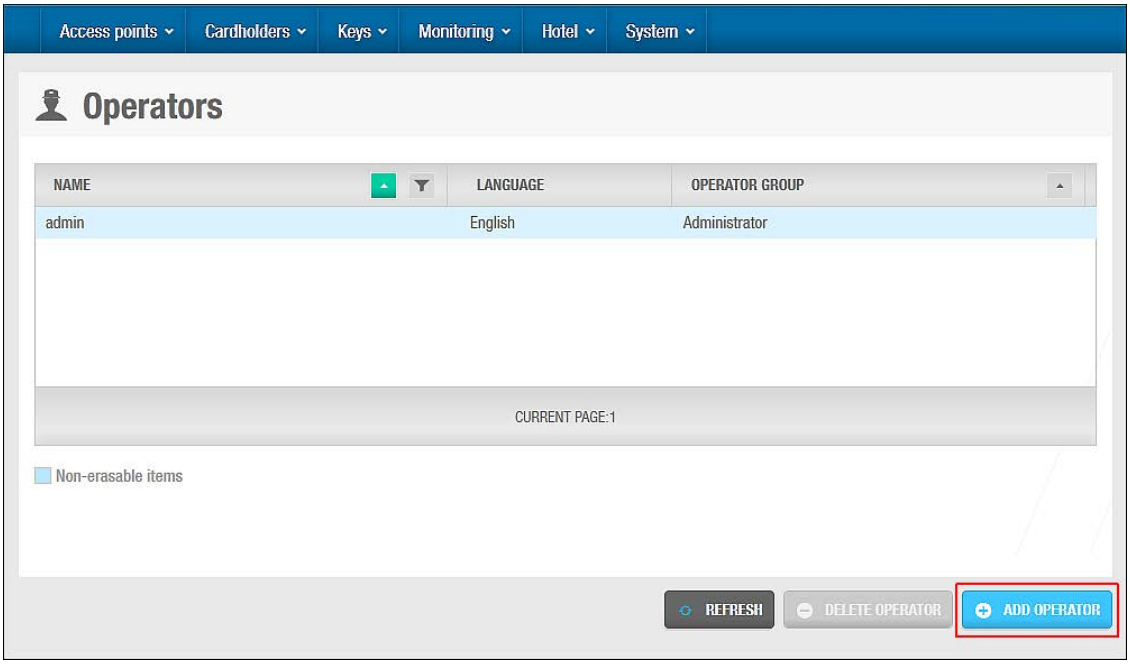


Figure 231: Operators screen

28. Click **Add Operator**. The **Operator** information screen is displayed.

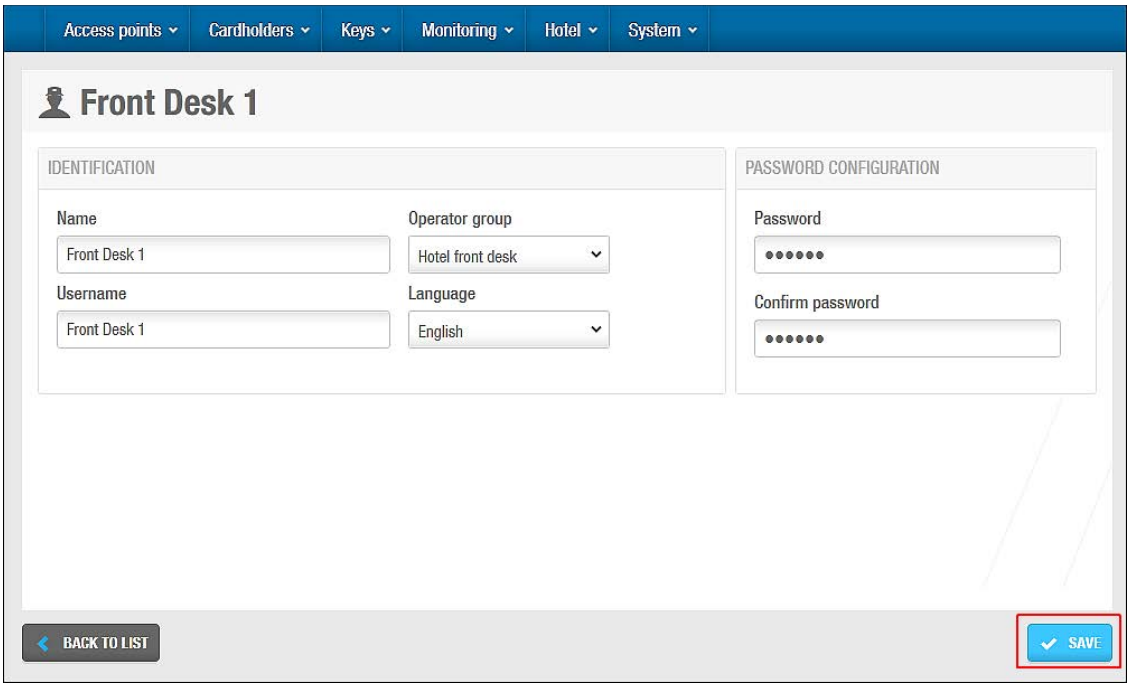


Figure 232: Operator information screen

29. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

30. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

    A maximum of 64 characters can be entered. The user name is not case sensitive.

31. Select the appropriate operator group from the **Operator group** drop-down list.
32. Select the display language for the operator in the **Language** drop-down list.

33. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.

34. Confirm the password.
35. Click **Save**.

12. 5. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

12. 5. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

36. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

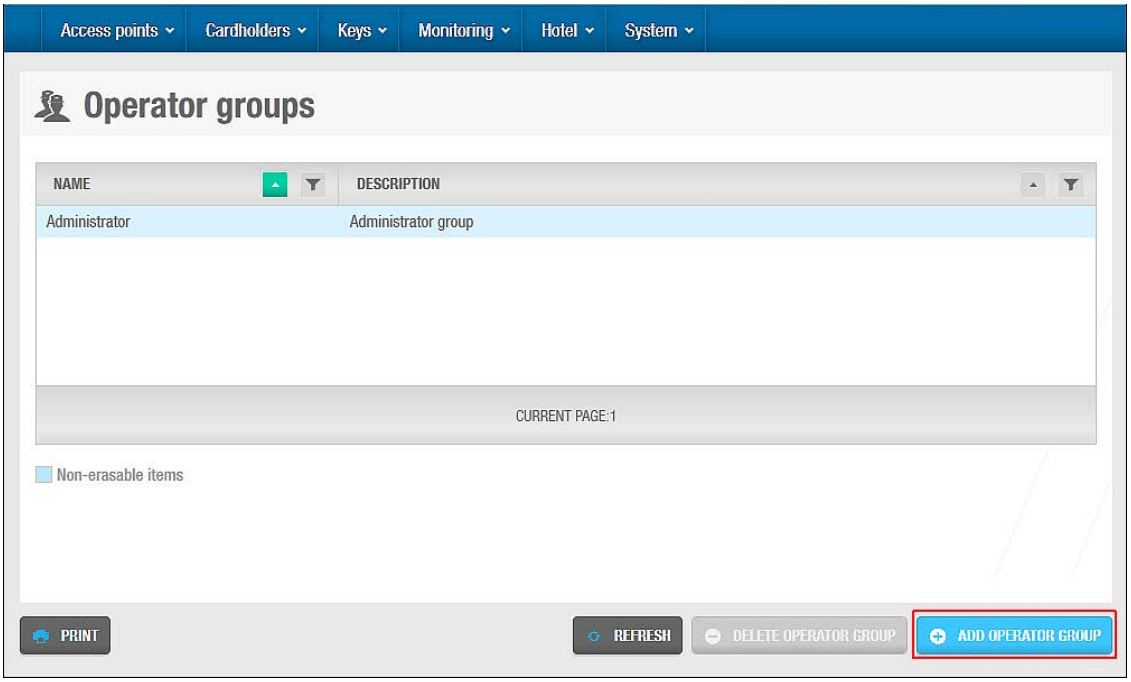


Figure 233: Operator groups screen

37. Click **Add Operator Group**. The **Operator group** information screen is displayed.

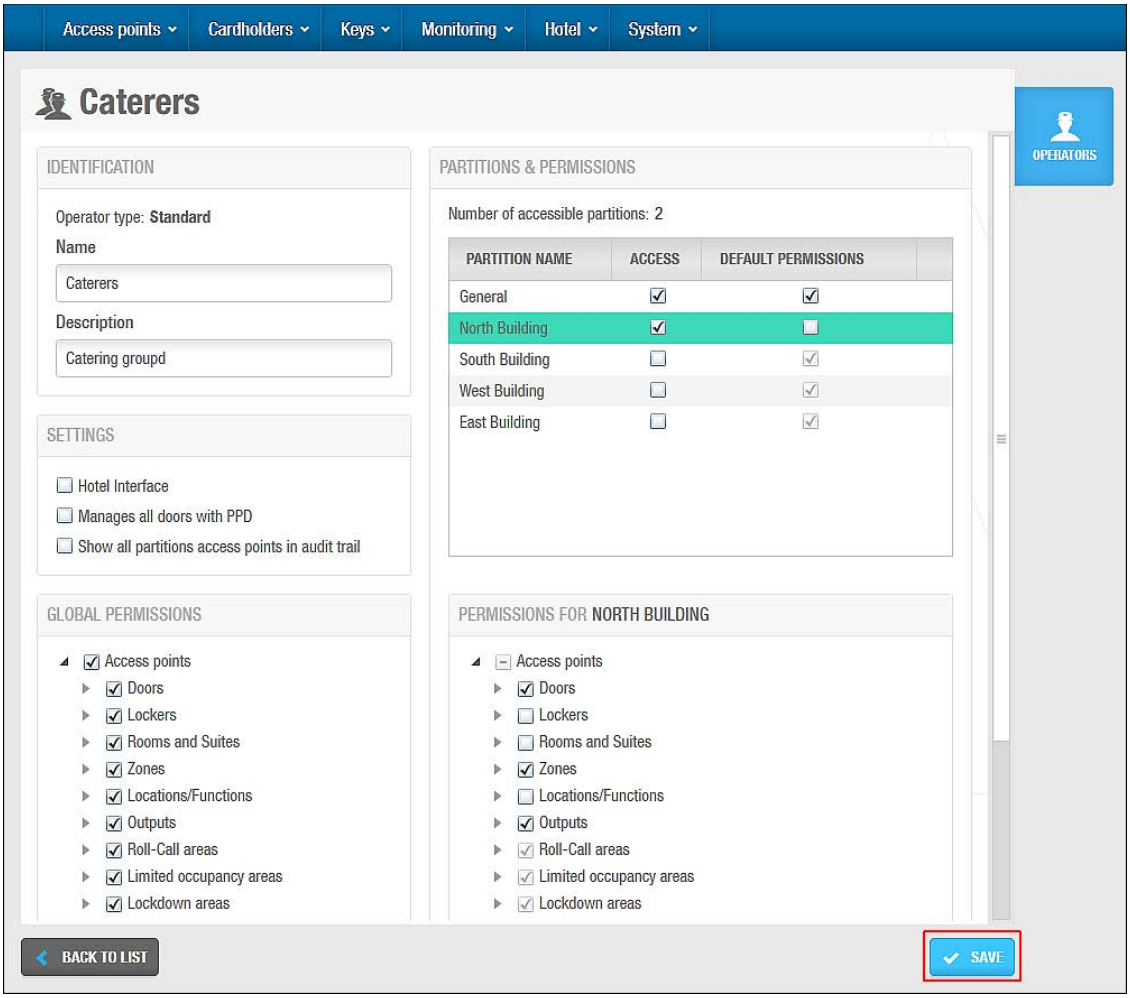


Figure 234: Operator group information screen

38. Type the name of the operator group in the **Name** field.
39. Type a description for the group in the **Description** field.
40. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.

41. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.

42. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes

in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.

43. Click **Save**.

12. 5. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

12. 5. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level **Monitoring** checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48*, *Table 49*, *Table 50*, *Table 51*, *Table 52*, *Table 53*, and *Table 54*.

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors

Permission	Description
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas

Permission	Description
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

12. 5. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

44. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
45. Double-click the operator group with the operator list you want to view.
46. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

12. 6. Partitions

Partitions are items in the system that are grouped together to allow operators to manage different parts of the SALTO network. Partitions make it easier for different operators to manage the various sections of a site. For example, a partition could be the Humanities building in a university. Operators who have access to this partition can manage the items belonging to it (such as particular access points, users, user access levels, etc.) depending on the partition permissions set by the admin operator. See *Creating Operator Groups* for more information about the permissions for partitions. Operators who do not have access to a partition cannot manage the items belonging to it.

NOTE: The partitions functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Partitions can include the following:

- Access points
- Access point timed periods
- Access point automatic changes
- Cardholders
- Access levels
- Cardholder timetables
- Audit trail advanced filters
- Check-in groups
- Calendars

There is one default partition on the system (General), which cannot be removed, but you can create as many additional partitions as required. An operator can view and modify their own partitions in accordance with the permissions set by the admin operator. However, only the admin operator can create and delete partitions. See *Operator Group Global Permissions* for more information.

NOTE: If you delete a partition, you must select another partition to which items in that partition should be moved.

12. 6. 1. Creating Partitions

To create a partition, perform the following steps:

1. Select **System** > **Partitions**. The **Partitions** screen is displayed.

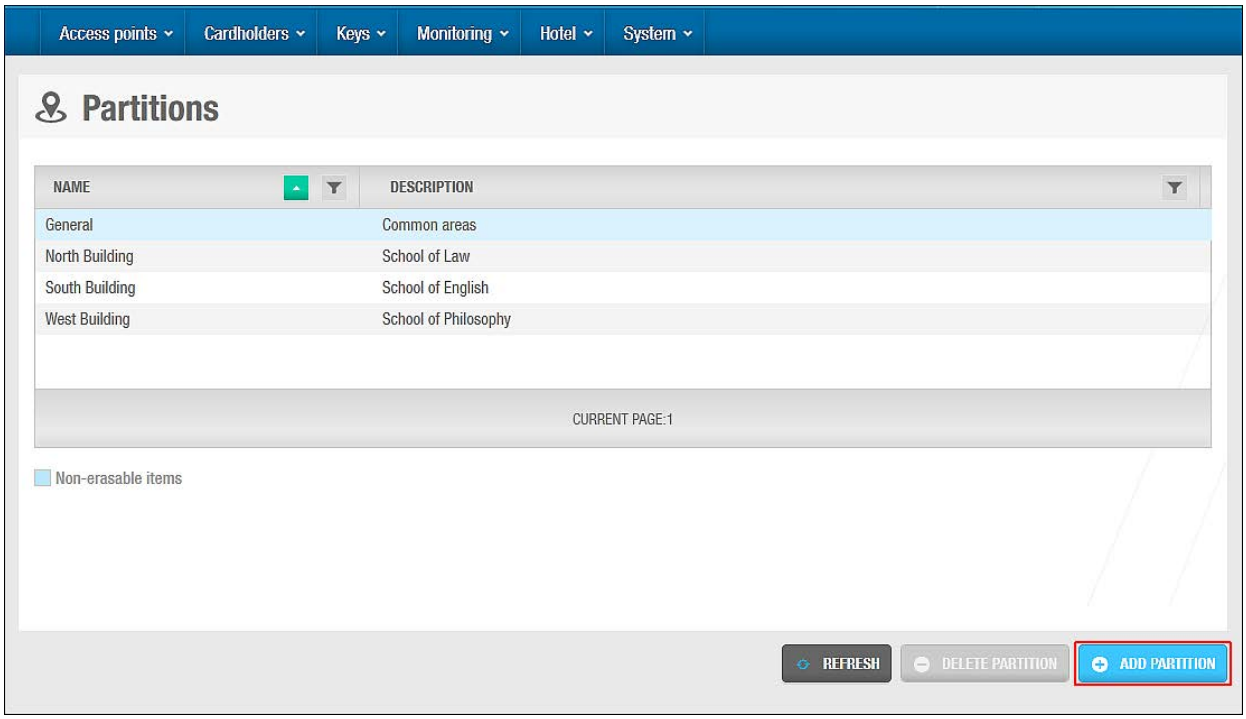


Figure 235: Partitions screen

2. Click **Add Partition**. The **Partition** information screen is displayed.

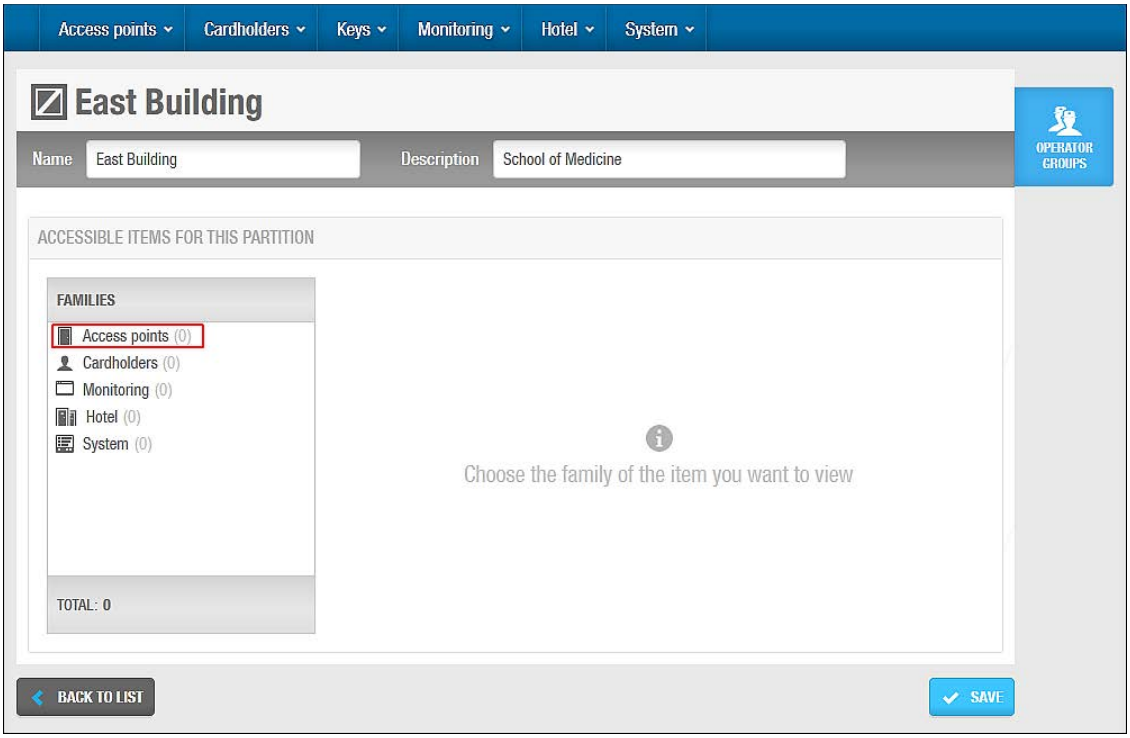


Figure 236: Partition information screen

3. Type a name for the partition in the **Name** field.
4. Type a description for the partition in the **Description** field.
5. Select **Access points** in the **Families** panel. The **Access Points** list is displayed.
6. Select **Doors** from the **Access points** list. The **Doors** panel is displayed on the **Partition** information screen.

7. Click **Add/Delete** in the **Doors** panel. The **Add/Delete** dialog box, showing a list of doors, is displayed.
8. Select the appropriate partition from the **Partition** drop-down list. The list updates to show all the doors in the selected partition.
9. Select the required door in the left-hand panel and click the chevron. The selected door is displayed in the right-hand panel.

   You can hold down the Ctrl key while clicking the doors to make multiple selections. You can also select different partitions from the **Partition** drop-down list to see a list of doors in each partition and add additional selected doors to the right-hand panel. Note that you can move a door in the right-hand panel back to its original partition if required. However, if you want to move the door to a different partition, you must do the following:

   a) Click **Accept** in the **Add/Delete** dialog box.
   b) Click **Save** on the **Partition** information screen.
   c) Click **Add/Delete** to display the **Add/Delete** dialog box again.
   d) Select the partition to which you want to move the door from the **Partition** drop-down list.
   e) Select the door in the right-hand panel and click the chevron. The selected door is displayed in the left-hand panel.

   If you do not follow steps a-e above, a **Lock** icon is displayed beside the name of the door when you select a different partition from the **Partition** drop-down list.
10. Click **Accept**. The selected door is displayed in the **Door** panel on the **Partition** information screen.

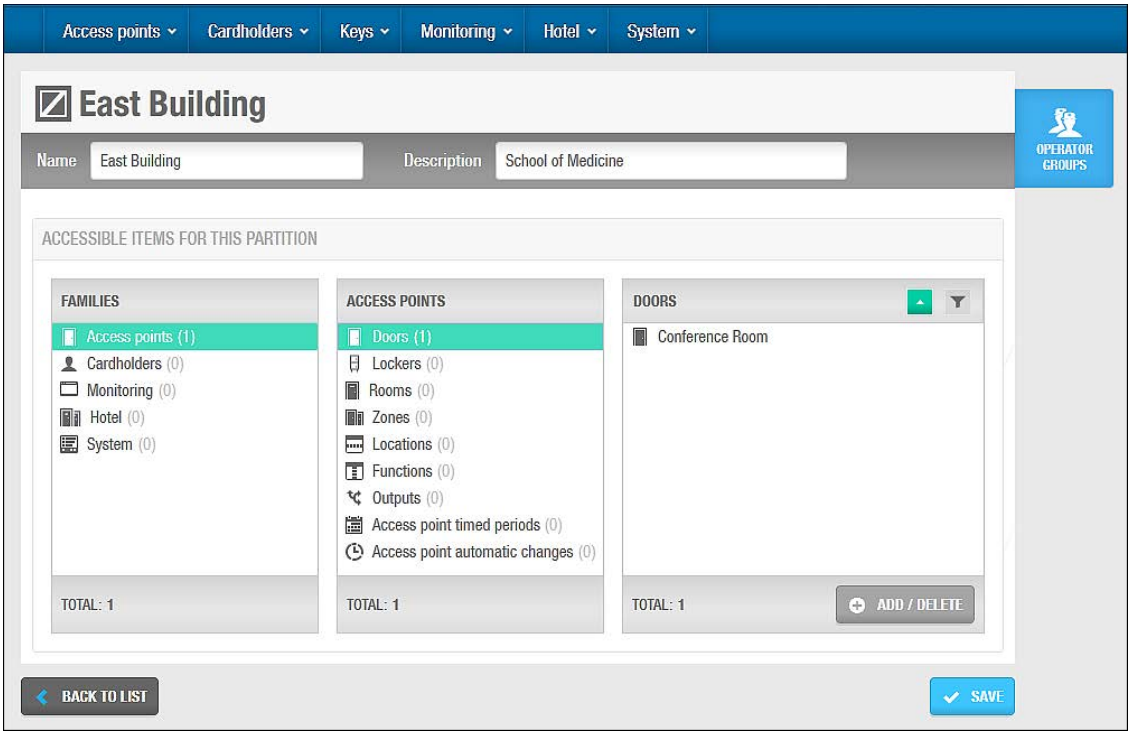


Figure 237: Select door

11. Follow the procedure described in Steps 6 to 10 for each entry in the **Access points** list.
12. Follow the procedure described in Steps 5 to 10 for each family in the **Families** panel.

    The family types are described in *Partition Family Types*.

13. Click **Save** when you have finished adding items for each family to the **Partition** information screen. All of the selected items are added to the partition.

NOTE: When you create partitions, you can move items (such as doors or users) from one partition to another using the **Add/Delete** dialog boxes on the appropriate **Partition** information screen. You can also do this on the information screen for each item. For example, you can move a door to a different partition by selecting the new partition in the **Partition** field on the **Door** information screen and clicking **Save**. Note that you must select **Access points** > **Doors** and double-click the required door on the **Doors** screen to view the **Door** information screen.

12. 6. 1. 1. Partition Family Types

You can add different items to partitions. These items are grouped into five families on the **Partition** information screen.

They are described in the following table.

Table 55: Family types

Family	Description
Access points	Includes the following items: ▪ Doors ▪ Lockers ▪ Rooms ▪ Zones ▪ Functions ▪ Locations ▪ Outputs ▪ Access point timed periods ▪ Access point automatic changes
Cardholders	Includes the following items: ▪ Users ▪ Visitors ▪ User access levels ▪ Visitor access levels ▪ Guest access levels ▪ Cardholder timetables
Monitoring	Includes audit trail advanced filters
Hotel	Includes check-in groups
System	Includes calendars

12. 6. 2. Associating Partitions

After you have created a partition and added items to it, you must associate operator groups with that partition. You can do this by selecting the partition in the **Partitions** panel on the **Operator groups** information page. See *Creating Operator Groups* for more information.

To view the operator groups associated with a partition, perform the following steps:

1. Select **System** > **Partitions**. The **Partitions** screen is displayed.
2. Double-click the partition with the operator group list you want to view. The **Partition** information screen is displayed.

3. Click **Operator Groups** in the sidebar. The **Operator groups** dialog box, showing a list of operator groups, is displayed.

12. 7. PPD

PPDs are connected to the operator's local PC through either a USB or COM port. See *PPD Settings* for more information. PPDs allow data to be transferred between the operator's PC and the locks. Data is downloaded from the PC to the PPD, and the PPD is used to perform tasks such as lock initialization and emergency openings. In the process, the PPD retrieves information (such as battery status) from the locks. This information is communicated to the system when the PPD is connected to the operator's PC.

See the *Portable Programming Device by SALTO* document for more information about PPDs and their configuration settings.

Table 56: PPD

 Portable Programming Device (PPD)	Used by admin operators to transfer configuration changes to a lock or by maintenance operators to check the battery status of the lock and collect the lock's audit trail

NOTE: It is important that the time is set correctly for the PC on which the SALTO software is running, as this controls the time and date settings for locks.

12. 7. 1. Peripheral Types

The functionality of the PPD is described in the following table.

Table 57: Peripheral types

Peripheral	Functionality
PPD	Communicates information to the locks such as door identification and configuration details. The operator downloads the information from their PC to the PPD and the PPD can then be connected to the lock. In this way, information is transferred to the lock. PPDs are used to: ▪ Update configuration changes to the lock (door profile, calendars etc.) ▪ Manually retrieve the audit trail stored on the lock for uploading to the server ▪ Perform a firmware diagnostic evaluation of the locking electronic components ▪ Upgrade the firmware of the locking components ▪ Open a door in the event of an emergency ▪ Read the battery status of the lock ▪ Perform a general diagnostic evaluation of the system

PPDs are configured in ProAccess SPACE General options. See *Devices Tab* for more information. The **PPD** information screen in ProAccess SPACE is used to download access point data to PPDs. This allows you to perform tasks with PPDs such as initializing and

updating locks. You can also view the status of PPDs and update their firmware by using the **PPD** information screen.

12. 7. 2. PPD Menu Options

PPDs have seven menu options. Some of the menu options are available by default. Others are enabled when you select particular options on the **PPD** information screen in ProAccess SPACE, and download access point data to the PPD. See the *Portable Programming Device by SALTO* document for more information about using PPDs.

The options are described in the following table.

Table 58: PPD menu options

Option	Description
Update locks	Used to update a lock when the PPD is connected to it. To enable this menu option, you must download the appropriate access point data to the PPD by using the **PPD** information screen.
Firmware diagnostic	Used to perform a firmware diagnostic of the locking electronic components
Update firmware	Used to update the firmware of the locking electronic components
Collect audit trail	Used to collect audit trail data from offline doors and transfer it to the operator's local PC
Emergency opening	Used to perform an emergency opening if the lock battery dies or a reader error occurs. To enable this menu option, you must select the **Allow emergency opening** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. Alternatively, you can set this as a default option in ProAccess SPACE General options. You can also set a password for performing emergency openings using the PPD if required. See *Performing Emergency Door Openings* and *Devices Tab* for more information.
Initialize lock	Used to transfer access data to new locks or existing locks that have been fitted on a different access point and renamed. To enable this menu option, you must select the **Initialize locks** checkbox on the **PPD** information screen and download the appropriate access point data to the PPD. See *Initializing Locks* for more information.
Diagnostic	Used to retrieve information from the lock such as the battery status or serial number

12. 7. 3. Viewing PPD Status

You can view the status of a PPD you have connected to the PC by selecting **System** > **PPD**.

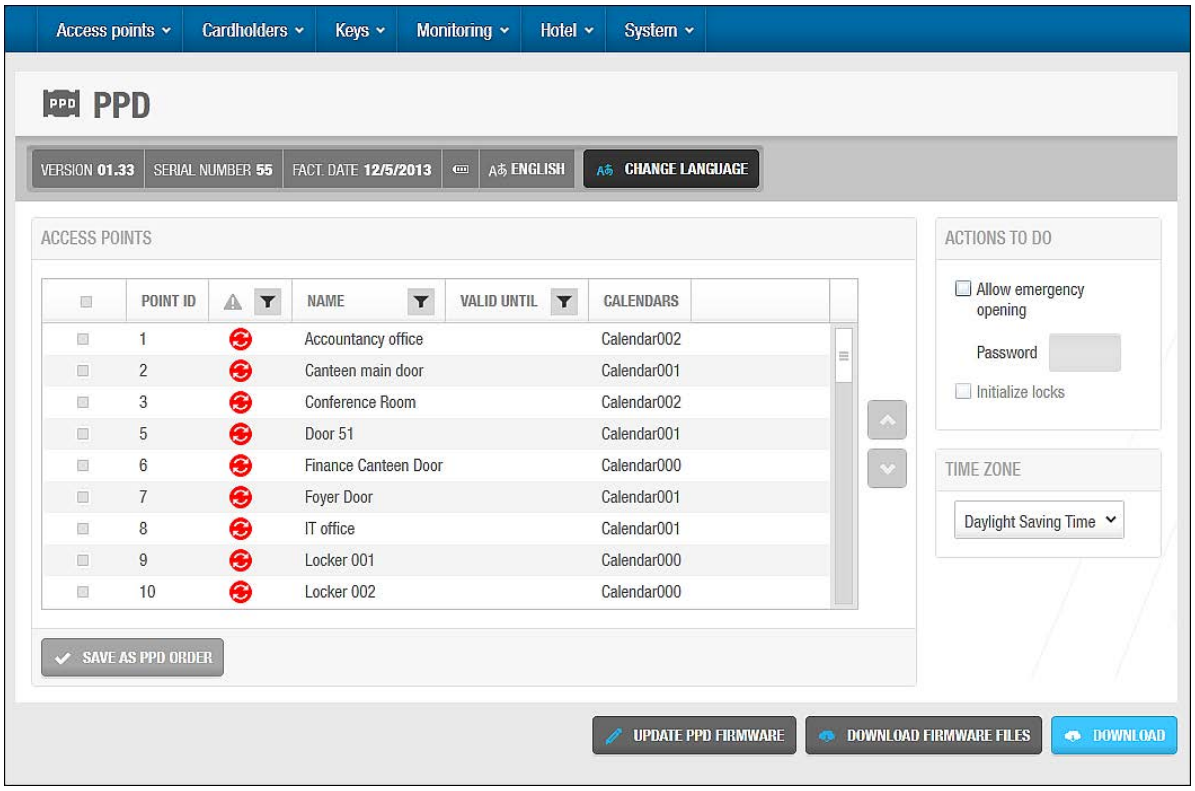


Figure 238: PPD information screen

The **PPD** information screen shows the following information about the PPD:

- Version
- Serial number
- Factory date (or date of manufacture)
- Battery status
- Language

12. 7. 4. Changing the PPD Language

You can change the language of the display messages in the PPDs if required.

To change the language displayed in a PPD, perform the following steps:

4. Connect the PPD to the PC.
5. Select **System** > **PPD**. The **PPD** information screen is displayed.
6. Click **Change Language**. The **Change language** dialog box is displayed.

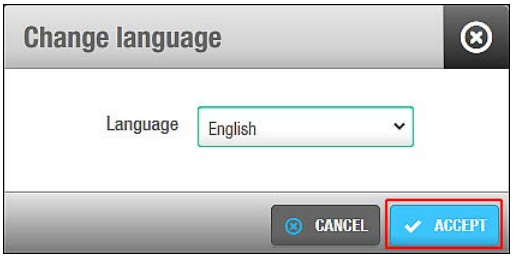


Figure 239: Change language dialog box

7. Select the required language from the **Language** drop-down list.
8. Click **Accept**. The **PPD** progress screen is displayed.

9. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
10. Click **OK**.

12. 7. 5. Using the PPD Information Screen

The **PPD** information screen displays a list of access points. This list varies depending on which time zone is selected in the **Time Zone** panel. It is important to remember that only access points for the selected time zone are displayed. Note that you must enable the multiple time zones functionality in ProAccess SPACE General options to display this panel in ProAccess SPACE. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Access points that need to be updated have a red **Update required** icon on the left-hand side of their name. You can download access point data to a PPD you have connected to the PC by selecting the required access points and clicking **Download**. You can then perform tasks such as updating locks with the PPD. See *Updating Locks* for more information. You must select additional options in the **Actions To Do** panel for certain tasks, for example, initializing locks. See *Initializing Locks* and *Performing Emergency Door Openings* for more information about this panel.

The following table describes some useful screen items.

Table 59: PPD information screen items

Item	Description
Access point checkboxes	Allow you to select individual access points
Checkbox column header	Allows you to select all of the displayed access points. To do so, select the checkbox in the column header.
Chevrons	Allow you to move entries up and down in the access point list
Save As PPD Order button	Allows you to save the access point list order. This specifies the order in which access point data is downloaded to the PPD and displayed in the PPD's menu.
Expand icon	Allows you to view the ESDs for rooms and suites. This icon is displayed on the left-hand side of the room and suite names.

12. 7. 6. Updating PPD Firmware

Firmware is software that is programmed on the read-only memory (ROM) of hardware devices. Firmware updates are available when a new version of the SALTO software is downloaded. Your SALTO technical support contact may also recommend specific firmware updates if required.

To update the firmware of a PPD, perform the following steps:

11. Connect the PPD to the PC.
12. Select **System** > **PPD**. The **PPD** information screen is displayed.

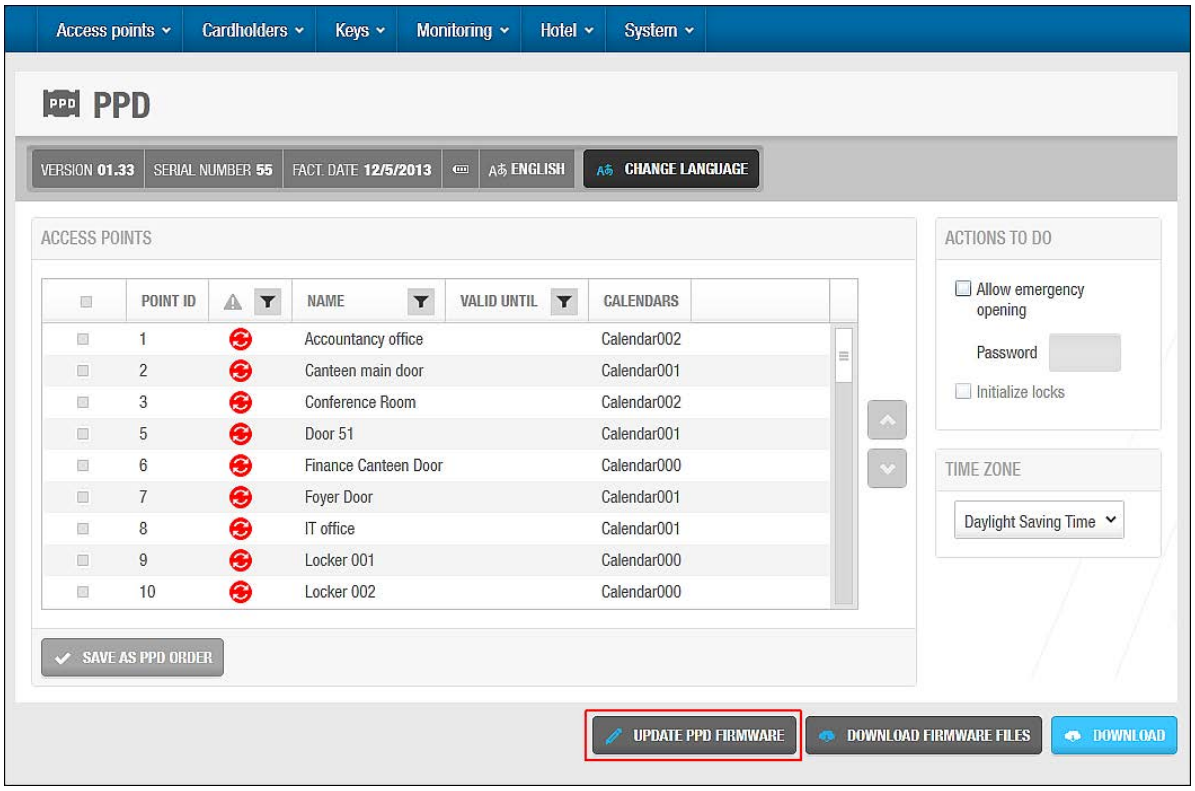


Figure 240: PPD information screen

13. Click **Update PPD Firmware**. The **Update PPD Firmware** dialog box, showing the available firmware files, is displayed.

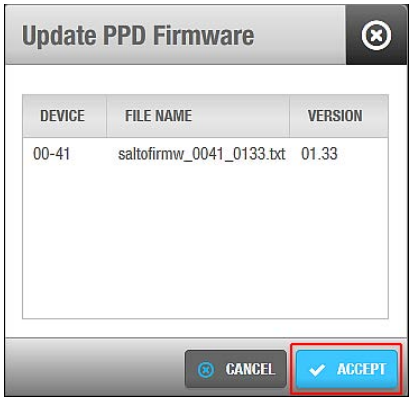


Figure 241: Update PPD Firmware dialog box

14. Select the required file.
15. Click **Accept**. The **PPD** progress screen is displayed.
16. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
17. Click **OK**.

12. 7. 7. Downloading Firmware Files

You can download firmware files to the PPD and use it to update the locking electronic components.

To download a firmware file to a PPD, perform the following steps:

18. Connect the PPD to the PC.
19. Select **System** > **PPD**. The **PPD** information screen is displayed.

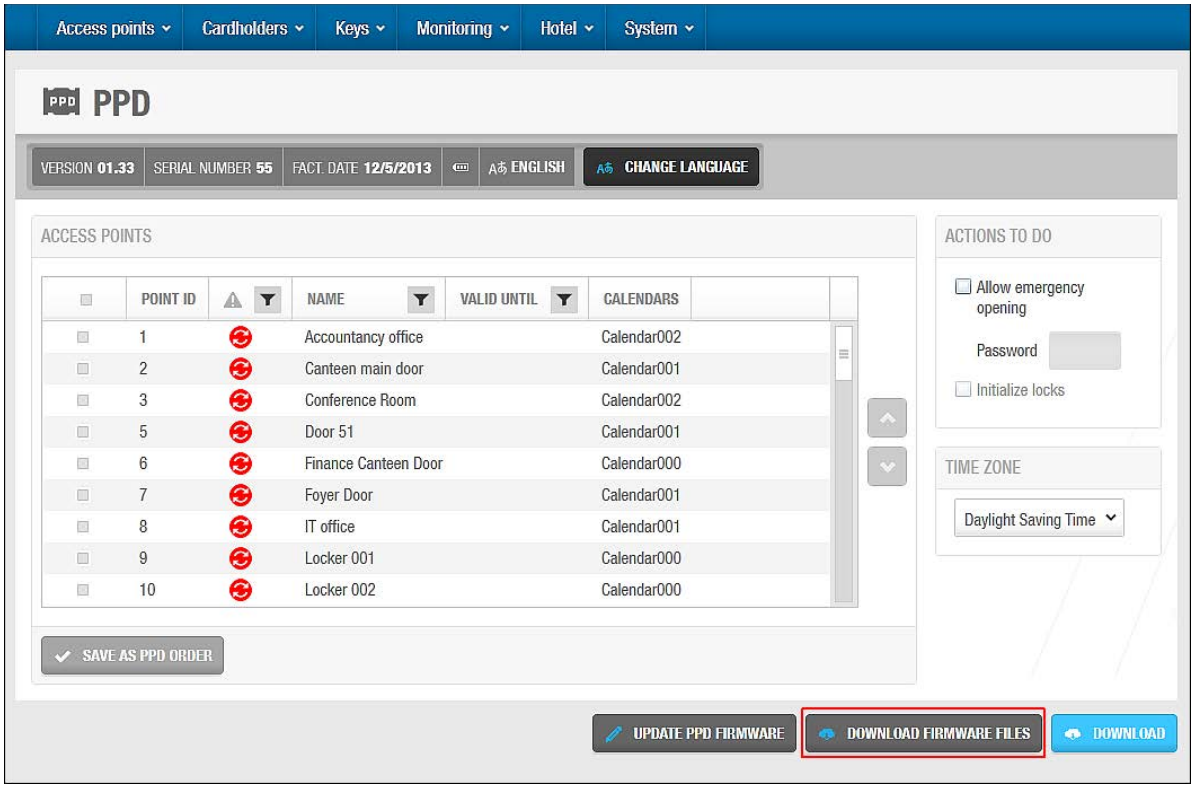


Figure 242: PPD information screen

20. Click **Download Firmware Files**. The **Download Firmware files** dialog box, showing the available firmware files, is displayed.

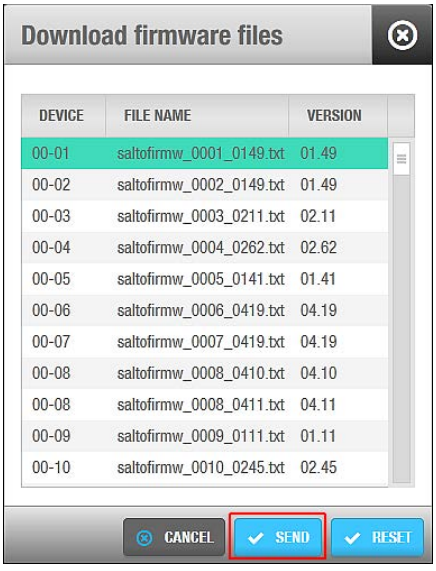


Figure 243: Download firmware files dialog box

21. Select the required file.

    You can hold down the Ctrl key while clicking the files to make multiple selections. Note that you can click **Reset** to delete any firmware files you have already downloaded.

22. Click **Send**. The **PPD** progress screen is displayed.
23. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
24. Click **OK**.

    You can now use the PPD to update the firmware of locking electronic components by selecting **Update Firmware** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

12. 7. 8. Initializing Locks

You must initialize each lock when it is installed. This programmes the lock, and transfers access point data relating to time zones and calendars, for example.

It is recommended that you connect the PPD to the PC after you initialize locks to communicate the most up-to-date information about the locks to the system.

NOTE: You can configure PPDs to assign IP addresses to online IP (CU5000) doors during initialization if required. You must enter each IP address on the system by using the **Access point: Online IP CU5000** information screen. Note that you must select **System** > **SALTO Network** and double-click the required online IP (CU5000) door on the **SALTO Network** screen to view the information screen. You must enable this option in ProAccess SPACE General options by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

PPDs can also be used to transfer SAM data to SALTO locks and wall readers during initialization (or when you perform updates). See *SAM and Issuing options General* options

See *General options* section.

SAM and Issuing Data for more information.

To initialize a lock, perform the following steps:

25. Connect the PPD to the PC.
26. Select **System** > **PPD**. The **PPD** information screen is displayed.

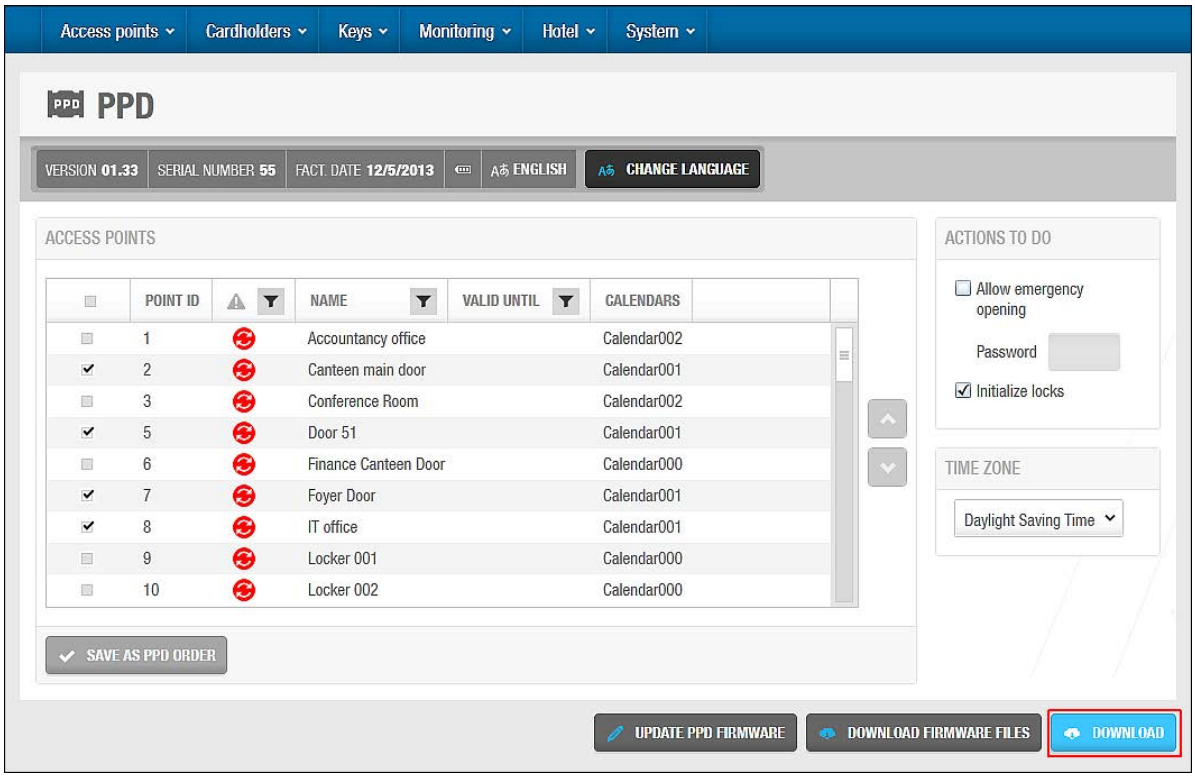


Figure 244: PPD information screen

27. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

28. Select the checkbox of the access point for which you want to initialize the lock.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

29. Select the **Initialize locks** checkbox in the **Actions To Do** panel.
30. Click **Download**. The **PPD** progress screen is displayed.
31. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.

    You can now use the PPD to initialize the lock of the selected access point by selecting **Initialize Lock** in the PPD's menu and connecting the PPD to the lock. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: If you initialize a lock that is already in use, its audit trail is deleted.

12. 7. 9. Initializing Rooms and ESDs

The procedure for initializing rooms and ESDs is the same as for initializing locks. See *Initializing Locks* for more information and a description of the steps you should follow.

NOTE: You can initialize rooms and their associated ESDs either together or separately. However, all of the rooms and ESDs that you select during the initialization process must have the same calendar.

12. 7. 10. Updating Locks

You must update offline locks when you make certain changes to access point data, such as enabling anti-passback or changing the opening mode of doors. You can view locks that need to be updated on the **PPD** information screen by selecting **System** > **PPD**. Note that you must connect a PPD to the PC before you can access the **PPD** information screen. Access points that need to be updated have a red **Update required** icon on the left-hand side of their name.

It is recommended to update offline locks at least every six months to ensure that the clock and calendars are up to date. You must also update locks after you replace their batteries. This is because access point data relating to time zones and calendars, for example, must be restored after a lock's battery dies.

You should connect the PPD to the PC after you update locks to communicate the most up-to-date information about the locks to the system.

To update a lock, perform the following steps:

32. Connect the PPD to the PC.
33. Select **System** > **PPD**. The **PPD** information screen is displayed.

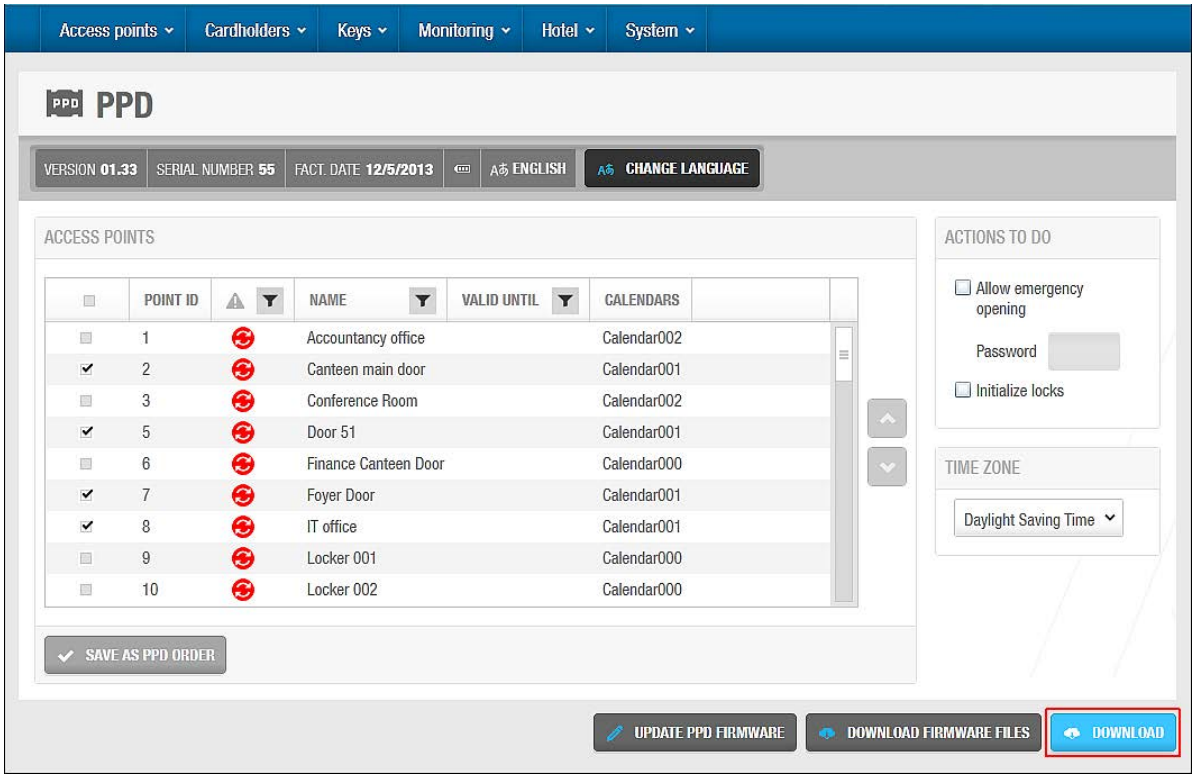


Figure 245: PPD information screen

34. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have

enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

35. Select the checkbox of the access point for which you want to update the lock.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

36. Click **Download**. The **PPD** progress screen is displayed.
37. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
38. Click **OK**.

    You can now use the PPD to update the lock of the selected access point by selecting **Update Locks** in the PPD's menu and connecting the PPD to the lock. Alternatively, you can simply connect the PPD to the lock. In this case, it recognizes the lock and automatically displays the appropriate data. See the *Portable Programming Device by SALTO* document for more information about this process.

NOTE: You can configure PPDs to automatically collect audit trail data when they are used to update locks. You must enable this option in ProAccess SPACE General options by selecting the **Collect audit trails automatically when updating locks** checkbox in **System** > **General options** > **Devices**. See *Devices Tab* for more information.

12. 7. 11. Performing Emergency Door Openings

You can use the PPD to perform an emergency opening if the lock battery dies or a reader error occurs, for example.

NOTE: You can perform emergency openings of online doors without using a PPD. See *Lockdown* for more information.

To perform an emergency opening, perform the following steps:

39. Connect the PPD to the PC.
40. Select **System** > **PPD**. The **PPD** information screen is displayed.

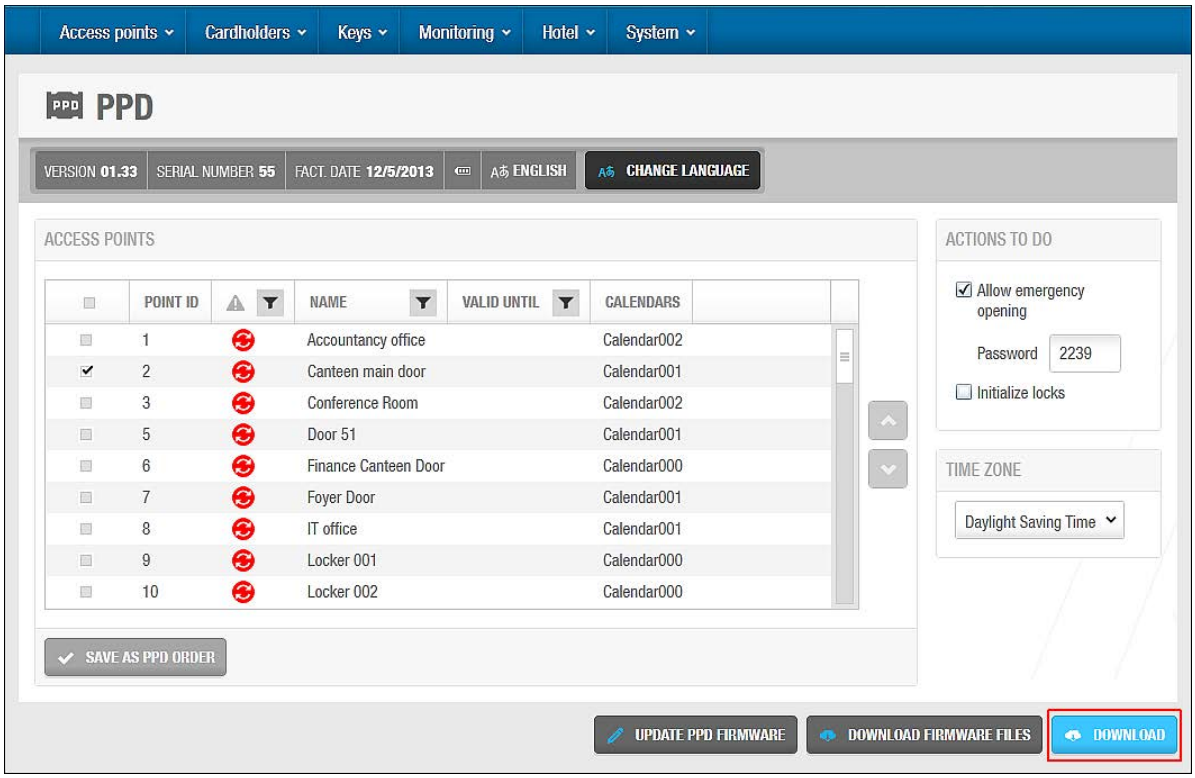


Figure 246: PPD information screen

41. Ensure that the appropriate time zone is selected in the **Time Zone** drop-down list.

    Only access points for the time zone you select in the **Time Zone** panel are shown on the **PPD** information screen. Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

42. Select the checkbox of the access point for which you want to perform the emergency opening.

    You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar. If you select a different time zone from the **Time Zone** drop-down list, any access points you have previously selected are cleared.

43. Select the **Allow emergency opening** checkbox in the **Actions To Do** panel.

    The checkbox is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options. See *PPD Tab* for more information. Otherwise, you must select it each time you want to perform an emergency opening.

44. Type a password for the emergency opening in the **Password** field if required.

    The password can only contain digits. If you type a password, you must enter this password in the PPD before you can perform the emergency opening. Otherwise, the PPD does not require a password. The **Password** field is greyed out if you have set emergency opening as a default option in ProAccess SPACE General options and entered a password there already for the option. See *Devices Tab* for more information. Your PPD firmware must be version 01.29 or higher to use this option.

45. Click **Download**. The **PPD** progress screen is displayed.

46. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.
47. Click **OK**.

    You can now use the PPD to perform an emergency opening of the selected access point by selecting **Emergency Opening** in the PPD's menu and connecting the PPD to the lock. Note that you are required to enter a password in the PPD if you have enabled this option in either ProAccess SPACE PPD window or ProAccess SPACE Devices window. See the *Portable Programming Device by SALTO* document for more information about this process.

12. 7. 12. Collecting Audit Trail Data from Offline Doors

See *Audit Trails* for more information about audit trails. You must use a PPD to collect audit trail data from offline doors. See the *Portable Programming Device by SALTO* document for more information about this process. When you have collected the data, you can view it in ProAccess SPACE.

To view the audit trail data on the system, perform the following steps:

48. Connect the PPD to the PC.
49. Select **System** > **PPD**. The **PPD** information screen is displayed.

    The **Audit Trail** information screen is automatically updated with the information from the connected PPD when you display the **PPD** information screen.
50. Select **Monitoring** > **Audit Trail**. The **Audit trail** information screen, showing the new audit trail data, is displayed.

12. 8. SALTO Network

The SALTO network includes items like encoders, gateways, radio frequency (RF) nodes, CU4200 nodes, online doors, and CUs. These are added and managed in ProAccess SPACE. See *SALTO Virtual Network* for more information about the SALTO network.

The RF and CU4200 functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

NOTE: You can view the enabled channels for RF signals in ProAccess SPACE General options. To do so, select **System** > **General options** > **Devices**. There are 16 channels available and all of these are enabled by default. The frequency range of each channel is also displayed. You can disable a channel if required by clearing the checkbox for the channel and clicking **Save**.

RF mode 2 technology is compatible with ProAccess SPACE. However, RF mode 1 technology is not. If your site uses RF mode 1, an upgrade to ProAccess SPACE is not possible, which means that you must continue to use HAMS or ProAccess RW.

You can view the list of SALTO network items by selecting **System** > **SALTO Network**.

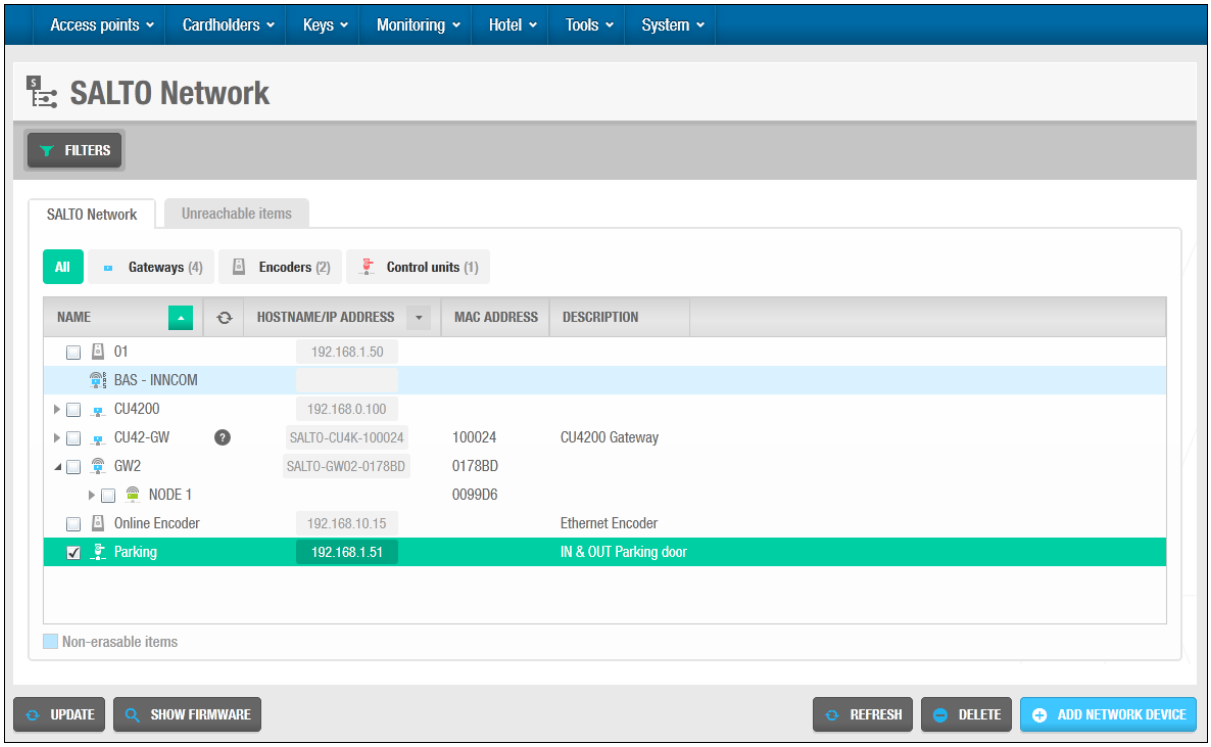


Figure 247: SALTO Network screen

The **SALTO Network** screen displays a list of all network items that have been added and are currently connected to the system.

The information is displayed in four different filtered views:

- **All**: This view shows all of the gateways, encoders, and CUs on the system.
- **Gateways**: This view shows RF gateways and CU4200 gateways. When you click the triangular **Expand** icon on the left-hand side of gateway names, all of the items to which they are connected are displayed. You can view all of the RF nodes and online RF (SALTO) access points connected to each RF gateway, and all of the CU4200 nodes and online IP (CU4200) access points connected to each CU4200 gateway. See *Configuring Online Connection Types* for more information.

NOTE: A BAS gateway may also be displayed on the **SALTO Network** screen. This gateway is created by default if you have fully configured your BAS integration in ProAccess SPACE General options. See *BAS Integration Tab* for more information.

- **Encoders**: This view shows the encoders on the system.
- **Control units**: This view shows online IP (CU5000) access points. See *Configuring Online Connection Types* for more information.

Click the appropriate tab to display each filtered view. The screen also includes an **Unreachable items** tab. Click on this tab to view and configure all items that require additional connection information.

The following table describes the buttons use on the SALTO network main screen.

Table 60: SALTO Network main screen buttons

Item	Description

Item	Description
Update	Allows you to update the selected access point.
Show firmware	Allows you to show the firmware of the selected access point and update it.
Refresh	Allows you to refresh the window with the most updated peripherals status.
Delete	Allows you to delete the selected peripheral.
Add Network device	Allows you to add a new online device.

12. 8. 1. Adding Network Devices

You can add the following network devices to the system:

- Ethernet encoders
- RF gateways
- RF nodes
- CU42E0 gateways
- CU4200 nodes

The following sections describe how to add these devices.

12. 8. 1. 1. Adding Ethernet Encoders

See *Encoders* for more information about encoders.

To add an Ethernet encoder, perform the following steps:

51. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
52. Click **Add Network Device**. The **Add network device** dialog box is displayed.
53. Select **Encoder** from the drop-down list.
54. Click **OK**. The **Encoder** information screen is displayed.

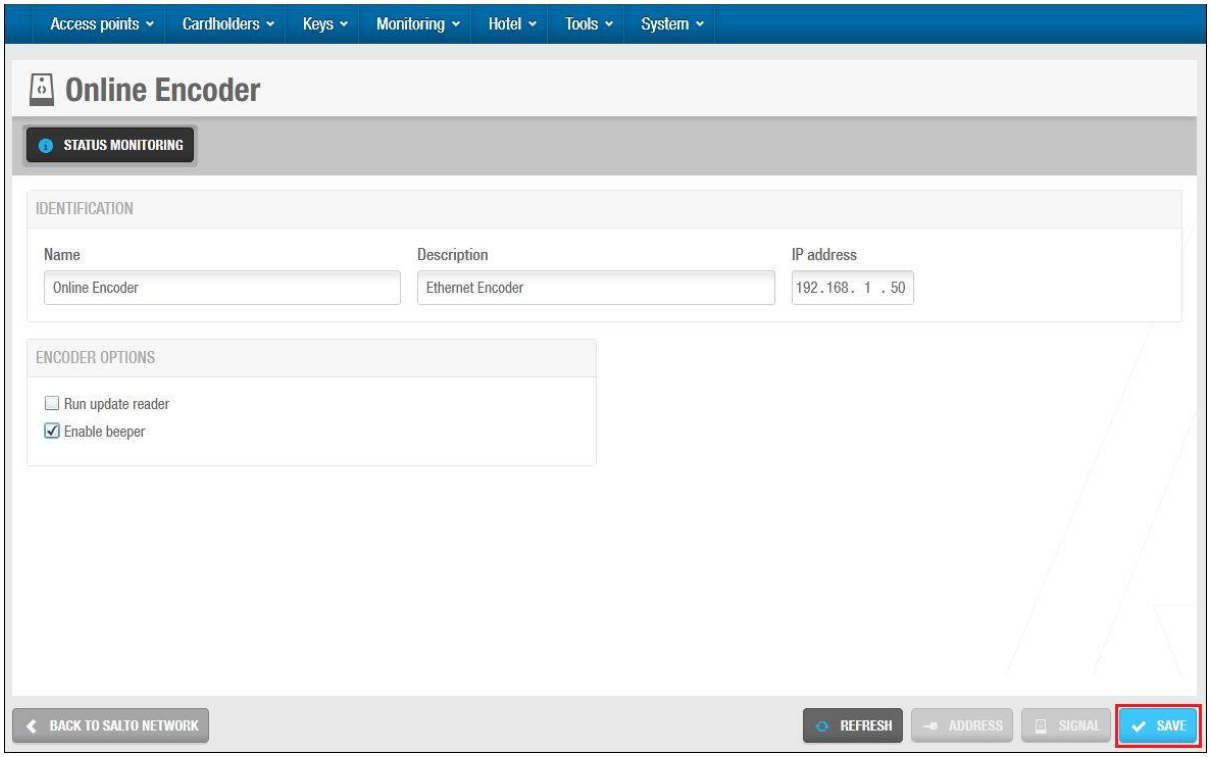


Figure 248: Encoder information screen

55. Type a name for the encoder in the **Name** field.
56. Type a description for the encoder in the **Description** field.
57. Type an IP address for the encoder in the **IP address** field.
58. Select the **Run update reader** checkbox if required.

    This option is used to configure an Ethernet encoder to update user keys automatically when users present their keys to it. If you select this option, the encoder runs continuously but it can only update keys. It cannot be used to encode keys with access data from the SALTO software. See *Updating Keys* for more information.
59. Select the **Enable beeper** checkbox if required.

    If you select this option, the encoder emits beeps when in use.
60. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.

Click **Save**.

12. 8. 1. 2. Adding RF Gateways

Gateways are hardware devices that provide a link between networks that use different base protocols. RF gateways allow data to be transmitted from the system to the SALTO RF locks, and from the RF locks to the system. RF gateways control RF nodes. See *Adding RF Nodes* for more information about RF nodes.

You must physically connect RF nodes to an RF gateway using an RS485 cable to establish communication between the RF nodes and the RF gateway. See the *SALTO Datasheet_Gatewayx2_xxx* document for more information about this process. You must also connect RF nodes and RF gateways in ProAccess SPACE so the system can show which nodes and gateways are connected.

To add an RF gateway, perform the following steps:

61. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
62. Click **Add Network Device**. The **Add network device** dialog box is displayed.
63. Select **RF gateway** from the drop-down list.
64. Click **OK**. The **RF gateway** information screen is displayed.

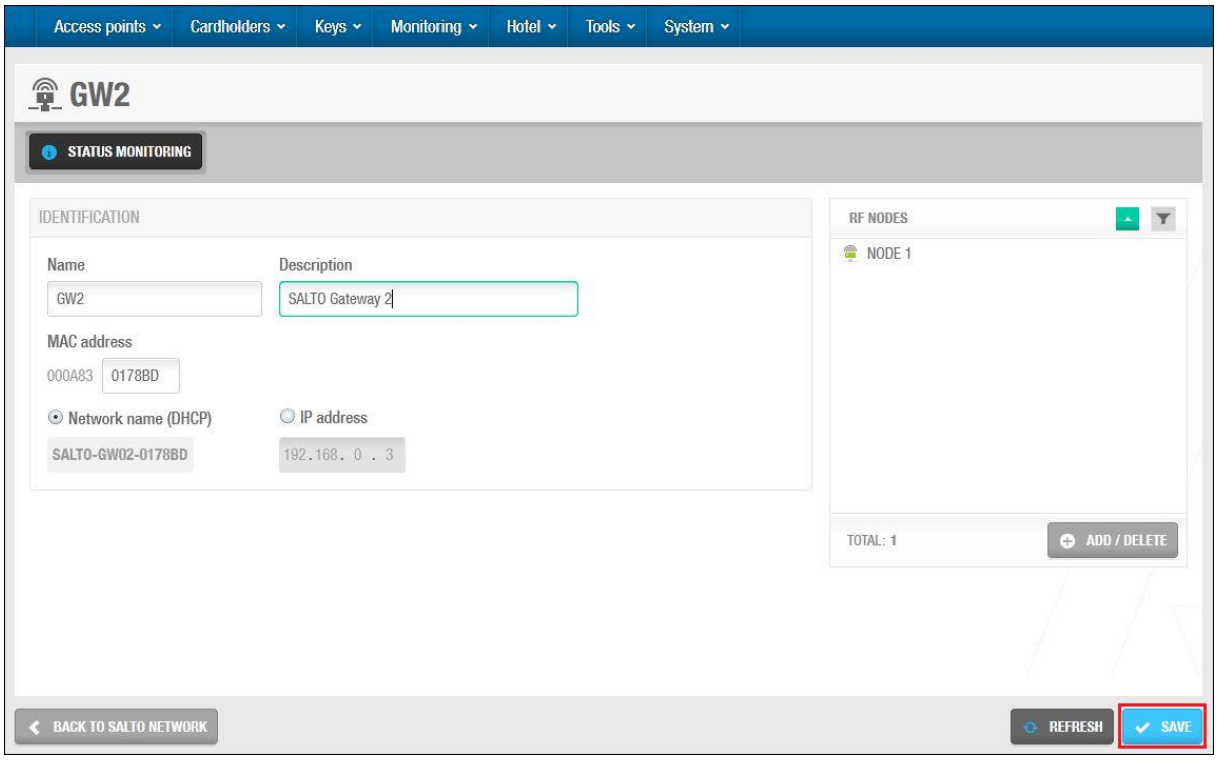


Figure 249: RF gateway information screen

65. Type a name for the RF gateway in the **Name** field.
66. Type a description for the RF gateway in the **Description** field.
67. Type the media access control (MAC) address in the **MAC address** field.

    This is usually displayed on the Ethernet board of the RF gateway.
68. Select either the **Network name (DHCP)** or **IP address** option.

    If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the RF gateway. A Dynamic Host Configuration Protocol (DHCP) server and a DNS are required for this option. If you select the **IP address** option, you must type a static IP address in the field.
69. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.
70. Click **Add/Delete** in the **RF Nodes** panel. The **Add/Delete** dialog box, showing a list of RF nodes, is displayed.

    The **Add/Delete** dialog box only displays RF nodes if you have already added them to the system. You can also connect RF nodes to RF gateways when you add RF nodes to the system. See *Adding RF Nodes* for more information.
71. Select the required RF node in the left-hand panel and click the chevron. The selected RF node is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the RF nodes to make multiple selections. You cannot add RF nodes that already belong to another gateway.
72. Click **Accept**. The selected RF node is displayed in the **RF Nodes** panel.
73. Click **Save**.

12. 8. 1. 3. Adding RF Nodes

RF nodes are network connection points that are physically connected to an RF gateway using an RS485 cable. See *Adding RF Gateways* for more information. This establishes communication between the RF nodes and the RF gateways. Also, in ProAccess SPACE you must connect RF nodes to RF gateways, and RF access points to RF nodes. This means that the system can show which items are connected.

NOTE: You must select **Online RF (SALTO)** in the **Connection Type** panel on the **Door** or **Room** information screen to define a door as an RF access point.

To add an RF node, perform the following steps:

74. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
75. Click **Add Network Device**. The **Add network device** dialog box is displayed.
76. Select **RF node** from the drop-down list.
77. Click **OK**. The **RF node** information screen is displayed.

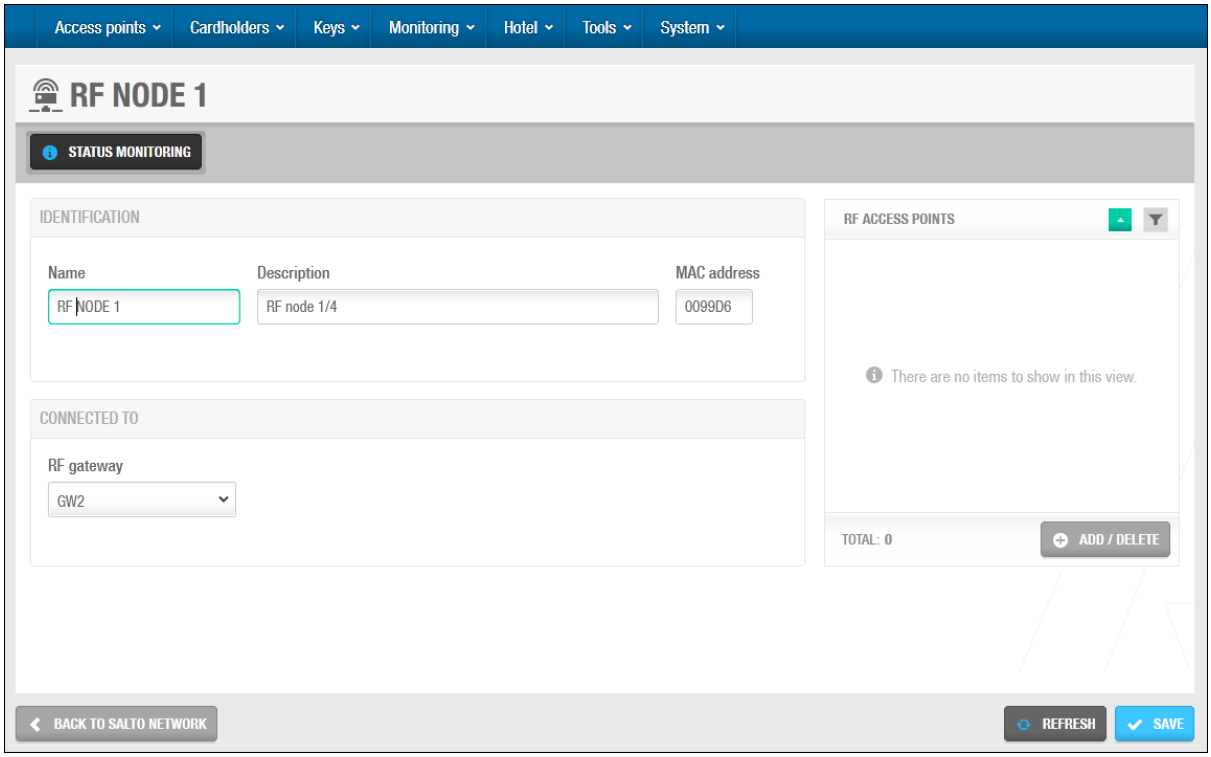


Figure 250: RF node information screen

78. Type a name for the RF node in the **Name** field.
79. Type a description for the RF node in the **Description** field.
80. Type the MAC address of the antenna in the **MAC address** field.
81. Select the RF gateway to which you want to connect the RF node from the **Connected to** drop-down list.

    The default option is **None**.
82. Click **Add/Delete** in the **RF Access Points** panel. The **Add/Delete** dialog box, showing a list of RF access points, is displayed.

    The **Add/Delete** dialog box only displays RF access points if you have already defined doors as RF access points by selecting **Online RF (SALTO)** in the **Connection Type** panel on the **Door** or **Room** information screens. You can also connect online RF

(SALTO) doors to RF nodes by using the **Connected to** field on the **Online RF (SALTO)** information screen. See *Online RF (SALTO)* for more information.

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

    You can hold down the Ctrl key while clicking the RF access points to make multiple selections. You cannot add RF access points that already belong to another RF node.
84. Click **Accept**. The selected RF access point is displayed in the **RF Access Points** panel.
85. Click **Save**.

NOTE: RF gateways have a mini node connected to them. You must add this node in ProAccess SPACE by following the procedure for adding RF nodes. Also, you must connect the mini node to the RF gateway in ProAccess SPACE.

12. 8. 1. 4. Adding CU42E0 Gateways

CU42E0 gateways are CUs that are connected to a local area network (LAN) using a network cable. They connect to the SALTO network using a TCP/IP connection. CU42E0 gateways can control CU4200 nodes. See *Adding CU4200 Nodes* section below for more information about CU4200 nodes.

The CU42E0 gateways provide a link between the CU4200 nodes and the SALTO system, and transmit data to the nodes. This means the CU4200 nodes do not require a TCP/IP connection. You must physically connect CU4200 nodes to a CU42E0 gateway using an RS485 cable. This establishes communication between the CU4200 nodes and the CU42E0 gateway. You must also link CU42E0 gateways and CU4200 nodes in ProAccess SPACE so the system can show which nodes and gateways are connected.

CU42E0 gateways control access to doors by activating their relays. Each CU42E0 gateway can control a maximum of two doors. They can also update user keys.

The CU42E0 supports up to 4 auxiliary CU4200 nodes, meaning this that up to 10 online doors can be controlled using a single IP address (1 CU42E0 gateways + 4 CU4200 nodes)

In stand-alone mode, dipswitches on the CU4200 node units must be set up to 0000, if online, each node should have its own configured address, using the suitable dipswitch combination in binary format. See the CU42X0 installation guide for more details. See image below for an example.

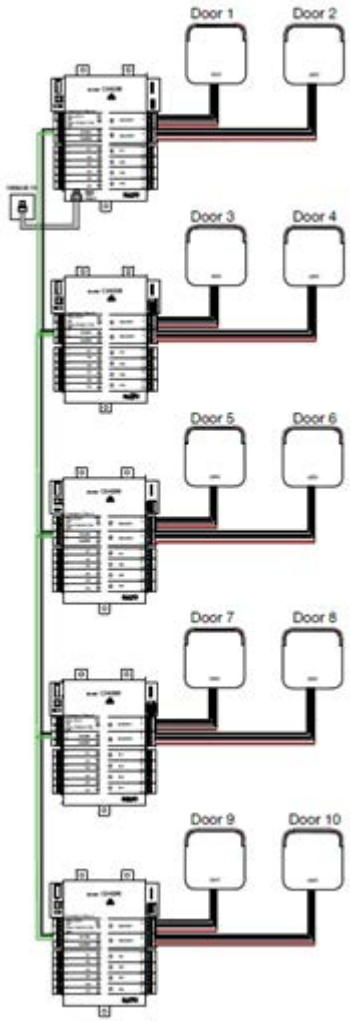


Figure 251: CU42E0 and CU4200 example

NOTE: The maximum distance between the gateway (CU42E0) and the last node (CU4200) in line cannot be over 300 meters.

To add a CU42E0 gateway, perform the following steps:

86. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
87. Click **Add Network Device**. The **Add network device** dialog box is displayed.
88. Select **CU42E0 gateway** from the drop-down list.
89. Click **OK**. The **CU42E0 gateway** information screen is displayed.

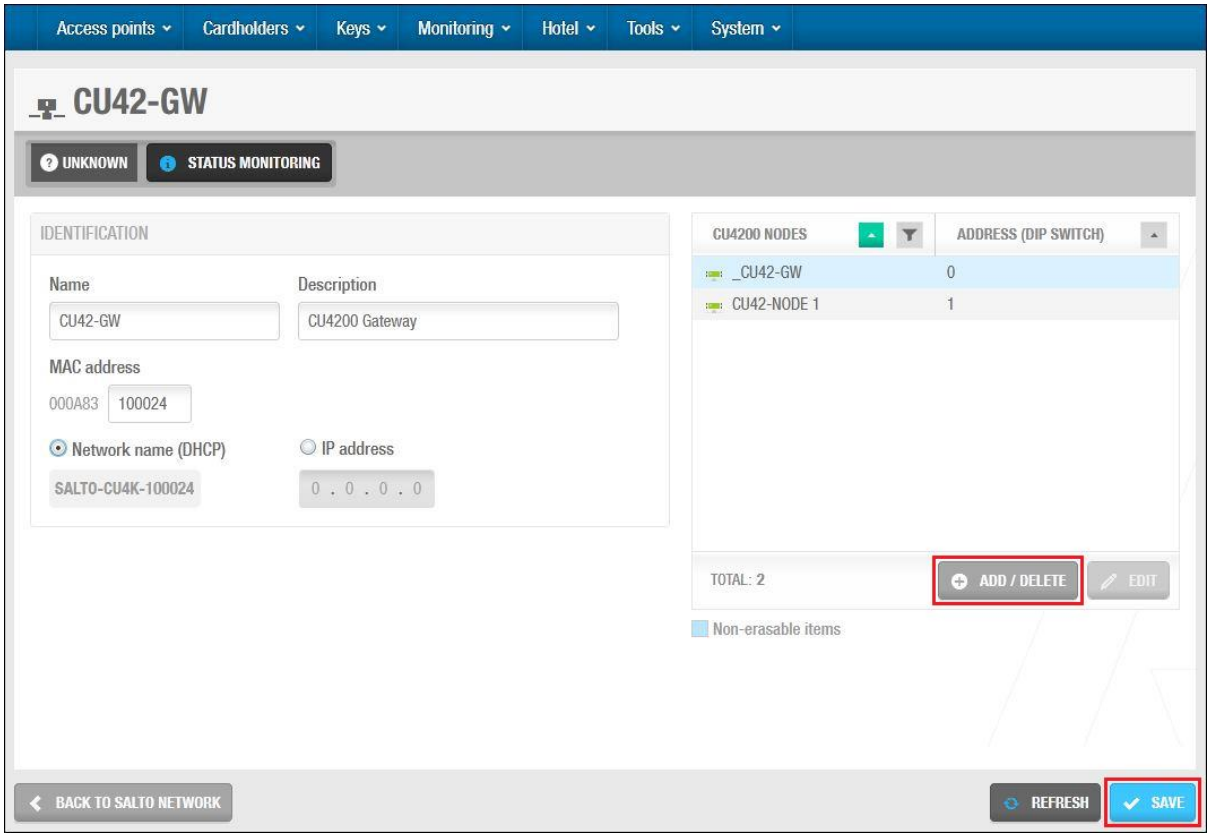


Figure 252: CU4200 gateway information screen

90. Type a name for the CU42E0 gateway in the **Name** field.
91. Type a description for the CU42E0 gateway in the **Description** field.
92. Type the MAC address in the **MAC address** field.

    The MAC address is displayed on a sticker on the CU.
93. Select either the **Network name (DHCP)** or **IP address** radio button.

    If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the CU42E0 gateway. A DHCP server and a DNS are required for this option. If you select the **IP address** option, you must type an IP address in the field.
94. Select the appropriate time zone from the **Time Zone** drop-down list.

    Note that the **Time Zone** panel is only displayed if you have enabled the multiple time zones functionality in ProAccess SPACE General options. See *Activating Multiple Time Zones* and *Time Zones* for more information.
95. Click **Add/Delete** in the **CU4200 Node** panel. The **Add/Delete** dialog box, showing a list of CU4200 nodes, is displayed.

    The **Add/Delete** dialog box only displays CU4200 nodes if you have already added them to the system. You can also connect CU4200 nodes to CU42E0 gateways when you add CU4200 nodes to the system. See *Adding CU4200 Nodes* for more information.
96. Select the required CU4200 node in the left-hand panel and click the chevron. The selected CU4200 node is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the CU4200 nodes to make multiple selections. You cannot add CU4200 nodes that already belong to another CU4200 gateway.

NOTE: When you add a CU42E0 gateway, an embedded CU4200 node is automatically created. This cannot be deleted. Each CU42E0 gateway can support its embedded CU4200 node and a maximum of four other CU4200 nodes. The name of the embedded node will be always the same than the parent CU42E0 gateway preceeded by an underscore. For example: **_CU4200**.

97. Click **Accept**. The selected CU4200 node is displayed in the **CU4200 Node** panel.

    You can select the CU4200 node and click **Edit** to change the number in the **Address (dip switch)** column if required. See *Adding CU4200 Nodes* for more information about the **Address (dip switch)** field. Note that embedded CU4200 nodes have a fixed number (0). This cannot be changed.
98. Click **Save**.

12. 8. 1. 5. Adding CU4200 Nodes

CU4200 nodes are network connection points that are physically connected to a CU42E0 gateway using an RS485 cable. See *Adding CU42E0 Gateways* for more information about CU42E0 gateways. This establishes communication between the CU4200 nodes and the CU42E0 gateway.

The CU4200 nodes receive data from the CU42E0 gateway so they do not require a TCP/IP connection. Instead, they communicate with the SALTO network through the CU42E0 gateway to which they are connected.

You must connect CU4200 nodes to CU42E0 gateways in ProAccess SPACE. You must also connect CU4200 nodes to access points. This means that the system can show which items are connected. Each CU4200 node can control a maximum of two doors.

NOTE: You must select **Online IP (CU4200)** in the **Connection Type** panel on the **Door** and in **Room** information screen before you can connect an access point to a CU4200 node.

To add a CU4200 node, perform the following steps:

99. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
100. Click **Add Network Device**. The **Add network device** dialog box is displayed.
101. Select **CU4200 node** from the drop-down list.
102. Click **OK**. The **CU4200 node** information screen is displayed.

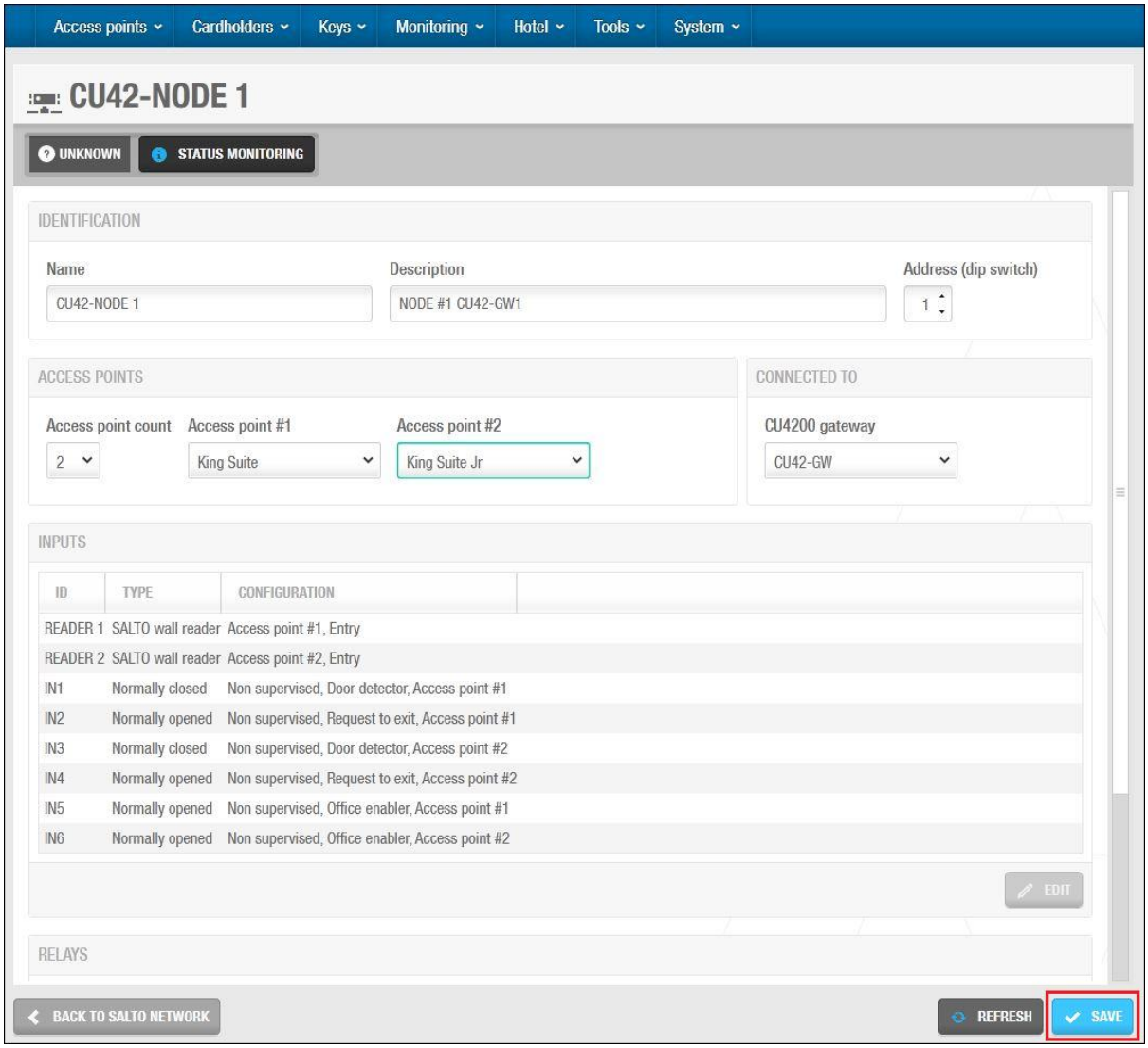


Figure 253: CU4200 node information screen

103. Type a name for the CU4200 node in the **Name** field.
104. Type a description for the CU4200 node in the **Description** field.
105. Select the required number by using the up and down arrows in the **Address (dip switch)** field.

    This number corresponds to the switches on the dip switch panel. The system allows you to select any number between 1 and 99. However, you must select a number between 1 and 15 due to hardware limitations. A CU42E0 gateway can support an embedded CU4200 node and a maximum of four other CU4200 nodes. Each CU4200 node that you connect to a specific CU42E0 gateway must have a unique number, for example, 1, 2, 3, until 15. Note that the value 0 is used for embedded CU4200 nodes. Bear in mind that addresses set up on the nodes should follow the physical dipswitches' configuration on each CU4200 unit.

Table 61: Dipswitch configuration

Dip switch	Address (dip switch)
0000	Address 0, only for embedded CU4200 nodes.
0001	Address 1

Dip switch	Address (dip switch)
0010	Address 2
0011	Address 3
0100	Address 4
0101	Address 5
0110	Address 6
0111	Address 7
1000	Address 8
1001	Address 9
1010	Address 10
1011	Address 11
1100	Address 12
1101	Address 13
1110	Address 14
1111	Address 15

See the following image as an example;

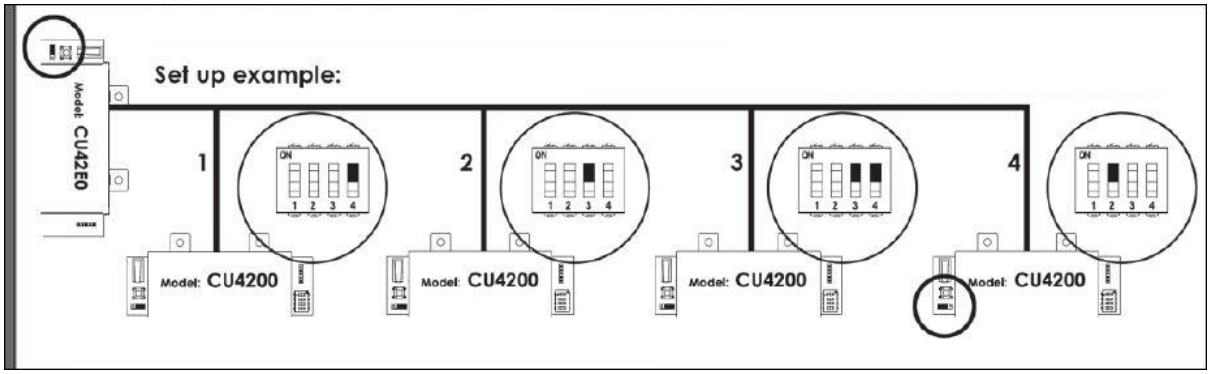


Figure 254: CU4200 dip switches set up

106. Select the required number from the **Access point count** drop-down list.

You can select either **1** or **2**. This defines the number of doors you want the CU4200 node to control. Each CU4200 node can control two readers. This means it can control either one door that has two readers or two doors where each has one reader. If a door has two readers, one reader controls access from inside to outside, and the other reader controls access from outside to inside. You should select **1** if a door has two readers. If you select **2**, an **Access point #2** field is displayed on the right-hand side of the **Access point #1** field, and you can select an additional door from the drop-down list.

107. Select the required door from the **Access point #1** drop-down list.

The **Access point** drop-down lists only display doors if you have already defined some as CU4200 access points. This is done by selecting **Online IP (CU4200)** in the **Connection Type** panel on the **Door** information screen. You can also connect online IP (CU4200) doors to CU4200 nodes in the **Connected to** field on the **Online IP (CU4200)** information screen. See *Online IP (CU4200)* for more information.

108. Select the CU42E0 gateway to which you want to connect the CU4200 node from the **Connected to** drop-down list.
109. Click **Save**.

12. 8. 1. 6. Using CU4200 Inputs

Inputs are the signals or data received by the CU4200. You can setup the inputs in ProAccess SPACE so the CU4200 can understand how to act. You can set Inputs for **Reader 1** and **Reader 2**. You can also set up to 6 inputs from third party devices.

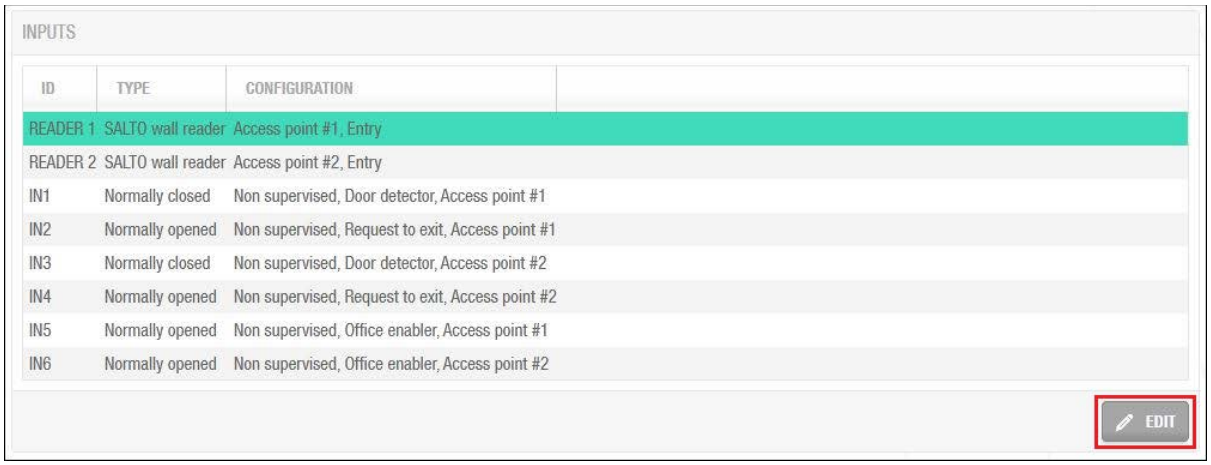


Figure 255: CU4200 node Inputs

You can set the CU4200 outputs according with the wall reader input. To manage the wall reader input, select the reader and click **Edit**.

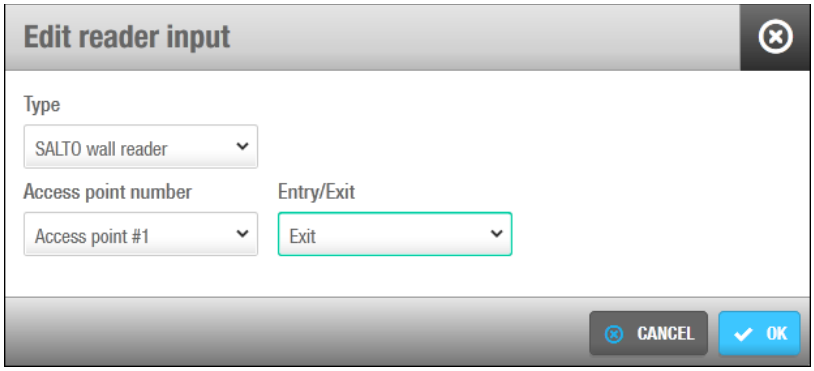


Figure 256: CU4200 node Reader Input

The **Reader input** fields are described in the following table.

Table 62: Reader Inputs fields

Field	Functionality
Type	You can select **None** if no SALTO wall reader is connected or **SALTO wall reader** if it is a SALTO wall reader. Other options may appear in the future. If **None** is selected, inputs 3, 4 and 5, 6 can be used with a third party wall reader.
Access point number	As the CU4200 can manage up to two different access points, you can decide whether the reader will trigger an opening in access point #1 or #2. See *Adding CU4200 Nodes* for more information.

Field	Functionality
Entry/Exit	Select whether the wall reader is an Entry or an Exit.

The CU4200 node can manage inputs from third party devices. Depending the signal or data arrived to the input the CU4200 Node can act accordingly. Select the **Input ID** and click **Edit**.

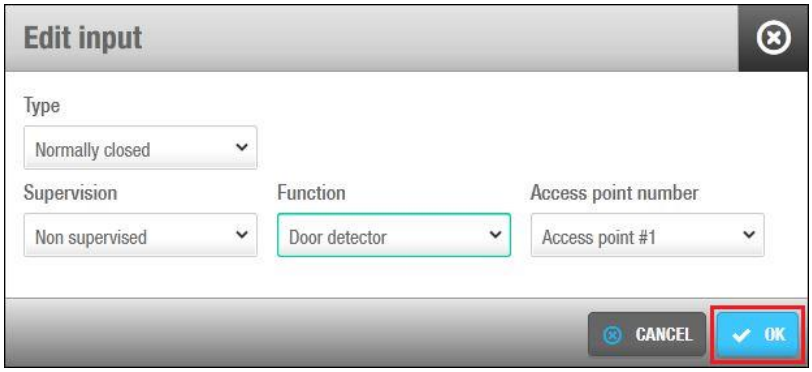


Figure 257: CU4200 node Reader Input

The **Inputs** fields are described in the table below,

Table 63: Inputs fields

Field	Functionality
Type	Status of the relay in normal position. The relay can be normally in closed position or opened position.
Supervision	Select the resistance as required for the supervision. A supervised input is protected against external attacks.
Function	Select the function you want for the relay. Options include doo Door detector, Office enabler, Intrusion inhibition, Request to open roller blind, Request to close roller blind, Request to Exit or Request to Open.

For example, according to the image below, a relay in normally opened position could send a request to open a roller blind when presenting a valid key in reader #1 from IN1 and request to close the roller blind from IN2.

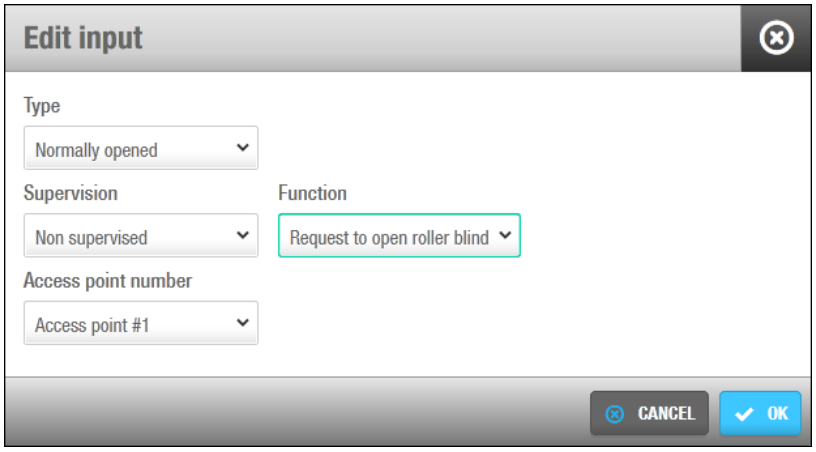


Figure 258: Roller blind example

A reader that is not from SALTO can also be used. **Edit Reader Input** Type must be set to **None**. **Type** field in **Edit Input** shows the **Third party reader** option in the dropdown menu. Only a **Wiegand** code is supported. See *Devices Tab* in General options for more information about how to configure the Wiegand format. An authorization code has to be entered for each user in the **Authorization code** field on the **User** profile. See *Users* in **Cardholders** menu for more information. Select the **Access point** from the **Access point number** dropdown menu and if it will be an **Entry** or an **Exit.**

12. 8. 1. 7. Managing CU4200 Relays

A relay is an electrically operated switch. It is used where it is necessary to control a circuit by a low-power signal. For example, you can control an electric or magnetic strike, trigger a camera recording or turn an alarm off.

The CU4200 node has 4 relays that can be configured independently. Select the relay ID and click **Edit**. The **Edit Relay** fields are described in the table below

Table 64: Edit Relay fields

Field	Functionality
Type	Select the appropriate type as needed.
Access point number	Select the access point in question. It can be **Access point #1**, **Access point #2** or both.
Output	The **Output** dropdown menu is shown when Output is selected in **Type** dropdown menu. Select the Output from the dropdown menu. The list of outputs have to be created first in **Outputs** list, in the **Access points** menu. See Access points *Outputs* for more information about how to create Outputs. The relay will be triggered when a key with a valid output is presented to the wall reader. See User *Outputs* for more information about how to add outputs in the user access.
Conditions	Select **Combined** in the **Type** dropdown menu to select a combination of conditions. According to the image below, the relay will be triggered if in Access point #1 the **Door is left opened**, if there is an **Intrusion** or if there is a **Card rejected**.

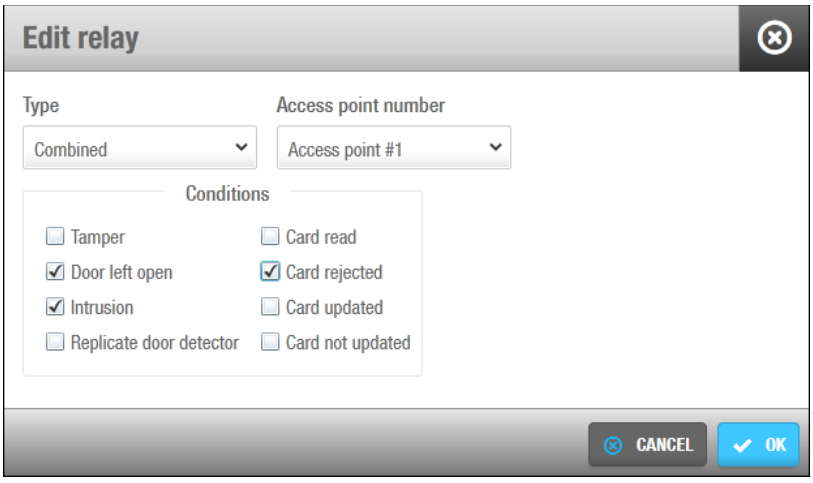


Figure 259: Combined relay type

12. 8. 1. 8. CU42X0 devices initialization and update

The CU42E0 gateways and CU4200 nodes are initialized and updated automatically. See table below for the frequency of each.

Table 65: CU42x0 Initialization and Update

Automatic process	Check Frequency	Notes
CU4K doors initialization	1 minute	Includes initialization + update
CU4K doors update	5 minutes	Can be executed on request
CU4K nodes initialization	1 minute	Includes initialization + update
CU4K nodes update	5 minutes	Can be executed on request

NOTE: Even if updates are performed automatically every 5 minutes for the CU42x0, a manual update can be performed immediately by selecting the device and clicking the **Update** button in **SALTO network**.

12. 8. 2. Filtering SALTO Network Data

You can filter SALTO network data by type, name, description, and/or IP address.

You can filter by the following item types:

- Online IP (CU5000)
- CU42E0 gateway
- CU4200 node
- Online IP (CU4200)
- Encoder
- RF gateway
- RF node
- Online RF (SALTO)
- BAS gateway
- Online RF (BAS integration)

To filter the SALTO network data, perform the following steps:

110. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
111. Click **Filters**. The **Items filtering** dialog box is displayed.
112. Select a pre-defined search term from the **Type** drop-down list.
113. Type the name of the item you want to search for in the **Name** field.
114. Type the description of the item you want to search for in the **Description** field.
115. Type the IP address in the **IP address** field if appropriate.

    The **IP address** field is only displayed for relevant search term types.

116. Click **Apply Filter**. A filtered SALTO network list is displayed.

    When a filter has been applied, on the **SALTO Network** screen when you have applied a filter, the search type is displayed in light blue. You can click the search type to once again display all items on the list screen. You can click **Delete Filter** to delete the filter and to redefine the filter parameters.

117. Click the **Close** icon in the **Applied Filters** field when you have finished reviewing the filtered list or click **Filters** to apply another filter.

12. 8. 3. Configuring Online Connection Types

When adding a door or room to the system, you must specify the appropriate connection type – either online or offline. When you select an online connection type, the door or room is displayed on the **SALTO Network** screen, and you can double-click the entry to configure it.

There are four online connection types:

- Online IP (CU5000)
- Online IP (CU4200)
- Online RF (SALTO)
- Online RF (BAS integration)

NOTE: Your BAS integration must be fully configured in ProAccess SPACE General options before you can select this option. See *BAS Tab* for more information.

See *Connection Types* for more information about selecting the correct connection types in non-hotel sites. For information about connection types in non-hotel sites, see *Connection Types*.

12. 8. 3. 1. Online IP (CU5000)

To configure an online IP (CU5000) door, perform the following steps:

118. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
119. Double-click the online IP (CU5000) door that you want to configure. The **Access point: Online IP (CU5000)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU5000) doors are online SVN points.

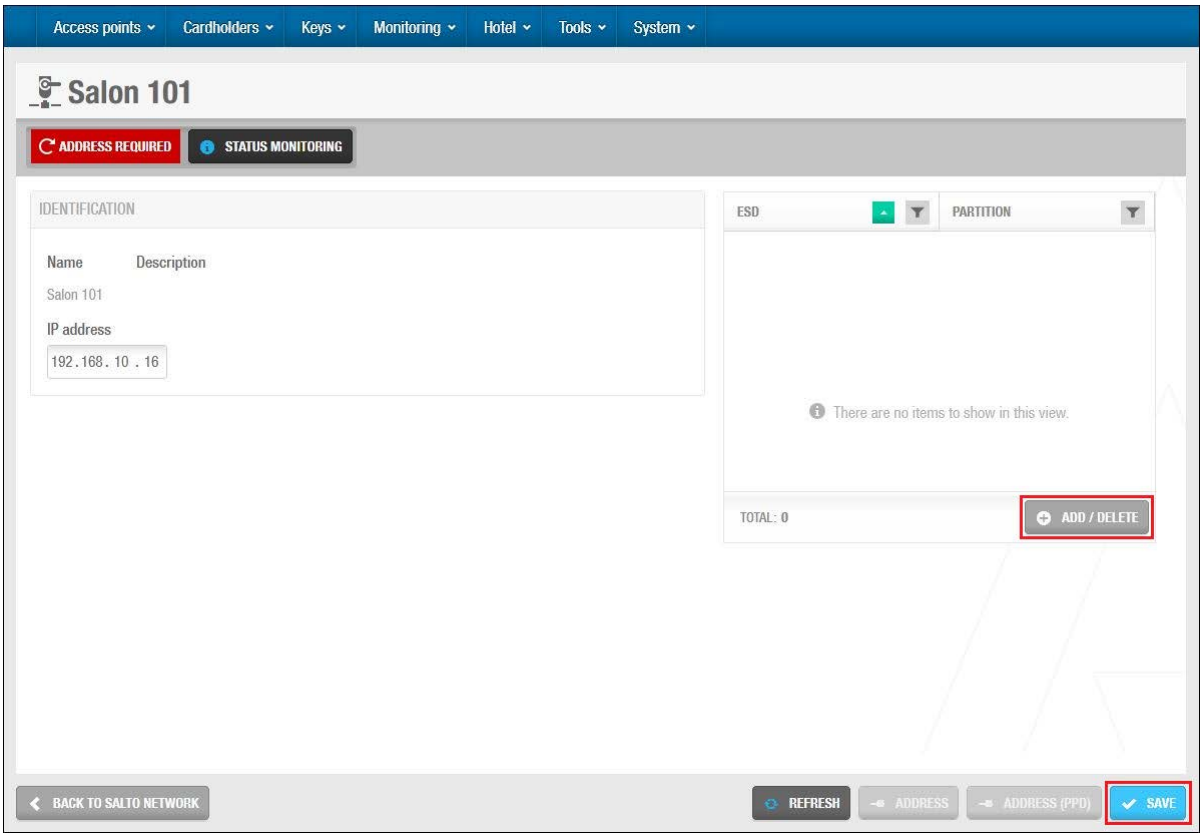


Figure 260: Access point: Online IP (CU5000) information screen

120. Type an IP address for the door in the **IP address** field.
121. Click **Add/Delete** in the **ESD** panel. The **Add/Delete** dialog box, showing a list of ESDs, is displayed. See *ESDs* for more information about ESDs.
122. Select the required ESD in the left-hand panel and click the chevron. The selected ESD is displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the ESDs to make multiple selections.
123. Click **Accept**. The selected ESD is displayed in the **ESD** panel.
124. Click **Save**.

12. 8. 3. 2. Online IP (CU4200)

To configure an online IP (CU4200) door, perform the following steps:

125. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
126. Double-click the online IP (CU4200) door that you want to configure. The **Online IP (CU 4200)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online IP (CU4200) doors that are not connected to CU4200 nodes are displayed in the **Unreachable items** tab. See *Adding CU4200 Nodes* for more information about CU4200 nodes.

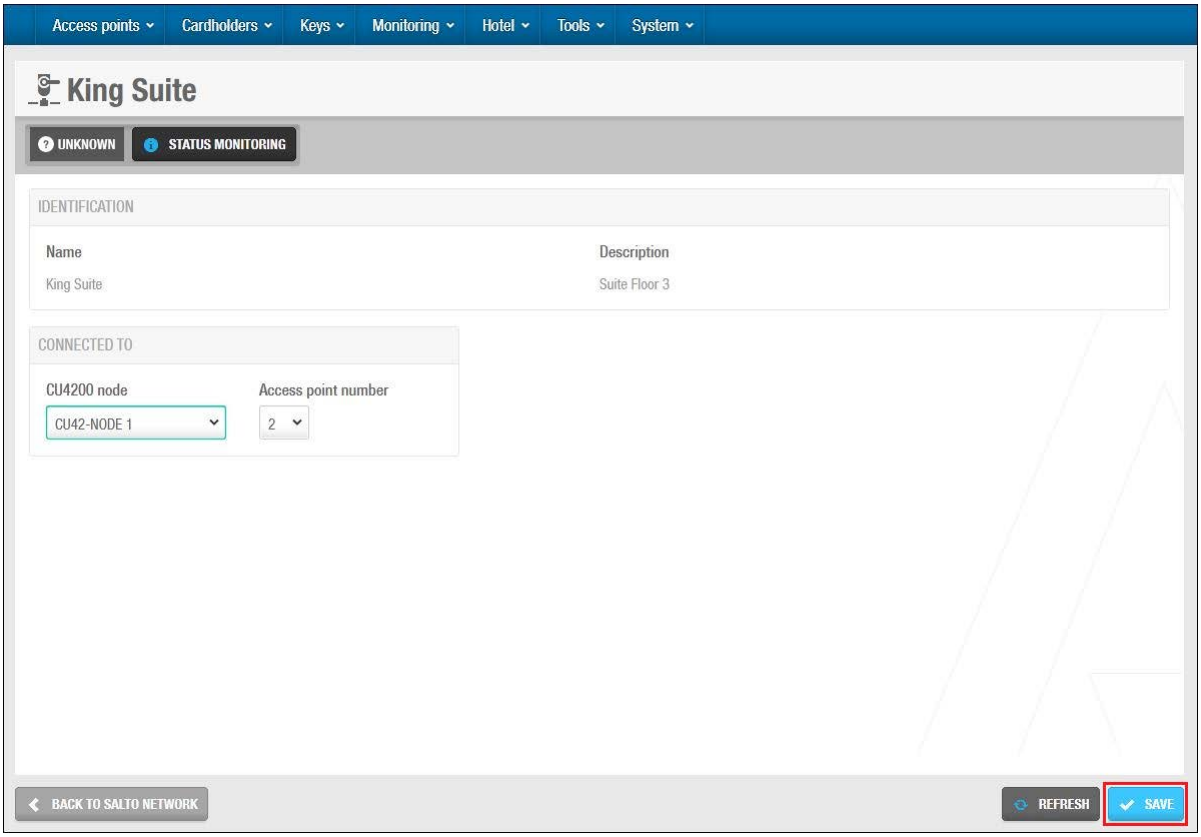


Figure 261: Online IP (CU4200) information screen

127. Select the CU4200 node to which you want to connect the door from the **Connected to** drop-down list.
128. Select either **1** or **2** from the **Door number** drop-down list.

    You cannot select **2** unless you have selected **2** in the **Access point count** drop-down list on the **CU4200 node** information screen. Otherwise, this exceeds the door number count for the node. See *Adding CU4200 Nodes* for more information.
129. Click **Save**.

12. 8. 3. 3. Online RF (SALTO)

To configure an online RF (SALTO) door, perform the following steps:

130. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
131. Double-click the online RF (SALTO) door that you want to configure. The **Online RF (SALTO)** information screen is displayed.

NOTE: The connection type is displayed when you hover the mouse pointer over the icon beside the door name in the **Name** column. Online RF (SALTO) doors that are not yet connected to RF nodes are displayed in the **Unreachable items** tab. See *Adding RF Nodes* for more information about RF nodes.

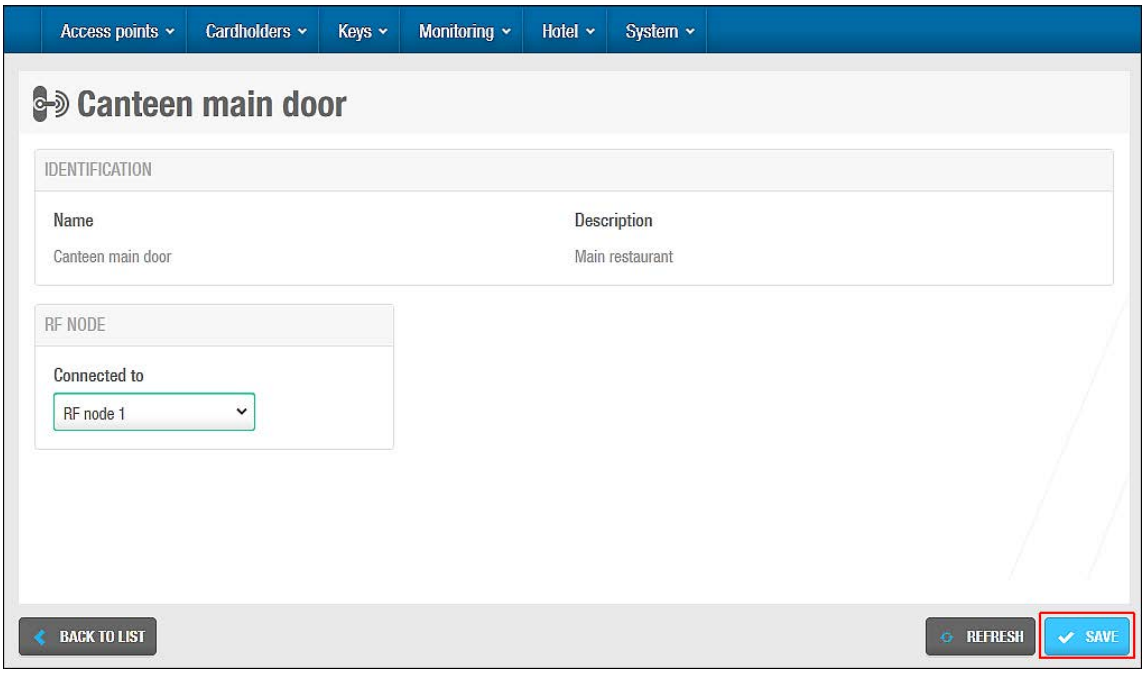


Figure 262: Online RF (SALTO) information screen

132. Select the RF node to which you want to connect the door from the **Connected to** drop-down list.
133. Click **Save**

12. 8. 4. Peripherals Addressing and Maintenance

SALTO network items like Control units, Ethernet encoders, gateways and RF nodes can be added and managed in ProAccess SPACE where you can also make changes such as updating online CUs or updating firmware.

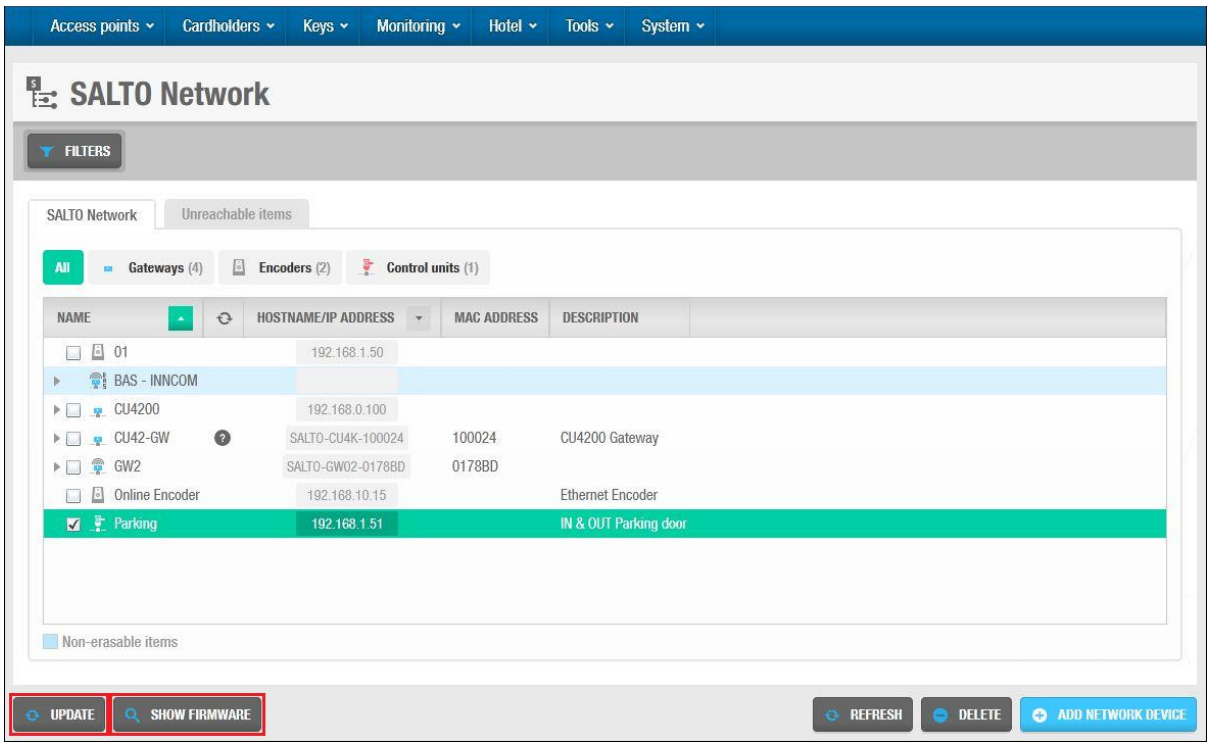


Figure 263: Address and Maintenance

The **Address** and **Maintenance** tab buttons are described in the following table.

Table 66: Maintenance buttons

Button	Functionality
Update	Allows updates to the SALTO database to be communicated to the selected network items. In addition, it allows blacklists to be transmitted automatically to doors without the need to visit each door with an updated key. SAM cards can also be used to transfer information to online doors and to update offline escutcheons and cylinders. See *SAM and Issuing Data* for more information. To SAM a local encoder, click **Supported Keys** on the **Settings** screen in ProAccess SPACE. See *Encoder Settings* for more information. You will find this button in all updatable devices such as control unit CU5000 and CU4200.
Show firmware	Displays the firmware version of the selected item. You can check the firmware version for any online device, CU, RF door, or Ethernet encoder. We recommended that you use the latest firmware version with the SALTO system. Online CUs consist of an Ethernet board and a CU board. This may require updating an individual or multiple online CUs to the most recent firmware version. See *Updating Firmware* for more information about updating multiple online CUs simultaneously. You will find this button in all firmware updatable devices such as control unit CU5000, CU4200 gateways and Ethernet encoders.
Address	Assigns an IP address that you have entered on the system for an Ethernet encoder or an online IP (CU5000) door if the peripheral is in the same network. When you click **CLR** on the online CU, for example, the device enters listening mode. When you click **Address** on the **Monitoring** tab, the software sends a broadcast to the online CU. When the broadcast reaches the online CU, it initializes it with the new IP and other door parameters. Note that you can only address one peripheral at a time when using this option. See *Adding Ethernet Encoders* and *Online IP (CU5000)* for more information about entering IP addresses for Ethernet encoders and online IP (CU5000) doors. You will find this button in all updatable devices such as control unit CU5000 and Ethernet encoders.
Address (PPD)	Assigns an IP address, using a PPD, to an online CU if the peripheral is in a different network. When the online CU is initialized by the PPD, click **Address (PPD)** on the **Monitoring** tab. This creates an authentication between the system and the peripheral. You must enable this option by selecting the **Enable control unit IP addressing by PPD** checkbox in **System** > **General options** > **Devices** in ProAccess SPACE. See *Devices Tab* for more information. See also *PPD* for more information. You will find this button in all updatable devices such as control unit CU5000.
Signal	Used to help identify the physical Ethernet encoder that corresponds to the applicable IP/peripheral. After you select the peripheral in the list and click **Signal**, the LED of the applicable encoder starts flashing. At this point, the SAMing process can take place. See *SAM and Issuing Data* for more information.

The columns at the top of the **Maintenance** tab are described in the following table.

Table 67: Maintenance columns

Column	Functionality

Column	Functionality
Name	Specifies the name of the item (the icon immediately before the item name indicates the peripheral type)
Update Status	Shows the peripheral update status. If no update is required, no icon will be shown. The status could be **Update required**, **Address required** or **Unknown.** Note that this column does not have a title on the screen.
Hostname/ IP address	Specifies the network name that identifies the item
MAC Address	Specifies the MAC address of the device.
Description	Matches the details of the item entered in the **Description** field in ProAccess SPACE

12. 8. 4. 1. Updating Firmware

Firmware is software that is programmed on the ROM of hardware devices.

NOTE: SALTO provides firmware updates when new functionality is available or when a software bug is fixed. Each component has a unique file. Contact your SALTO technical support contact before updating any firmware file.

To update the firmware version of an item, perform the following steps:

134. Select **System** > **SALTO Network**. The **SALTO Network** screen is displayed.
135. Select the required item and click **Show firmware**. The **Firmware information** dialog box is displayed.

Figure 264: Peripheral firmware update dialog box

You can select multiple items on the **SALTO Network** peripheral list if required.

136. Select the checkbox next to the item that you want to update. The **Browse** button is enabled.

    If required, you can click **Check all** to update the firmware for multiple items simultaneously. You can only update multiples of the same item (for example, online CUs only or Ethernet encoders only) simultaneously.
137. Click **Browse** to select the required firmware file.
138. Click **Send firmware**. A confirmation screen is displayed when the firmware update is complete.

NOTE: You can update the firmware for local encoders by using the **Show Firmware** button on the **Settings** screen in ProAccess SPACE. See *Updating Encoder*

Firmware for more information.

12. 9. Calendars

The calendars functionality defines your organization's working calendar. For example, you can define public holidays, company holidays, and company shutdowns. If your organization consists of multiple sites that operate according to different workday calendars, a separate calendar can be created for each site. Up to 255 calendars can be set up on the SALTO system.

A calendar day can be defined as a normal day, a holiday (H1), or a special day (there are two special day definitions available, S1 and S2). Special days may be site-specific holidays or site shutdown days. After you have created a calendar, you can then set up time periods, automatic changes, and cardholder timetables specific to each day type or user. See *Access Point Times Periods*, *Access Point Automatic Changes*, and *Cardholder Timetables* for more information.

12. 9. 1. Creating Calendars

To create a calendar, perform the following steps:

1. Select **System** > **Calendars**. The **Calendars** screen is displayed.

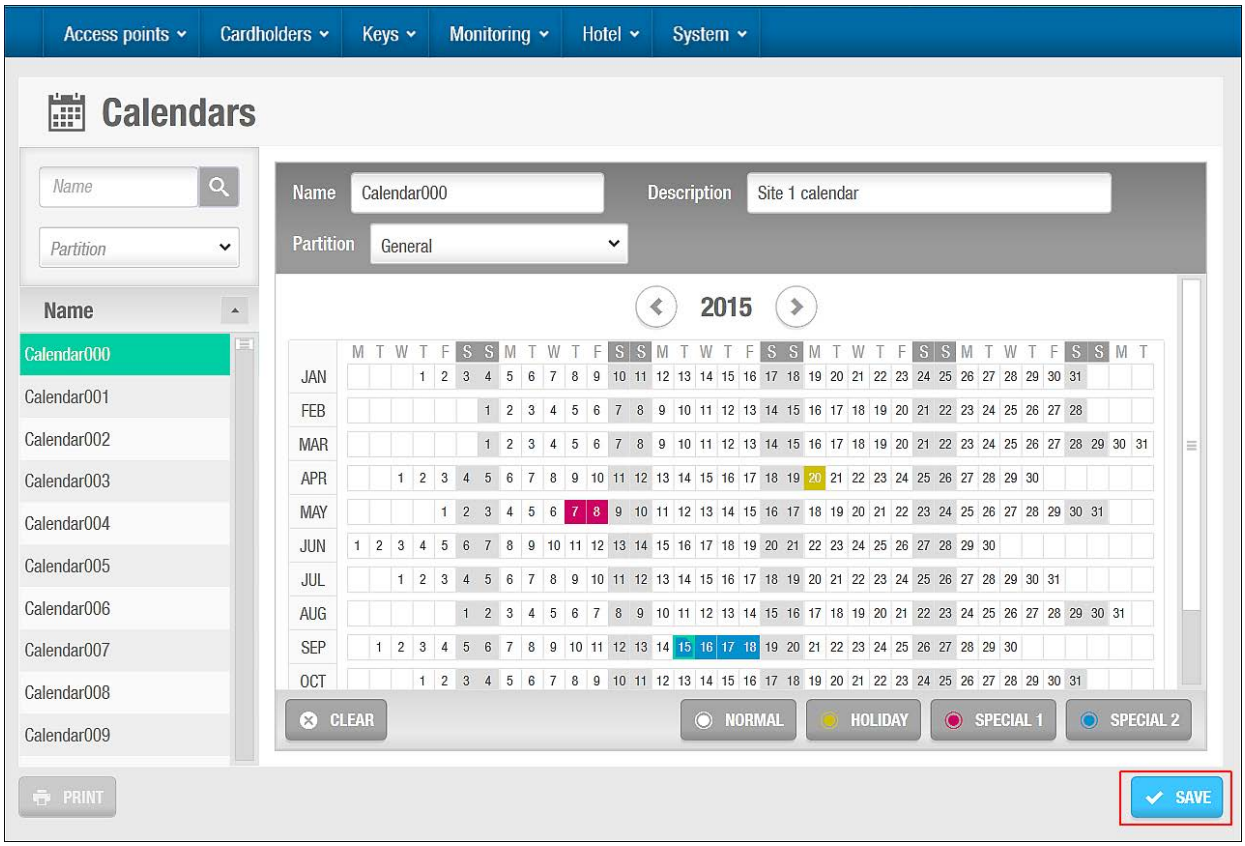


Figure 265: Calendars screen

2. Select a calendar from the **Name** panel.

   You can change the name of the calendar to something meaningful for your organization. For example, if your organization has multiple sites that have different

holiday periods, you could choose a name such as London – Canary Wharf. You can also add a description to further differentiate calendars.

3. Select a partition from the **Partition** drop-down list if required.

   See *Partitions* for more information about partitions.

4. Select the appropriate year.

   By default, the current year is displayed. You can use the arrow keys to scroll backwards or forwards. It is recommended that you configure calendars for the current year and the following year.

5. Click on the date that you want to define as a holiday or a special day.

   By default, all days are defined as normal.

6. Click **Holiday**, **Special 1**, or **Special 2** as appropriate.

   Repeat this step until you have entered all holidays and special days for the specific site. If you are editing an existing calendar, you can redefine a holiday or a special day as a normal day by clicking **Normal**.

NOTE: If users are given access to doors on days that have been defined as holidays or special days, their cardholder timetables must be set up accordingly. See *Cardholder Timetables* for more information.

7. Click **Save**. The calendar is saved.

12. 10. Time Zones

The system has one default time zone. However, you can use multiple time zones in ProAccess SPACE if required. If, for example, a company has offices operating in different time zones, this should be reflected in the system.

You must enable the multiple time zones functionality by using the **General** tab in ProAccess SPACE General options. See *Activating Multiple Time Zones* for more information. When you activate this functionality, an **Add Time Zone** button is added to the **Time zones** screen. This allows you to add time zones and configure the DST for them as appropriate.

A **Time Zone** drop-down list is also displayed on various screens in ProAccess SPACE, for example, the **Door**, **Room**, and **Locker** information screens. You can use the drop-down list to select the time zone that you want to apply to locks and network devices such as encoders and gateways. See *Adding Network Devices* for more information.

12. 10. 1. Adding Time Zones

To add a time zone, perform the following steps:

1. Select **System** > **Time zones**. The **Time zones** screen is displayed.

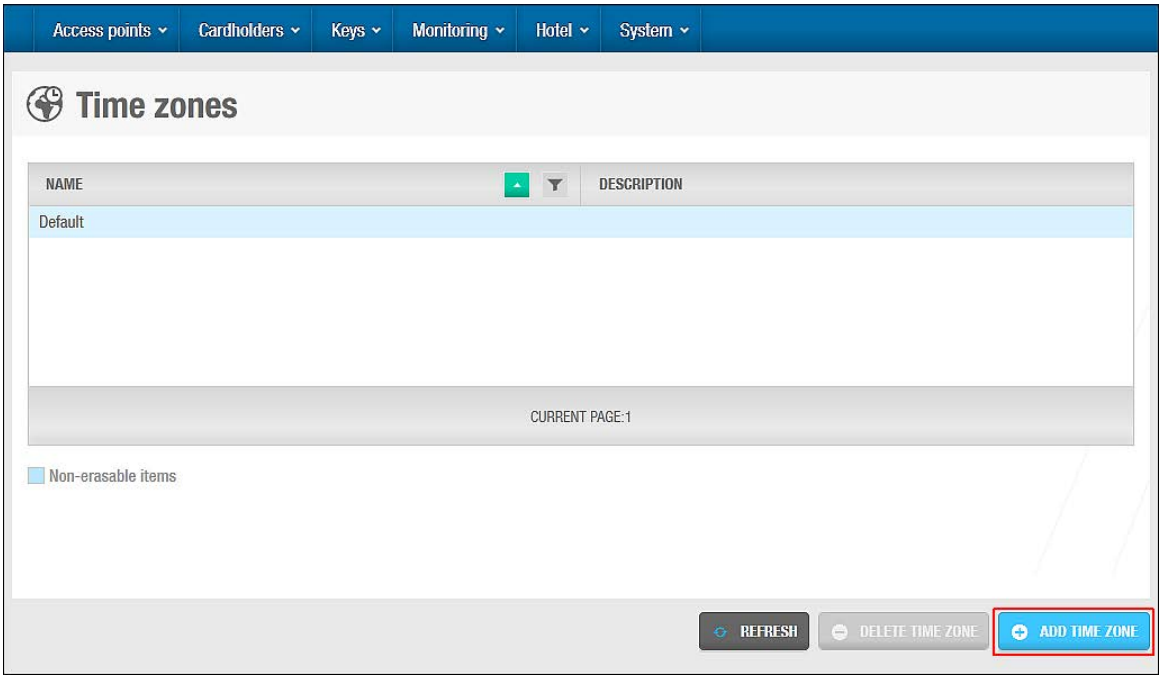


Figure 266: Time zones screen

2. Click **Add Time Zone**. The **Time zone** information screen is displayed.

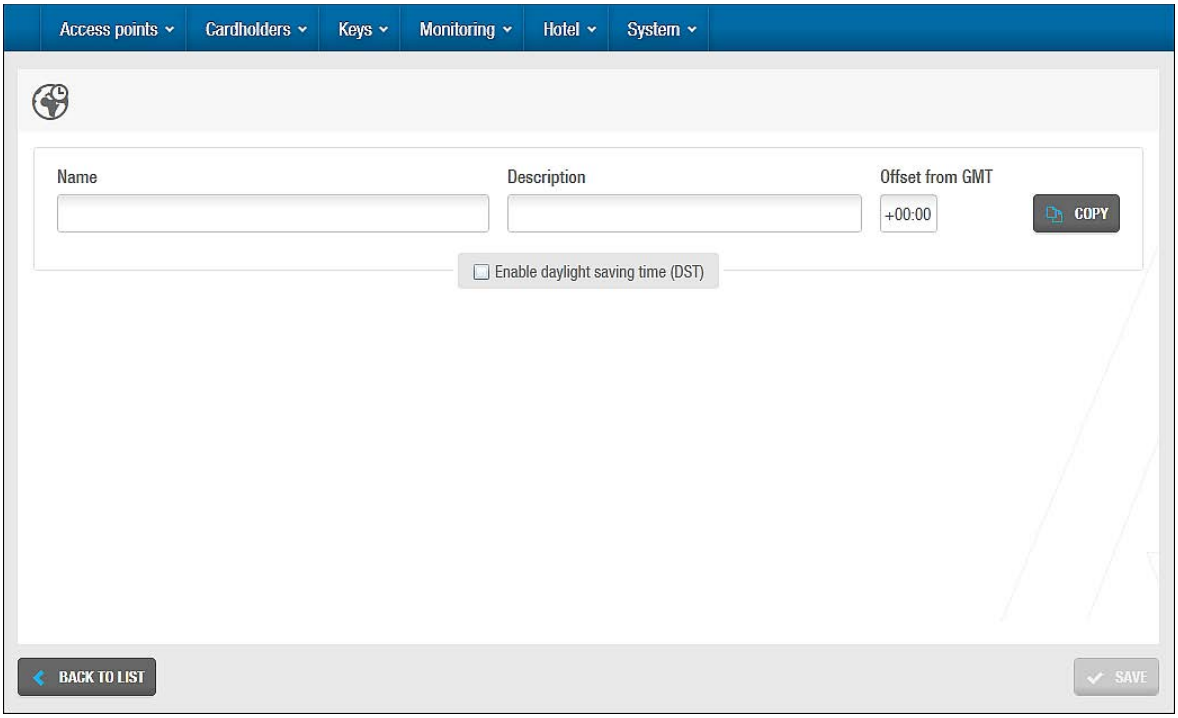


Figure 267: Time zone information screen

3. Click **Copy**. The **System world time zones** dialog box, showing a list of time zones, is displayed.

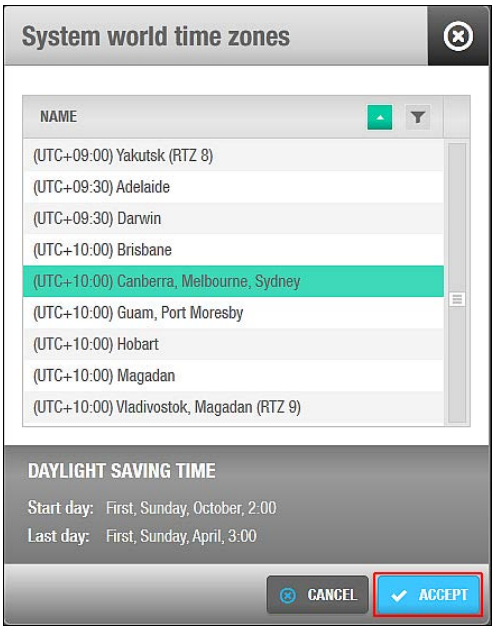


Figure 268: System world time zones dialog box

4. Select the required time zone.
5. Click **Accept**. The **Name**, **Description**, and **Offset from GMT** fields, and the fields for the **DST Rule** option on the **Time zone** information screen are populated with the information for the selected time zone.

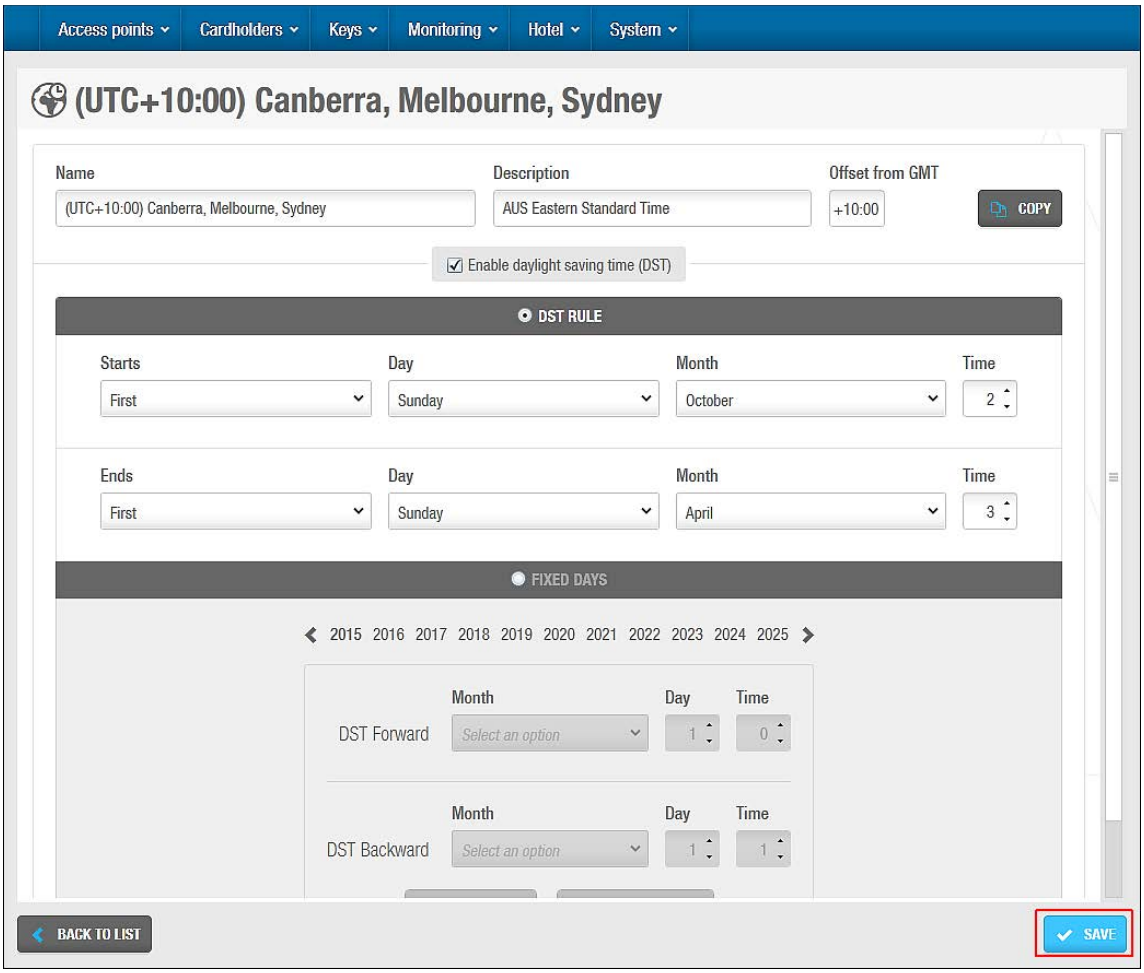


Figure 269: Time zone information screen

Note that the fields for the **DST Rule** option are not populated if the time zone you select does not use DST. You must manually enter the details for the **Fixed Days** option on the system if required. Both options are described in *DST Options*.
Alternatively, you can manually enter the appropriate information for the time zone in the fields on the **Time zone** information screen.

6. Click **Save**.

You can select a time zone on the **Time zones** screen and click **Delete** to delete it. However, you cannot delete the default system time zone.

12. 10. 2. Daylight Saving Time

Daylight saving time (DST) is the practice of moving clocks forward by one hour in Spring to extend light in the evening, and moving clocks back by one hour in autumn.

By default, SALTO electronic locks perform these time changes automatically. However, you can disable this option if required. See *Configuring DST* for more information.

NOTE: It is recommended that you allow the system to update for DST automatically. Otherwise, you must manually update each door with a PPD on the date of the time change.

12. 10. 2. 1. Configuring DST

You can select the month, week, day, and hour when time changes occur for the default system time zone. You can also set the time changes for future years in advance if required.

To configure DST, perform the following steps:

1. Select **System** > **Time zones**. The **Time zones** screen is displayed.

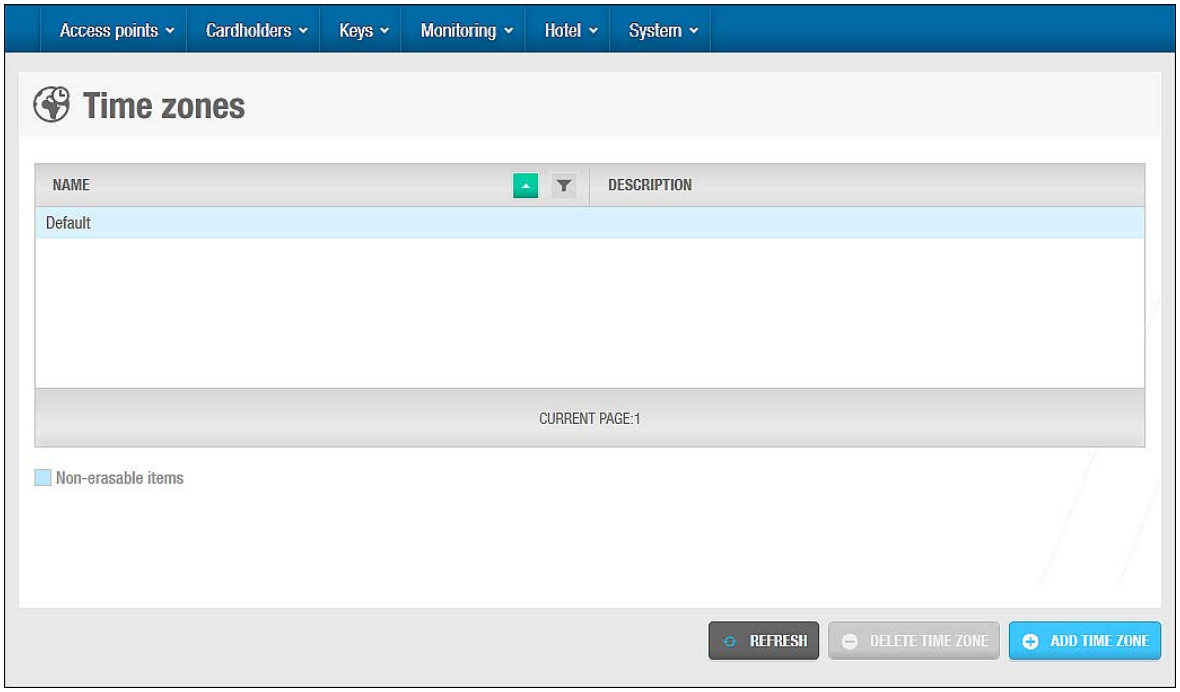


Figure 270: Time zones screen

2. Double-click the **Default** entry. The **Default** information screen is displayed.

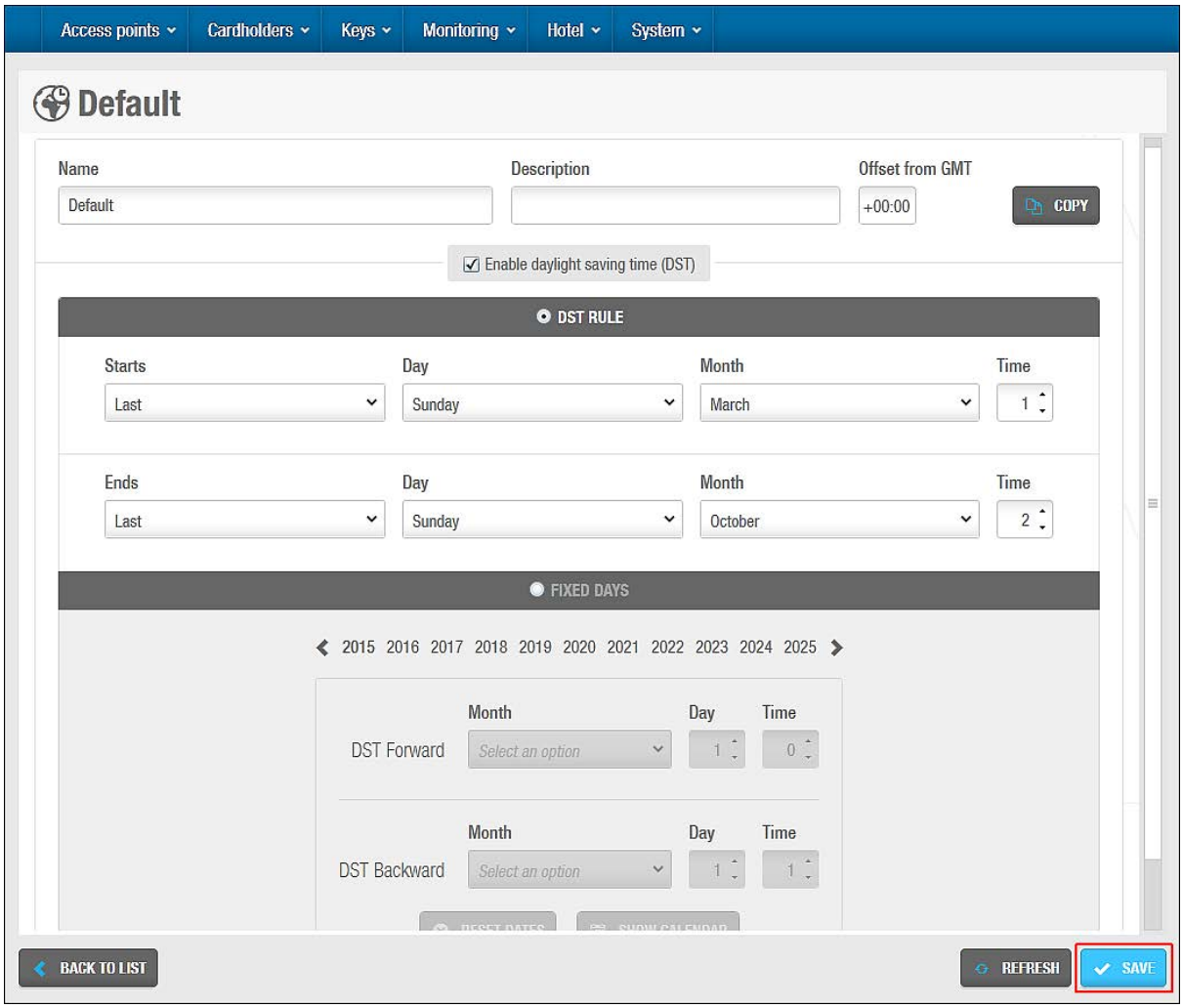


Figure 271: Default information screen

3. Clear the default text and type a name in the **Name** field, for example, Daylight Saving Time. The new screen name is displayed.
4. Type a description for the DST in the **Description** field.

   The **Enable daylight saving time (DST)** checkbox is selected by default. If you clear this checkbox and click **Save**, this disables the DST feature, and the **DST Rule** and **Fixed Days** options are not displayed.
5. Type the appropriate value in the **Offset from GMT** field.

   This value is used to calculate the time zone according to Greenwich Mean Time.
6. Select either the **DST Rule** or the **Fixed Days** option.

   The **DST Rule** option is selected by default. Both options are described in *DST Options*. You can click **Copy** to display the **System world time zones** dialog box and select a time zone from the list. When you do this, the **Name**, **Description**, and **Offset from GMT** fields, and the fields for the **DST Rule** option are populated with the information for the selected time zone. The fields for the **DST Rule** option are not populated if the time zone you select does not use DST. You must manually enter the details for the **Fixed Days** option on the system.
7. Click **Save**.

12. 10. 2. 2. DST Options

The DST options are described in the following table.

Table 68: DST options

Option	Description
DST Rule	Allows you to set the month, week, day, and hour when the forward and backward time changes occur. To do so, select the appropriate parameters in the **Month**, **Starts**, **Ends**, **Day**, and **Time** fields. Note that you cannot set the forward time change to occur after 22:00 or the backward time change to occur after 23:00 on the selected day. You can click **Copy** on the **Time zone** information screen to select a world time zone and populate the fields for the **DST Rule** option with the relevant information for the time zone.
Fixed Days	Allows you to set the month, day, and hour of forward and backward time changes for individual years. To do so, select the appropriate year from the list of years, select the appropriate parameters in the **DST Forward** and **DST Backward** fields, and click **Save**. Note that you cannot set the forward time change to occur after 22:00 or the backward time change to occur after 23:00 on the selected day. You should repeat this process for each required year. You can click **Show Calendar** to select parameters using the calendar view, and click **Reset Dates** to reset the parameters for selected years.

12. 11. General options

See *General options* section.

12. 12. SAM and Issuing Data

Keys must be configured before they can be used with the SALTO system. This process is called key issuing. SALTO can supply sites with keys that have already been issued. Alternatively, sites may request keys that they can configure themselves. This configuration is done by using the **SAM and issuing options** in ProAccess SPACE System. Note that the key issuing functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Sites using the SALTO system have two options for issuing keys:

- Use keys that have been issued and supplied by SALTO. These keys are then ready to be assigned and encoded.
- Use keys that they will configure (issue) themselves for use with the SALTO system

SALTO Authorization Media (SAM) cards are used to reserve and secure space on keys for the SALTO software. This space is already reserved in SALTO keys. However, you must complete this task for keys from third-party manufacturers. You can perform the configuration for Mifare and Legic keys on site by using the **SAM and issuing data** tab. This allows you to create customized configurations for issuing keys. When this task has been completed, these keys cannot be reused in other sites.

The SAMing process involves three steps:

1. Issuing the keys

   This reserves and secures a designated space on keys for the SALTO application.

2. SAMing the SALTO readers

   You must add the SAM keys to the SALTO readers. This enables the readers to access the reserved space in keys and read the SALTO data.

3. SAMing the encoders

   You must add the SAM keys to the system encoders. This enables the encoders to access, and read and write data to the reserved space.

NOTE: If you need to use multiple SAM cards for Mifare or Legic keys, you may need to perform your SAM configuration manually. In this case, you should consult the *SALTO SAMing* documentation and your SALTO technical support contact. SALTO can provide a unique SAM kit to sites.

Select **System** > **SAM & issuing options**.

Ensure that the appropriate key types are selected in the **Active cards** panel.

This defines the key types that will be read by the SALTO locks, encoders, and readers. All of the checkboxes in the panel are selected by default. You should clear the checkboxes for key types that are not used in your site as this increases the speed of the SALTO readers. If you disable a key type, the SALTO readers will not recognize it, even if they are compatible with the key type. You must use a PPD to update the SALTO locks with these changes. See *Updating Locks* for more information.

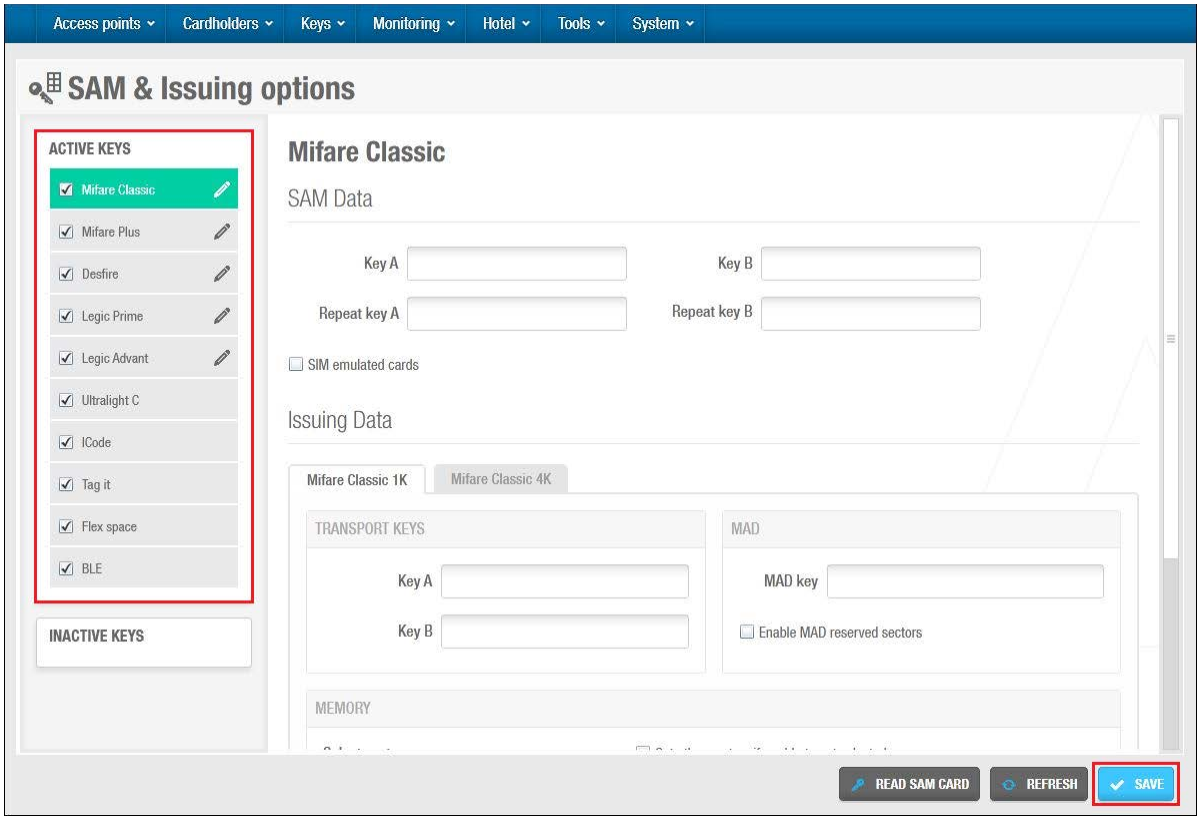


Figure 272: SAM and issuing data

NOTE: The BLE readers use a little more of battery power. If the lock is not meant to be used with the JustIN mobile application BLE can be unchecked to save battery life. See *Assigning a user JustIN mobile key* for more information.

Select the checkbox in **Active keys** to enable and configure each option and define the required key technology. You can then download this information to the PPD, and transfer it to offline or online locks when they are initialized or updated. See *Initializing Locks* and *Updating Locks* for more information.

You can transfer the information to online doors or encoders by using the **SALTO Network** dialog box in ProAccess SPACE. For doors, you must select the required door on the **SALTO Network** and click **Update**. For Ethernet encoders, you must select the required encoder on the **SALTO Network** tab and click **Signal**. See *SALTO Network* for more information. The SAMing is done automatically for local encoders when you use them to read SAM cards. You can also SAM local encoders by clicking the **Supported Keys** button on the **Settings** screen in ProAccess SPACE. See *Encoder Settings* for more information.

SALTO readers are compatible with the SAM functionality. However, you need specific software and hardware versioning to use PPDs or the **SALTO Network Update** option with the SAM functionality.

The following table shows the required software and hardware versioning.

Table 69: Minimum hardware and software requirements for the SAM functionality

Component	Requirement
Software	Version 12.0.1.195 or higher
Encoder	Version 04.11 or higher
XS4 reader module	Version 04.11 or higher
Aelement	Version 01.31 or higher
XS4 locker	Version 01.31 or higher
GEO cylinder	Version 01.12 or higher
Wall reader	Version 04.11 or higher

NOTE: The SAM functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

12. 12. 1. Configuring Mifare Classic Settings

You can configure the settings for Mifare Classic technology by using the **SAM and Issuing options** dialog box.

This process involves two steps:

1. Entering the SAM card data using the **Read SAM card**.

   Note that this step adds the SAM keys to the SALTO software. It also SAMs the local encoder.
2. Entering the data for issuing Mifare Classic 1K and Mifare Classic 4K keys using the **Issuing data** tab

NOTE: It is assumed that operators performing Mifare configurations would be familiar with the technologies and associated terms mentioned in this section.

12. 12. 1. 1. Step One: Entering the SAM Card Data

To complete Step one:

1. Select **System** > **SAM & Issuing options**.
2. Click the **Mifare** pencil in the **Active keys** box.

SAM Data displays information that is transferred to the SALTO locks, encoders, and readers.

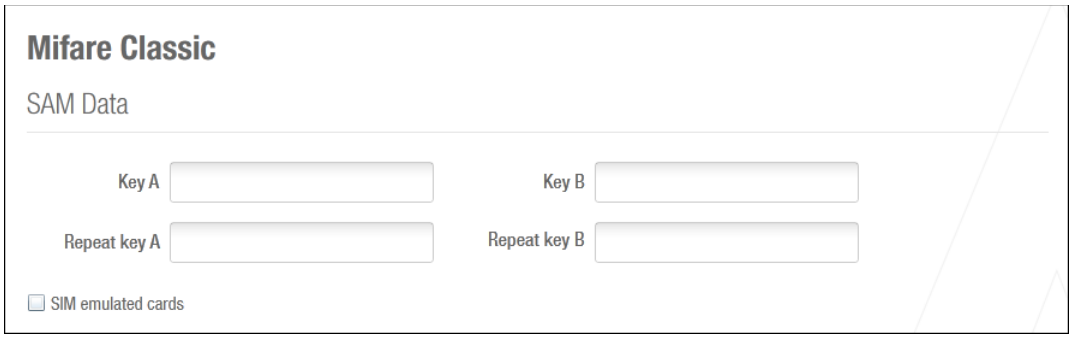


Figure 273: SAM data dialog box

Issuing data displays information required for issuing keys.

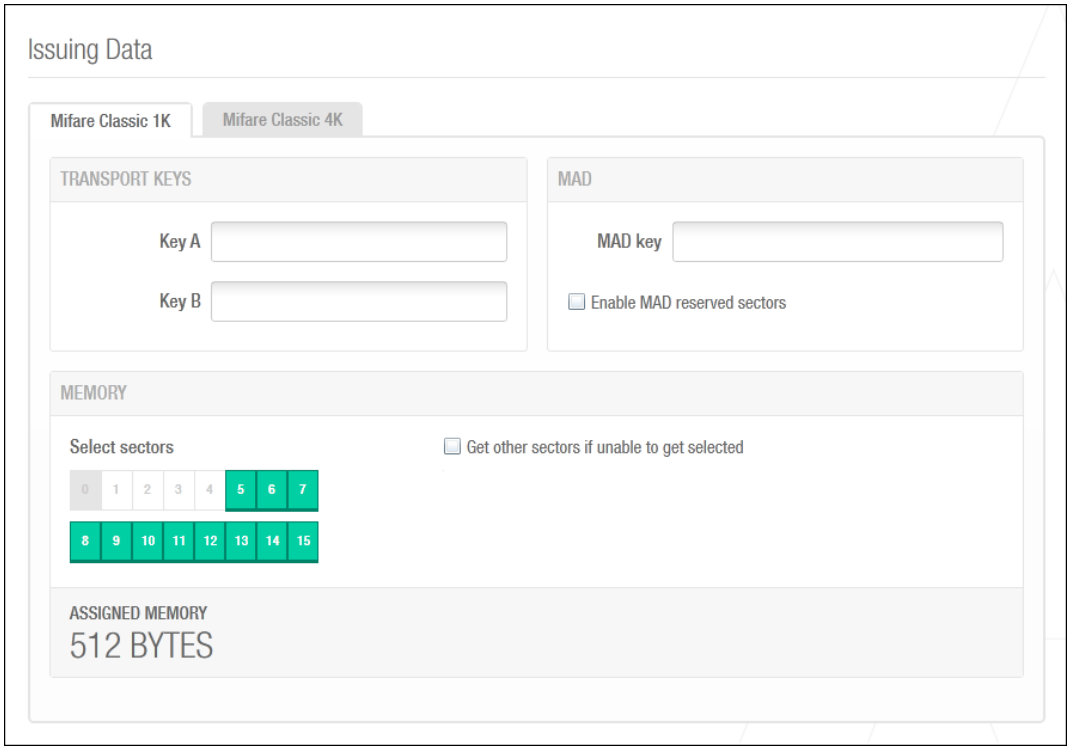


Figure 274: Issuing data dialog box

The **Mifare Classic** and **Mifare Plus** fields, and the **AMK 3DES** and **AMK AES** fields in the **DESfire** panel are editable if you have the SAM custom keys defined by user

functionality enabled in your license. In this case, you can add the key data manually in the required fields. Otherwise, these fields are automatically populated with the relevant Mifare Classic, Mifare Plus, and DESfire keys data when you read the SAM card. See *Registering and Licensing SALTO Software* for more information.

NOTE: In special cases, the system can be configured to allow operators to create SAM cards and use them with the SALTO software. You should consult with your SALTO technical support contact if you want to avail of this option.

3. Click **Read SAM card** if required. A pop-up is displayed asking you to present the key to the encoder.

   This copies the key data on the SAM card to the SALTO software.

4. Place the appropriate SAM card on the encoder when the LED light begins to flash.

   Different SAM cards are used for the Mifare and Legic technologies.

NOTE: You can verify what keys are supported by clicking **Supported Keys** on the **Settings** screen in ProAccess SPACE. See *Encoder Settings* for more information.

5. Select the **SIM emulated cards** checkbox if required.

   You should consult with your SALTO technical support contact if you require additional information about this option.

6. Click **Save**.

   When you click **Save** the key data is masked on the screen for security purposes.

12. 12. 1. 2. Step Two: Entering the Data for Issuing Keys

Complete Step two as appropriate. This depends on whether you are using Mifare or DESFire keys in your site.

Mifare Keys

To complete Step two:

1. Step two is performed in the **Issuing data** section.

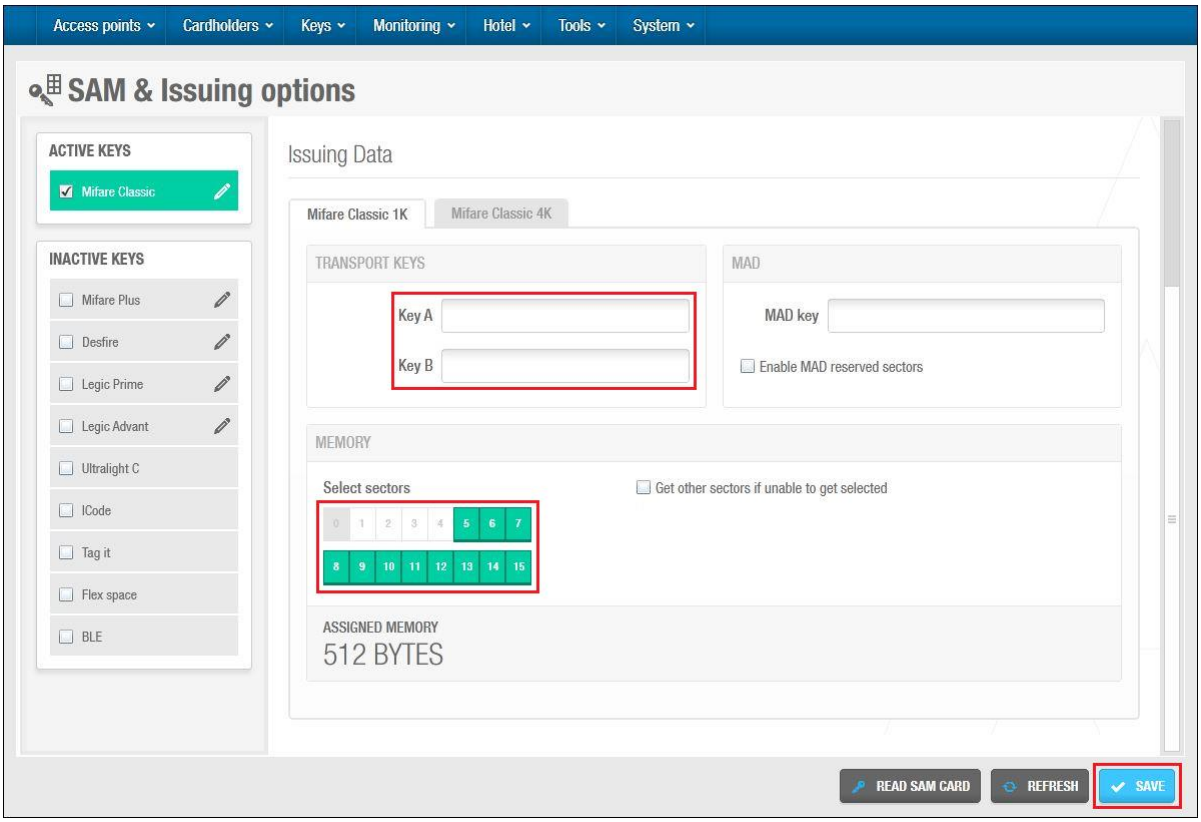


Figure 275: Issuing data tab

The **Mifare 1K** option is selected in the **Card type** panel by default, which means that the configuration fields for this option are displayed.

2. Type the required keys in the **Key A** and **Key B** fields in the **Transport keys** panel.

   You must use hexadecimal format for these. Note that you may need to request these from your SALTO technical support contact.

3. Type the Mifare Application Directory (MAD) key in the **MAD key** field.

   You must use hexadecimal format. All Mifare keys have a MAD, which is the directory of the key, and contains data about the properties of the key sectors.

4. Click **Read SAM** card. A pop-up is displayed asking you to present the key to the encoder.
5. Place the appropriate SAM card on the encoder when the LED light begins to flash.
6. Select the **Get other sectors if unable to get selected** checkbox if required.

   This option allows the SALTO software to select another key sector if a selected sector is already in use by another application.

7. Select the **Enable MAD reserved sectors** checkbox if required.

   This enables the MAD key and secures reserved sectors on the key for the SALTO software.

8. Select the checkboxes for the appropriate key sectors in the **Mifare 1K** panel.

   When you select the checkbox for each sector, this reserves it for the SALTO software. However, you must issue keys for the changes to take effect. This can be done by assigning the keys to users. If you make changes to this selection subsequently, they take effect when you update keys. See *Assigning User Keys* and *Updating Keys* for more information. Note that you can only reserve sectors in keys if you are using a SAM

card distributed by SALTO. The amount of space reserved for SALTO data in keys is displayed in the **Assigned memory** field. You cannot manually amend the value that is shown in this field.

9. Repeat the process to complete the configuration for the **Mifare 4K**, **Mifare Plus 2K**, and **Mifare Plus 4K** options in the **Card type** panel.

   When you select each option, the screen is updated to show the appropriate configuration fields. The checkboxes and the number of key sectors available vary for each option.

NOTE: You can reserve up to 39 key sectors when configuring the Mifare 4K and Mifare Plus 4K keys. If you need to encode these keys with information from multiple sites (rather than a single SALTO site), you must assign at least one of the last four sectors (36, 37, 38, and 39) to each site. The maximum number of sites that can be included in these key types is four. You are required to SAM the Mifare keys if you use this option, so the SALTO readers can operate effectively.

12. 12. 2. Configuring DESFire Keys Settings

Click on the **Desfire** pencil in **Active keys**.

The **SALTO AID** option is selected by default. This option uses the application identifier. However, you can select one of the institutional options that have been integrated with the SALTO software if required. These options are applicable if you are using keys provided by government institutions that can be used with various applications. This is relevant for certain countries.

Institutional keys are predefined SAM keys that are included in the SALTO software by default and embedded in ProAccess SPACE. A certain amount of memory space is reserved for SALTO data on institutional keys. You should consult with your SALTO technical support contact if you are unsure which institutional option to select or require additional information about this functionality. Note that a custom format can be used if you want to include the AMK key in institutional keys. This functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

To complete Step two:

1. Select the **DESFire** option in the **Card type** panel. The screen is updated to show the configuration fields for the option.

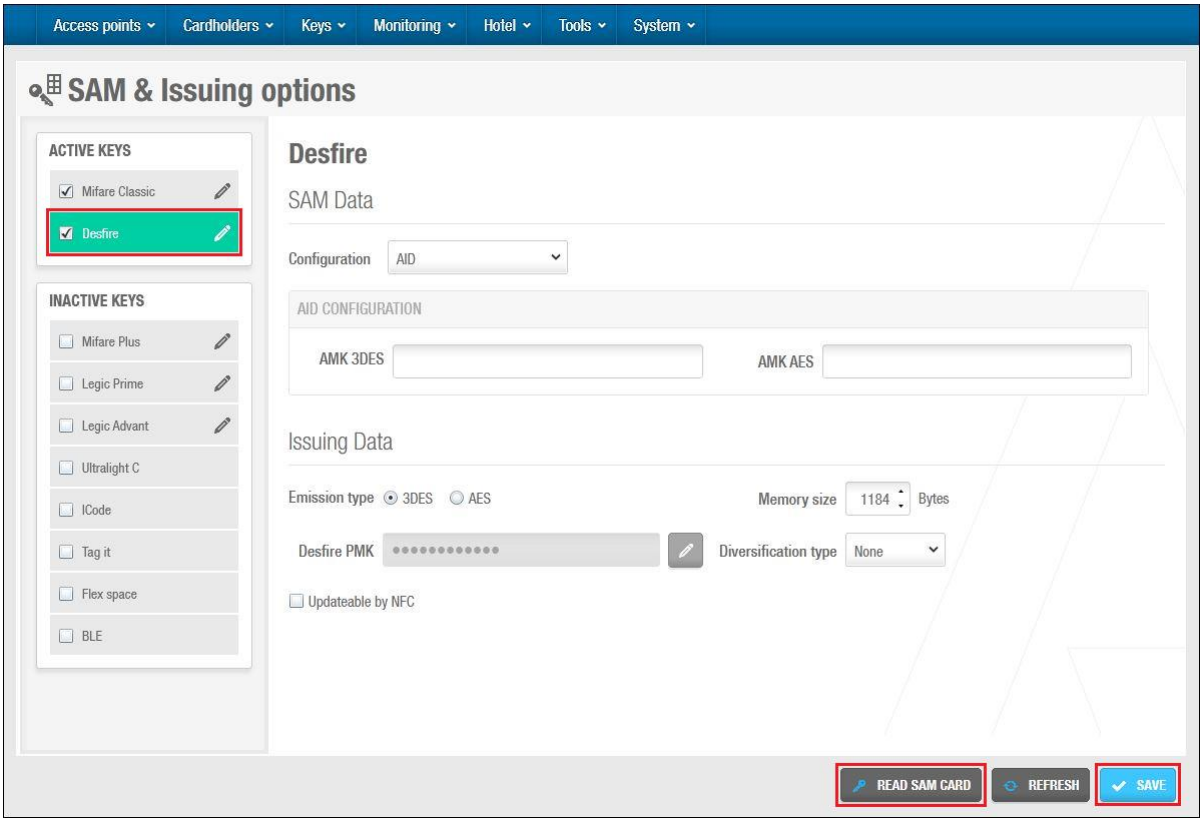


Figure 276: Desfire configuration fields

The **DESFire PMK** field is not editable. This field is automatically populated with the relevant Desfire keys data when you read the SAM card.

2. Click **Read SAM card**. A pop-up is displayed asking you to present the key to the encoder.
3. Place the appropriate SAM card on the encoder when the LED light begins to flash. The **DESFire PMK** field is populated.
4. Select either the **3DES** or **AES** option in the **Emission type** field.

   The **AES** option uses a more complex form of bits encryption.
5. Select the **Updateable through NFC** checkbox if required.

   You should consult with your SALTO technical support contact if you require additional information about this option.
6. Select the appropriate value in the **Memory size** field by using the up and down arrows.

   This value defines the amount of memory space that is reserved for SALTO data in DESFire keys.
7. Select an option from the **Diversification type** drop-down list if required.

   The default option is **None**. Diversification types are only available for specific SALTO projects. You should consult with your SALTO technical support contact if you require additional information about this option.
8. Click **Save**.
9. Click **Close**. The **SAM & Issuing options** is updated to show the **MIFARE** option is enabled.
10. Click **Save**.

12. 12. 3. Configuring Legic Settings

To configure the Legic settings, perform the following steps:

1. Select **System** > **SAM & Issuing options**.
2. Select **Legic Prime** or **Legic Advant** as required in **Active keys**. The **SAM & Issuing options** dialog box is displayed.

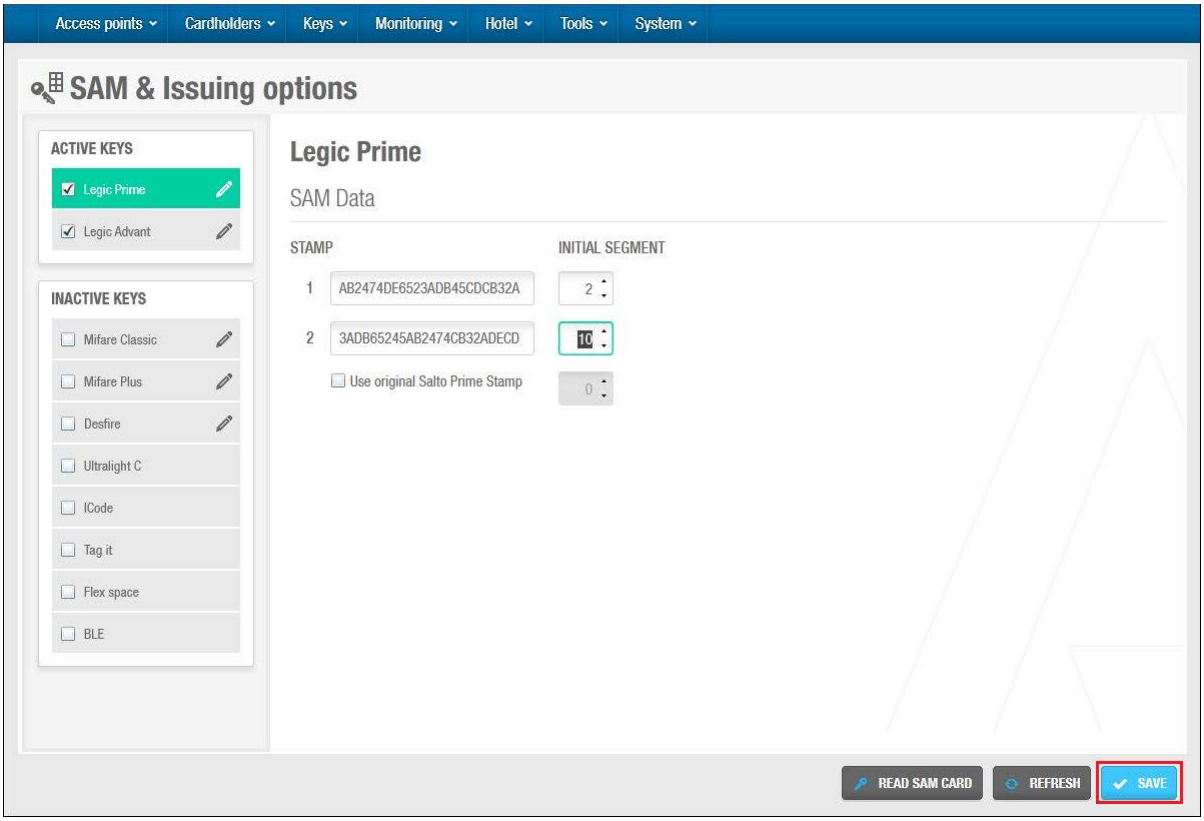


Figure 277: SAM & Issuing options dialog box

3. Select the **Enabled** checkbox.
4. Type a stamp in the **1** field in the **Legic Prime** panel.

   This stamp allows the SALTO software to read the Legic segment data. SALTO readers can support up to three different stamps at once for Legic Prime and Legic Advant keys.
5. Select the appropriate number in the **Initial segment** drop-down list for the stamp.

   This defines the first segment from which the key data is read. There are 127 numbered segments and the default option is **0**. If you do not know the initial segment, it is recommended not to change the default value. The SALTO readers will not access the correct key data if you enter an incorrect value for this segment.
6. Type a stamp in the **2** field.
7. Select the appropriate number in the **Initial segment** drop-down list for the stamp.
8. Select the **Use original SALTO Prime Stamp** checkbox if required.

   If you select this option, you must select the appropriate number in the **Initial segment** drop-down list for the stamp. Any Legic key supplied by SALTO can be used with this option.
9. Repeat the process for required stamps in the **Legic Advant** panel.
10. Select the appropriate options in the **Active cards** panel.

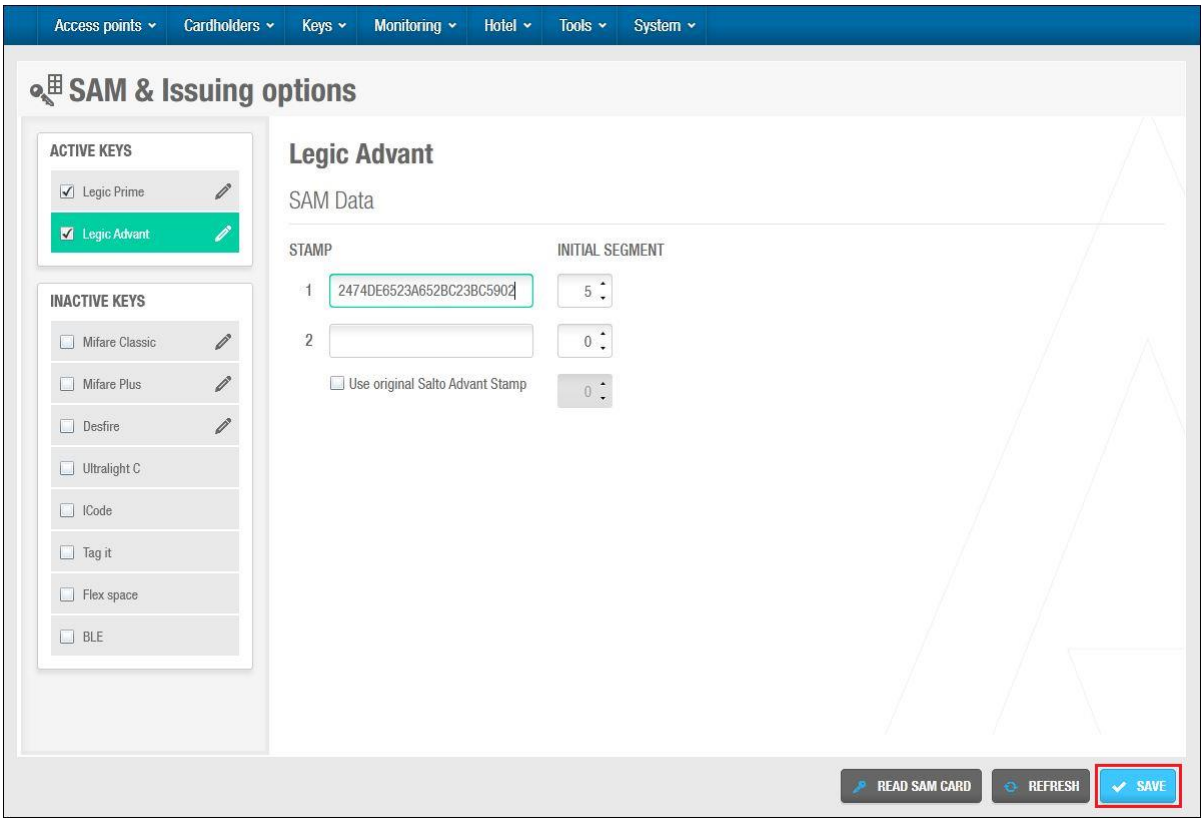


Figure 278: SAM & Issuing options dialog box

This defines the key types that can be used with the SALTO locks, encoders, and readers. You should not select key types that are not used in your site as this can slow the speed of the SALTO readers. If you disable a key type, the SALTO readers will not recognize it, even if they are compatible with the key type. You must use a PPD to update the SALTO locks with these changes. See *Updating Locks* for more information.

11. Click **Save**.
12. Click **Close**. The **SAM and issuing data** tab is updated to show the **LEGIC** option is enabled.
13. Click **Save**.

12. 13. PMS Authorizations

When you use PMS software with the SALTO software, you must assign an authorization number to outputs, associated devices, and zones in a hotel where guest access is optional. See *Zones* for more information about defining guest access points as optional. The PMS software requires these authorization numbers. Otherwise, you cannot give guests access to optional facilities when performing check-ins using the PMS software.

To create an authorization list, perform the following steps:

1. Select **System** > **PMS Authorizations**.
2. Click **Authorization list**. The **Authorization list** dialog box, showing 62 numbered entries, is displayed.

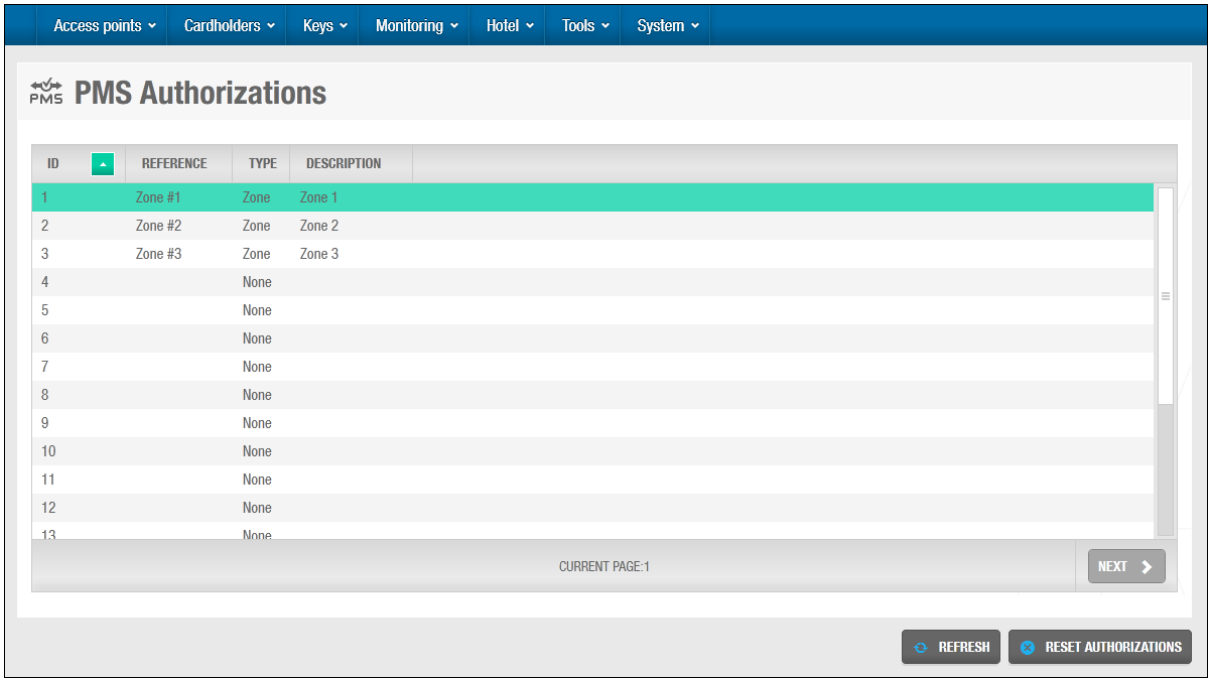


Figure 279: Authorization list dialog box

This is the default number of entries for the Micros-Fidelio and Industry Standard protocols.

3. Double Click the required entry number. The **Authorization data** dialog box is displayed.

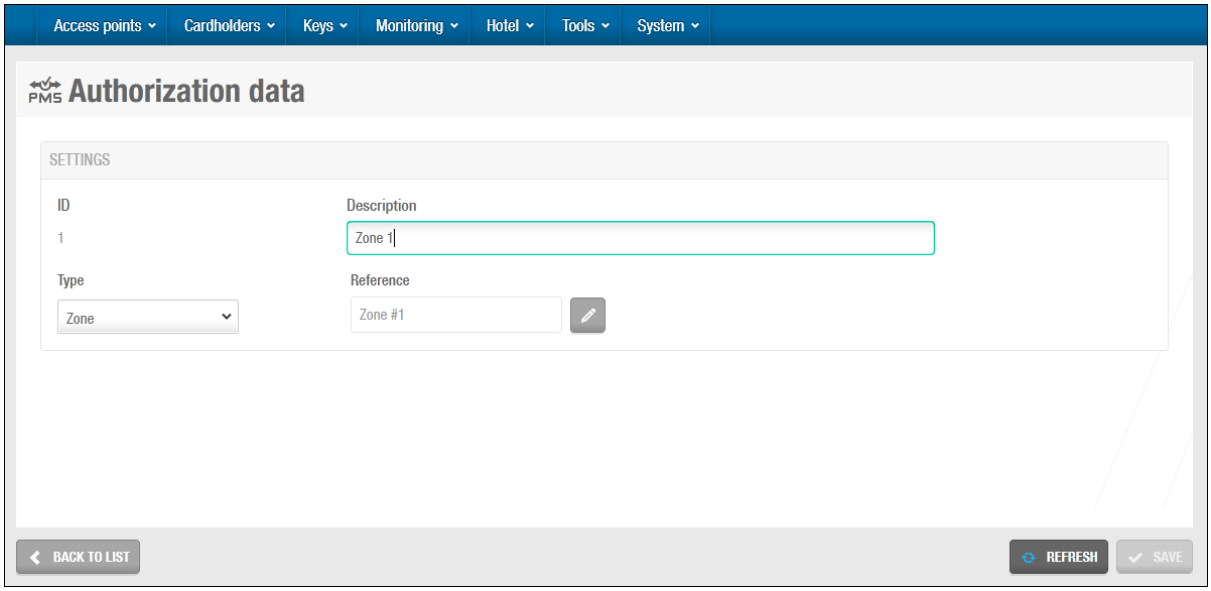


Figure 280: Authorization data dialog box

You cannot amend the value in the **Authorization** field.

4. Type a description in the **Description** field.
5. Select the appropriate option from the **Type** drop-down list.

   You can select a zone, an output, or an associated device.
6. In **Reference** click the **pencil**. The **Reference item** dialog box, showing a list of zones, is displayed.

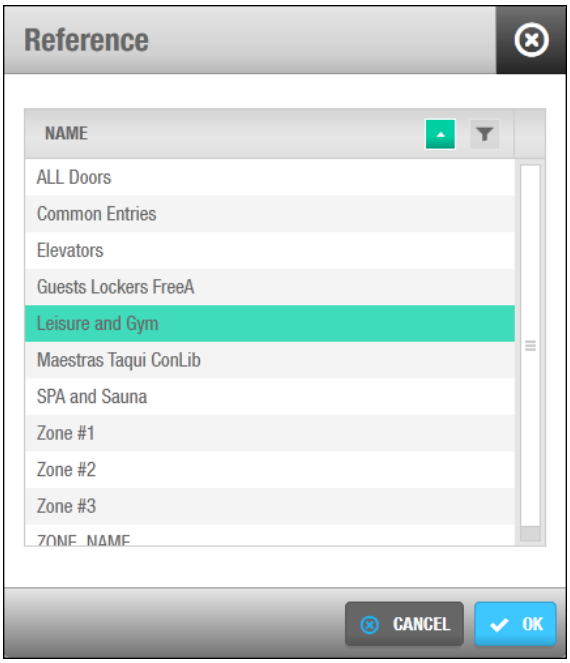


Figure 281: Select item dialog box

The items displayed in this dialog box vary, depending on the selected option in the **Type** drop-down list. For example, if you select the **Output** option, a list of outputs is displayed.

7. Click the required zone to select it and click **Ok**. The selected zone is displayed in the **Reference** field.
8. Click **Save**.
9. Click **Close**. The entry details are displayed in the authorization list.

   You can click **Clear** to delete selected entries. You can also click **Print** to display the **Print Preview** dialog box and print the authorization list.
10. Repeat the process for each required entry.
11. Click **Close** when you have finished adding entries to the authorization list.

NOTE: The authorization list you create is applied to all of the PMS protocols on the system. The same authorization numbers must be used in the PMS and SALTO software so they can communicate with each other. For example, if you assign number 62 to the hotel leisure centre, this number must also be assigned to the leisure centre in the PMS software.

12. 14. System Resources

You can view the blacklist status by selecting **System** > **System resources**.

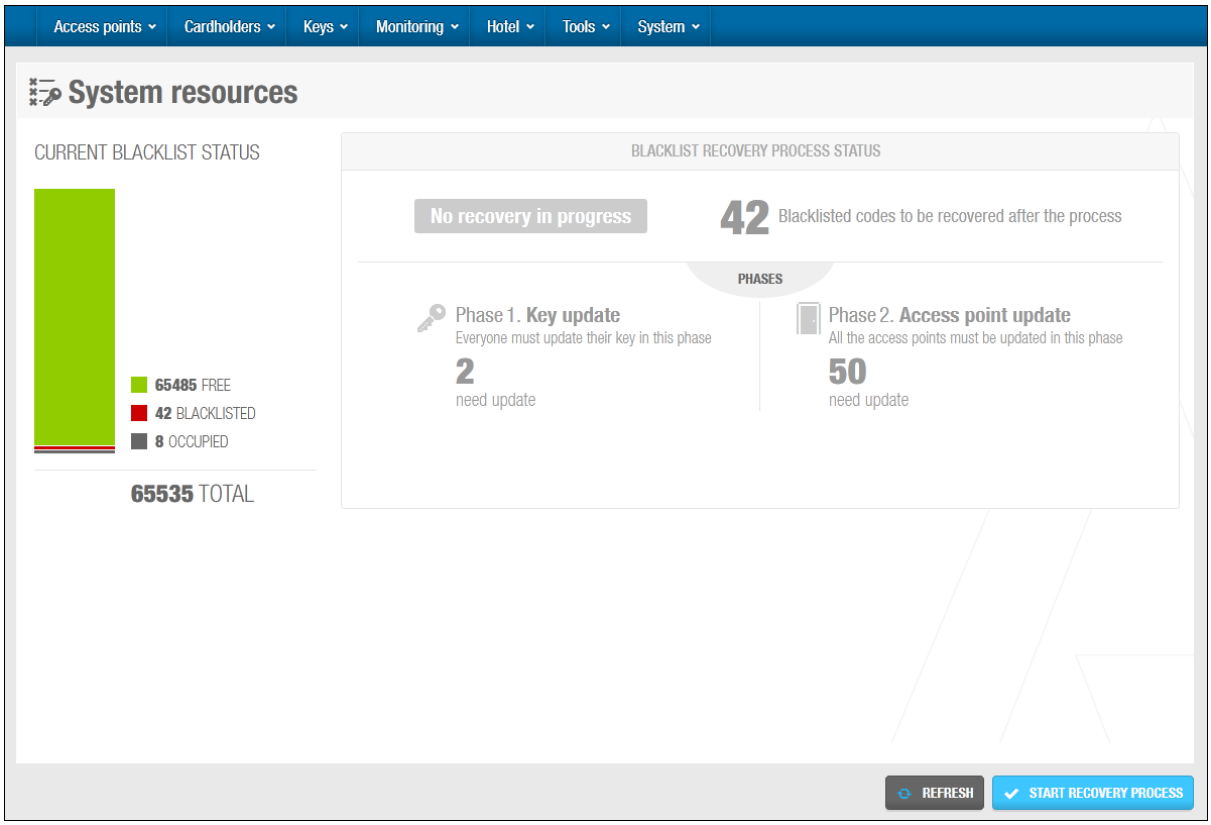


Figure 282: System resources screen

The **System resources** screen shows the following information:

- Free codes

  This represents the number of blacklist codes that are still available for keys. A blacklist code is used each time a key is cancelled.

- Blacklisted codes

  This represents the number of keys that have been sent to the blacklist to date.

- Occupied codes

  This represents the number of keys that have been configured to be sent to the blacklist when deleted or cancelled.

A maximum of 65,535 keys can be cancelled through the blacklist. See *About Blacklists* for more information about blacklists.

NOTE: If the blacklist is full, you can perform a blacklist recovery. You must consult your SALTO technical support contact for more information about this process.

13. PROACCESS SPACE GENERAL OPTIONS

This section contains the following parts:

13. 1. About ProAccess SPACE General options

The **General options** menu option in ProAccess SPACE allows you to enable and configure different options within ProAccess SPACE. It is important to remember that the display of certain fields in ProAccess SPACE is controlled by the options you select in ProAccess SPACE General options. These settings are generally configured by system administrators. It is recommended that you consult with your SALTO technical support contact before making any substantial changes.

You can click the **General options** in ProAccess SPACE **System** to view the **Options** screen, which contains different tabs.

This chapter explains these tabs in detail, and describes the various configuration tasks related to each.

13. 1. 1. Applying Configuration Changes

SALTO enables the most common features for sites in ProAccess SPACE General options to prevent security issues and allow for ease of operation. However, you can make any required amendments to these settings if you have the appropriate permissions.

NOTE: You can click the **Print** button on any of the tabs on the **Options** screen in ProAccess SPACE to print a hard copy of all of your configuration settings.

13. 2. General Tab

You can enter general system configuration information, view the blacklist status, and activate multiple time zones by using the **General** tab.

Select **System** > **General options** > **General** to view the tab.

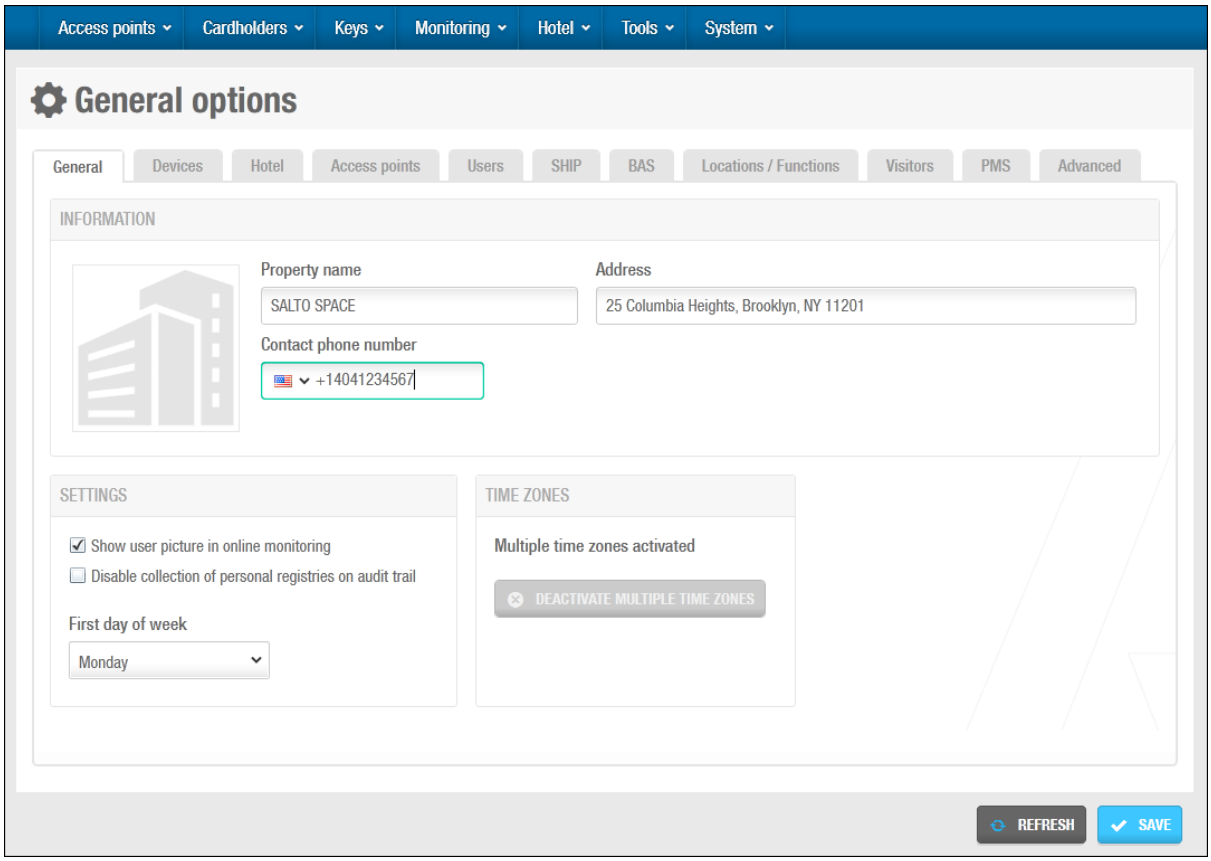


Figure 283: General tab

The tab items are described in the following table.

Table 70: General tab items

Item	Description
Property name field	Displays the name of the database. This field is automatically populated with the name that was given to the database during the installation process. However, you can amend the name in the field if required. See *Installation* for more information.
Address field	Allows you to enter the address in which your site is located
Contact phone number field	Allows you to enter the contact phone number
Show user picture in online monitoring field	Displays the picture of the user in online monitoring when the user is entering through an online wall reader.
Disable collection of personal registries on audit trail checkbox	Restricts the type of data that is displayed in the audit trail. When you select this checkbox, operators cannot view opening and closing events, or failed access attempts. Instead, only entries for lock and key updates that occur are displayed.
First day of week drop-down list	Specifies the first day of the week in the system calendar. The selected day is displayed as the first day of the week in the **Days** panel on the **Cardholder timetables** screen in ProAccess SPACE.

Item	Description
Activate multiple time zones button	Activates the multiple time zones functionality in ProAccess SPACE. See *Activating Multiple Time Zones* ***Error! Reference source not found.*** and *Time Zones* for more information.

13. 2. 1. Activating Multiple Time Zones

To activate multiple time zones, perform the following steps:

1. Select **System** > **General options** > **General**.
2. Click **Activate multiple time zones**. The **Time zone information** dialog box is displayed.

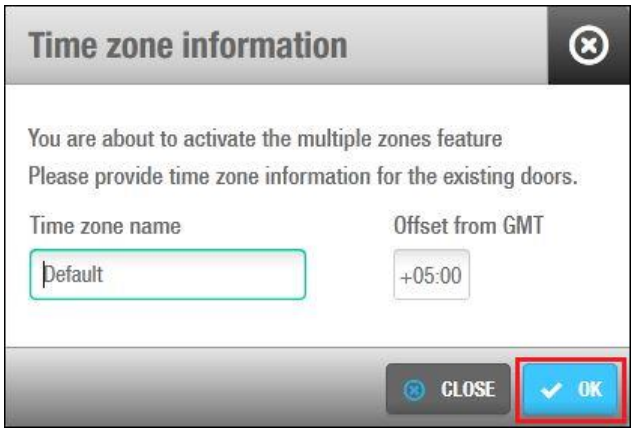


Figure 284: Time zone information dialog box

   The **Time zone name** field displays the name of the default system time zone. You can amend this text if required.
3. Select the appropriate time parameter using the up and down arrows in the **Offset from GMT** field.

   The value you enter is used to calculate the time zone according to Greenwich Mean Time.
4. Click **Ok**. The **General** tab is updated to show that multiple time zones are enabled.

   You can click **Deactivate multiple time zones** to deactivate the multiple time zones functionality at any time. However, you must delete any additional time zones you have created in ProAccess SPACE before you can do this.
5. Click **Save**.

See *Time Zones* for more information about using the multiple time zones functionality.

13. 3. Devices Tab

You can specify the User Datagram Protocol (UDP) port range and the encoder to be used for the SALTO Service by using the **Devices** tab. The SALTO Service uses this UDP port to communicate with the system peripherals. See *Checking ProAccess SPACE Configuration* for more information. The dongle encoder is used to encrypt key data when sites use third-party encoders, for example.

Select **System** > **General options** > **Devices** to view the tab.

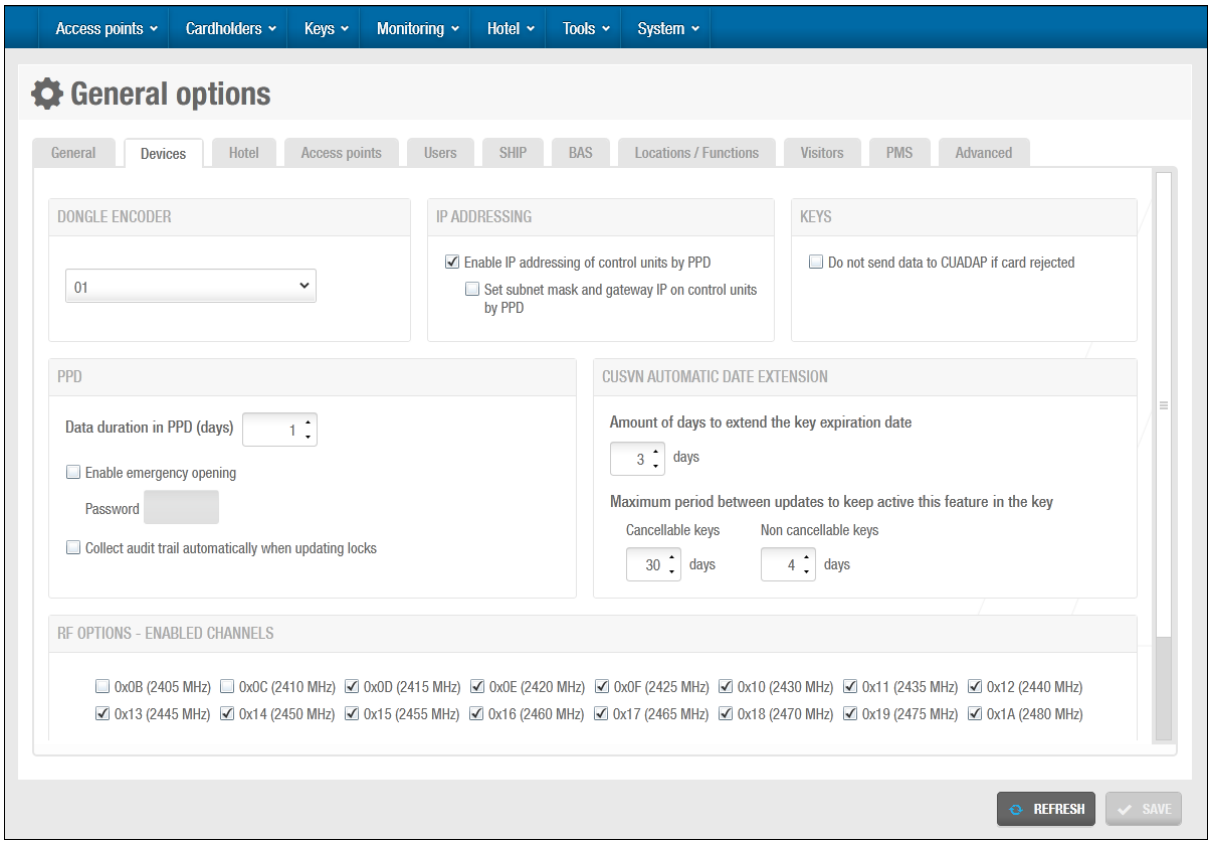


Figure 285: Online tab

The tab items are described in the following table.

Table 71: Devices tab

Item	Description
Dongle encoder for SALTO service drop-down list	Allows you to select a dongle encoder to be used for the SALTO Service. This Ethernet encoder has to be online. It is used to encrypt the data that is sent over the air (OTA) or when using a third party encoder. Any of the online Ethernet encoders from the system can be selected.
Enable control unit IP addressing by PPD checkbox	Controls whether PPDs assign the IP address you have entered on the system to online IP (CU5000) doors during initialization. See *Initializing Locks* and *Online IP (CU5000)* for more information. This is useful for online IP (CU5000) doors that are on different networks.
Set Subnet mask and gateway IP on CUs by PPD checkbox	Activates a subnet mask and a gateway for IP addresses for online IP (CU5000) doors in order to improve router efficiency. When you select this checkbox, a **Subnet mask** field and a **Gateway IP address** field are displayed on the **Access point: Online IP (CU5000)** information screen in ProAccess SPACE. Note that you must select **System** > **SALTO Network** and double-click the required online IP (CU5000) door on the **SALTO Network** screen to view the information screen. To use this option, your CU 5000 board firmware must be version 02.01 or higher, and your Ethernet board firmware must be version 01.40 or higher.
Do not send data to CUADAP if card rejected checkbox	Controls whether track data is transferred to the CU adaptor when user cards are rejected

Item	Description
Data duration in PPD (days) field	Defines the number of days for which access data downloaded to a PPD is stored in the PPD's memory. The data is no longer displayed in the PPD's menu after the specified expiry date. The default value is one day but you can change this if required.
Enable emergency opening checkbox	Sets emergency opening as a default option in ProAccess SPACE. When you select this checkbox, the **Allow emergency opening** checkbox on the **PPD** information screen in ProAccess SPACE is greyed out, and you can perform emergency openings each time you download data for specified access points to the PPD. See *Performing Emergency Door Openings* for more information. It is important to be careful when using this option, as a security risk could arise if an unauthorized person comes into possession of the PPD.
Password field	Allows you to enter a password for performing emergency openings with a PPD. The specified password must be entered in the PPD before you can perform emergency openings. If you enter a password in this field, the **Password** field on the **PPD** information screen in ProAccess SPACE is greyed out, and you cannot use it to change the PPD password or enter a password. Otherwise, you can edit the **Password** field in ProAccess SPACE. See *Performing Emergency Door Openings* for more information.
Collect audit trail automatically when updating locks checkbox	Controls whether PPDs automatically collect audit trail data when they are used to update locks
Amount of days to extend the key expiration date field	Defines the number of days for which keys are revalidated when they are updated at a CU that is operating offline due to a network issue, for example. The default option is three days. You can amend this value if required. However, it cannot be higher than 15 days. You must enable the CUSVN_DATE_EXT parameter to activate this option. See *Advanced Tab* in General Options for more information.
Maximum period between updates to keep active this feature in the key field	Defines the maximum period for which the CUSVN automatic date extension feature can be used with keys. Outside of this period, keys cannot be revalidated at a CU that is operating offline. Instead, they must be updated at an online CU. The default option for cancellable keys is 30 days. However, you can set this value as high as 730 days if required. For non-cancellable keys, the default option is four days. You can amend this value but it cannot be higher than seven days.
RF option – Enable Channels checkboxes	Enabled channels for RF signals in ProAccess SPACE. There are 16 channels available and all of these are enabled by default. The frequency range of each channel is also displayed. You can disable a channel if required by clearing the checkbox for the channel and clicking **Save**.
Wiegand format for third party readers field	Defines the code format for Wiegand keys. See *Configuring Wiegand codes* for more information

13. 4. Hotel Tab

You can activate or amend options for rooms and suites, and configure associated devices by using the **Hotel** tab.

Select **System** > **General options** > **Hotel** to view the tab.

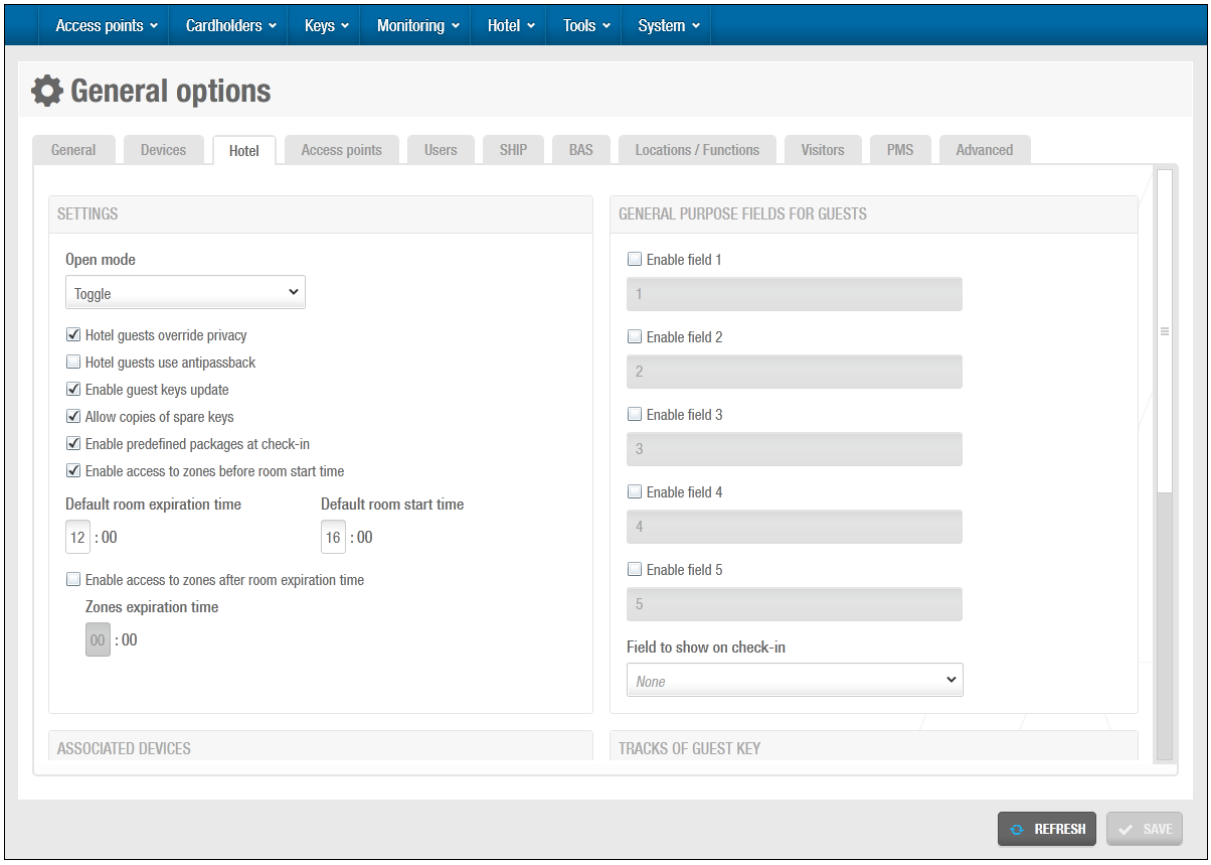


Figure 286: Hotel tab

The tab items are described in the following table.

Table 72: Hotel tab items

Item	Description
Open mode drop-down list	Defines the opening mode for room and suite doors. You can select Standard, Toggle, Exit leaves open or Toggle + Exit leaves open opening mode. The specified opening mode is applied to all external room and suite doors. However, it is not applied to doors in subsuites. See *Opening Modes and Timed Periods* for more information about opening modes.
Hotel guests override privacy checkbox	Controls whether guests can enter their room when the door has been locked from the inside. If you select this option, all guests who have been checked in to the room can enter it at any time, even if the door is locked from the inside. If you do not select this option, they cannot enter if the door is locked.

Item	Description
Hotel guests use anti-passback checkbox	Controls whether the anti-passback functionality is used for guests. Note that this applies to guest access points that have been defined as optional but not rooms or suites. Optional facilities can include the hotel leisure centre, for example. When you select this checkbox, the option is applied to all guests. See *Enabling Anti-passback* and *Zones* for more information.
Enable guest keys update checkbox	Controls whether guest keys can be updated at an SVN wall reader. This is useful for re-rooming guests. If guest keys can be updated with new access information at an SVN wall reader, the guest does not have to return to the front desk before accessing their new room. See *Re-Rooming* for more information about re-rooming guests.
Allow copies of spare keys checkbox	Controls whether copies of spare keys can be edited. When you select this checkbox, an **Edit Spare Key Copies** button is displayed on the **Programming & spare keys** screen in ProAccess SPACE. See *Editing Spare Key Copies* for more information about this process.
Enable predefined package at check-in checkbox	Predefined amount of check-in days for the guest stay. According to the guest arrival day, various options will be shown; Weekend: from Friday to Sunday, Week: from Monday to Sunday and Midweek: from Monday to Friday. Selecting one of these option will automatically sets the departure date. See *Guest check-ins* for more information.
Enable access to zones before room start time checkbox	Controls whether guests can be given access to zones in a hotel site before the specified time that they can access their room on the day of check-in. See *Zones* for more information about giving guests access to zones. When you select this option, the **Rooms activation time** drop-down list is displayed on the **Hotel** tab and the **Start date time** field is displayed on the **Hotel check-in** screen in ProAccess SPACE. Note that they are also displayed when you enable the CHECKIN_START_TIME parameter in ProAccess SPACE General options. See *Advanced Tab* for more information.
Default Room expiration time field	Defines the hour when guests must vacate their rooms on the day they check out of a hotel site. If you select **13** in the drop-down list, for example, the guest's key cannot be used to access their room after 13:00 on the day of check-out. This value is displayed in the **Date of expiry time** field on the **Hotel check-in** screen in ProAccess SPACE, but you can change the value for individual guests if required.
Default Rooms start time field	Defines the hour when guests can enter their room on the day they check in to a hotel site. If you select **16**, for example, the guest's key can be used to access their room any time after 16:00 on the day of check-in. This value is displayed in the **Start date time** field on the **Hotel check-in** screen in ProAccess SPACE, but you can change the value for individual guests if required. Note that this option is displayed on the **Hotel** tab when you enable the CHECKIN_START_TIME parameter in ProAccess SPACE General options. See *Advanced Tab* for more information. It is also displayed when you select the **Enable access to zones before room start time** checkbox on the **Hotel** tab.

Item	Description
Enable access to zones after room expiration time checkbox	Defines the hour after which a guest's access to zones in a hotel site expires on the day of check-out, for example, the hotel leisure centre. See *Zones* for more information about giving guests access to zones.
Enable field checkboxes	Allow you to add up to five general purpose fields for guests. When you select the checkbox for each field, it is displayed on the **Guest** information screen in ProAccess SPACE. You can name the general purpose fields in accordance with the information you want to capture by typing a name in the field underneath each checkbox, for example, special requirements.
Field to show on check-in drop-down list	Allows you to select what General purpose fields, from 1 to 5. When you select the field, it is displayed on the **Check-in** screen in ProAccess SPACE. This field can be used to add guest-related information related with the guest. If required, the content of the general purpose field can be added to a track. See *Configuring Tracks* for more information.
Associated devices checkbox	Gives you the option to enable associated devices in rooms and suites. When you select this option, an **Associated device List** panel is added to the **Room** and **Suite** information screens in ProAccess SPACE. See *Associated Device Lists* for more information.
Show details button	Allows you to change the configuration options for associated devices. See *Configuring Associated Devices* for more information.
Hide room name in mobile app checkbox	When selected, the room name won't be shown in the mobile phone screen. The JustIN mobile app is license dependent. See *Guest check-ins* for more information.
Default notification message for mobile guest keys field	Allows you to enter a default notification message for mobile guest keys. Guests receive this message when mobile keys are sent to their phones. See *Room Options* for more information about the mobile guest keys option.
Track #1 checkbox for hotel guests	Enables track 1 on guest keys. When you select this checkbox, you can use the track to write additional data on guest keys, for example, the key expiration date. See *Configuring Tracks* for more information.
Size fields	Allows you to define the number of bytes that are used for tracks. You need to specify the size for each track used.
Content fields	Allows you to specify what data is written on tracks. You need to specify the content for each track used. See *Configuring Tracks* for more information.
Track #2 checkbox for hotel guests	Enables track 2 on guest keys. When you select this checkbox, you can use the track to write additional data on guest keys.
Track #3 checkbox for hotel guests	Enables track 3 on guest keys. When you select this checkbox, you can use the track to write additional data on guest keys.
Wiegand code checkbox for hotel guests	Activates the Wiegand code option for guest keys. This enables the SALTO system to send the Wiegand code to third-party applications if required. Note that only a constant Wiegand code can be used for guest keys. This is a fixed code that is the same for all guests.

13. 4. 1. Configuring Associated Devices

You can amend the configuration settings for associated devices such as ESDs if required.

To amend the configuration settings for ESDs, perform the following steps:

1. Select **System** > **General options** > **Hotel Tab**.
2. Click **View details** in the **Associated devices** panel. The **Associated device** dialog box is displayed.

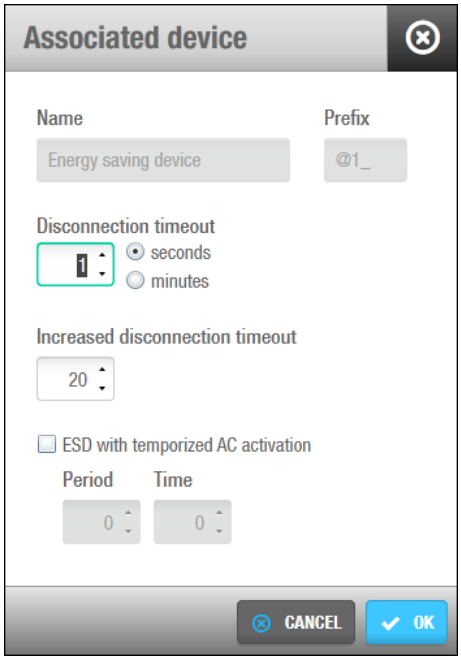


Figure 287: Associated device dialog box

You cannot amend the default characters in the **Prefix** field. The prefix is included at the beginning of ESD entries for hotel rooms and suites in ProAccess SPACE, for example, @1_101.

3. Enter the required time parameters in the **Disconnection timeout** field by clearing the default numerical value and typing a new value, and selecting either the **seconds** or **minutes** option from the drop-down list.

   These parameters define the period for which the ESD remains active after you remove a key from it.

4. Clear the default value in the **Increased disconnection timeout** field and type a new value if required.

   This feature is designed for disabled or 'hands full' users or guests. The ESD remains active for the increased period that you specify after users or guests remove their keys from it. You must also enable this option in the user's or guest's profile.

5. Select the **ESD with temporized AC activation** checkbox if required.

   This sets the AC in the room to activate automatically for a certain period at specified time intervals. Note that access to the AC is controlled by the system-generated ESD_#2 entry. This is one of the outputs that activate the relays for ESDs. See *Associated Device Lists* for more information.

6. Type a value in the **Period** and **Time** fields.

These values control the automatic activation of the AC. For example, if you type '60' in the **Period** field and '5' in the **Time** field, the AC is automatically activated for five minutes every hour.

7. Click **Ok**.
8. Click **Save**.

13. 4. 2. Configuring Tracks

Keys have three tracks or areas in which you can encode data (track 1, track 2, and track 3). You can enable these tracks on user and guest keys to store information from specific ProAccess SPACE fields, for example room names, or key expiration dates. See *Hotel Tab* or *Users Tab* for more information. You must define what data is written on each track, and this is displayed when you read keys. See *Reading Keys* for more information about reading keys.

To configure a track, perform the following steps:

1. Select **System** > **General options** > **Hotel**.
2. Select the checkbox for the required track.
3. Type the appropriate value in the **Size** field.

   This defines the number of bytes on the key that are used for the track.
4. Click the button on the right-hand side of the **Content** field. The **Tracks content configuration** dialog box is displayed.

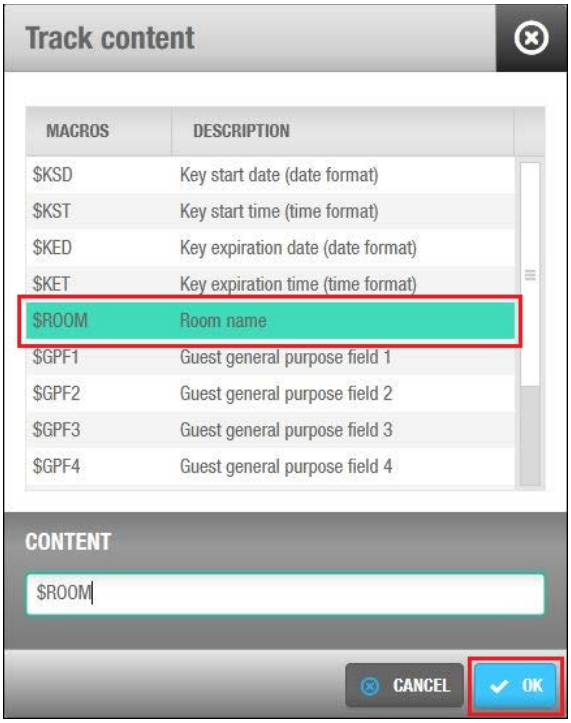


Figure 288: Tracks content configuration dialog box

This dialog box allows you to specify the data that is written by default when new keys are encoded.

5. Click the required macro in the **Macros** field to select it.

Macros are available for a number of the fields in ProAccess SPACE. Note that you can use the $ASC macro for ASCII characters or non-printable characters.

6. Click **OK**. The selected macro is displayed in the **Content** field.

   You can include a constant value before or after each macro by typing it in the **Content** field, for example, 'Date' or '-'.

7. Click **Ok** when you have finished inserting macros and the correct macro format is displayed in the **Content** field.
8. Click **Save**.

13. 5. Access points Tab

You can activate or amend options for locks by using the **Lock** tab.

Select **System** > **General options** > **Access points** to view the tab.

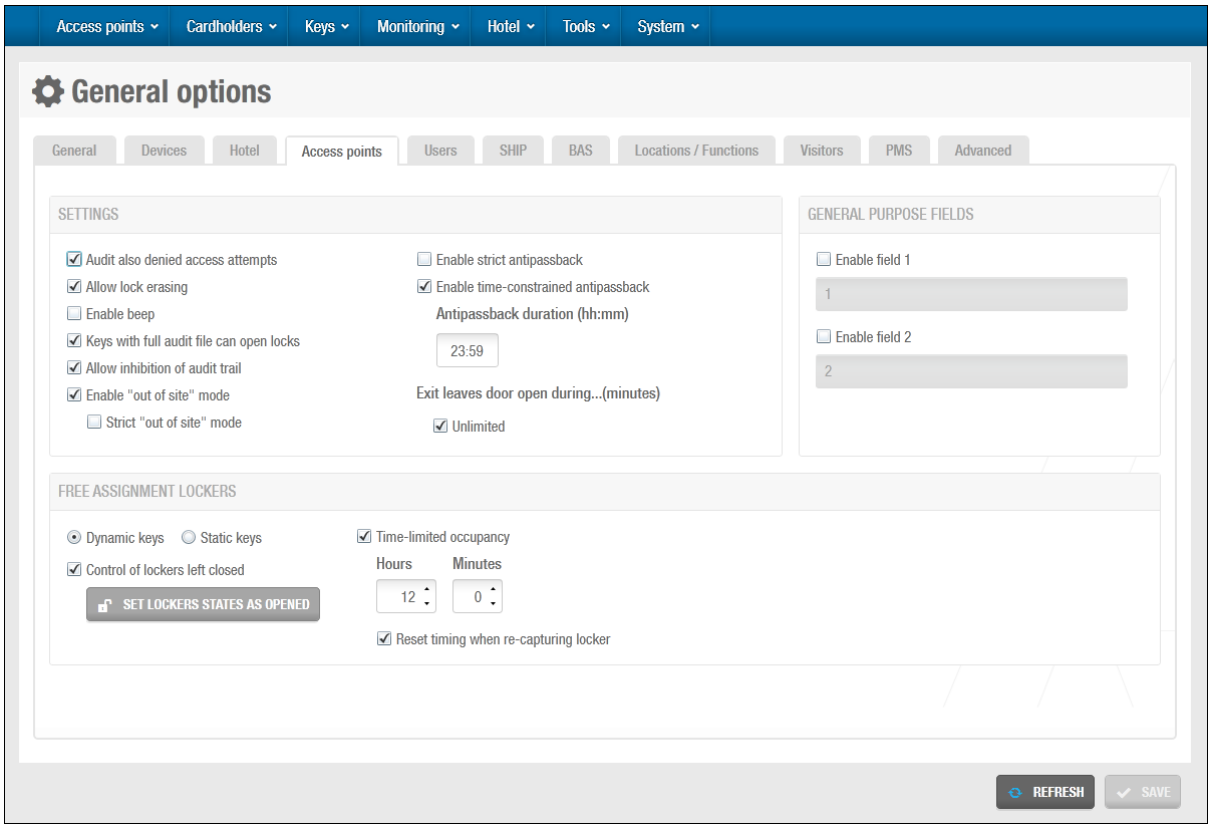


Figure 289: Access points tab

The tab items are described in the following table.

Table 73: Lock tab items

Item	Description
Audit also shows denied access attempts checkbox	Controls whether failed access attempts are displayed in the audit trail. When you select this option, it is applied to all system locks.

Item	Description
Allow lock erasing checkbox	Controls whether locks can be reset and initialized for use with a different database. If you select this checkbox, you can reset any of the locks on the system and then initialize them with a PPD. See *Initializing Locks* for more information about initializing locks.
Enable beep checkbox	Controls whether locks emit beeps during operation. When you select this option, it is applied to all system locks.
Keys with full audit file can open locks checkbox	Controls whether keys that have a full audit trail can be used to open locks. This option is selected by default but you can change this if required. The option applies to all system locks. If the option is not enabled, keys that have a full audit trail cannot be used to open locks until they are updated at an SVN wall reader or with an encoder.
Allow audit trail inhibition checkbox	Controls whether you can inhibit the collection of audit trail data for doors. When you select this option, an **Inhibit audit trail** checkbox is displayed on the **Door** and **Room** information screens. Select this checkbox to ensure the lock does not memorize openings in its audit trail. See *Door Options* for more information.
Enable "out of site" mode checkbox	Controls whether Out of site mode can be enabled for online IP (CU5000) and online IP (CU4200) doors. This option generally applies to users only. Also, you can only use it with doors that have two readers. You can enable this mode by selecting the **Out of site** checkbox on the **Door** information screen in ProAccess SPACE. See *Door Options* for more information. Out of site mode strengthens system security. If a cardholder exits a site through either of these door types, the expiration period for their key is shortened when they present it to the exit SVN wall reader. A brief period is set for revalidation of their key upon re-entry. This period can vary depending on what time the key is presented to the exit reader, but it is never longer than 15 minutes. The cardholder's key is revalidated when they present it to the entrance SVN wall reader of the door, or another door that has Out of site mode enabled. However, they must do so within the specified period. Otherwise, access is denied as their key is not revalidated. When you select the **Enable "out of site" mode** checkbox, the **Strict 'out of site' mode** checkbox is also activated in ProAccess SPACE General options. This mode works in the same way. However, the cardholder's access permissions are also removed from their key when they present it to the exit SVN wall reader. Note that Strict out of site mode can only be used in cases where the SVN wall reader is located at a final exit point in a site. For example, it cannot be used if the cardholder must subsequently enter an offline door in order to leave the site.
Enable strict anti-passback checkbox	Enables the strict antipassback functionality. See *Enabling Anti-passback* for more information about strict antipassback.

Item	Description
Enable time-constrained anti-passback chekbox	Allows to enable **Anti-passback duration (hh:mm).** Anti-passback duration (hh:mm) displays the period of time in hours and minutes before a cardholder can re-enter a door that has the anti-passback option enabled. See *Enabling Anti-passback* for more information about antipassback. The default value is 23:59 but you can amend this time parameter if required. Note that if you enter 00:00, the anti-passback period is unlimited, and cardholders must always exit a door before they can re-enter it. You must update user keys using an encoder when you select this option or amend the time parameters. See *Updating Keys* for more information.
Exit leaves door open during...(minutes) checkboxes	If the unlimited checkbox is selected, the door in **Exit leaves open** mode will remain unlocked until the valid key is presented to the reader again. If **Unlimited** is not checked, a box will appear and allow to enter how many minutes the lock has to remain unlocked until it re-locks automatically.
Enable field checkboxes	Allows you to add up to two general purpose fields for locks. When you select the checkbox for each field, it is displayed on the **Door**, **Locker**, and **Room** information screens in ProAccess SPACE. You can name the general purpose fields in accordance with the information you want to capture by typing a name in the field underneath each checkbox.
Dynamic keys option	Defines whether dynamic keys can be used with free assignment lockers. When you select this option, users can choose any locker within a free assignment zone each time they enter the zone. They do not have to use the same locker each time. See *Creating Free Assignment Zones* for more information. Note that you must select this option if your site uses both free assignment lockers and lockers that have assigned access.
Static keys option	Defines whether static keys can be used with free assignment lockers. When you select this option, users can choose any locker the first time they enter a free assignment zone, but they must use the same locker subsequently. This option also applies to sites that only use lockers with assigned access.
Control of lockers left closed checkbox	Controls whether you can opt to reset the status of available lockers to 'open' on the system. This task can be performed by reception staff for information purposes, for example. It shows which lockers are available for use. However, it does not affect the physical lockers. When you select this checkbox, the **Set locker state as opened** button on the **Keys** tab is activated, and a **Set Lockers States As Opened** button is added to the **Lockers** screen in ProAccess SPACE. You can click this button to reset the status of all the available lockers in the system. This changes the status of the lockers to **Open** on the **Locker** information screen in ProAccess SPACE. Note that this option is generally used in sites where only free assignment lockers are in use, for example, gyms or spas.
Set locker state as opened button	Allows you to reset the status of available lockers to **Open** on the system. The changed status is displayed on the **Locker** information screen in ProAccess SPACE.

Item	Description
Time-limited occupancy checkbox	Limits the amount of time for which keys can be used to open free assignment lockers after they are chosen by users. When you select this checkbox, you must enter the appropriate time parameters in the **Hours** and **Minutes** fields. Outside of the specified time period, for example, four hours, only a master key can open lockers.
Reset timing when recapturing locker checkbox	Controls whether the time-limited occupancy period for free assignment lockers is reset each time lockers are opened and closed by users. For example, if the time-limited occupancy period is set to four hours, and a user opens and closes the locker again after three hours have elapsed, they can then use the locker for four more hours.

13. 6. User Tab

You can activate or amend options for users, permanently delete users, and select options for automatic key assignment by using the **User** tab.

Select **System** > **General options** > **User** to view the tab.

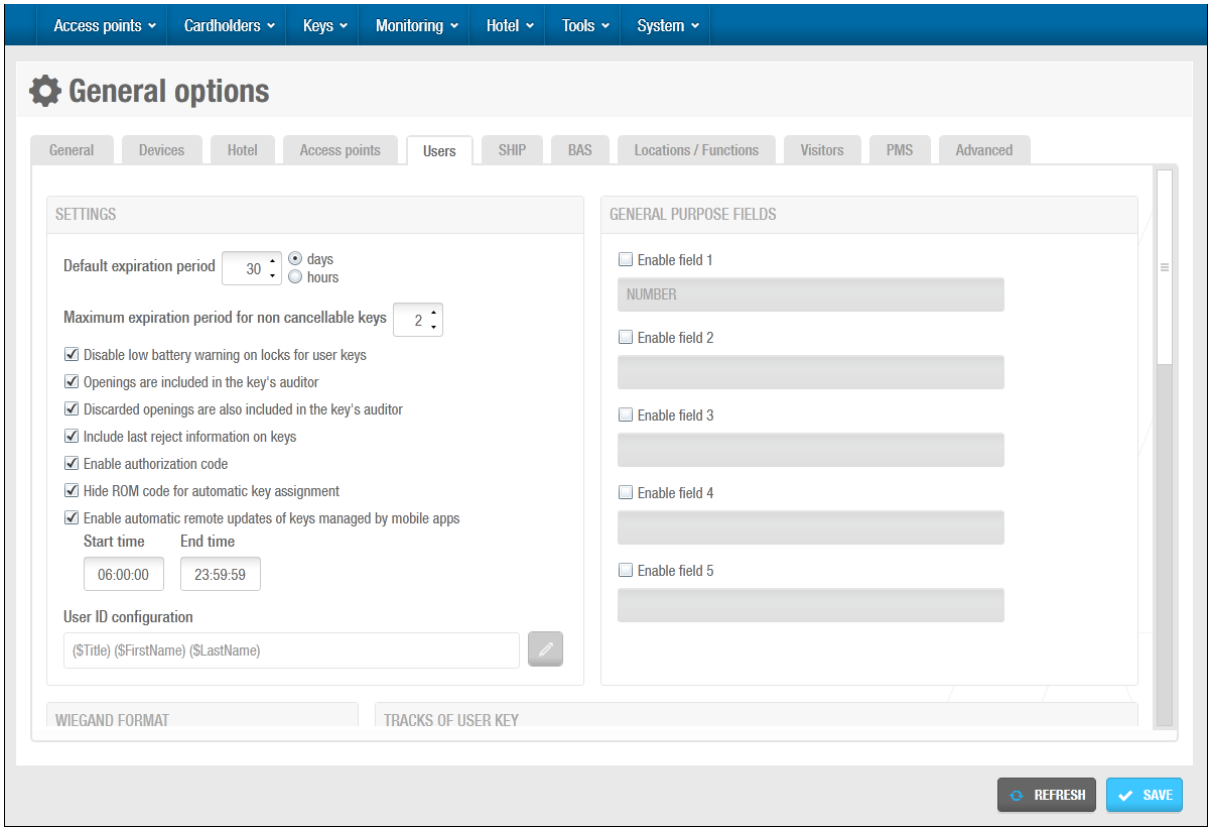


Figure 290: User tab

The tab items are described in the following table.

Table 74: User tab items

Item	Description

Item	Description
Default expiration period field	Defines a default revalidation period for user keys. This can be a period of days or hours. The time parameters you select are displayed in the **Update period** field in the **User and Key Expiration** panel on the **User** information screen in ProAccess SPACE. However, you can amend these parameters for individual users if required. See *User and Key Expiration* for more information.
Maximum expiration period for non cancellable keys field	Defines the maximum revalidation period that is allowed in the system for non cancellable user keys. Non cancellable keys are keys that are not sent to the blacklist when you cancel them. The default option is three days. You can amend this value if required, but it cannot be higher than seven days. See *Managing Blacklists* for more information. To activate this option, you must enable the MORE_THAN_64K_USERS parameter in ProAccess SPACE General options. See *Advanced Tab* for more information.
Disable low battery warning on locks for staff keys checkbox	Controls whether locks emit a low battery warning sound when staff (user) keys are used. If the lock battery is low, the reader emits four successive beeps of one second in duration. Note that low battery warnings are displayed in the audit trail by default.
Openings are included in the key's auditor checkbox	Controls whether opening events are included in audit trail entries for user keys.
Discarded openings are also included in the key's auditor checkbox	Controls whether failed opening events are included in audit trail entries for user keys.
Include last reject information on keys checkbox	Controls whether data about a user's most recent failed access attempt is stored on keys. When you select this option, you can access the data by reading keys. See *Reading Keys* for more information.
Enable authorization code checkbox	Enables a field in the user profile a code for third party applications.
Hide ROM code for automatic key assignment checkboxes	Hides the ROM code field in the user profile.
Enable automatic remote updates of key managed by mobile apps checkbox	Controls whether keys can be automatically updated by mobile phones using OTA programming. You can select a specific time period during which data updates can be sent to user phones by using the **Start time** and **End time** fields underneath the checkbox. Outside of this period, the system does not send updates to user phones. See *Key Options* for more information.
User ID configuration field	Defines the format of user IDs. There is a default format on the system, but you can amend this if required. See *Configuring User IDs* for more information.
Enable field checkboxes	Allow you to add up to five general purpose fields for users. When you select the checkbox for each field, it is displayed on the **User** information screen in ProAccess SPACE. You can name the general purpose fields in accordance with the information you want to capture by typing a name in the field underneath each checkbox.
Wiegand format field	Defines the code format for Wiegand keys. See *Configuring Wiegand Codes* for more information.

Item	Description
Default notification message field	Allows you to enter a default notification message for mobile app keys. Users receive this message when mobile keys are sent to their phones.
Track #1 checkbox for staff keys	Enables track 1 on user keys. When you select this checkbox, you can use the track to write additional data on user keys.
Track # 2 checkbox for staff keys	Enables track 2 on user keys. When you select this checkbox, you can use the track to write additional data on user keys.
Track #3 checkbox for staff keys	Enables track 3 on user keys. When you select this checkbox, you can use the track to write additional data on user keys.
Wiegand code checkbox for staff keys	Activates the Wiegand code option for users. When you select this checkbox, the Wiegand code is written on user keys when they are encoded. Also, a **Wiegand code** field is displayed on the **User** information screen in ProAccess SPACE. This field is automatically populated during data synchronization jobs. You can also edit the field manually if you have the required code. You must select either the **Profile code** or **Constant code** option in ProAccess SPACE General options when you select the **Wiegand code** checkbox. The profile code is the code included in user profiles. The constant code is a fixed code that is the same for all users. If you select the **Constant code** option, you must enter the constant code in the **Constant code** field.
Automatic key assignment enabled option	Specifies a mode for automatic key assignment. You must select the **#1** option, which is the standard mode. The **#2** option is used by SALTO staff for demonstration purposes only, as it allows the reuse of cancelled keys for automatic key assignment. See *Assigning Keys Automatically* for more information. SHIP cardholder must be selected only if a SHIP integration exists. This allows an automatic key assignment for users created with SHIP.
Card serial number option	Controls whether the serial numbers of keys are used for automatic key assignment. You must select either the **Card serial number** or **Card data** option. See *Assigning Keys Automatically* for more information.
Card data option	Controls whether key data is used for automatic key assignment. This allows you to use codes that are located in a specific sector in keys that is specified by the key manufacturer. You must select either the **Card serial number** or **Card data** option. See *Assigning Keys Automatically* for more information.

13. 6. 1. Configuring User IDs

Generally, the system does not allow you to create two cardholders with the same name. However, you can configure user IDs to include the information contained in various user-related ProAccess SPACE fields. This option applies to users only. In cases where two users have the same name, for example, you can use this option to change the default format of user IDs to make each one unique. User IDs are displayed in the **Name** column on the **Users** screen in ProAccess SPACE.

To configure the format of user IDs, perform the following steps:

1. Select **System** > **General options** > **Users**.
2. Click the button on the right-hand side of the **User ID** configuration field. The **User ID configuration** dialog box, showing the default macro format for user IDs, and a list of available macros, is displayed.

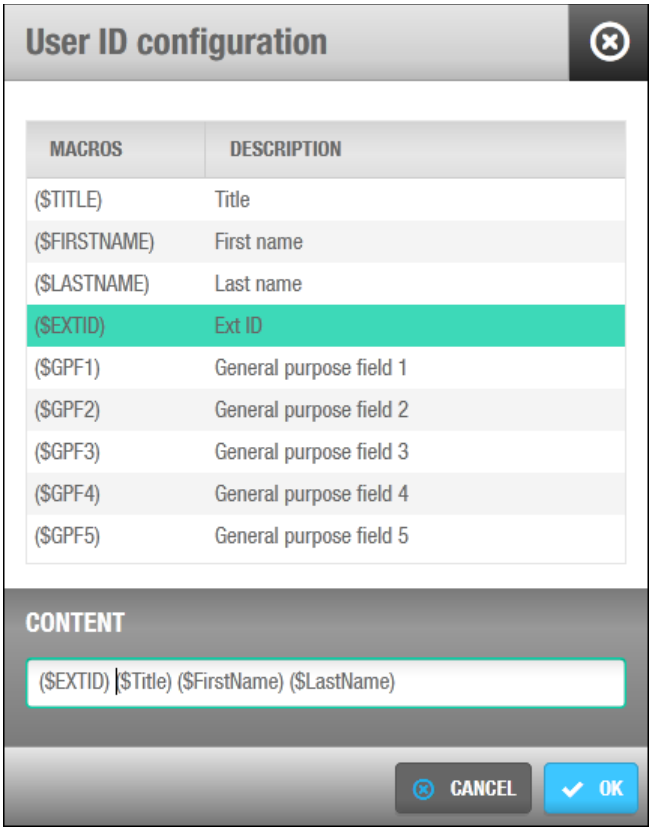


Figure 291: User ID configuration dialog box

   The default macro format is displayed in the **Content** field.

3. Double click the required macro in the **Macros** field to select it. It will be added to the **Content** field.

   You can place the cursor where you want to insert a macro within the existing entry in the **Content** field, or delete the entry to insert a new macro format.

4. Click **Ok** when you have finished inserting macros and the correct macro format is displayed in the **Content** field.

NOTE: The new user data is displayed the next time you log in to ProAccess SPACE.

13. 6. 2. Configuring Wiegand Codes

Wiegand codes are used by external applications such as time and attendance software to identify individual users. You can configure the Wiegand code in ProAccess SPACE General options.

You must perform the following steps:

5. Define the parts of the Wiegand code.
6. Define the format of the Wiegand code.

The sections below describe how to complete each step.

13. 6. 3. Step One: Defining the Parts of the Wiegand Code

To complete Step one:

1. Select **System** > **General options** > **Users**.
2. Click button **Configure** in the **Wiegand Format** panel. The **Wiegand code configuration** dialog box is displayed.

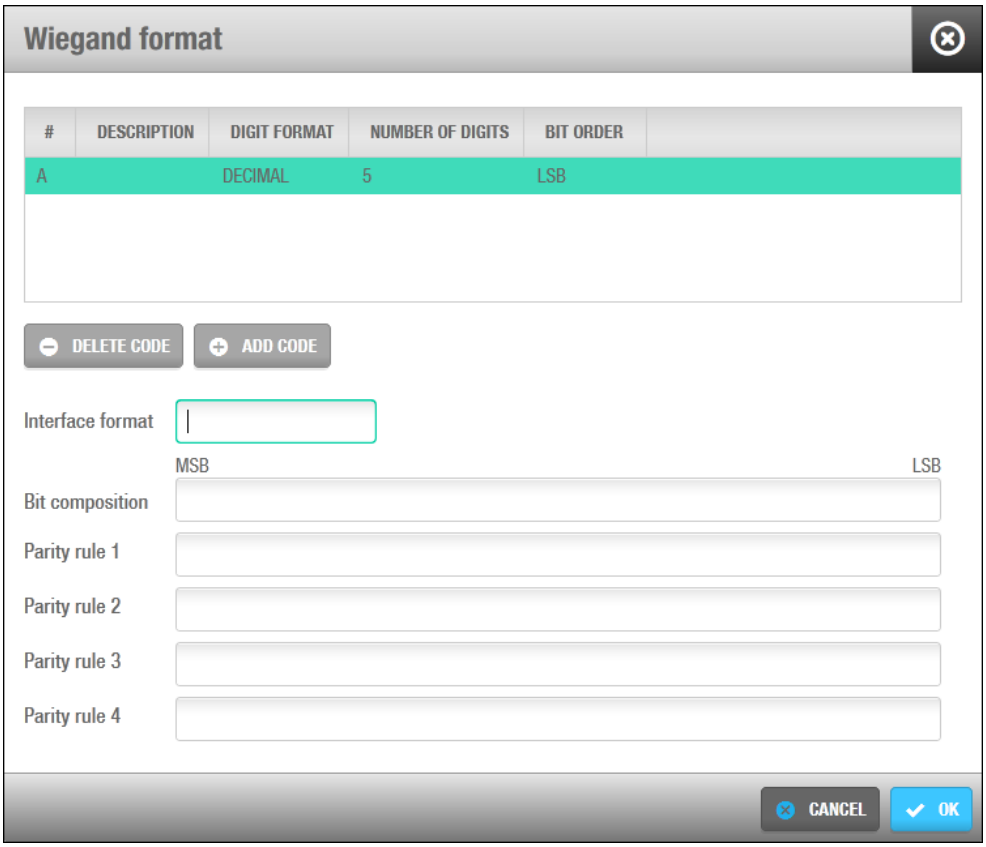


Figure 292: Wiegand code configuration dialog box

3. Click **New**. The **Wiegand code definition** dialog box is displayed.

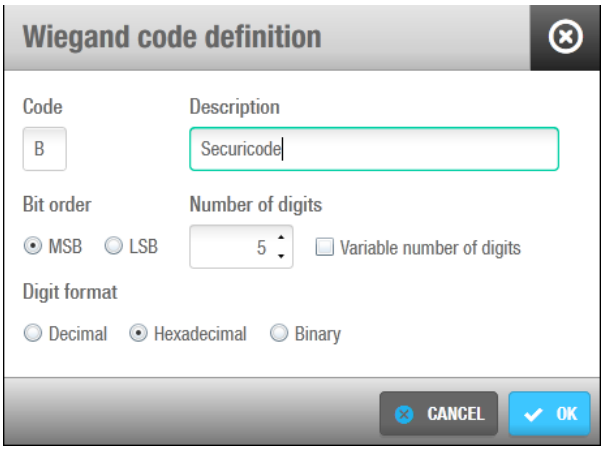


Figure 293: Wiegand code definition dialog box

This allows you to specify the different parts that form the Wiegand code, and define their characteristics.

4. Type a letter to identify the code in the **Code** field.

   The default option is **A** but you can change this if required. Any letter can be entered except 'P' as this is used to identify the parity of the codes at the beginning and end of the Wiegand code.

5. Type a description for the code in the **Description** field.
6. Select the appropriate digit format for the code in the **Digit format** panel.
7. Select the appropriate bit ordering option for the code in the **Bit order** panel.

   If you select the **MSB** option, the bit order begins with the most significant bit. If you select the **LSB** option, the bit order begins with the least significant bit.

8. Type the appropriate number of code digits in the **Number of digits** field.

   The default value is 5 but you can change this if required.

9. Select the **variable number of digits** checkbox if required.

   You must select this checkbox if the code has a variable number of digits. When you select it, the value in the **Number of digits** field is automatically set to 0.

10. Click **Save**. The code details are displayed in the list of codes.

    You can click **View details** to change the code details or click **Delete** to delete the code.

11. Click **New** again and repeat the process for each required code.

13. 6. 4. Step Two: Defining the Format of the Wiegand Code

To complete Step two:

1. Type the separators that you want to use for the codes in the **Interface format** field when you have finished adding codes.

   This controls how the codes are communicated between the different components in the system. For example, if you have three codes named A, B, and C, you can type 'A-B/C'. In this case, code A is separated from code B by a dash (-), and code B is separated from code C by a slash (/).

2. Type the appropriate order of the Wiegand code in the **Bit composition** field.

   This defines how each code you have created in the code list is ordered in the Wiegand code. The length of the entry should correspond to the number of digits in each code you include, and it should begin and end with the parity (P). In the example above, if the codes A, B, and C contain 5, 12, and 10 digits respectively, you could enter 'PAAAAABBBBBBBBBBBCCCCCCCCCCP'. The parity indicates whether the number of bits is odd or even.

3. Type the appropriate parity format for even numbers in the **Parity rule1** field.

   The parity is calculated according to the specified order so it is important that this is entered correctly. The text you enter should correspond to each bit in the Wiegand code. You should enter an 'X' for the bits you do not want to be used to calculate the parity. Use a dash (-) for bits you do want to be used.

4. Type the appropriate parity format for odd numbers in the **Parity rule2** field.

   You can type additional parity rules to specify the format of the Wiegand code in the **Parity rule3** and **Parity rule4** fields if required.

5. Click **Save** when the Wiegand code configuration is complete and correct. The format information is displayed in the **Format** field.

13. 6. 5. Configuring Tracks

Keys have three tracks or areas in which you can encode data (track 1, track 2, and track 3). You can enable these tracks on user and guest keys to store information from specific ProAccess SPACE fields, for example room names, or key expiration dates. See *Users Tab* ***Error! Reference source not found.*** for more information. You must define what data is written on each track, and this is displayed when you read keys. See *Reading Keys* for more information about reading keys.

To configure a track, perform the following steps:

6. Select **System** > **General options** > **Users**.
7. Select the checkbox for the required track.
8. Type the appropriate value in the **Size** field.

   This defines the number of bytes on the key that are used for the track.
9. Click the button on the right-hand side of the **Content** field. The **Tracks content configuration** dialog box is displayed.

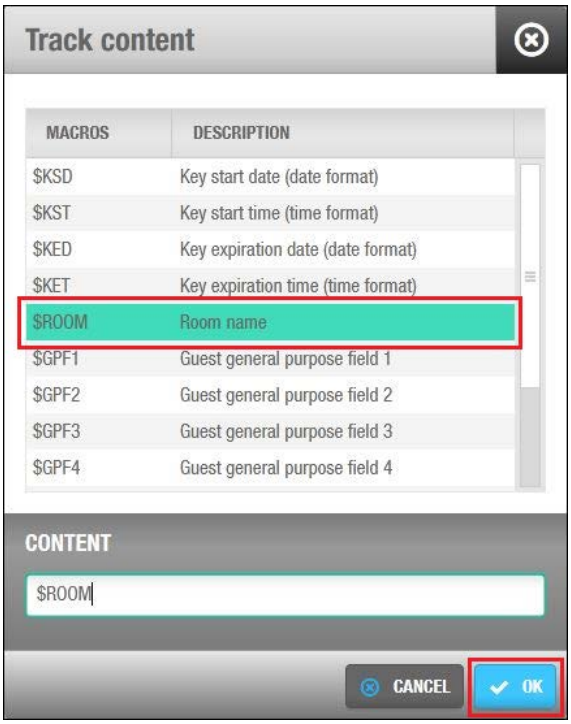


Figure 294: Tracks content configuration dialog box

   This dialog box allows you to specify the data that is written by default when new keys are encoded.
10. Click the required macro in the **Macros** field to select it.

    Macros are available for a number of the fields in ProAccess SPACE. Note that you can use the $ASC macro for ASCII characters or non-printable characters.
11. Click **OK**. The selected macro is displayed in the **Content** field.

    You can include a constant value before or after each macro by typing it in the **Content** field, for example, 'Date' or '-'.

12. Click **Ok** when you have finished inserting macros and the correct macro format is displayed in the **Content** field.
13. Click **Save**.

13. 6. 6. Automatic Key Assignment

You can configure the system to assign keys to users automatically. See *Assigning Keys Automatically* for more information about usage.

Note that this functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

The following table shows the firmware versions required to use the automatic key assignment functionality.

Table 75: Minimum firmware requirements for the automatic key assignment functionality

Component	Requirement
Ethernet board	Version 01.41 or higher
CU5000 board	Version 02.02 or higher
Wall reader	Version 02.65 or higher

To configure the settings for automatic key assignment, perform the following steps:

1. Select **System** > **General options** > **Users**.
2. Select the appropriate mode in the **Automatic key assignment** panel.
3. Select either the **Card serial number** or the **Card data** option.

   You should select the **Card serial number** option if you want to use the serial number of keys for the automatic key assignment. This means the SALTO readers will use the ROM or Unique Identifier (UID) to identify user keys. When you select this option, you must select the appropriate UID format from the **Key UID format** drop-down list. The default option is **7-byte ROM Code (SALTO Format)** but you may need to select a different option, depending on the type of keys you are using. It is important to select the correct option so that the SALTO readers can correctly read the keys. Alternatively, you can select the **Card data** option if you want to use another code instead of the serial number for the automatic key assignment. See *Configuring the Card Data Option* for more information.

NOTE: SALTO readers include any device that can read keys, including wall readers, electronic locks, or encoders.

4. Click **Save**.

13. 6. 7. Configuring the Card Data Option

The configuration settings for the **Card data** option, which is used for automatic key assignment, vary depending on the type of key you select. See *Assigning Keys Automitically* for more information.

Mifare

To configure the settings for the **Card data** option for Mifare, perform the following steps:

1. Select **Mifare** from the **Card data** drop-down list in the **Automatic key assignment** panel on the **User** tab. The **Automatic key assignment** panel is updated to show the Mifare configuration settings.

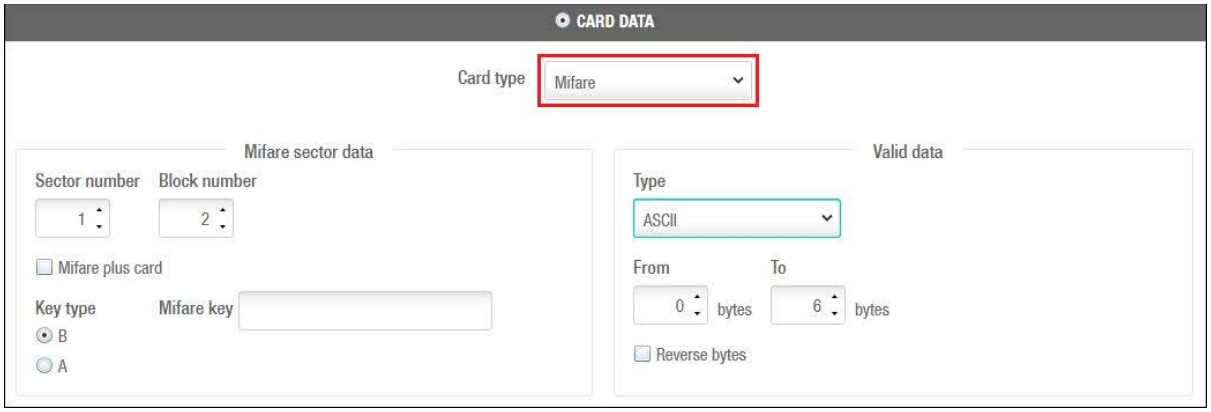


Figure 295: Mifare configuration settings

See *Assigning Keys Automitically* for information about the other options in the **Key assignment** panel.

2. Select the appropriate number from the **Sector** number drop-down list.

   This number indicates the sector on the Mifare key where the code is located.

3. Select the appropriate number from the **Block number** drop-down list.

   This number indicates the block on the Mifare sector where the code is located. The sectors are divided into 16 blocks numbered from 0 to 15.

4. Select the **Mifare plus card** checkbox if required.

   You should select this if you are using Mifare Plus keys.

5. Select either the **B** or **A** option in the **Key type** field.

   This information is required if the Mifare sector is protected. The **A** option is used to read the data in the sector. The **B** option is used to read the data in the sector and write data to it. In this case, you can use either of the options.

6. Type the unblocking key in the **Key** field.

   The unblocking key is a hexadecimal code. It is required if the Mifare sector is protected. Note that you may need to request this from the key manufacturer.

7. Select the appropriate option from the **Type** drop-down list.

   This defines the format of the data.

8. Select the appropriate parameters in the **From** and **To** drop-down lists.

   This specifies the order of the bytes or bits for reading the code.

9. Select the **Reverse bytes** checkbox if required.

   This allows the SALTO readers to interpret the code correctly if it is reversed in the selected card data type.

10. Click **Save**.

DESFire

To configure the settings for the **Card data** option for DESFire, perform the following steps:

1. Select **DESFire** from the **Card data** drop-down list in the **Automatic key assignment** panel on the **User** tab. The **Automatic key assignment** panel is updated to show the DESFire configuration settings.

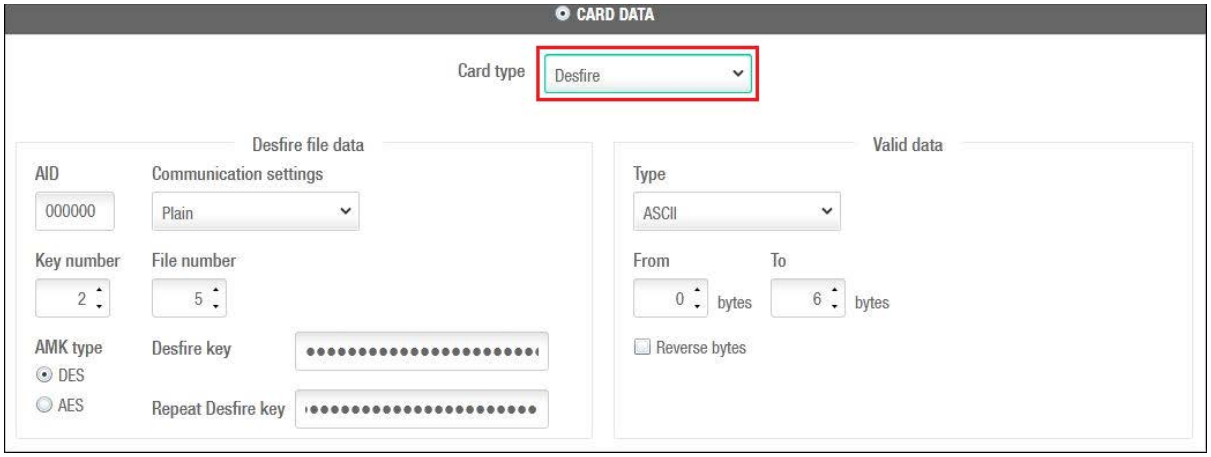


Figure 296: DESFire configuration settings

2. Type the Application Identifier (AID) number of the DESFire data application in the **AID** field.
3. Select the appropriate option in the **Key number** drop-down list.

   This specifies which key is used.
4. Select the appropriate option from the **Comm. Settings** drop-down list if required.

   This activates an additional security for the use of DESFire key data as it changes the format of the key identifier.
5. Select the appropriate option from the **File number** drop-down list.

   This information is required if the DESFire data application contains more than one file.
6. Select either the **DES** or **AES** option in the **AMK type** field.

   The **AES** option uses a higher level of encryption than the **DES** option. Note that AMK refers to Application Master Key.
7. Type the unblocking key in the **Key** field if required.

   The unblocking key is a hexadecimal code. It is required if the DESFire sector is protected. Note that you may need to request this from the key manufacturer.
8. Follow Steps 7, 8, and 9 in *Mifare* to select the appropriate settings in the **Card data** field.
9. Click **Save**.

Legic

To configure the settings for the **Card data** option for Legic, perform the following steps:

1. Select **Legic** from the **Card data** drop-down list in the **Automatic key assignment** panel on the **User** tab. The **Automatic key assignment** panel is updated to show the Legic configuration settings.

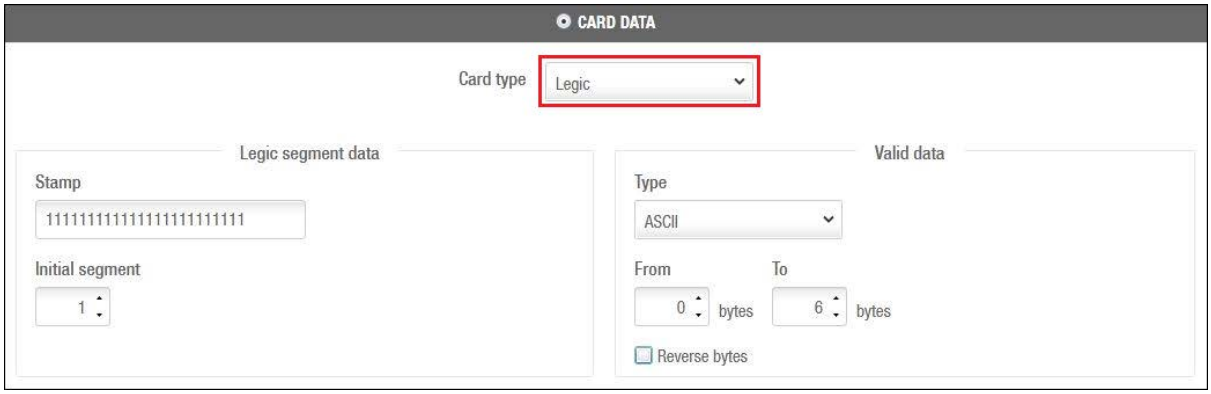


Figure 297: Legic configuration settings

2. Type a stamp for the segment in the **Legic segment data** field.

   This stamp allows the SALTO software to read the Legic segment data.
3. Select the appropriate option from the **Initial segment** drop-down list.

   This defines the first segment from which the data is read. If the initial segment is unknown, you should not change the default value of 0.
4. Follow Steps 7, 8, and 9 in *Mifare* to select the appropriate settings in the **Card data** field.
5. Click **Save**.

13. 7. SHIP Tab

You can configure the SALTO Host Interface Protocol (SHIP) option by using the **SHIP** tab. When SHIP integration is performed, only doors are managed by the SALTO system. Users are managed by a third-party application, which controls their access permissions. You can enable a SALTO server and/or a host server to communicate with this third-party application. Note that you must stop and restart the SALTO Service before certain changes you make on the **SHIP** tab take effect.

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

NOTE: You must discuss your SHIP integration with your SALTO technical support contact. A non-disclosure agreement must be signed before you can use this feature.

Select **System** > **General options** > **SHIP** to view the tab.

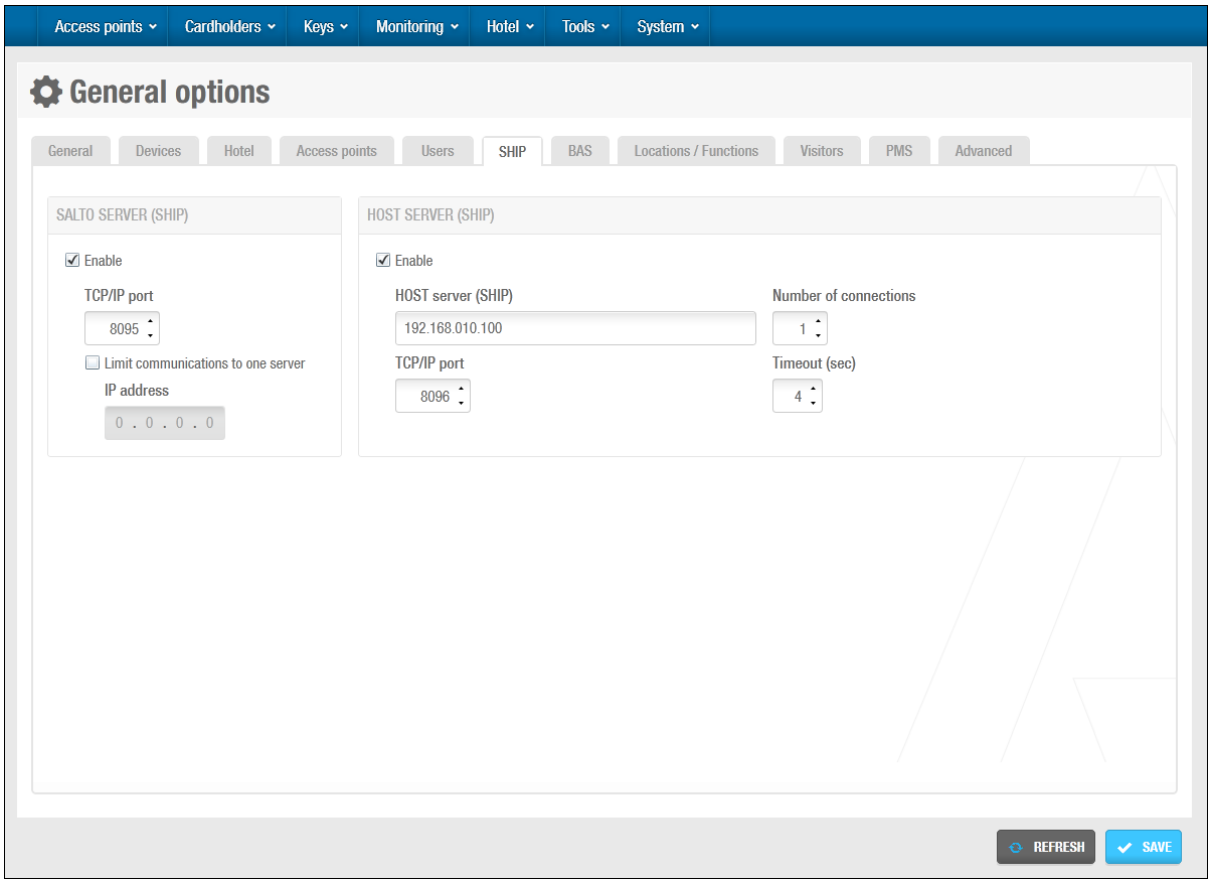


Figure 298: SHIP tab

The tab items are described in the following table.

Table 76: SHIP tab items

Item	Description
Enabled checkbox for SALTO server (SHIP)	Enables the SALTO SHIP server
TCP/IP port field	Specifies a TCP/IP port for server communication
Limit communications to one server checkbox	Limits communications to one server in the network. When you select this option, you must enter the IP address for the third-party server you have selected for the communications in the **IP address** field underneath the checkbox. This means that the SALTO software will only communicate with that server (using SHIP protocol). If you do not select this option, other servers in the network will be able to send commands to the SALTO server.
Enabled checkbox for HOST server	Enables a host SHIP server
HOST server (SHIP) field	Allows you to enter the name or IP address of the PC that will act as the host server
Number of connections field	Defines the number of server connections that are to be established
TCP/IP port field	Specifies a TCP/IP port for server communication
Timeout (sec) field	Defines the length of time that ProAccess SPACE waits for a response from the server before it times out

13. 8. BAS Tab

If your site requires the SALTO system to be integrated with a building automation system, you can configure this by using the **BAS** Integrations tab. The BAS integration functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

NOTE: It is strongly recommended that you consult with your SALTO technical support contact about your BAS integration, as this should be done under supervision.

Select **System** > **General options** > **BAS** to view the tab.

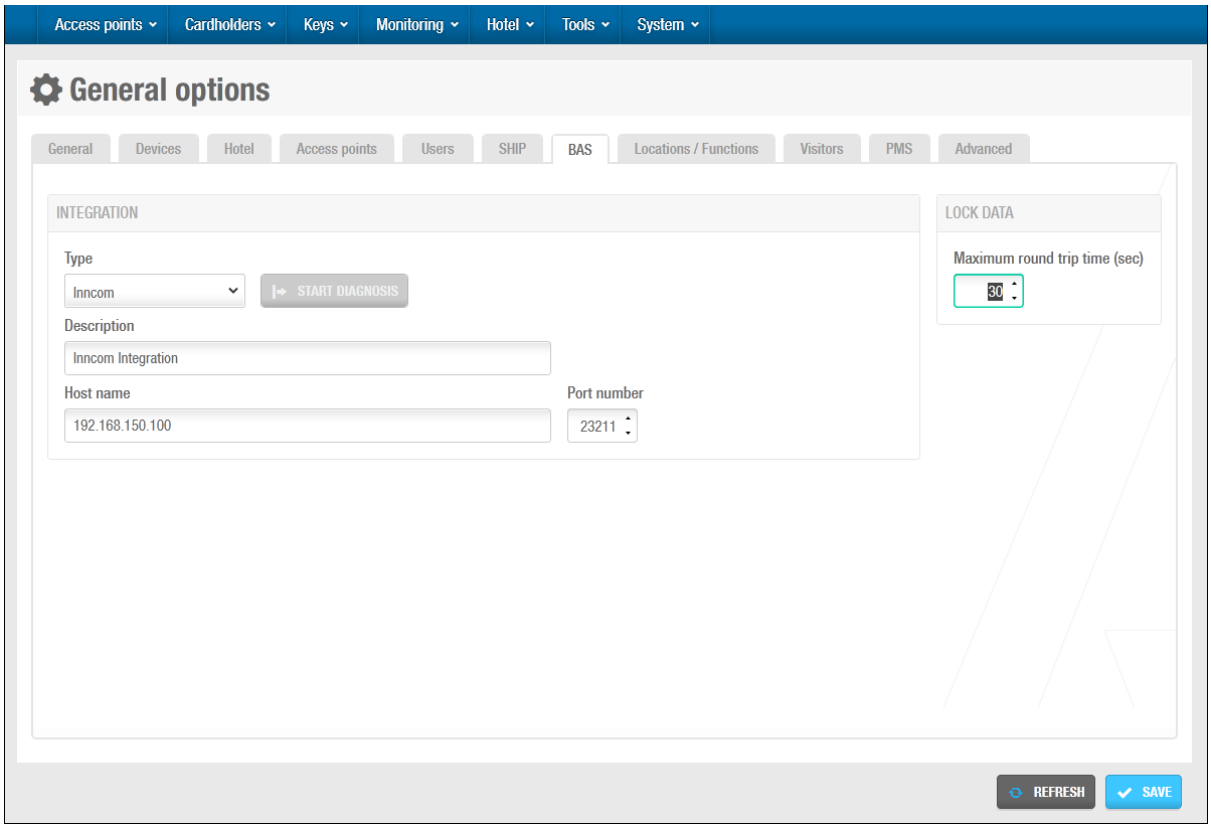


Figure 299: BAS Integrations tab

The tab items are described in the following table.

Table 77: BAS Integrations tab items

Item	Description
Integration type field	Allows you to select a building automation system. Currently, only INNCOM systems can be integrated with the SALTO system.
Start Diagnosis button	Allows starting a diagnosis to troubleshoot any communication problem with the third party system. The diagnosis data will only be useful for SALTO developers, hence, before starting the diagnosis, contact with your SALTO technical support.
Description field	Allows you to enter a description of the specified integration type.
Host name field	Defines the host name for the building automation system server.

Item	Description
Port number field	Specifies the port number that the building automation system uses to connect with the SALTO system and the SALTO network
Maximum round trip time (sec) field	Defines the maximum time period allowed for data to travel from the system to the locks and from the locks back to the system. The system times out if this period is exceeded.

13. 9. Locations/Functions Tab

Locations and functions allow you to give users access to large areas of designated access points and specific categories of permissions within them. This enables easier access management in large sites. You can add groupings for locations and functions by using the **Locations/Functions** tab. This is not mandatory. However, it is recommended that you do this to organize your locations and functions. For example, if an organization has multiple offices in Melbourne, Sydney, and Perth, you can create a separate grouping for all of the offices in each of these cities.

When you add a location grouping, a **Location grouping** drop-down list is displayed on the **Access points** > **Location** information screen in ProAccess SPACE. You can select a group from the list to add the location to the specified group. Similarly, when you add a function grouping, a **Function grouping** drop-down list is displayed on the **Function** information screen in ProAccess SPACE. You can then select a group to which you want to add the function.

See *Locations* and *Functions* for more information about locations and functions.

NOTE: The locations and functions functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

13. 9. 1. Adding Location Groupings

To add a location grouping, perform the following steps:

1. Select **System** > **General options** > **Locations/Functions**.

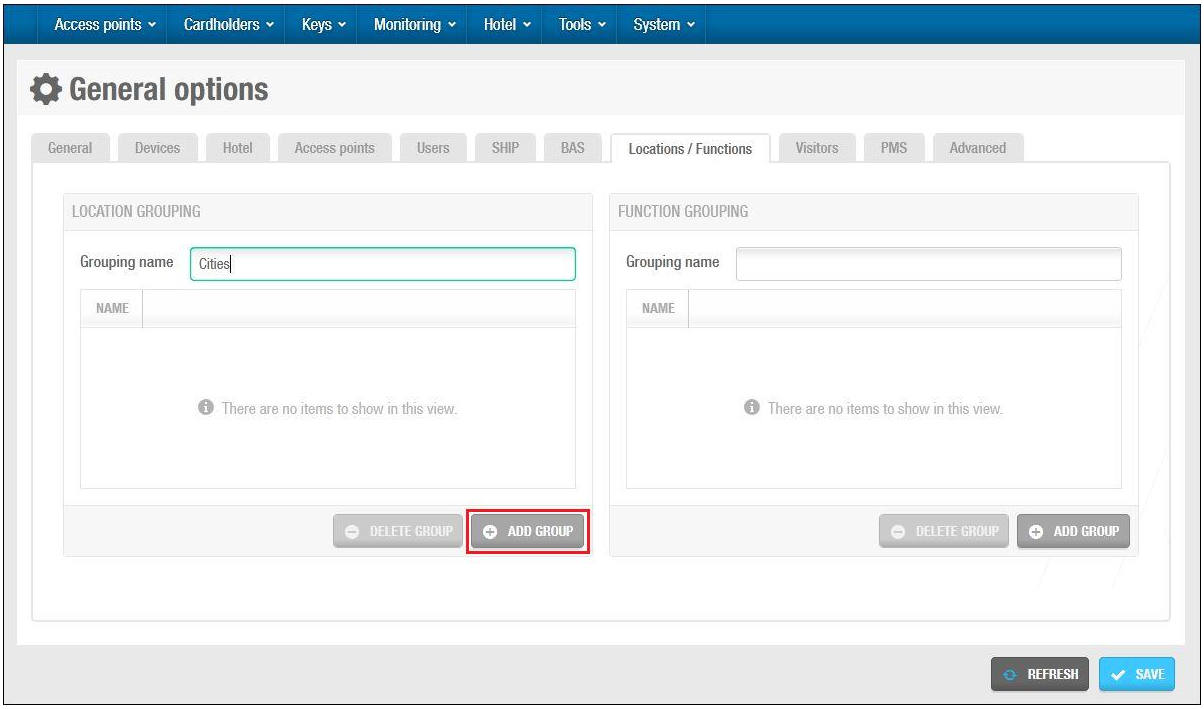


Figure 300: Locations/Functions tab

2. Type a name for the location grouping in the **Grouping name** field.
   This name is applied to the drop-down list that is displayed on the **Location** information screen in ProAccess SPACE.
3. Click **Add Group** to add a new group. The **Enter name** dialog box is displayed.

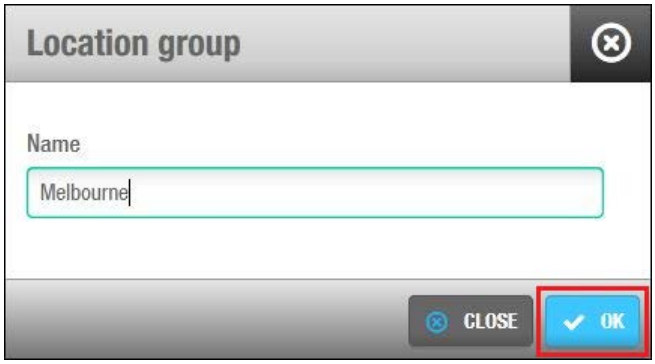


Figure 301: Enter name dialog box

4. Clear the default text and type a name for the new group.
5. Click **Ok**. The group is added to the **Location grouping** list on the **Locations/Functions** tab.
   You can select the group and click **Rename** to rename it, or click **Delete** to delete the group.
6. Click **Save** when you have finished adding all the required groups.

13. 9. 2. Adding Function Groupings

The procedure for adding function groupings is the same as for adding location groupings. See *Adding Location Grouping* for more information and a description of the steps you should follow.

13. 10. Visitors Tab

You can activate or amend options for visitors by using the **Visitors** tab.

Select **System** > **General options** > **Visitors** to view the tab.

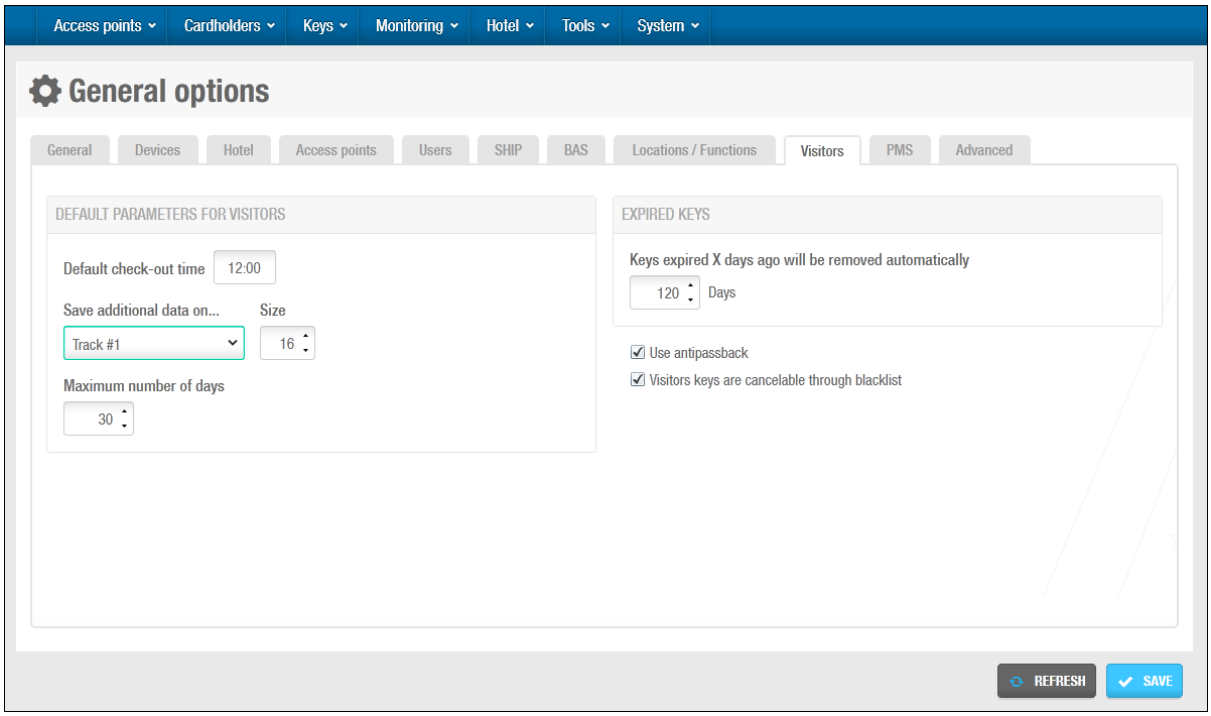


Figure 302: Visitors tab

The tab items are described in the following table.

Table 78: Visitors tab items

Item	Description
Default checkout time field	Defines the default check-out time for visitors on the date their access expires. This value is displayed in the **Date of expiry** field on the **Visitor check-in** screen in ProAccess SPACE, but you can change the value for individual visitors if required.
Save additional data on drop-down list	Allows you to add an extra data field for visitors and defines which track is used for writing the data on visitor keys. See *Error! Reference source not found.* for more information about tracks. The default option is **None**. When you select a track, an **Additional Data** field is displayed on the **Visitor check-in** screen in ProAccess SPACE.
Size field	Defines the character size for the selected track in the **Save additional data on** drop-down list
Maximum number of days field	Defines the maximum number of days for which a visitor can be granted access. The default value is 30 days but you can amend this if required. When you check in a visitor, the date of expiry for the visitor cannot exceed the specified value.

Item	Description
Keys expired X days ago will be removed automatically field	Defines the number of days after which expired visitor keys are automatically deleted by the system. This option only applies if expired visitors have not been deleted manually in ProAccess SPACE. See *Deleting Expired Visitors* for more information.
Use anti-passback checkbox	Controls whether the anti-passback function is used for visitors. When you select this checkbox, the option is applied to all visitors. See *Enabling Anti-passback* for more information about anti-passback.
Visitors keys are cancellable through blacklist checkbox	Controls whether visitor keys are sent to the blacklist when cancelled. If you select this option, it is applied to all visitor keys in the system. See *Deleting Expired Visitors* and *Managing Blacklists* for more information. You must enable the MORE_THAN_64K_USERS parameter to activate this checkbox. See *Advanced Tab* for more information.

13. 11. PMS Tab

You can configure Property Management System (PMS) options by using the **PMS** tab. This creates a link between the SALTO system and any PMS software used to issue guest keys in a hotel site, for example, and allows them to work together. You must stop and restart the SALTO Service before certain changes you make on the **PMS** tab take effect. The PMS functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Select **System** > **General options** > **PMS** to view the tab.

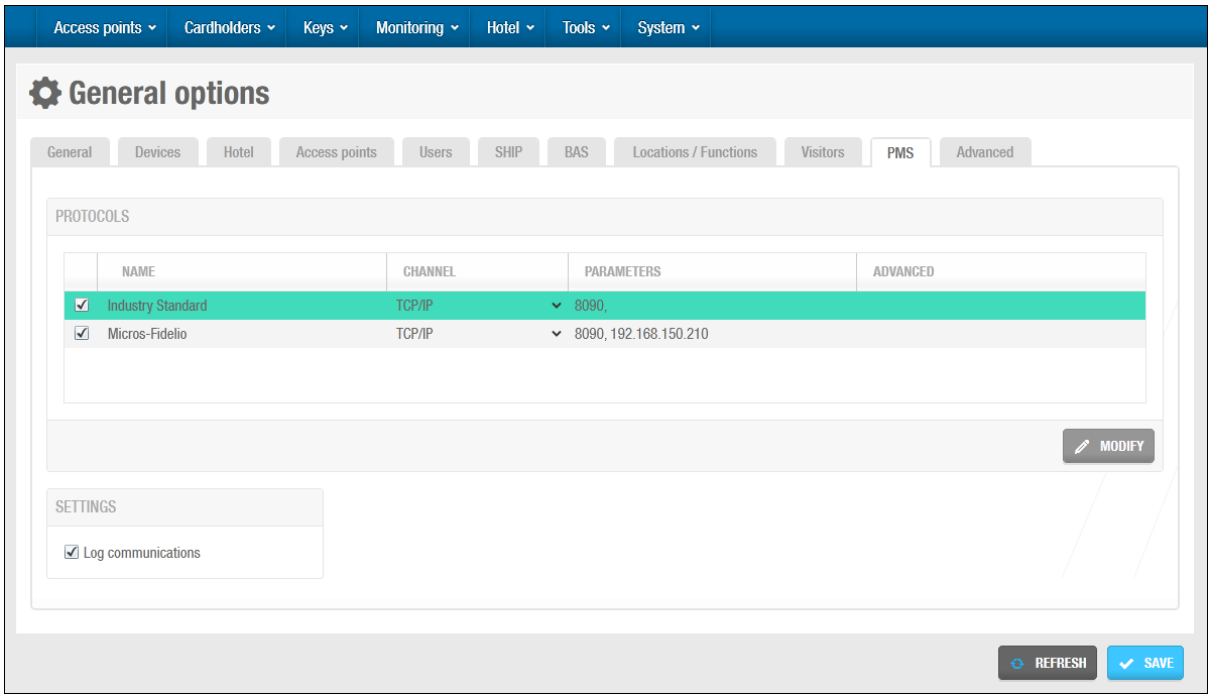


Figure 303: PMS tab

The tab items are described in the following table.

Table 79: PMS tab items

Item	Description
Protocol checkboxes	Allows you to enable PMS protocols that can be used with the SALTO system. Two protocols are currently available: Micros-Fidelio and Industry Standard. If you are unsure of which protocol to select, it is recommended that you consult your PMS administrator. You can select more than one protocol if required. When you select a protocol, you can use the drop-down arrows in the **Channel** column to select a communication port for the PMS connection. The default option is an RS232 serial port but you can select the **TCP/IP** option can be selected if required.
Modify button	Allows you to configure the communication settings for the port you have selected for the protocol. Note that you must click the required protocol to highlight it before you click the **Modify** button.
Authorization list button	Allows you to assign an authorization number to outputs, associated devices, and zones where guest access is optional. See *Zones* for more information about defining guest access points as optional. See also *PMS Authorizations* for more information.
Log communications checkbox	Controls whether the PMS software communication data is stored. If you select this option, the data is stored as a text file in the following location: C:\SALTO\ProAccess Space\logs\ PMS_LOG. It is recommended that you only enable this option if technical issues occur. This is because the log file expands very quickly.

13. 11. 1. Configuring Communication Settings

You must configure the communication settings for the PMS protocols that are used. The settings vary depending on the specific protocol and port option selected.

13. 11. 2. Micros-Fidelio Protocol

You can choose to use either a TCP/IP port or an RS232 serial port for the Micros-Fidelio protocol.

TCP/IP Ports

To configure the settings for a TCP/IP port, perform the following steps:

1. Select **System** > **General options** > **PMS**.
2. Select the checkbox for the Micros-Fidelio protocol in the **Protocol** panel.
3. Click the Micros-Fidelio protocol to highlight it.
4. Click **Modify**. The **TCP/IP com. parameters** dialog box is displayed.

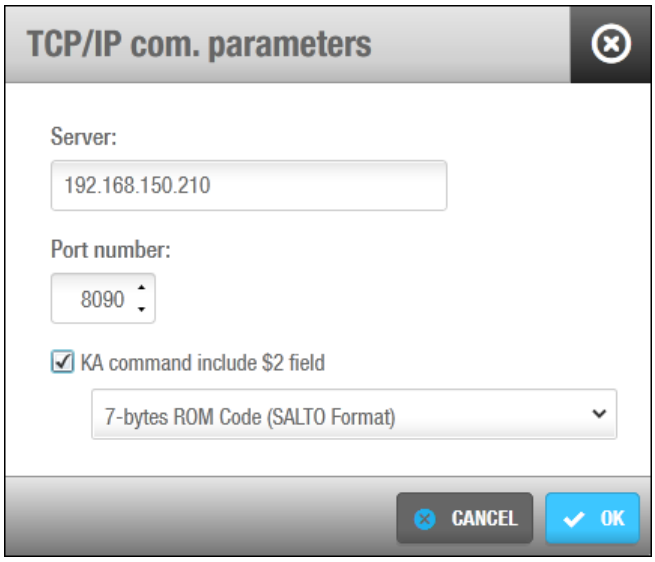


Figure 304: TCP/IP com. Parameters dialog box

5. Type the address of the server in the **Server** field.

   Typically, the IP address of the Micros-Fidelio server is generally entered in this field.
6. Type the port number in the **Port number** field.

   This is the port number that is available for SALTO in the PMS server. The port number should be the same in the SALTO and PMS software.
7. Select the **KA command include $2** checkbox if required.

   When you select this checkbox, the UID code of guest keys is transferred to the PMS software when the key is encoded. The default option for the code format is **7-byte ROM Code (SALTO Format)** but you can select a different option from the drop-down list if appropriate.
8. Click **Ok**. The configuration information is displayed in the **Param** and **Advanced** columns in the **Protocol** panel.
9. Click **Save**.

RS232 Ports

To modify the settings for an RS232 serial port, perform the following steps:

1. Select **System** > **General options** > **PMS**.
2. Select the checkbox for the Micros-Fidelio protocol in the **Protocol** panel.
3. Click the Micros-Fidelio protocol to highlight it.
4. Click **Modify**. The **Serial com. parameters** dialog box is displayed.

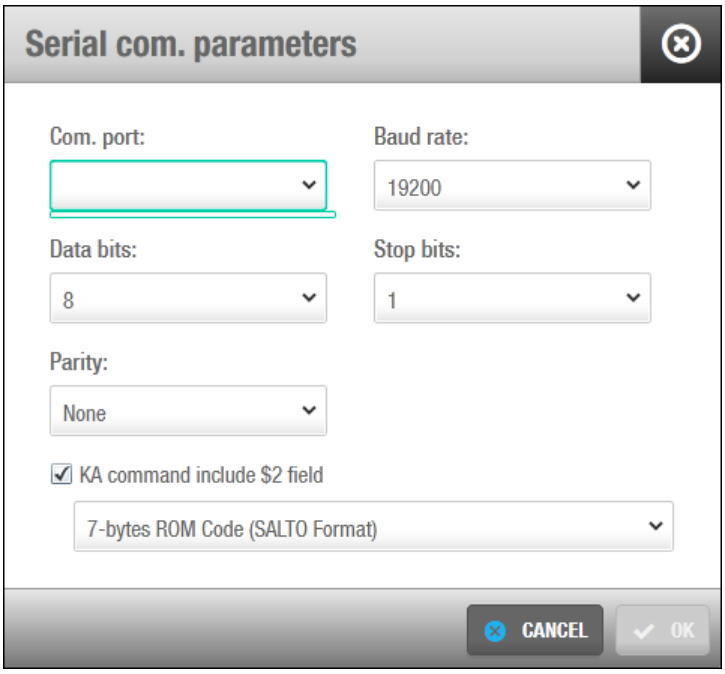


Figure 305: Serial com. parameters dialog box

5. Select the appropriate COM port from the **Com. Port** drop-down list.
6. Select the appropriate number from the **Data bits** drop-down list.

   This value defines the number of data bits in each data character. The default option is **8** but you can select one of the other available values if required.
7. Select the appropriate option from the **Parity** drop-down list if required.

   This allows you to specify the parity method used to detect data transmission errors. The default option is **None**.
8. Select the appropriate option from the **Baud rate** drop-down list.

   This value defines the speed at which data is transmitted.
9. Select the appropriate number from the **Stop bits** drop-down list.

   This value defines the number of stop bits that are included at the end of each data character.
10. Select the **KA command include $2** checkbox if required.

    When you select this checkbox, the UID code of guest keys is transferred to the PMS software when the key is encoded. The default option for the code format is **7-byte ROM Code (SALTO Format)** but you can select a different option from the drop-down list if appropriate.
11. Click **Ok**. The configuration information is displayed in the **Param** and **Advanced** columns in the **Protocol** panel.
12. Click **Save**.

NOTE: When you use RS232 serial ports, you must use the same configuration settings for both the SALTO and PMS software. The number of data bits and stop bits, and the baud rate and parity type you select must be the same for both.

13. 11. 3. Industry Standard Protocol

You can choose to use either a TCP/IP port or an RS232 serial port for the Industry Standard protocol.

TCP/IP Ports

To configure the settings for a TCP/IP port, perform the following steps:

1. Select **System** > **General options** > **PMS**.
2. Select the checkbox for the Industry Standard protocol in the **Protocol** panel.
3. Click the Industry Standard protocol to highlight it.
4. Click **Modify**. The **TCP/IP com. parameters** dialog box is displayed.

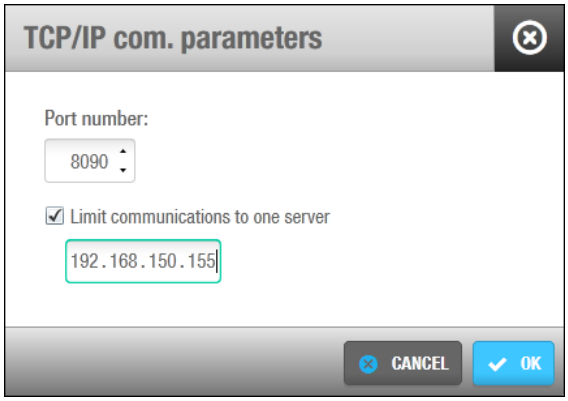


Figure 306: TCP/IP com. parameters

5. Type the port number in the **Port number** field.

   If the PMS and SALTO software are not running on the same PC, the port number you enter must be 5010 or higher. In this case, you must also use the same port number for each of them.
6. Select the **Limit communications to one server** checkbox if required.

   You can limit communications to one PC in the network if required. This means that the system will only process key requests from that PC. You must enter the IP address of the PC in the IP address field.
7. Click **Ok**. The configuration information is displayed in the **Param** column in the **Protocol** panel.
8. Click **Save**.

RS232 Ports

To modify the settings for an RS232 serial port, perform the following steps:

1. Select **System** > **General options** > **PMS**.
2. Select the checkbox for the Industry Standard protocol in the **Protocol** panel.
3. Click the Industry Standard protocol to highlight it.
4. Click **Modify**. The **Serial com. parameters** dialog box is displayed.

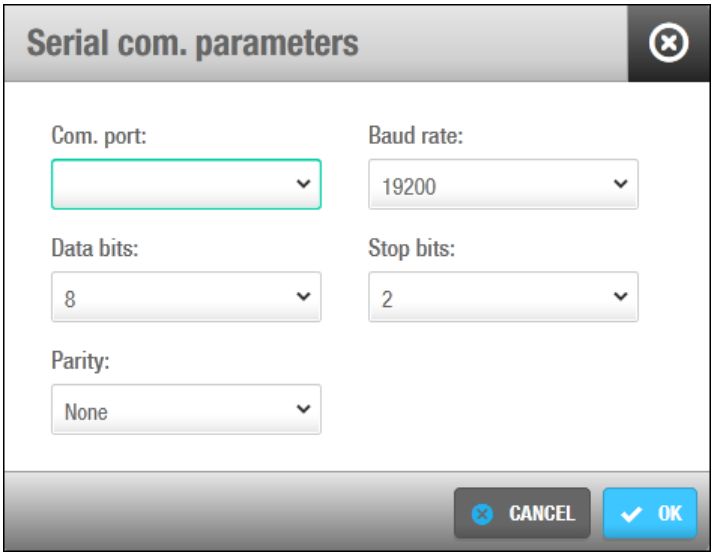


Figure 307: Serial com. parameters dialog box

5. Select the appropriate COM port from the **Com. Port** drop-down list.
6. Select the appropriate number from the **Data bits** drop-down list.

   This value defines the number of data bits in each data character. The default option is **8** but you can select one of the other available values if required.
7. Select the appropriate option from the **Parity** drop-down list if required.

   This allows you to specify the parity method used to detect data transmission errors. The default option is **None**.
8. Select the appropriate option from the **Baud rate** drop-down list.

   This value defines the speed at which data is transmitted.
9. Select the appropriate number from the **Stop bits** drop-down list.

   This value defines the number of stop bits that are included at the end of each data character.
10. Click **Ok**. The configuration information is displayed in the **Param** column in the **Protocol** panel.
11. Click **Save**.

13. 12. Advanced Tab

You can enable advanced parameters in ProAccess SPACE by using the **Advanced** tab.

To enable an advanced parameter, perform the following steps:

1. Select **System** > **General options** > **Advanced**.

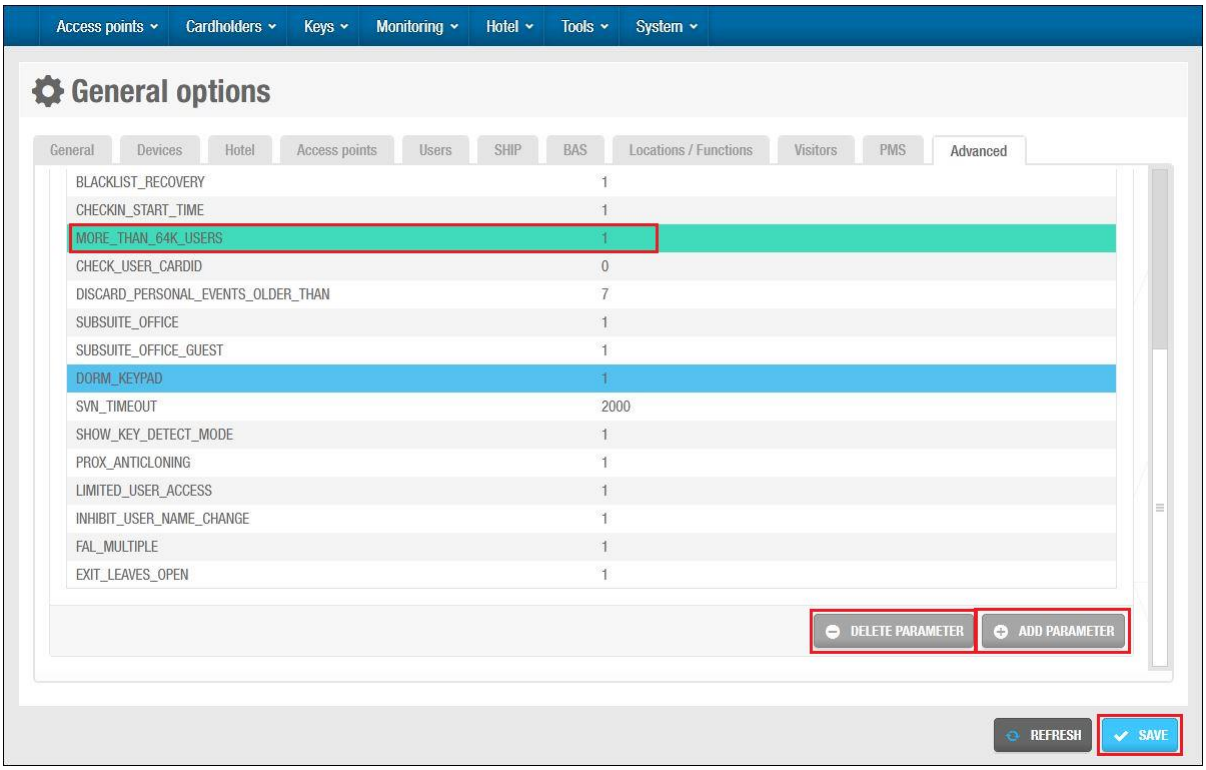


Figure 308: Advanced tab

The **Advanced** tab shows a list of available parameters. These are described in *Advanced Parameter Options*. Any parameters you have enabled are displayed in the **Advanced parameters** field.

2. Click the **Add parameter** button. The parameters list is displayed in the **Add parameters** screen.

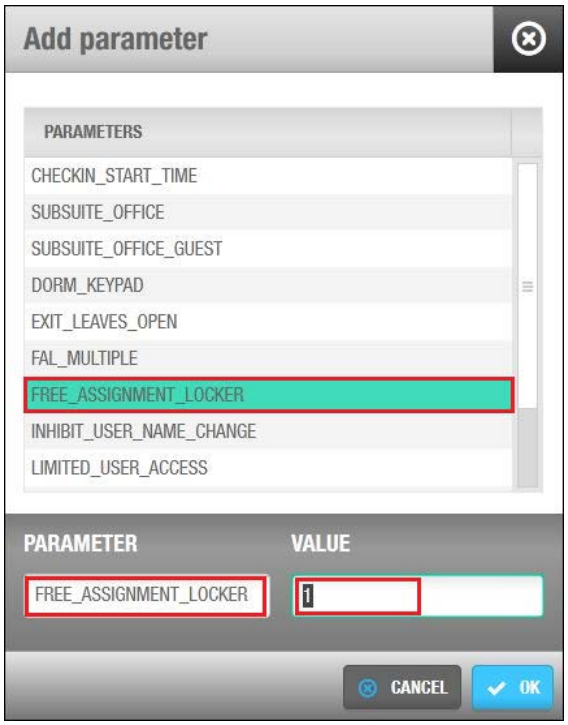


Figure 309: Advanced parameters

3. Double-click on the required parameter under the **Parameters** column. The **Value** field '1' means the parameter is enabled.

   You can adjust the parameter value if required. See *Table 80* for more information.
4. Click **OK**.

NOTE: You can consult the *SALTO RW Advanced Parameters* document for more information about advanced parameters. The **Value** field is Boolean data type, having two values (usually denoted true= 1 and false= 0). In some cases, a different value will be requires such as DISCARD_PERSONAL_EVENTS_OLDER_THAN=7 or AUTO_LOGOFF_TIMEOUT=120. See *Table 80* for more information about the values.

To remove an **Advanced parameters** from the list, highlight the parameter and click **Delete parameter**. One or more parameters can be selected at a time by holding the CTRL key and pressing **Delete parameter** button.

13. 12. 1. Advanced Parameter Options

The advanced parameters are described in the following table.

Table 80: Advanced parameter options

Advanced Parameter	Description
AUTO_LOGOFF_TIMEOUT	Defines the automatic logout time. The system automatically logs you out of ProAccess SPACE after 120 seconds of inactivity. However, you can change this logout time by enabling the AUTO_LOGOFF_TIMEOUT parameter and defining a value (in seconds) as appropriate.
CHECK_USER_CARDID	Activates additional system checks that are performed when the encoder is used to encode new keys for users. The system verifies that the user has a valid card serial number (CSN) and that it corresponds to the CSN on the key being encoded. Otherwise, the encoder operation is cancelled.
CHECKIN_START_TIME	Allows you to define a start time for guest keys. This means you can encode a guest's key at check-in, but specify the exact time from which it can be used. When you enable this parameter, a **Start date time** field is displayed on the **Hotel check-in** screen in ProAccess SPACE. Also, the **Rooms activation time** drop-down list is added to the **Hotel** tab in ProAccess Space General options. This field is used to control the default start date time in ProAccess SPACE. Note that the **Rooms activation time** drop-down list and the **Start date time** field are also displayed when you select the **Enable access to zones before room start time** checkbox on the **Hotel** tab. See *Adding Check-In Information* and *Hotel Tab* for more information.

Advanced Parameter	Description
CUSVN_DATE_EXT	Allows you to specify whether keys that are presented to CUs are revalidated as normal even if the CU is offline. When you enable this parameter, an **Extended expiration (offline)** checkbox is displayed on the information screen for online IP (CU5000) and online IP (CU4200) doors in ProAccess SPACE. See *Connection Types* for more information about connection types. A **CUSVN automatic date extension** field is also displayed on the **Deveces** tab in ProAccess SPACE General options. This allows you to adjust the time parameters for the option. See *Devices Tab* for more information.
DISCARD_PERSONAL_EVENTS_OLDER_THAN	Allows you to set system restrictions on the collection of audit trail data. This can be done for the purposes of privacy. You must define this value in days. There is no limit on the number of days you can enter. For example, DISCARD_PERSONAL_EVENTS_OLDER_THAN =7 means that data older than seven days is not collected from the locks or displayed in the audit trail. If you set the value to 0, the parameter is not enabled.
DORM_KEYPAD	Allows you to specify whether user keys automatically update lock keypads with changes to the keypad code when the key is presented to the lock. When you enable this parameter, a **Dormitory Door** panel is displayed on the **User** information screen in ProAccess SPACE. See *Dormitory Doors* for more information.
EXIT_LEAVES_OPEN	Activates the Exit leaves open mode for rooms and suites, and adds the **Exit leaves open** option to the opening mode options on the **Door** information screen in ProAccess SPACE. See *Opening Modes and Timed Periods* for more information about opening modes.
FAL_MULTIPLE	Enables additional locker zone options that allow you to specify whether users can access lockers within two different free assignment zones using the same key. When you enable this parameter, **Group#1 and Group#2** options are displayed on the **Zone** information screen in ProAccess SPACE. You can select these options when the zone has been defined as a free assignment zone. See *Configuring Zones* for more information.
FREE_ASSIGNMENT_LOCKER	Enables the free assignment locker option, which allows users to choose any locker within a zone (rather than a pre-assigned locker). When you enable this parameter, an **Is free assignment locker** checkbox is displayed on the **Locker** information screen in ProAccess SPACE. See *Creating Free Assignment Zones* and *Locker Options* for more information.

Advanced Parameter	Description
INHIBIT_USER_NAME_CHANGE	Activates system restrictions for user names. When this parameter is enabled, you cannot amend a user's name in the **Title**, **First name**, and **Last name** fields on the **User** information screen in ProAccess SPACE if you have assigned them a key at any point. If you need to change a user name, for example, you must delete the existing user and create a new user profile for them. This ensures that the audit trail data for users is accurate. Note that when the parameter is enabled, you can amend a user's name if they have never been assigned a key.
LIMITED_USER_ACCESS	Allows you to specify the number of individual users that can be granted access to a particular door. Note that this restriction does not apply to users in a user access level associated with the door, or users that have access to a zone with which the door is associated. When you enable this parameter, a **Limit user access** field is displayed on the **Door** information screen in ProAccess SPACE. See *Door Options* for more information.
MORE_THAN_64K_USERS	Allows you to specify whether user, visitor, and guest keys are sent to the blacklist when cancelled. When this parameter is enabled, a **New key can be cancelled through blacklist** checkbox is displayed on the **User** information screen in ProAccess SPACE. In addition, a **Maximum expiration period for non cancellable keys** field is displayed on the **User** tab in ProAccess SPACE **General options** > **Users** tab. See *Cancelling Keys* for more information. A **Visitors keys are cancellable through blacklist** checkbox is also displayed on the **Visitors** tab in ProAccess SPACE General options. See *Visitors Tab* for more information.
PROX_ANTICLONING	Controls the display of proximity card data. When you enable this parameter, data written in proximity cards is mixed with key ROM codes.
SHOW_EXT_ID	Controls the display of the **Ext ID** field. When you enable this parameter, the **Ext ID** field is added to various screens in ProAccess SPACE, for example, the **User** and **Door** information screens. The **Ext ID** field is populated when CSV file synchronization and database table synchronization is performed. See *Automatic CSV File Synchronization* and *Automatic Database Table Synchronization* for more information.

Advanced Parameter	Description
SHOW_KEY_DETECT_MODE	Allows you to define whether key detection is done in pulsed mode (instead of continuous) for locks with IButton readers. When you enable this parameter, an **IButton key detection: pulsed mode** checkbox is displayed on the **Door**, **Room**, and **Locker** information screens. See *Door Options* for more information. This option is only compatible with PPDs that have firmware version 1.02 or higher.
SHOW_ROM_CODE	Controls the display of ROM codes. When you enable this parameter, the ROM codes of user keys are displayed when you read keys or export audit trail data. See ***Error! Reference source not found.*** and *Automatic Audit Trail Exports* for more information.
SUBSUITE_OFFICE	Allows hotel staff (user) keys to be used to activate Office mode for doors in subsuites. See *Opening Modes and Timed Periods* for more information about opening modes.
SUBSUITE_OFFICE_GUEST	Allows guest keys to be used to activate Office mode for doors in subsuites (if the guest has been granted access to the suite). See *Opening Modes and Timed Periods* for more information about opening modes.
SVN_TIMEOUT	Defines the length of time (in milliseconds) before a CU times out when a key is presented for updating. If the CU times out before a response is received from the SALTO software, the key update is not performed. The default option is 2000 milliseconds but this value can be changed. This is useful if network communication is slow due to narrow bandwidth, for example.

NOTE: If an advanced parameter that you require is not displayed in the **Available parameters** field for any reason, you should consult with your SALTO technical support contact. The parameters shown are linked with your SALTO product licensing. Your licensing options may need to be updated if you do not have access to all the required functionality. See *Registering and Licensing SALTO Software* for more information.

14. PERIPHERALS

This chapter contains the following sections:

14. 1. About Peripherals

SALTO peripherals are external hardware devices that are used to perform routine system management tasks such as editing keys, downloading configuration changes to a lock, and controlling the activation of electrical devices in a room to conserve energy. Peripherals are set up within the system by the admin operator or by an operator with admin rights. See *PPD* for more information about the PPD

The two types of SALTO peripherals and the categories of operators who use them are shown in the following table.

Table 81: SALTO peripherals

Peripheral	Operator
 Encoder (USB and Ethernet)	Used by any operator who needs to set up access permissions and transfer data to keys
 Energy Saving Device (ESD)	Used by staff or hotel guests to activate electrical equipment in a room

Encoders and ESDs are set up in ProAccess SPACE. See *ProAccess Space Tools*

This chapter contains the following sections:

14. 2. About ProAccess SPACE Tools

System tools in ProAccess SPACE allow you to conduct tasks such as automatically scheduling data synchronization jobs, and purging and exporting system data. You can also view all tasks performed by each operator, as well as an audit trail of access point opening and closing events.

This chapter describes how to schedule system jobs, view and filter audit events, and view the status of system resources.

14. 3. Scheduling Jobs

Scheduled jobs are system tasks that are set up to be performed automatically. You can view the scheduled jobs on the system by selecting **System** > **Scheduled jobs**.

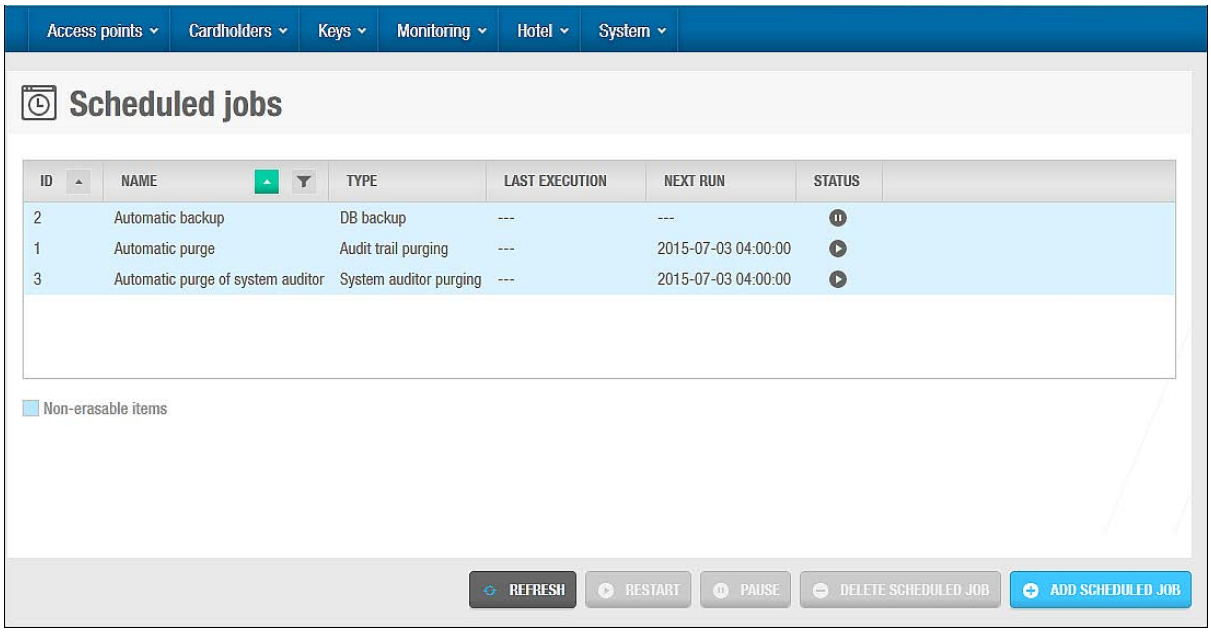


Figure 192: Scheduled jobs screen

The following three job types are scheduled on the system by default:

- Database backup
- Audit trail purging
- System auditor purging

Different icons are displayed in the **Status** column on the **Scheduled jobs** screen, depending on the status of each job. These icons are described in the following table.

Table 40: Scheduled job icons

Icon	Description
 Paused	Shows when a job is paused. You can select the job and click **Restart** to restart it.
 Running	Shows when a job is running. You can select the job and click **Pause** to pause it.

You can change the configuration and scheduling options for the default jobs, or create additional scheduled jobs. If you create an additional scheduled job, you have the option to delete the entry. However, you cannot delete any of the default job types.

NOTE: Scheduled jobs are not performed when the SALTO Service is not running.

14. 3. 1. Automatic Audit Trail Purging

Audit trail purging removes all audit trail data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location. See *Audit Trail* for more information about audit trails. Automatic purges of the audit trail are scheduled to be performed every 60 days by default but you can change the configuration and scheduling options for this job.

NOTE: It is strongly recommended that you purge the audit trail at least once a month. This is because system communication can slow down if the audit trail is very full. Regular audit trail purges also allow you to perform more efficient searches on audit trail entries.

The sections below describe how to complete each step in this process.

14. 3. 1. 1. Step One: Job Configuration

To complete Step one:

5. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
6. Double-click the audit trail purging entry. The **Job Configuration** screen is displayed.

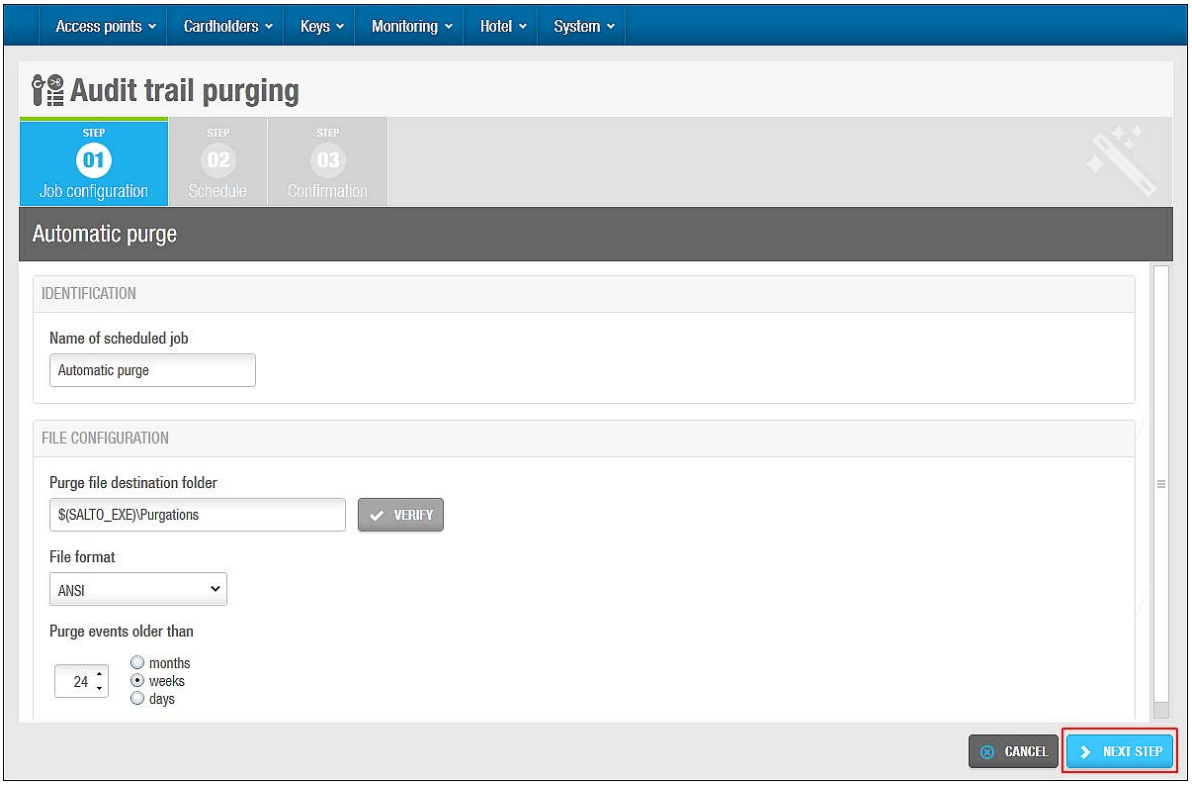


Figure 193: Job configuration screen

The **Name of scheduled job** and **Purge file destination folder** fields are automatically populated but you can change the text in these fields if required. It is recommended that you click **Verify** to verify the file directory exists and is correct.

7. Select a format from the **File format** drop-down list.

   This specifies the format of the file containing the purged events. The appropriate format depends on the alphabet you are using. In general, the system selects the required format by default. However, you can amend this if required.

8. Select the required time parameters using the up and down arrows and the options in the **Purge events older than** field.

   All events prior to the time you select are purged.
9. Click **Next Step**. The **Schedule** screen is displayed.

14. 3. 1. 2. Step Two: Schedule

To complete Step two:

10. Select the required number of days by using the up and down arrows in the **Frequency (days)** field on the **Schedule** screen.

    If you select **50,** for example, the job is performed every 50 days.

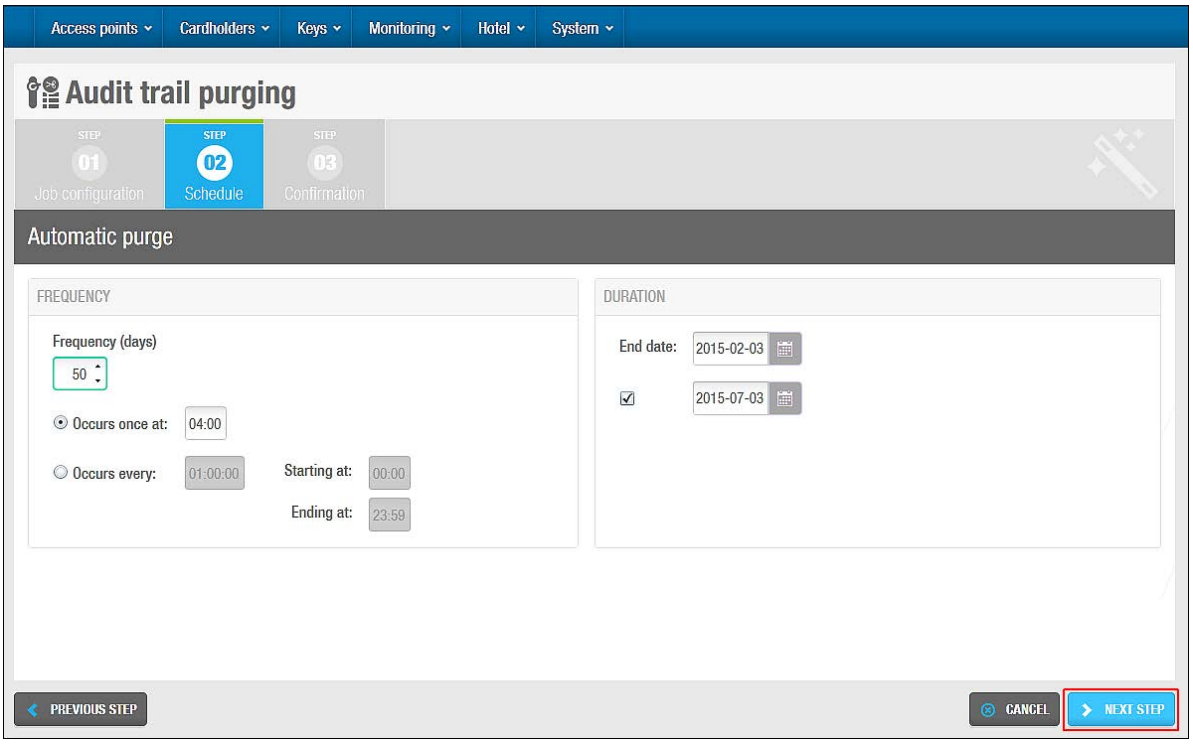


Figure 194: Schedule screen

11. Select either the **Occurs once at** or the **Occurs every** option and type the required time parameters for the selected option.

    These options allow you to specify whether the job occurs once on the scheduled day or at specific intervals during that day.
12. Select a start date for the job using the calendar in the **Start date** field in the **Duration** panel.
13. Select the **End date** checkbox and select an end date for the job using the calendar if required.

    If you do not select an end date the job is performed indefinitely.
14. Click **Next Step**. The **Confirmation** screen is displayed.

14. 3. 1. 3. Step Three: Confirmation

To complete Step three:

15. Review the job configuration and scheduling details on the **Confirmation** screen.

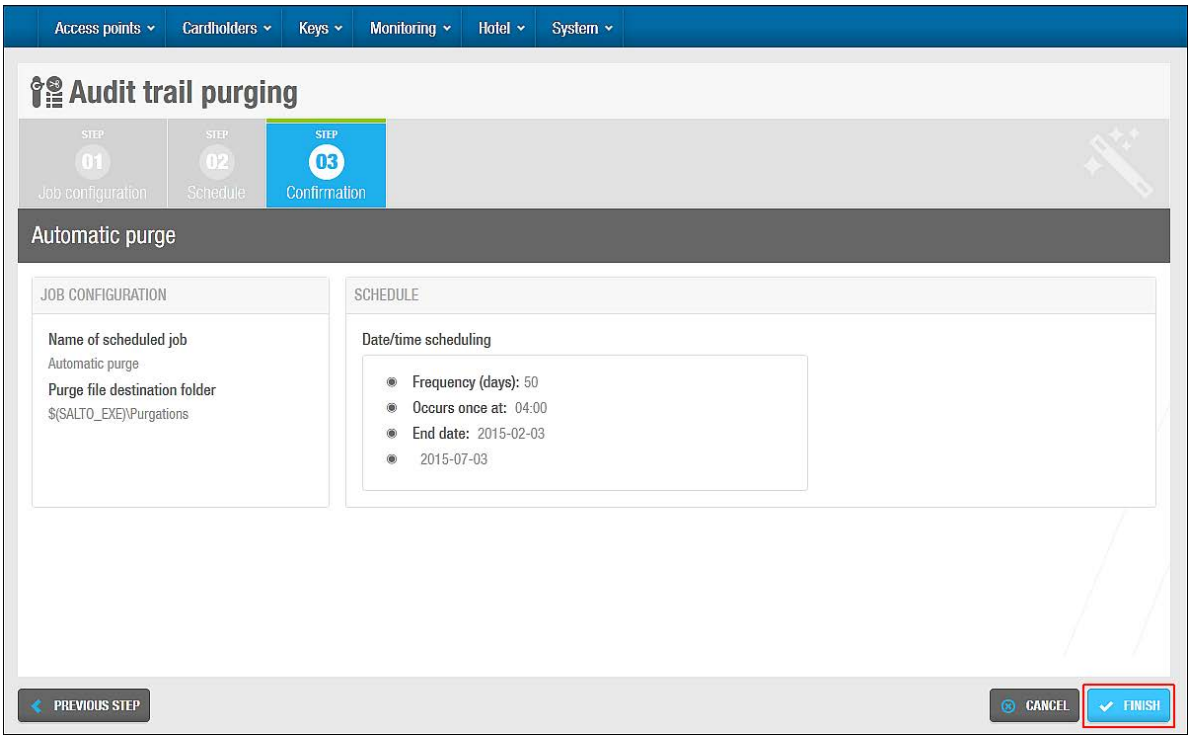


Figure 195: Confirmation screen

You can click **Previous Step** to amend the job configuration and scheduling details or click **Cancel** to discard all your configuration changes.

16. Click **Finish** if all your configuration is complete and correct.

14. 3. 2. Automatic System Auditor Purging

System auditor purging removes all system auditor data within a selected time frame from the system. See *System Auditor* for more information. The purged data is saved to a text file in a specified folder location. Automatic purges of the system auditor are scheduled to be performed every 60 days by default but you can change the configuration and scheduling options for this job.

NOTE: It is strongly recommended that you purge the system auditor at least once a month. They system auditor expands quickly as all system operator events are saved, and system communication can slow down if this is very full. It is particularly important to purge the system auditor regularly if you schedule automatic synchronization jobs. See *Automatic CSV File Synchronization* and *Automatic Database Table Synchronization* for more information.

The sections below describe how to complete each step in this process.

14. 3. 2. 1. Step One: Job Configuration

To complete Step one:

17. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
18. Double-click the system auditor purging entry. The **Job configuration** screen is displayed.

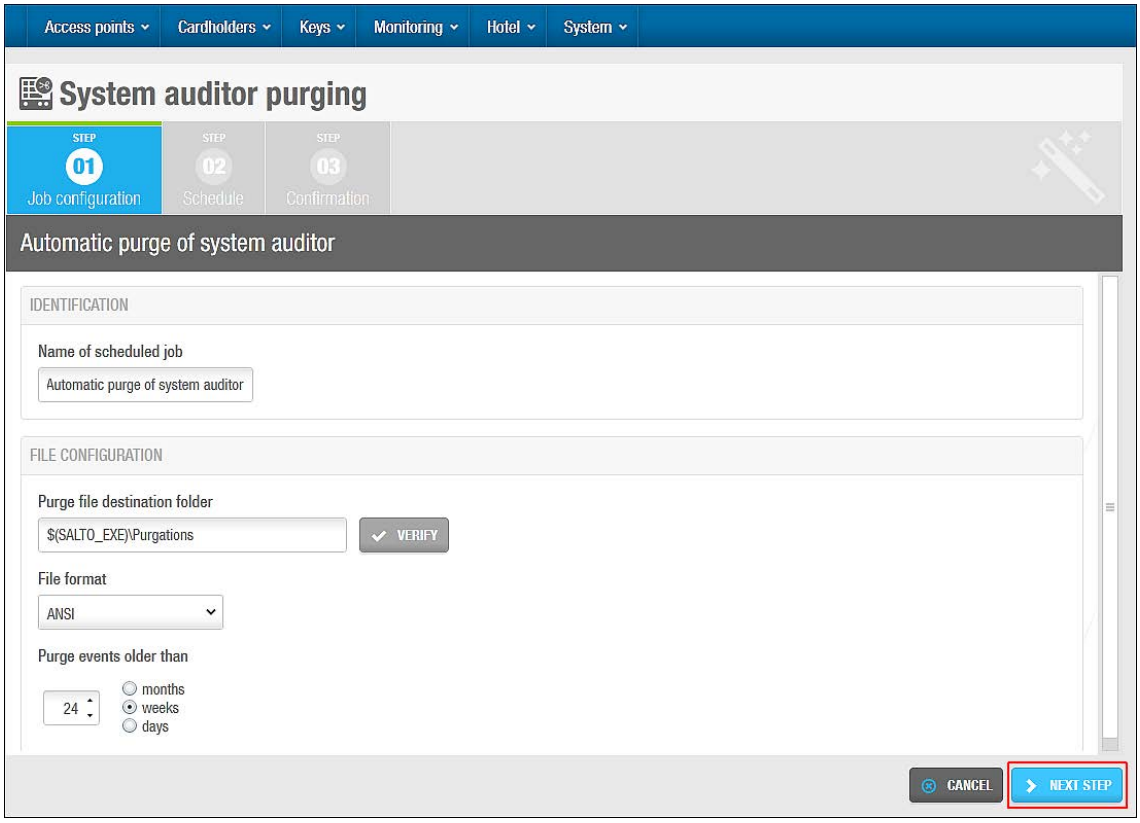


Figure 196: Job configuration screen

The **Name of scheduled job** and **Purge file destination folder** fields are automatically populated but you can change the text in these fields if required. It is recommended that you click **Verify** to verify the file directory exists and is correct.

19. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events. The appropriate format depends on the alphabet you are using. In general, the system selects the required format by default. However, you can amend this if required.

20. Select the required time parameters by using the up and down arrows and the options in the **Purge events older than** field.

    All events prior to the time you select are purged.

21. Click **Next Step**. The **Schedule** screen is displayed.

14. 3. 2. 2. Step Two: Schedule

All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

14. 3. 2. 3. Step Three: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

14. 3. 3. Automatic Database Backups

Automatic database backups are scheduled to be performed every seven days by default but you can change the configuration and scheduling options for this job.

You can also make database backups by using the appropriate menu option in ProAccess SPACE. See *Making Database Backups* for more information.

NOTE: It is recommended that you perform database backups once a week. This ensures data is up to date if you need to restore system backups. Large sites may opt to perform database backups daily. You should not allow more than a month to elapse between backups. System backups are the only means of restoring the system in the event of a total system crash.

The sections below describe how to complete each step in this process.

14. 3. 3. 1. Step One: Job Configuration

To complete Step one:

22. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
23. Double-click the database backup entry. The **Job configuration** screen is displayed.

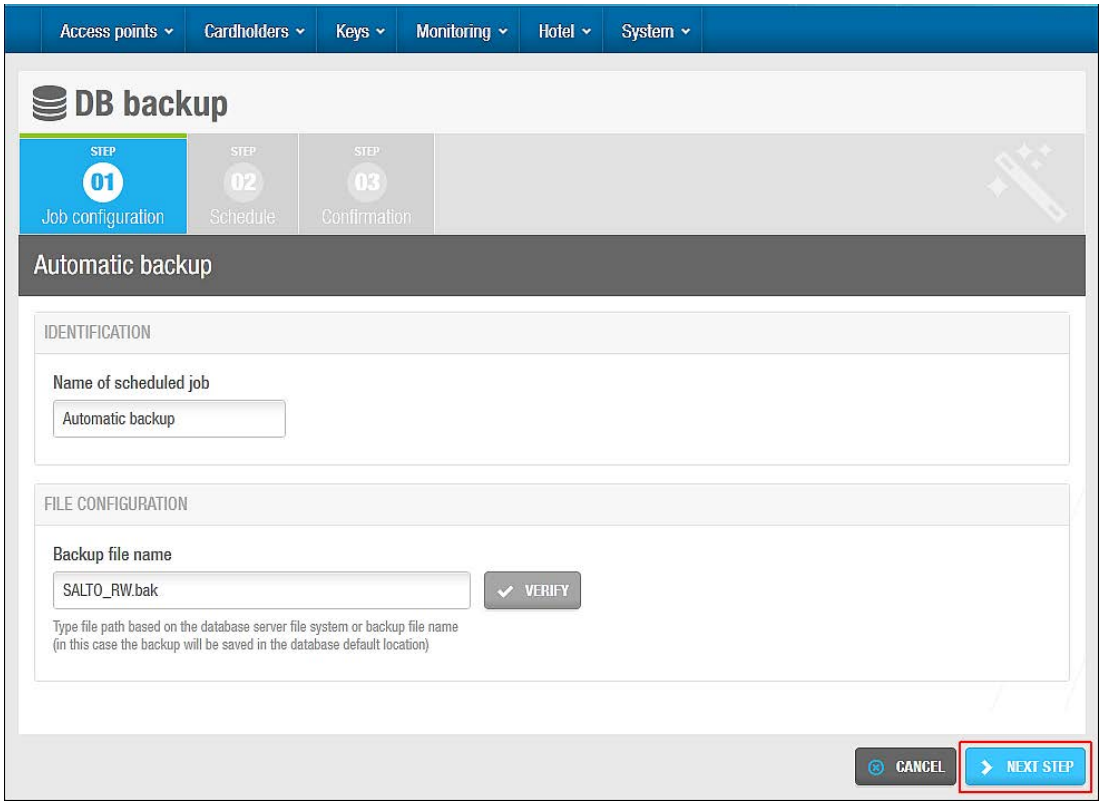


Figure 197: Job configuration screen

The **Name of scheduled job** and **Backup file name** fields are automatically populated but you can change the text in these fields if required. It is recommended that you click **Verify** to verify the file directory exists and is correct.

24. Click **Next Step**. The **Schedule** screen is displayed.

14. 3. 3. 2. Step Two: Schedule

All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

14. 3. 3. 3. Step Three: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

14. 4. Creating Scheduled Jobs

You can create the following types of scheduled job on the system:

- Comma-separated values (CSV) file synchronization
- Database table synchronization
- Audit trail export

When you create a job, it is displayed on the **Scheduled Jobs** screen. The following sections describe how to create these jobs.

The synchronization functionality is license-dependent. The export functionality is also controlled by your licensing options. See *Registering and Licensing SALTO Software* for more information.

14. 4. 1. Automatic CSV File Synchronization

CSV file synchronization allows you to synchronize user data from external system files with ProAccess SPACE. For example, in a university site, you can synchronize with the data in a student record system. You use data from a CSV or a text file to create entries and populate specified fields in ProAccess SPACE. This means you can automatically transfer data from other systems (rather than entering the same data manually in ProAccess SPACE).

NOTE: See the *SALTO_Data_Sync* document for more information about CSV file synchronization.

The sections below describe how to complete each step in this process.

14. 4. 1. 1. Step One: Job Configuration

To complete Step one:

25. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
26. Click **Add Scheduled Job**. The **Add scheduled job** dialog box is displayed.
27. Select **CSV file synchronization** from the drop-down list.
28. Click **OK**. The **Job Configuration** screen is displayed.

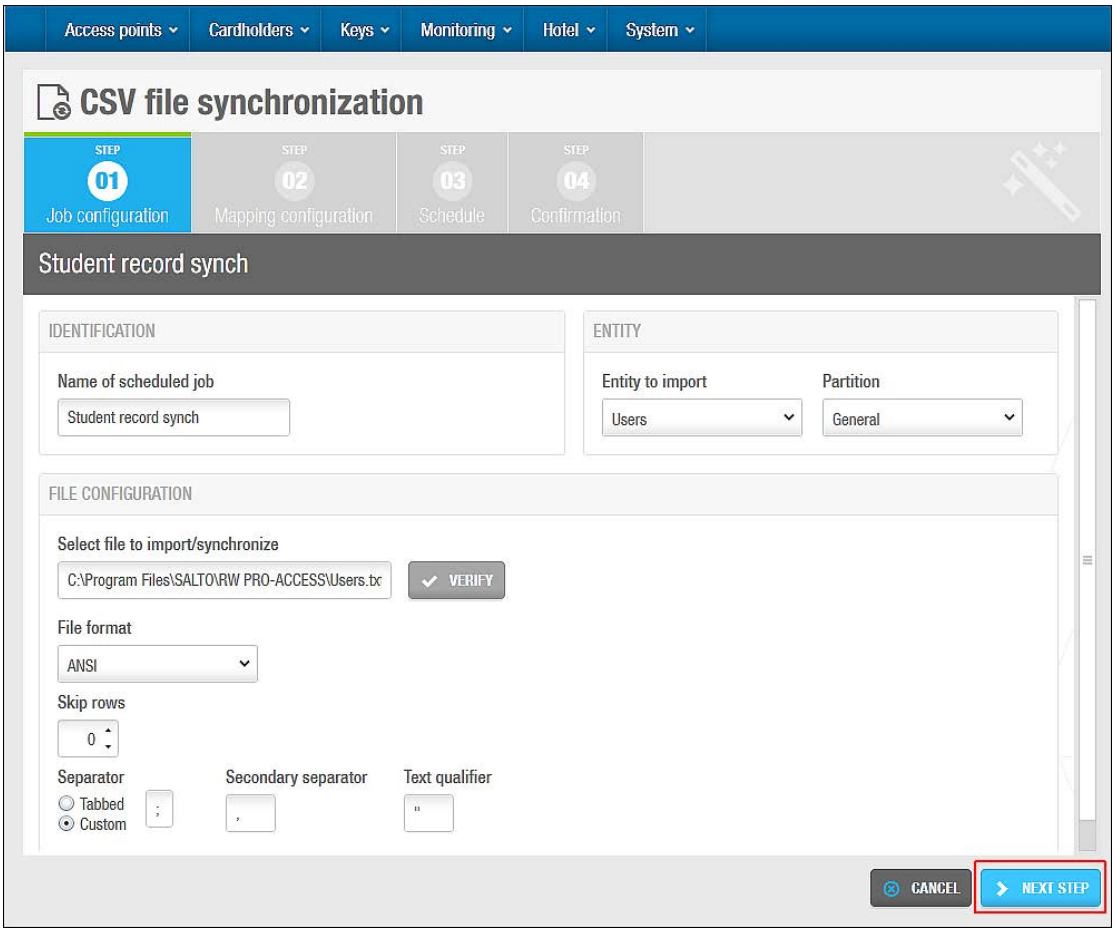


Figure 198: Job configuration screen

29. Type a name for the job in the **Name of scheduled job** field.
30. Type the name of the file that you want to import in the **Select file to import/synchronize** field.

    You can click **Verify** to verify the file directory exists and is correct.
31. Select the appropriate format from the **File format** drop-down list.
32. Select the required number of rows by using the up and down arrows in the **Skip rows** field.

    This specifies the row in the file where you want to begin importing data.
33. Select either the **Tabbed** or **Custom** option.

    The **Secondary separator** and **Text qualifier** fields are automatically populated but you can change the characters in these fields if required. The secondary separator is used to separate each access level ID in the file. The text qualifier is used for text fields that contain spaces.
34. Select the **Entity to import**. Two entities can be selected, **Users** and **Operators**.
35. Select a partition from the **Partition** drop-down list if required.

14. 5. See *Partitions* System Auditor

The **System Auditor** information screen shows a list of all system operator events. Each event has a date and time stamp. By default, the **System Auditor** information screen shows

events for the previous seven days only. To see earlier events, you must define the specific date range in the **Date/Time** filter. See *Filtering System Auditor Data* for more information.

You can view the **System Auditor** information screen by selecting **System** > **System auditor**.

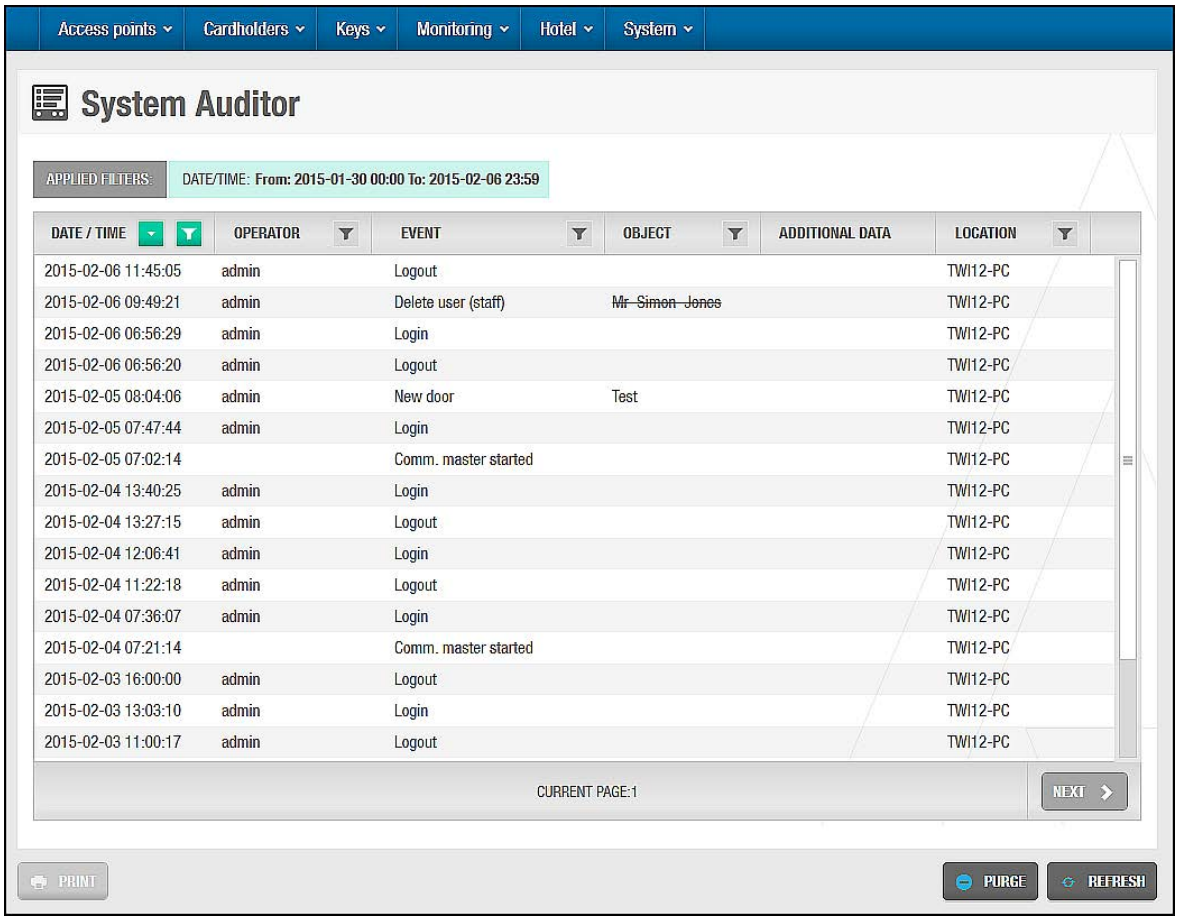


Figure 228: System Auditor information screen

14. 5. 1. Printing and Exporting System Auditor Lists

You can select **System** > **System auditor** and click **Print** on the **System Auditor** information screen to print a hard copy of the system auditor list, or export the list to a specified file format. See *Printing and Exporting Data in ProAccess SPACE* for more information and a description of the steps you should follow.

14. 5. 2. Filtering System Auditor Data

You can filter the system auditor data by event data/type, cardholder/operator, event, object, and/or location. See *Audit Trail Filters* for more information.

To filter the system auditor data, perform the following steps:

36. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.

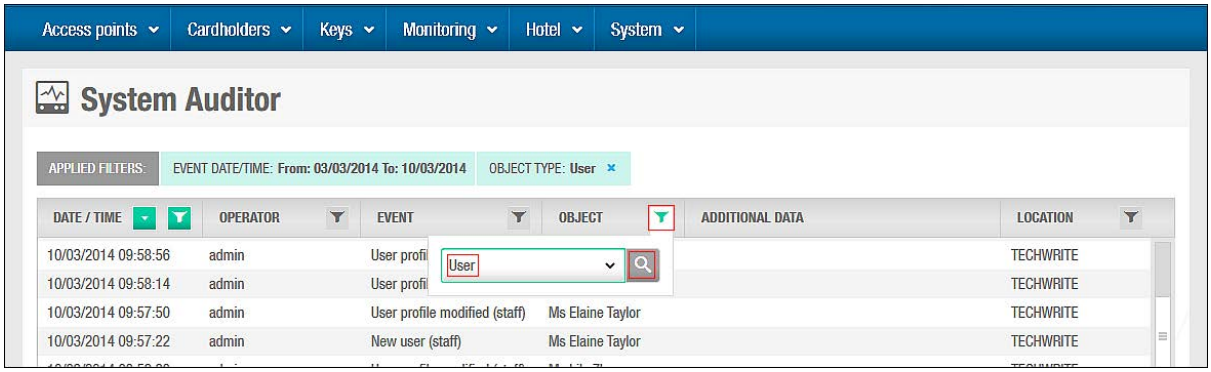


Figure 229: System Auditor information screen

37. Click the **Funnel** icon above the filter item. A search dialog box is displayed.

    For example, if you want to filter by operator type, click the **Funnel** icon at the top of the **Operator** column.

    For the **Event** and **Object** filters, you can see a predefined drop-down list of search terms by clicking the arrow in the dialog box.

    For the **Date/Time** range, you can define a date range by using the **From** and **To** fields.

38. Type your search term.

    Or

    Select a predefined search term from the drop-down list.

    Or

    Select a date range.

    You can apply multiple filters. The applied filters are displayed, highlighted in blue, at the top of your screen. You can click the **Close** icon on an applied filter to remove it.

    However, you cannot remove the **Date/Time** filter.

39. Click the **Search** icon. A filtered audit trail list is displayed.

14. 5. 2. 1. System Auditor Filters

You can use the **System Auditor** information screen filters to display only certain events.

The options are described in the following table.

Table 46: System auditor filters

Audit Data Filter	Description
Event Date/Time	Date and time upon which the event took place
Operator	Name of the operator who performed the event
Event	Details of the event, for example, check-in, new key edited, automatic purge
Object	Object of the event. For example, if a new key was issued to a user, the user is the object.
Location	Name of the organization operating the SALTO system

14. 5. 3. Purging System Auditor Data

Purging the system auditor removes all system auditor data within a selected time frame from the system. The purged data is saved to a text file in a specified folder location.

NOTE: Automatic purges of the system auditor are scheduled by default. See *Automatic*

System Auditor Purging for more information.

To purge the system auditor, perform the following steps:

40. Select **System** > **System auditor**. The **System Auditor** information screen is displayed.
41. Click **Purge**. The **Purge system auditor** dialog box is displayed.

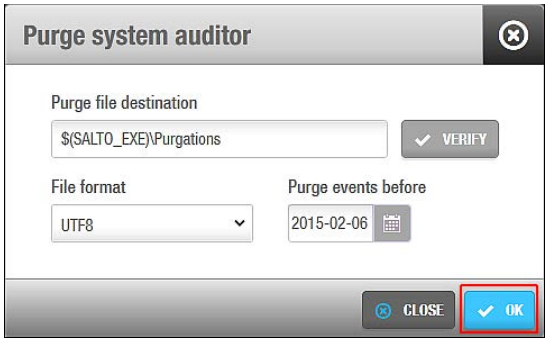


Figure 230: Purge system auditor dialog box

42. Type the appropriate destination folder name in the **Purge file destination** field.

    You can click **Verify** to verify the file directory exists and is correct.
43. Select a format from the **File format** drop-down list.

    This specifies the format of the file containing the purged events.
44. Select the required date by using the calendar in the **Purge events before** field.

    All events prior to the date you select are purged.
45. Click **OK**. A pop-up is displayed confirming the operation was completed successfully.
46. Click **OK**.

14. 6. Operators

The system has one default operator: admin. However, there are no limitations on the number of operators that can be added.

The admin operator has full access to all of the menus and functionality within ProAccess SPACE. However, other types of operators that you create, such as hotel operators, can have their access restricted to a subset of menus and functionality, depending on the permissions you set for their operator group. See *Admin Interface*, *Hotel Interface*, and *Operator Groups* for more information.

NOTE: Operators, as referred to throughout this manual, are operators of the SALTO applications, for example, access and security managers, hotel front-desk staff, or IT system administrators.

14. 6. 1. Adding Operators

You can add operators in ProAccess SPACE. See *Operator Groups* for more information.

To add a new operator, perform the following steps:

47. Select **System** > **Operators**. The **Operators** screen is displayed.

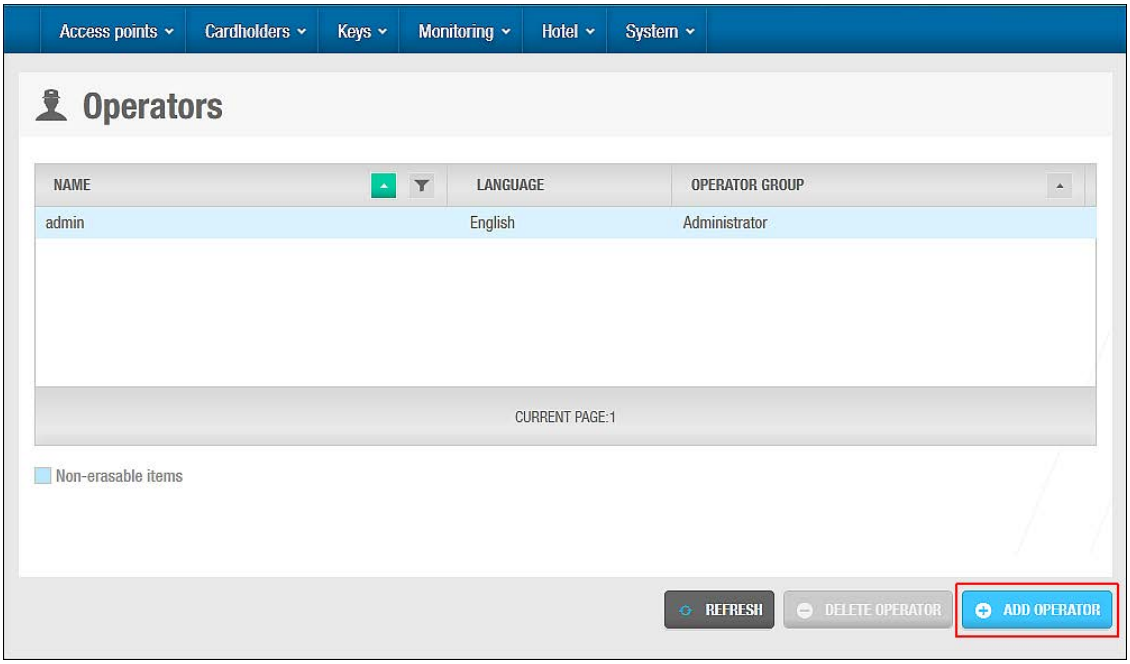


Figure 231: Operators screen

48. Click **Add Operator**. The **Operator** information screen is displayed.

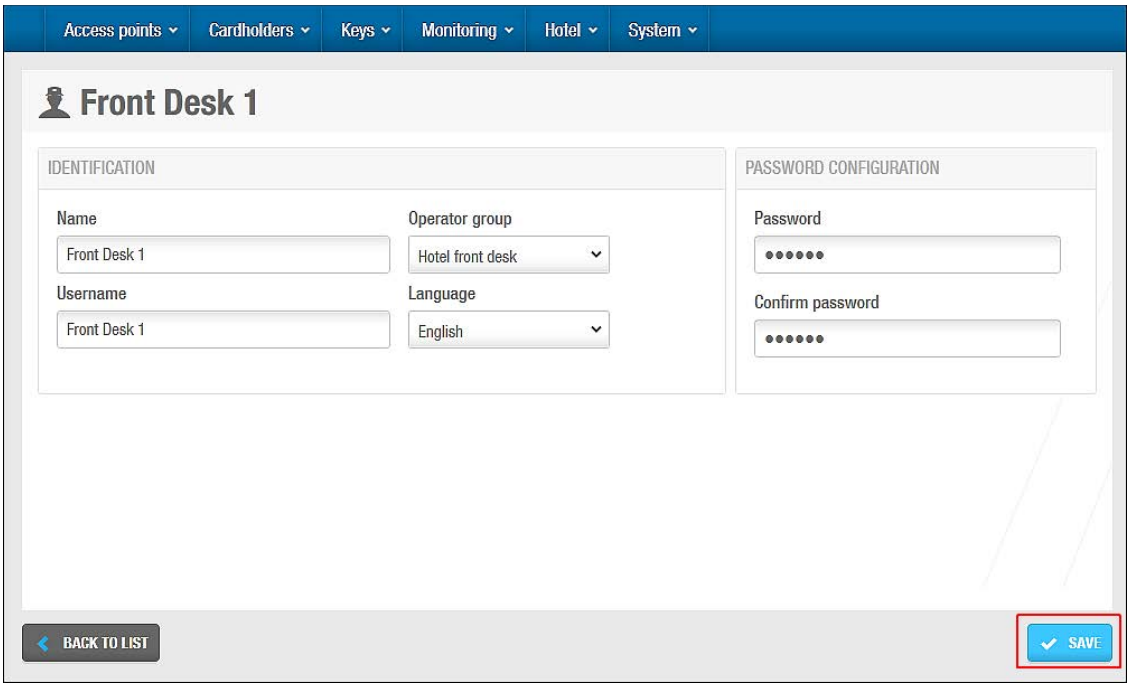


Figure 232: Operator information screen

49. Type the full name of the new operator in the **Name** field.

    A maximum of 56 characters can be entered. The name is not case sensitive.

50. Type the name the operator that will be used to access ProAccess SPACE in the **Username** field.

    A maximum of 64 characters can be entered. The user name is not case sensitive.

51. Select the appropriate operator group from the **Operator group** drop-down list.
52. Select the display language for the operator in the **Language** drop-down list.

53. Type a password for the new operator in the **Password Configuration** panel.

    The password is case sensitive.

54. Confirm the password.
55. Click **Save**.

14. 7. Operator Groups

The system has one default operator group: Administrator. An operator can create, delete, and edit operator groups within his own group depending on the operator group permissions set by the admin operator. An operator cannot give operator groups any permissions other than those that he himself has been granted themselves.

ProAccess SPACE displays all the operator groups that have been created in the system. However, the groups to which the operator does not belong are greyed out and cannot be accessed. See *Operator Group Global Permissions* for more information.

There are no limitations on the number of operator groups that can be added to the system. For example, you can create operator groups for hotel or maintenance staff.

Operator groups are defined according to two operator types:

- **Administrator**: This refers to the default operator group on the system.
- **Standard**: This refers to any operator group that you add to the system.

NOTE: If you delete an operator group, any operators associated with the operator group are also deleted. You cannot delete the default Administrator operator group on the system.

14. 7. 1. Creating Operator Groups

To add new operator groups, perform the following steps:

56. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.

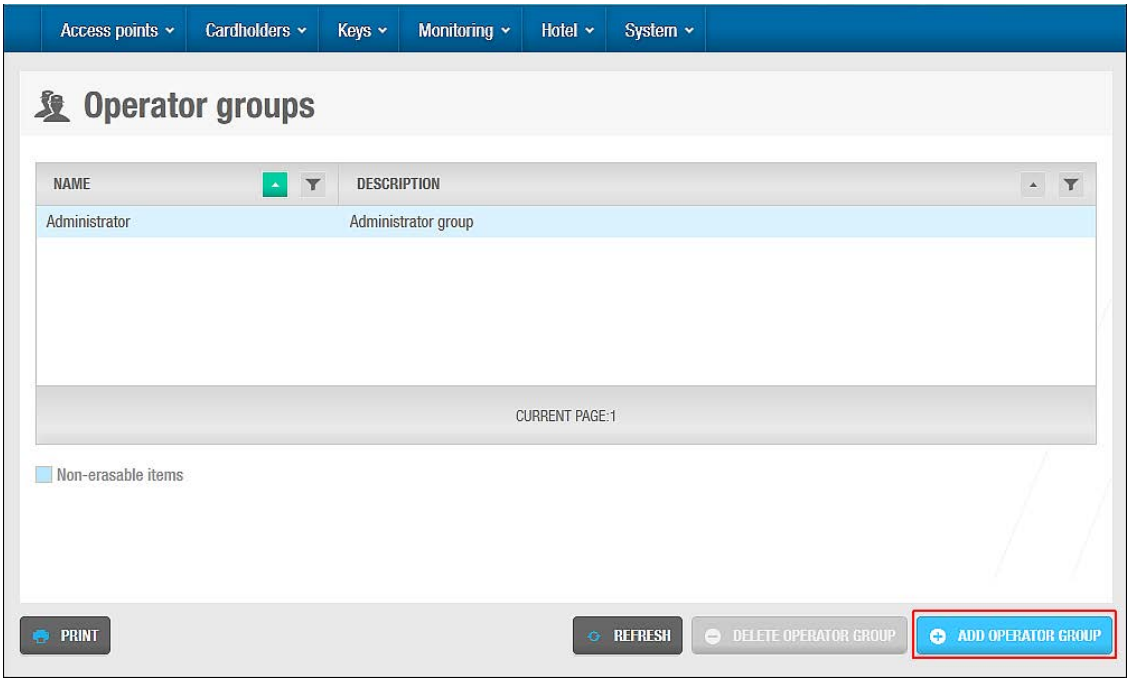


Figure 233: Operator groups screen

57. Click **Add Operator Group**. The **Operator group** information screen is displayed.

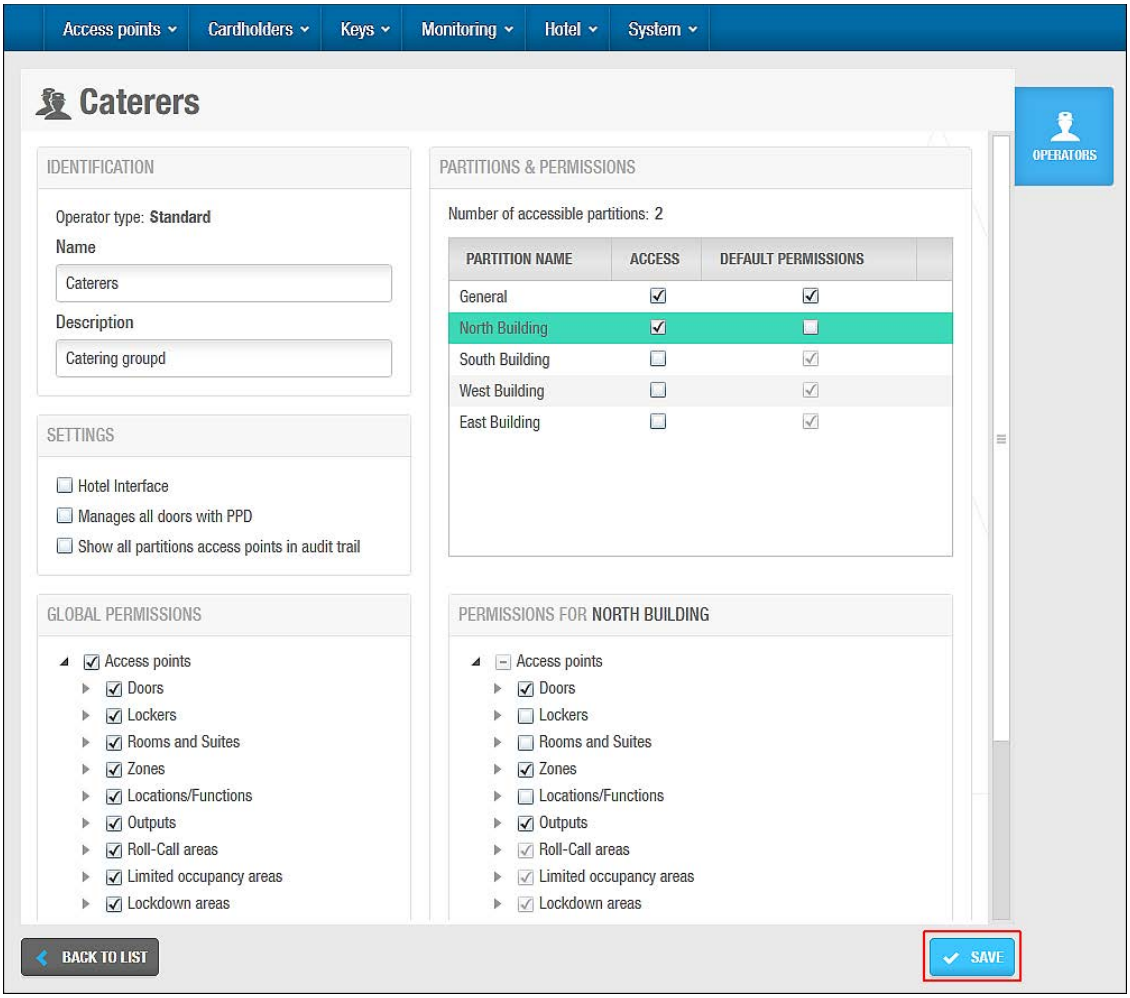


Figure 234: Operator group information screen

58. Type the name of the operator group in the **Name** field.
59. Type a description for the group in the **Description** field.
60. Select the appropriate options in the **Settings** panel.

    The options are described in *Operator Group Settings*.

61. Select the appropriate permissions in the **Global Permissions** panel.

    The options are described in *Operator Group Global Permissions*.

62. Select the appropriate partitions in the **Partitions** panel by selecting the checkboxes in the **Access** column.

    You can select as many partitions as required. See *Partitions* for more information about partitions. The **Default Permissions** option is selected by default for each partition. This means that the operator group global permissions that you have selected in the **Global Permissions** panel are automatically applied to the partition. See *Operator Group Global Permissions* for more information. If you clear the checkbox in the **Default Permissions** column, a **Permissions For** panel is displayed. This allows you to adjust the operator group permissions for that particular partition. You can clear the checkboxes

in the panel to remove certain permissions. However, you cannot grant a permission that has not already been selected in the **Global Permissions** panel.

63. Click **Save**.

14. 7. 1. 1. Operator Group Settings

The admin operator can define the operator group settings by selecting specific options in the **Settings** panel.

The options are described in the following table.

Table 47: Operator group settings

Option	Description
Hotel interface	Selecting this option means that the quick-access tiles specific to hotels are displayed when the operator logs in.
Manages all doors with PPD	Selecting this option means that the operator can use the PPD to perform tasks (such as updating locks) on doors in all of the partitions on the system. See *PPD* for more information.
Show all partitions access points in audit trail	Selecting this option means that the operator can view audit trail data for all of the partitions on the system on the **Audit trail** information screen. See *Audit Trails* for more information about audit trails.

14. 7. 1. 2. Operator Group Global Permissions

The admin operator can specify the tasks that an operator group is allowed to perform by selecting specific permissions in the **Global Permissions** panel.

If you select a top-level permission in the **Global Permissions** panel, all of its sub-level options are automatically selected. You can clear the checkboxes for individual sub-level options if required. If you do not select a top-level permission or any of its sub-level options, the corresponding menu and drop-down options are not displayed when members of the operator group log in to ProAccess SPACE. For example, if you do not select the top-level **Monitoring** checkbox or any of its sub-level options, then the **Monitoring** menu is not visible.

The options are described in *Table 48, Table 49, Table 50, Table 51, Table 52, Table 53,* and *Table 54.*

Access Points Permissions

See *Access Points* for more information about the various access point options described in the following table.

Table 48: Access points permissions

Permission	Description
Doors	Selecting these permissions means that operator group members can: ▪ View a list of doors applicable to their group ▪ Modify door parameters (opening modes etc.) ▪ Modify who has access to the doors ▪ Add and delete doors

Permission	Description
Lockers	Selecting these permissions means that operator group members can: ▪ View a list of lockers applicable to their group ▪ Modify the locker configuration settings ▪ Modify who has access to the lockers ▪ Add and delete lockers
Rooms and Suites	Selecting these permissions means that operator group members can: ▪ View the hotel room and suite list applicable to their group ▪ Modify the hotel room and suite configuration options ▪ Add and delete hotel rooms and suites
Zones	Selecting these permissions means that operator group members can: ▪ View a list of zones applicable to their group ▪ Modify the zone configuration settings ▪ Modify who has access to the zones ▪ Add and delete zones
Locations/Functions	Selecting these permissions means that operator group members can: ▪ View a list of locations and functions applicable to their group ▪ Modify who has access to the locations and functions ▪ Modify the location and function parameters ▪ Add and delete locations and functions
Outputs	Selecting these permissions means that operator group members can: ▪ View a list of outputs applicable to their group ▪ Modify the output configuration options ▪ Modify who has access to the outputs ▪ Add and delete outputs
Roll-Call areas	Selecting these permissions means that operator group members can: ▪ View a list of roll-call areas applicable to their group ▪ Modify the roll-call area configuration options ▪ Add and delete roll-call areas
Limited occupancy areas	Selecting these permissions means that operator group members can: ▪ View the limited occupancy list applicable to their group ▪ Modify the limited occupancy area configuration options ▪ Add and delete limited occupancy areas
Lockdown areas	Selecting these permissions means that operator group members can: ▪ View a list of lockdown areas applicable to their group ▪ Modify the lockdown area configuration options ▪ Add and delete lockdown areas

Permission	Description
Timed periods and Automatic changes	Selecting these permissions means that operator group members can: ▪ View a list of timed periods and automatic changes applicable to their group ▪ Modify the timed periods and automatic changes configuration settings

Cardholders Permissions

See *Cardholders* for more information about the various cardholder options described in the following table.

Table 49: Cardholders permissions

Permission	Description
Users	Selecting these permissions means that operator group members can: ▪ View a list of users applicable to their group ▪ Modify user configuration settings ▪ Add and remove banned users ▪ Add and delete users
Visitors	Selecting these permissions means that operator group members can: ▪ View the list of visitors ▪ Delete visitors from the system
User access levels	Selecting these permissions means that operator group members can: ▪ View the user access level list applicable to their group ▪ Modify the user access level configuration options ▪ Add and delete user access levels
Visitor access levels	Selecting these permissions means that operator group members can: ▪ View the visitor access level list applicable to their group ▪ Modify the visitor access level configuration options ▪ Add and delete visitor access levels
Guest access levels	Selecting these permissions means that operator group members can: ▪ View the guest access level list applicable to their group ▪ Modify the guest access level configuration options ▪ Add and delete guest access levels
Limited occupancy groups	Selecting these permissions means that operator group members can: ▪ View the limited occupancy groups list applicable to their group ▪ Modify the limited occupancy group configuration options ▪ Add and delete limited occupancy groups
Timetables	Selecting these permissions means that operator group members can: ▪ View the timetables applicable to their group ▪ Modify the timetables configuration settings

Keys Permissions

See *Keys* for more information about the various key options in the following table.

Table 50: Keys permissions

Permission	Description
Read key	Selecting this permission means that operator group members can read the data on a key using an encoder.
Delete key	Selecting this permission means that operator group members can delete the data on a key using an encoder.
Issue keys	Selecting this permission means that operator group members can issue new blank keys. Issuing a key reserves and protects a part of the key for SALTO. Assigning a key adds the access plan into the reserved part of the key.
Users	Selecting these permissions means that operator group members can: ▪ Assign user keys ▪ Update user keys ▪ Cancel user keys
Visitors	Selecting these permissions means that operator group members can: ▪ Check in visitors ▪ Check out visitors

Hotels Permissions

See *Hotels* for more information about the various hotel options described in the following table.

Table 51: Hotels permissions

Permission	Description
Check-in	Selecting this permission means that operator group members can check in hotel guests.
Check-out	Selecting this permission means that operator group members can check out guests.
Copy guest key	Selecting this permission means that operator group members can copy guest keys.
Edit guest cancelling key	Selecting this permission means that operator group members can edit a guest cancelling key. You can use these keys to invalidate guest keys so that guests can no longer access their room.
Cancellation of guest lost keys	Selecting this permission means that operator group members can cancel lost guest keys. Cancelling a guest's lost key adds that key to the blacklist.
One shot key	Selecting this permission means that operator group members can edit a one shot key.
Programming/spare key	Selecting this permission means that operator group members can edit a spare key kit. This kit consists of a programming key and spare keys.
Program room cleaner key	Selecting this permission means that operator group members can edit a room cleaner key.
Room status	Selecting this permission means that operator group members can view the room status list.

Monitoring Permissions

See *ProAccess Space Tools* for more information about the various system tool options described in the following table.

Table 52: Monitoring permissions

Permission	Description
Audit trail	Selecting these permissions means that operator group members can: ▪ View the audit trail list of opening and closing events for each access point ▪ Purge the list of audit trail events
Live monitoring	Selecting these permissions means that operator group members can: ▪ Open online locks ▪ Set or remove emergency state in locks ▪ View devices that require maintenance
Roll-Call	Selecting this permission means that operator group members can view the users that are in each roll-call area using ProAccess SPACE Roll-Call monitoring.
Limited occupancy	Selecting this permission means that operator group members can view and reset the number of people in each limited occupancy area in ProAccess SPACE Limited occupancy monitoring.
Lockdown	Selecting this permission means that operator group members can change the emergency state in lockdown areas in ProAccess SPACE Lockdown monitoring.
Graphical Mapping	Selecting this permission means that operator group members can access a graphical mapping application. This means they can: ▪ Access in setup mode ▪ Access in monitoring mode See *SALTO Graphical Mapping Manual* for more information. The graphical mapping functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

Peripherals Permissions

See *Peripherals* and *SALTO Network* for more information about the various peripheral options described in the following table.

Table 53: Peripherals permissions

Permission	Description
PPD	Selecting these permissions means that operator group members can: ▪ Download data to a PPD ▪ Allow emergency opening of access points using a PPD ▪ Initialize and update access points using a PPD ▪ Download firmware files to a PPD
SALTO Network	Selecting these permissions means that operator group members can: ▪ View all the peripherals within the SALTO network (SVN) ▪ Modify the SVN configuration ▪ Add and delete SVN peripherals

System Permissions

See *ProAccess SPACE System Process* for more information about the various system management and configuration options described in the following table.

Table 54: System permissions

Permission	Description
System Auditor	Selecting these permissions means that operator group members can: ▪ View the system auditor events list ▪ Purge the system auditor events list
Operators	Selecting these permissions means that operator group members can: ▪ View the operator list ▪ Modify the operator list ▪ Add and delete operators in the system
Operator groups	Selecting these permissions means that operator group members can: ▪ View the operator group list ▪ Modify the operator group list ▪ Add and delete operator groups in the system
Partitions	Selecting these permissions means that operator group members can: ▪ View the partitions list ▪ Modify the partition configuration options
Calendars	Selecting these permissions means that operator group members can: ▪ View the system's calendars ▪ Modify the system's calendars
Time zones	Selecting this permission means that operator group members can: ▪ View the time zones list ▪ Modify the system's DST settings ▪ Add and delete time zones
Tools	Selecting this permission means that operator group members can perform the following using the system tools: ▪ Configure the scheduled jobs ▪ Synchronize CSV files and DB tables ▪ Export items ▪ Make DB backups ▪ Create SQL DB users ▪ Create and manage card templates ▪ Manage the event stream See *ProAccess Space Tools* for more information about these system features.
Configuration	Selecting these permissions means that operator group members can perform the following types of configuration: ▪ General ▪ Local ▪ RF options

14. 7. 2. Associating Operator Groups

After you have created an operator group, you must associate operators with that group. You can do this by selecting the operator group from the **Operator group** drop-down list on the **Operator** information page. See *Adding Operators* for more information.

To view the operators associated with an operator group, perform the following steps:

64. Select **System** > **Operator groups**. The **Operator groups** screen is displayed.
65. Double-click the operator group with the operator list you want to view.
66. Click **Operators** in the sidebar. The **Operators** dialog box, showing a list of operators, is displayed.

    Partitionsfor more information about partitions. The file data is only imported to the partition you select.
67. Click **Next Step**. The **Mapping Configuration** screen is displayed.

14. 7. 2. 1. Step Two: Mapping Configuration

To complete Step two:

68. Click **Add** on the **Mapping configuration** screen. The number **1** is displayed in the **Source Fields** column.
69. Click the arrow on the right-hand side of the entry to view the **Destination Fields** drop-down list.

    The **[Do not import]** option is selected by default. The destination fields are the targeted ProAccess SPACE options. See the *SALTO_Data_Sync* document for a description of these fields.
70. Select the destination field to which you want to map the data from the source field. The selected option is displayed in the **Destination Fields** column.

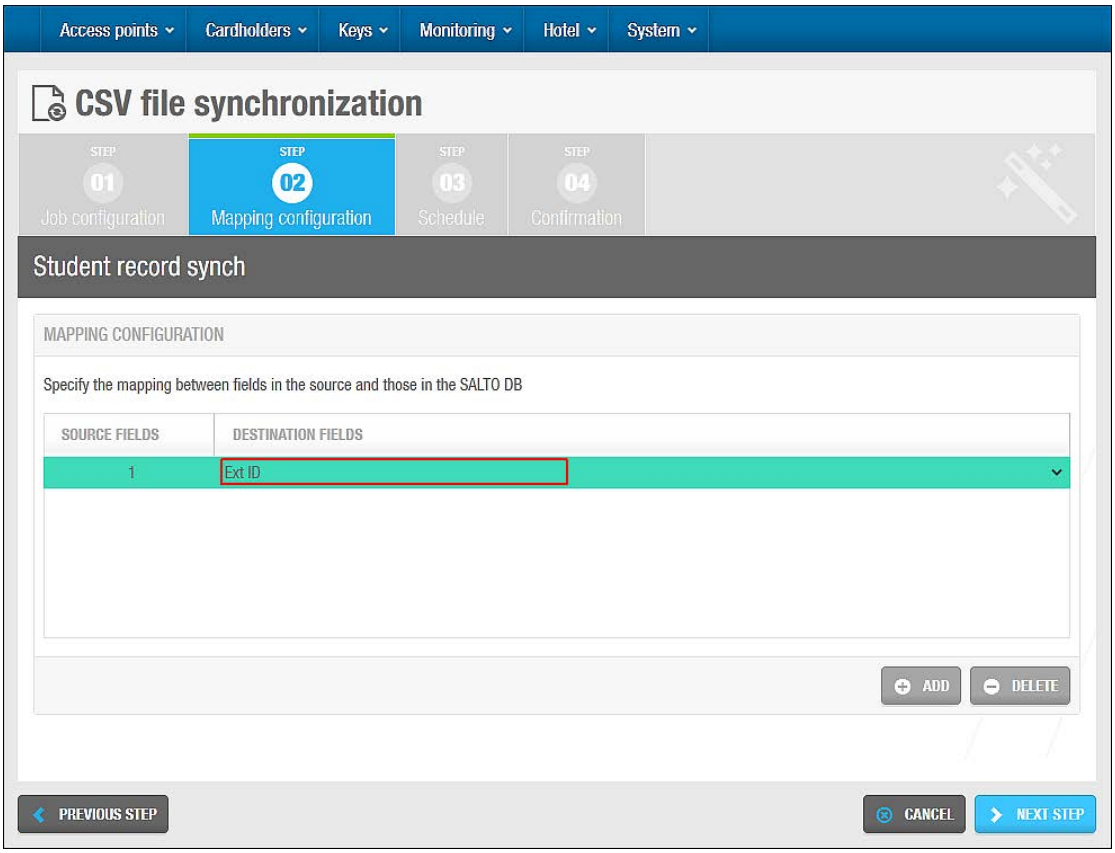


Figure 199: Select destination field

71. Repeat Steps 1, 2, and 3 until you have specified the mapping between all the appropriate source and destination fields and the order of the fields.

NOTE: You must select the **Ext ID** option as one of the destination fields to proceed to the next step. The extension ID is a unique ID that is used to identify users in the system. Selecting this option ensures that the file data is associated with the appropriate users.

72. Click **Next Step**. The **Schedule** screen is displayed.

14. 7. 2. 2. Step Three: Schedule

You can schedule CSV file synchronization to occur as frequently as required, for example, every 24 hours or every second. All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

14. 7. 2. 3. Step Four: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

14. 7. 3. Automatic Database Table Synchronization

Database table synchronization allows you to synchronize user data from external databases with the SALTO database. For example, in a university site, you can synchronize with the data in a human resources database. You can access data stored in an external database and use it to create entries and populate specified fields in ProAccess SPACE.

This means you can automatically transfer data from other databases (rather than entering the same data manually in ProAccess SPACE).

NOTE: See the *Salto_User_Sync_Staging_Table* document for more information about database table synchronization.

The sections below describe how to complete each step in this process.

14. 7. 3. 1. Step One: Job Configuration

To complete Step one:

73. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
74. Click **Add Scheduled Job**. The **Add scheduled job** dialog box is displayed.
75. Select **DB table synchronization** from the drop-down list.
76. Click **OK**. The **Job Configuration** screen is displayed.

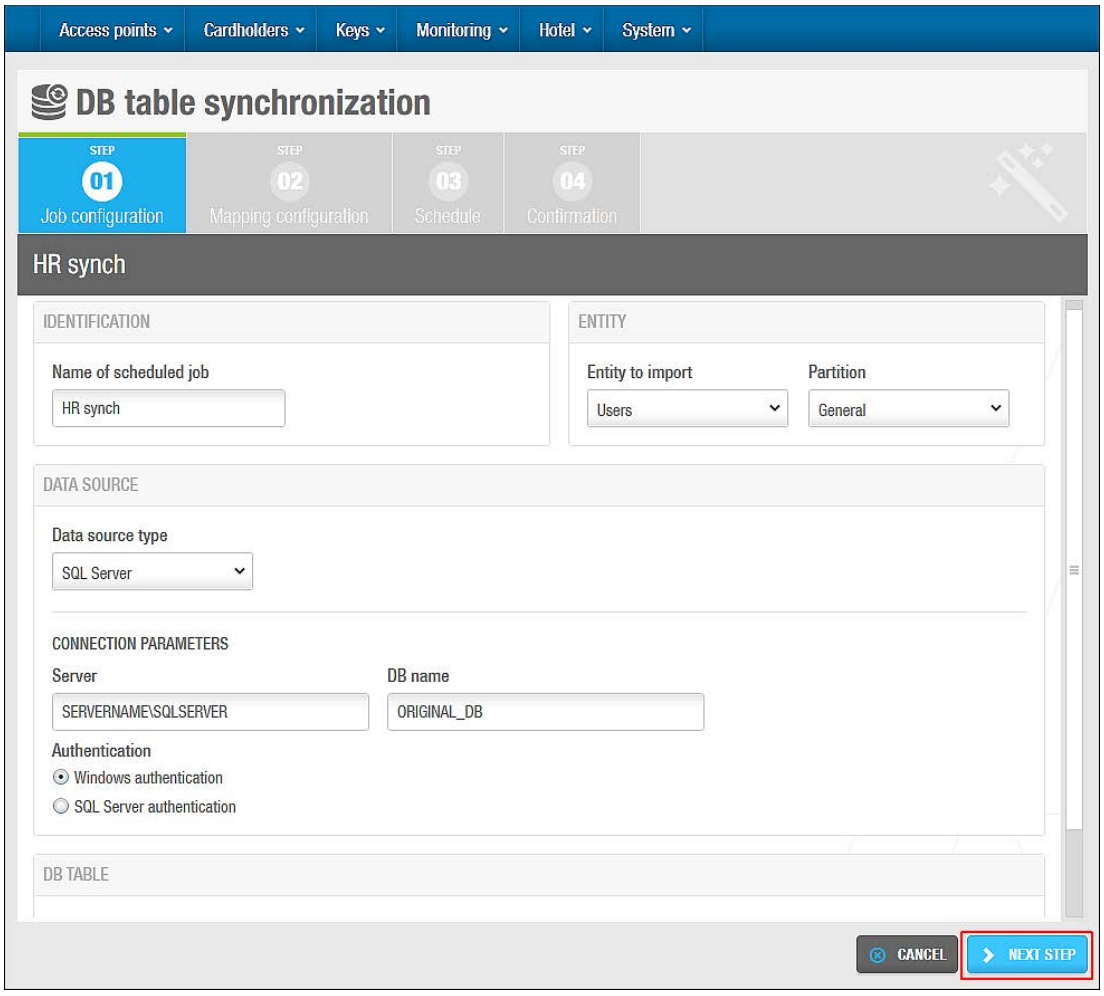


Figure 200: Job configuration screen

77. Type a name for the job in the **Name of scheduled job** field.
78. Select the appropriate data source type from the **Data source type** drop-down list.

    The following options are available:

    - SQL server
    - Oracle
    - ODBC data sources

79. Enter the required information in the fields in the **Connection Parameters** panel.

    The information you must enter in the **Connection Parameters** panel varies depending on which option you select from the **Data source type** drop-down list.
80. Type the name of the database table in the **Table name** field.

    The **Separator** field is automatically populated but you can change the character in this field if required.
81. Select the **Entity to import**. Two entities can be selected, **Users** and **Operators**.
82. Select a partition from the **Partition** drop-down list if required.

    See *Partitions* for more information about partitions. The data is only imported to the partition you select.
83. Click **Next Step**. The **Mapping configuration** screen is displayed.

14. 7. 3. 2. Step Two: Mapping Configuration

To complete Step two:

84. Click **Add** on the **Mapping configuration** screen. The number **1** is displayed in the **Source Fields** column.
85. Click the arrow on the right-hand side of the entry to view the **Destination Fields** drop-down list.

    The **[Do not import]** option is selected by default. The destination fields are the available SALTO database fields to which you can import data. Once imported into the SALTO database, the information is then displayed in the appropriate field in ProAccess SPACE. See the *Salto_User_Sync_Staging_Table* document for a description of these fields.
86. Select the destination field to which you want to map the data from the source field. The selected option is displayed in the **Destination Fields** column.

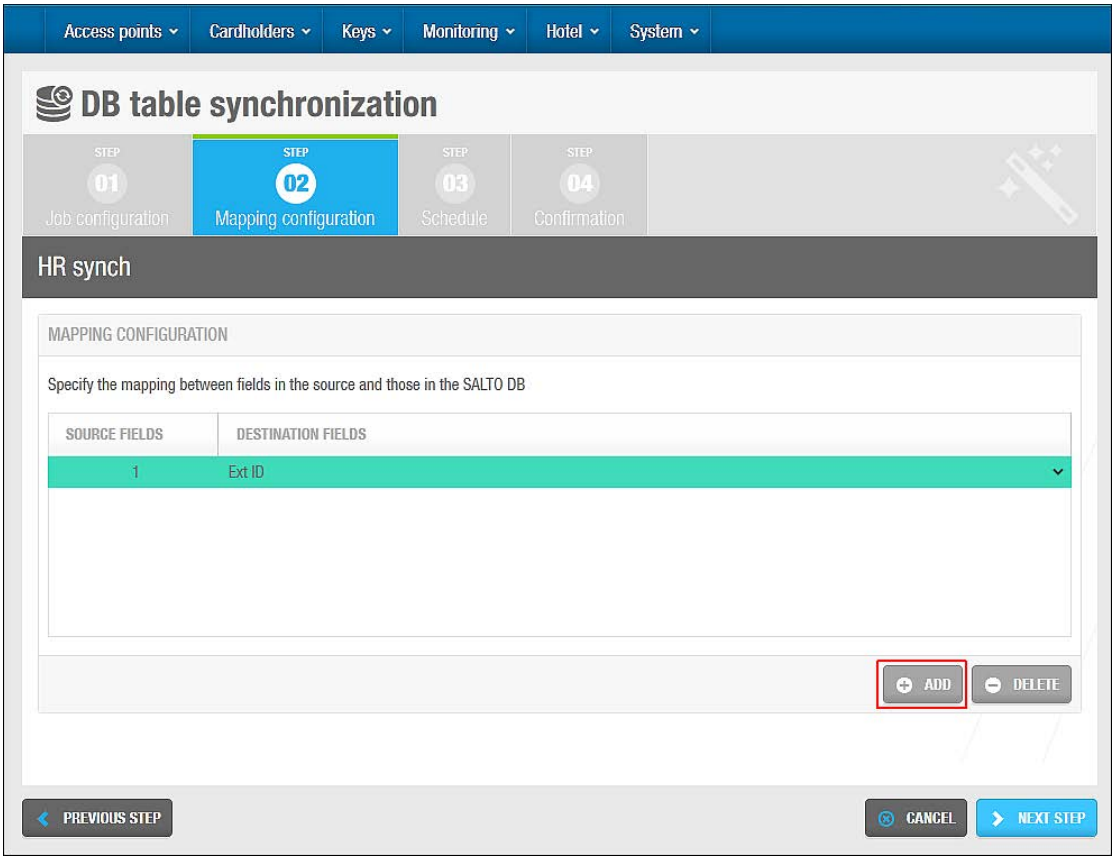


Figure 201: Select destination field

87. Repeat Steps 1, 2, and 3 until you have specified the mapping between all the appropriate source and destination fields and the order of the fields.

    You must select the following options as destination fields to proceed to the next step:

    - Ext ID
    - Control field (to be processed by SALTO)
    - Control field (processed date/time)
    - Control field (error code)
    - Control field (error message)

    The system uses these fields to write a report after database table synchronization occurs. If all of these options are not selected, the synchronization job cannot be performed.

88. Click **Next Step**. The **Schedule** screen is displayed.

14. 7. 3. 3. Step Three: Schedule

All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

14. 7. 3. 4. Step Four: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

14. 7. 4. Automatic Audit Trail Exports

You can export audit trail data from the SALTO database as a CSV file. This allows you to use the data in another system, for example, a time recording system.

NOTE: When you export audit trail data, you can still access the data in ProAccess SPACE as it is not removed. However, when you purge the audit trail, the data is permanently removed from the audit trail and the database. See *Automatic Audit Trail Purging* for more information.

See also the SaltoAutomaticExportOfAuditTrail document for more information about exporting audit trail data.

The sections below describe how to complete each step in this process.

14. 7. 4. 1. Step One: Job Configuration

To complete Step one:

89. Select **System** > **Scheduled jobs**. The **Scheduled jobs** screen is displayed.
90. Click **Add Scheduled Job**. The **Add scheduled job** dialog box is displayed.
91. Select **Audit trail export** from the drop-down list.
92. Click **OK**. The **Job Configuration** screen is displayed.

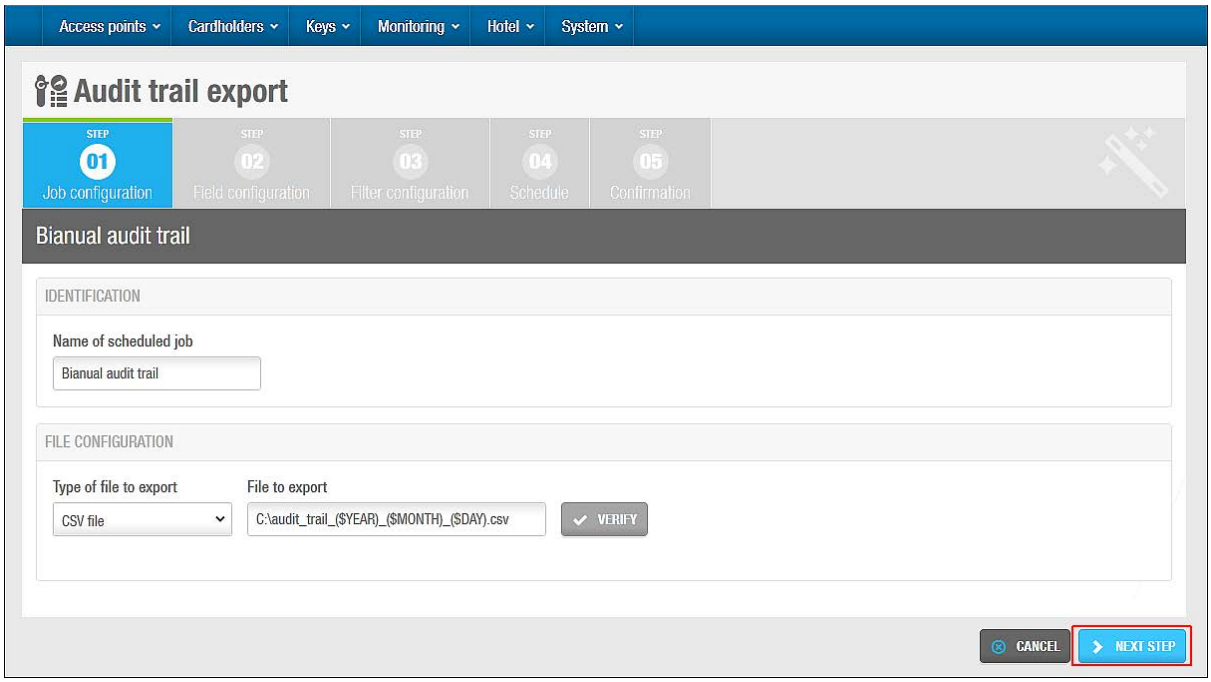


Figure 202: Job configuration screen

93. Type a name for the job in the **Name of scheduled job** field.

    The default option in the **Type of file to export** field is a CSV file. This option cannot be changed.
94. Type a name for the file that you want to export in the **File to export** field.
95. Press F2 to display the **File path** dialog box and insert macros in the file name if required.

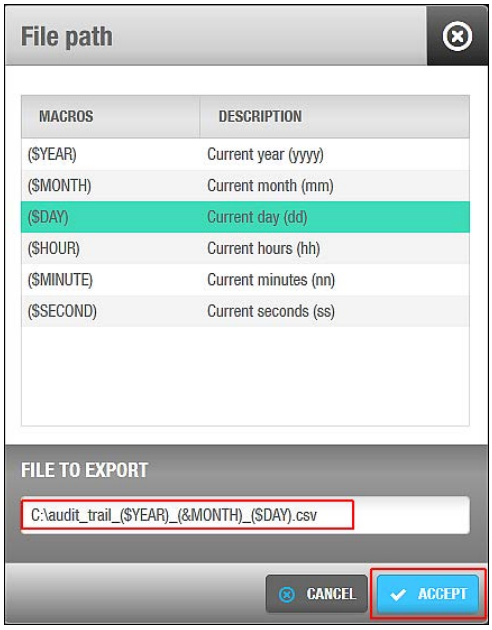


Figure 203: File path dialog box

Using macros, for example, ($YEAR), allows you to save the file with a unique name so it is not overwritten by the next file that is created.

96. Double-click the appropriate macro to insert it in the file name.

    Each macro you insert is displayed in the file name in the **File To Export** field.

97. Click **Accept** when you have finished inserting macros and the appropriate file name is displayed in the **File To Export** field.

    You can click **Verify** on the **Job configuration** screen to verify the file directory exists and is correct.

98. Click **Next Step**. The **Field configuration** screen is displayed.

14. 7. 4. 2. Step Two: Field Configuration

To complete Step two:

99. Select a format from the **File format** drop-down list on the **Field configuration** screen.

    This specifies the format of the file containing the exported audit trail data.

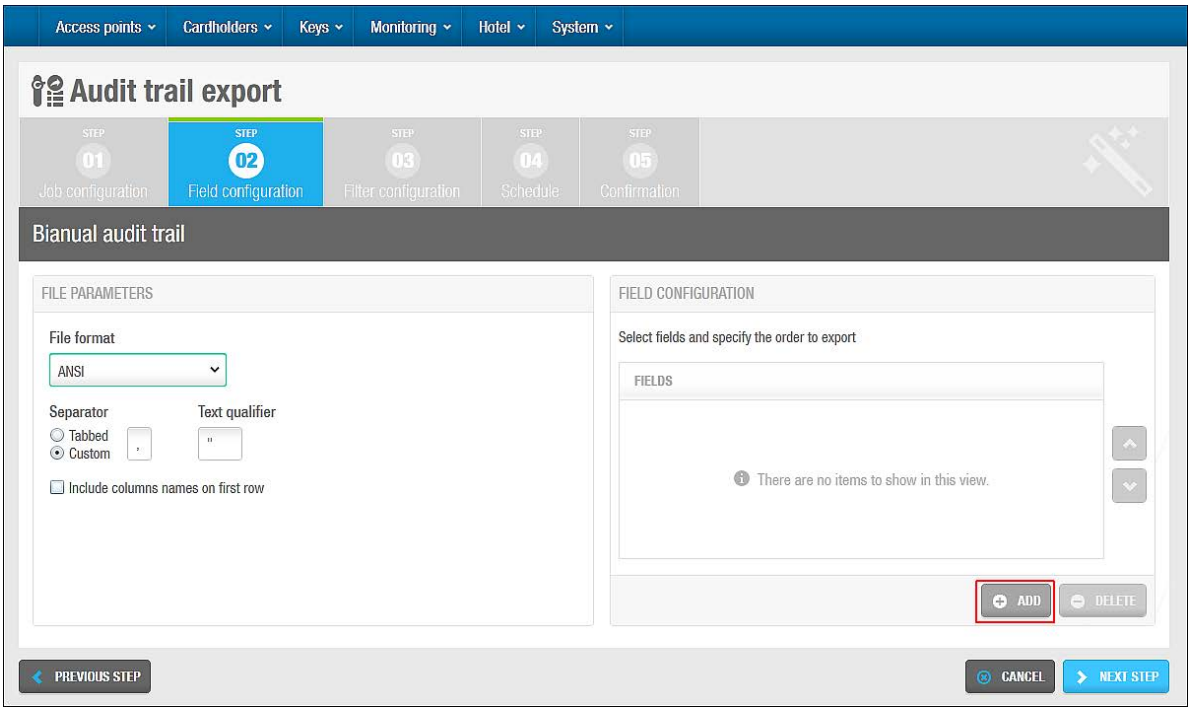


Figure 204: Field configuration screen

100. Select either the **Tabbed** or **Custom** option.

This specifies how the audit trail data is stored in the file. The **Separator** and **Text qualifier** fields are automatically populated but you can change the characters in these fields if required.

101. Select the **Include column names on first row** checkbox if required.

If you select this, the column names are included in the first row of the file.

102. Click **Add** in the **Field configuration** panel. The **Select fields** dialog box, showing a list of fields, is displayed.

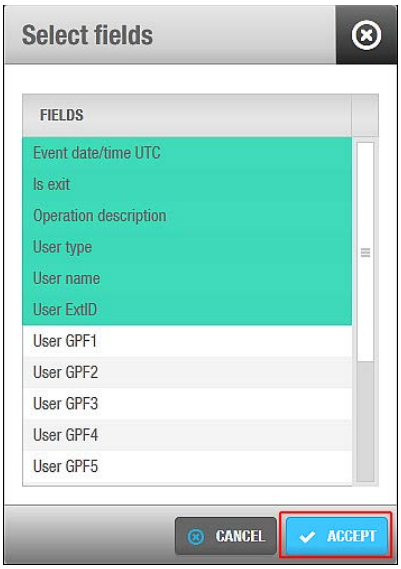


Figure 205: Select fields dialog box

See the *SaltoAutomaticExportOfAuditTrail* document for a description of these fields.

103. Select the required fields.

You can hold down the Ctrl key while clicking the fields to make multiple selections.

104. Click **Accept**. The selected fields are displayed in the **Fields** list on the **Field configuration** screen.

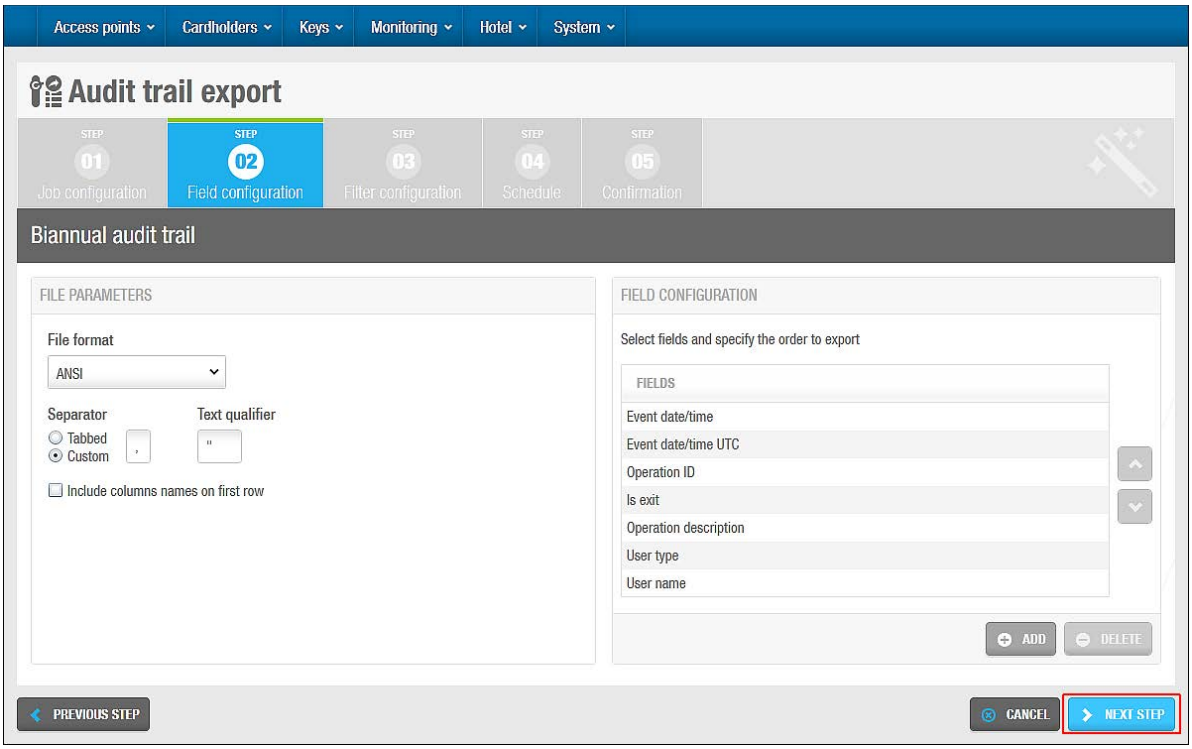


Figure 206: Select field

The order of the fields in the **Fields** list determines the order in which the fields are exported. You can select fields and click the up and down chevrons to change the order of the fields if required.

105. Click **Next Step**. The **Filter configuration** screen is displayed.

14. 7. 4. 3. Step Three: Filter Configuration

The filter configuration step allows you to filter the type of audit trail data that is exported within a specified time period. The default option is to export all of the audit trail data within the previous 12-month period.

You can filter audit trail events by the following:

- Cardholders and/or operators
- Access points
- Operations
- Date and time period

To complete Step three:

106. Click **Add/Delete** in the **Who** panel on the **Filter configuration** screen. The **Add/Delete** dialog box, which contains a list of cardholders and operators on two tabs, is displayed.

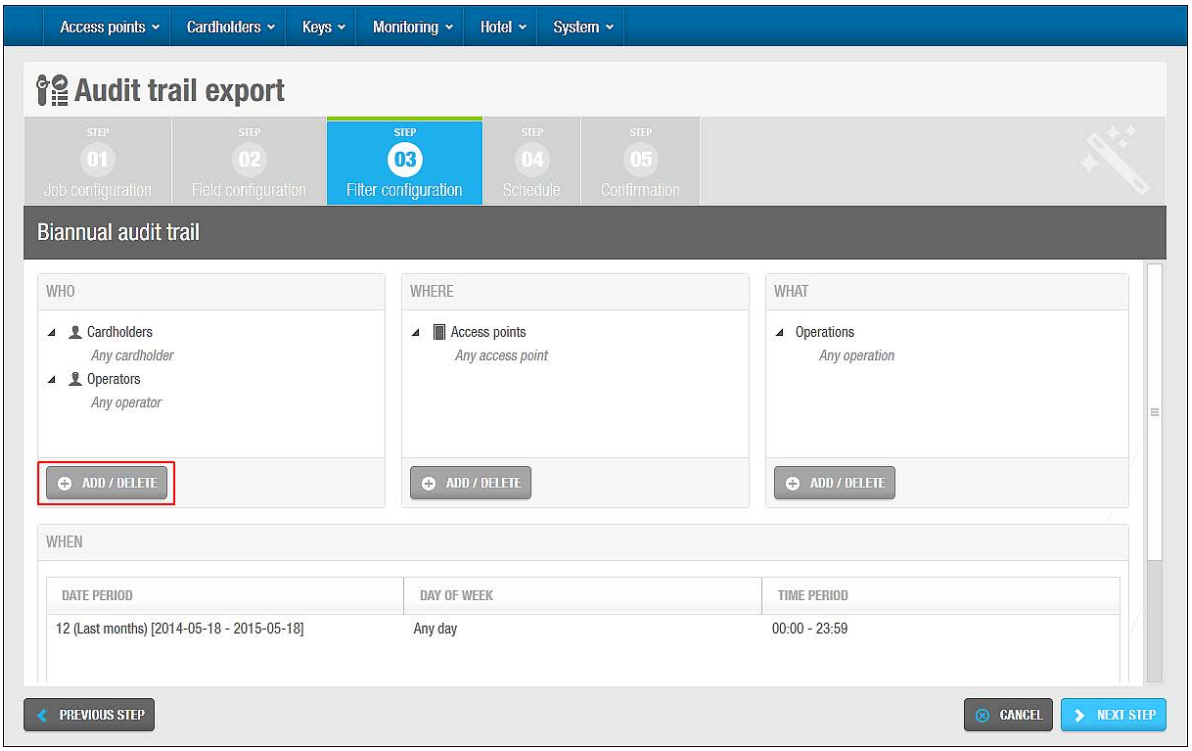


Figure 207: Filter configuration screen

107. Select the required cardholders in the left-hand panel and click the chevron. The selected cardholders are displayed in the right-hand panel.

    You can hold down the Ctrl key while clicking the fields to make multiple selections. As soon as you select a cardholder, the default **Any cardholder** option is automatically moved to the left-hand panel. You can use the default option if you want to export audit trail data for all the cardholders in the system.

108. Click the **Operators** tab if you also want to filter by operator. A list of operators is displayed.

109. Select the required operators in the left-hand panel and click the chevron. The selected operators are displayed in the right-hand panel.

110. Click **Accept**. The selected cardholders and operators are displayed in the **Who** panel.

111. Follow the procedure described in Steps 1, 2, and 5 to add the access points you want to filter to the **Where** panel.

112. Follow the procedure described in Steps 1, 2, and 5 to add the operations you want to filter to the **What** panel.

113. Click **Add/Delete** in the **When** panel. The **Add/delete periods** dialog box, showing the default period, is displayed.

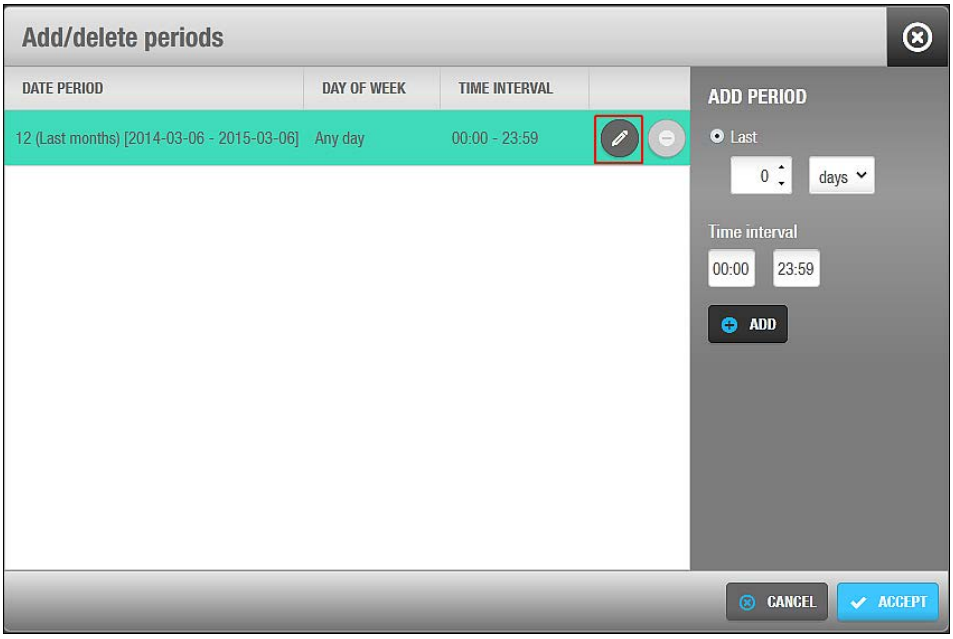


Figure 208: Add/delete periods dialog box

114. Click the **Edit** icon to change the date period and time interval if required.

    You can also click **Add** to add additional periods. For example, you can add a period to export the audit trail data between 09:00 and 11:00 each day within a specified date period, and add another period to export the audit trail data between 14:00 and 17:00 each day within the same date period.

115. Click **Accept** when you have finished editing or adding periods. The changes are displayed in the **When** panel.

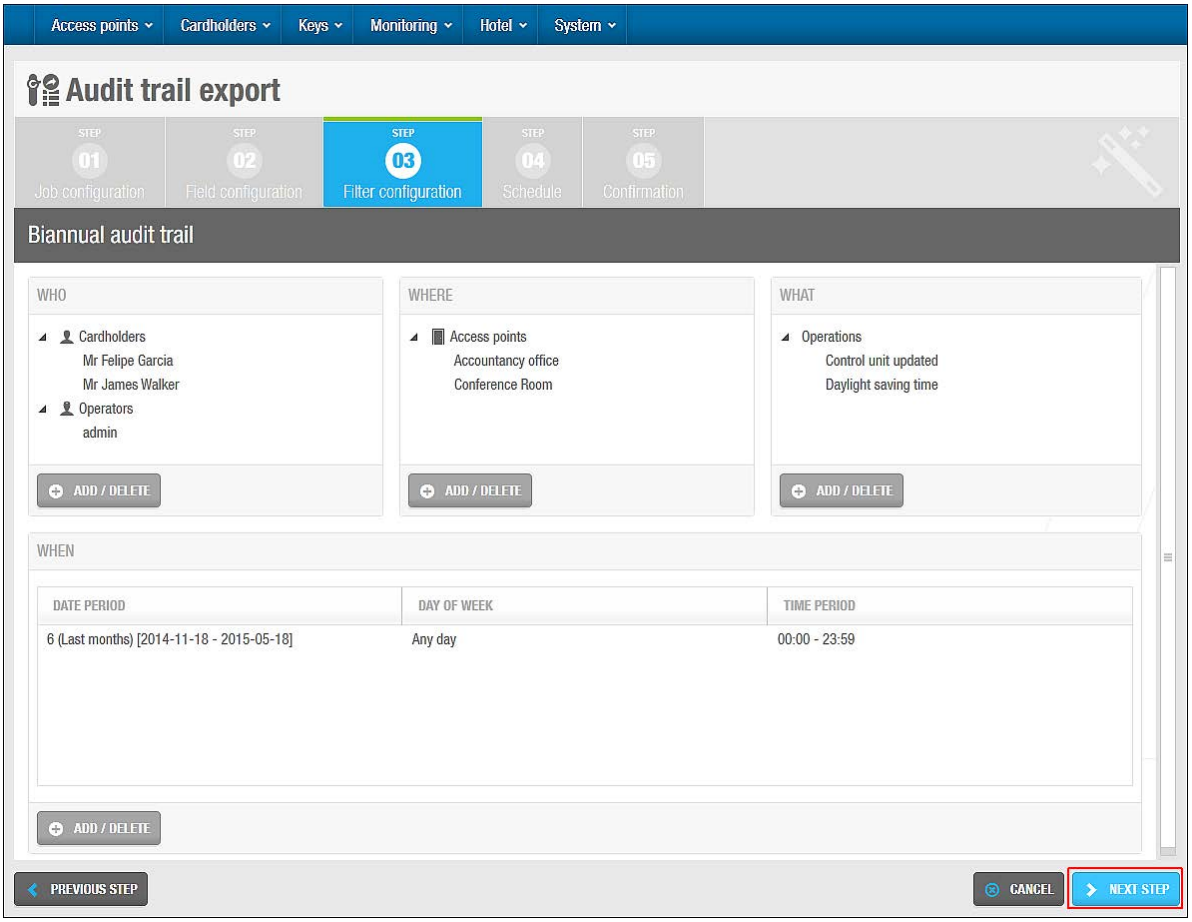


Figure 209: Edit period

116. Click **Next Step**. The **Schedule** screen is displayed.

14. 7. 4. 4. Step Four: Schedule

All the schedule steps for the jobs described in this chapter are performed in the same way. See *Step Two: Schedule* for more information and a description of the procedure you should follow.

14. 7. 4. 5. Step Five: Confirmation

All the confirmation steps for the jobs described in this chapter are performed in the same way. See *Step Three: Confirmation* for more information and a description of the procedure you should follow.

14. 8. Manual Synchronization

You can manually perform the following synchronization jobs on the system:

- CSV file synchronization
- Database table synchronization

You can start these jobs by selecting **System** > **Synchronization** and completing each step in the configuration process. Alternatively, you can schedule either of these jobs to be performed automatically on the **Scheduled jobs** screen. See *Automatic CSV File Synchronization* and *Automatic Database Table Synchronization* for a description of how to complete the required steps for each job.

NOTE: The scheduling steps in the sections referenced above are not relevant when you are manually performing CSV file synchronization or database table synchronization jobs.

14. 9. Making Database Backups

Database backups can be made from the SALTO system:

- Using ProAccess SPACE's **System** > **Make DB Backup** option

By default, system backups are stored in an SQL backup folder. For example:

C:\Program Files\Microsoft SQL Server\MSSQL12.SQLEXPRESS\MSSQL\Backup

Note that the SQL folder name may vary slightly depending on which SQL version is installed. It is recommended to create all SQL backups in this folder. The backup file is saved with a .bak extension.

NOTE: Automatic database backups are scheduled on the system by default. See *Automatic Database Backups* for more information.

To make a database backup in ProAccess SPACE, perform the following steps:

117. Select **System** > **Make DB Backup**. The **Make DB Backup** dialog box is displayed.

Figure 210: Make DB Backup dialog box

118. Type a file path based on the database server file system or backup file name.
119. Click **OK**. The database backup is performed. A pop-up is displayed confirming that the operation was completed successfully.
120. Click **OK**.

14. 9. 1. Restoring Database Backups

You cannot restore a backup while ProAccess SPACE is connected to an existing backup. The database backup can be restored using **Microsoft Management Studio** or the SALTO **DB Utils for RW-ProAccess Space** tool. For more info, please contact your SALTO technical support.

14. 10. Events Streams

The events stream functionality allows third parties to receive real-time notifications about events that occur (for example, a door opened by a particular cardholder) within the SALTO system. See the *Stream of events from the Salto software* document for more information.

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

An events stream conveys the following information about an event:

- Who produced it (for example, the cardholder)
- When it was produced (for example, the date/time)
- Where it was produced (for example, the location of the door)
- What type of event was produced (for example, the door was opened)

The aim of the events stream is to filter the audit trail. See *Audit Trails* for more information about audit trails. Sending selected events in the appropriate order to the system enables it to process the received information and perform real-time actions.

You must complete these steps within the wizard to create an events stream:

121. Configure the general settings.
122. Select the data fields.
123. Specify the parameters.
124. Confirm the configuration settings.

14. 10. 1. Step 1: Configuring the General Settings

The first step of creating an events stream is to provide general information such as the formatting and encoding of the events stream.

To provide the general information, perform the following steps:

125. Select **Tools** > **Events streams**. The **Events streams list** dialog box is displayed.
126. Click **New**. The **Events stream configuration** dialog box is displayed.

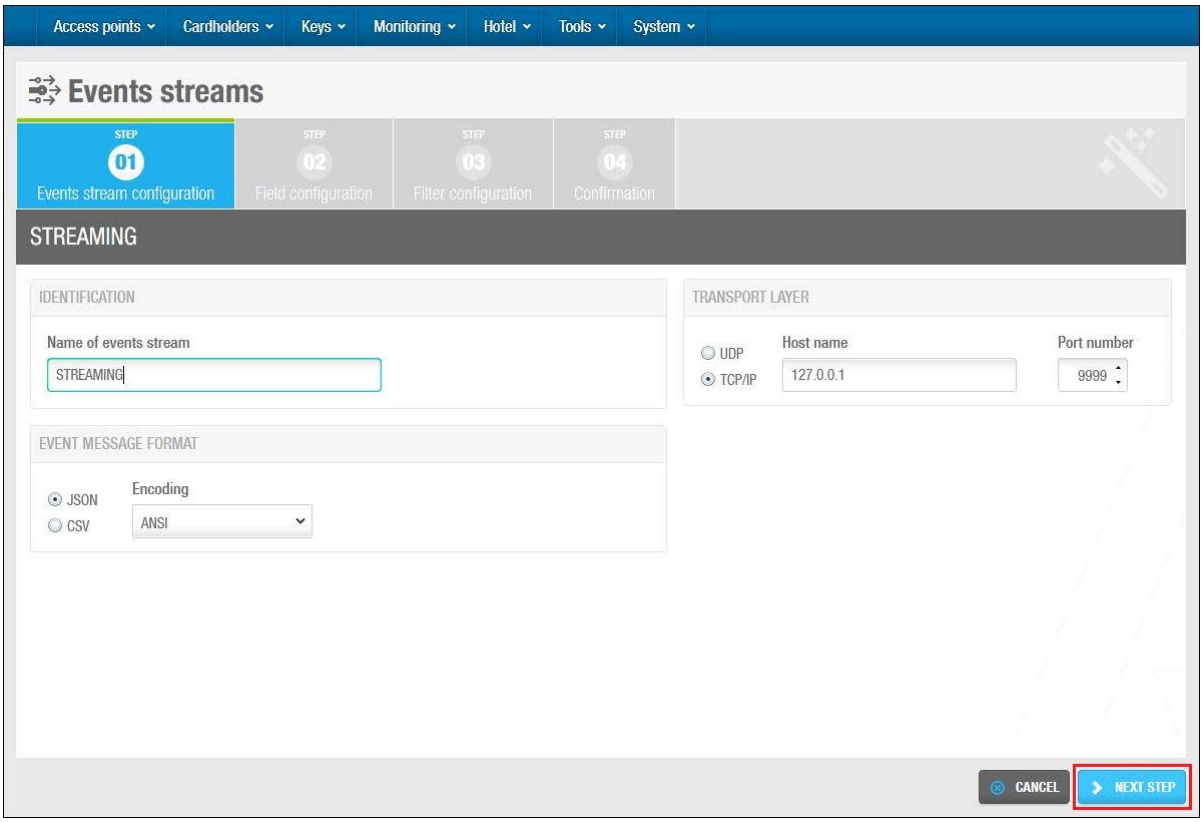


Figure 211: Events stream configuration dialog box

127. Click **Next**.
128. Type the events stream name in the **Name of events stream configuration** field.
129. Select either **UDP** or **TCP/IP** in the **Transport layer** panel.

Event streams can be received through UDP or TCP/IP protocols.

130. Type the machine name in the **Host name** field and the port number in the **Port number** field.

Event streams will be notified through the machine name and port number of the listening socket you specify.

131. Select either **JSON** or **CSV** in the **Event message format** panel.

JSON uses a string format. CSV uses a list format where a list of field values is separated by a semi-colon. See examples of each below.


```
[
{
"EventID" : "11223344556677889900",
"EventDateTime" : "2012-04-14T13:03:20",
SALTO HAMS……p.321
"EventTime" : "13:03:20",
"EventDateTimeUTC" : "2012-04-14T11:03:20Z",
"OperationID" : 17,
"OperationDescription": "Door opened: key",
"IsExit" : false,
"UserType" : 0,
"UserName" : "John Smith",
"UserGPF3" : "Marketing department",
"DoorName" : "Gym",
"DoorGPF1" : "Leisure area",
}
]
```


Figure 212: JSON format


```
EVENT_START "11223344556677889900"; 2012-04-14T13:03:20;
13:03:20; 2012-04-14T13:03:20z; 17; "Door opened: key"; false; 0;
"John Smith"; "Marketing department"; "Gym"; "Leisure area"
EVENT_END
```


Figure 213: CSV format

132. Select the applicable character encoding from the **Encoding** drop-down list.

You can select ANSI, UTF-8, Unicode, or Unicode Big Endian.

133. Click **Next**. The dialog box to select the data fields is displayed.

You can also click **Back** on any step to return to the previous dialog box.

14. 10. 2. Step 2: Selecting the Data Fields

After you provide the general information about the events stream, you need to select the data fields for the events stream.

To select the data, perform the following steps:

134. Click **Add/ Delete**. The **Select fields** dialog box is displayed.

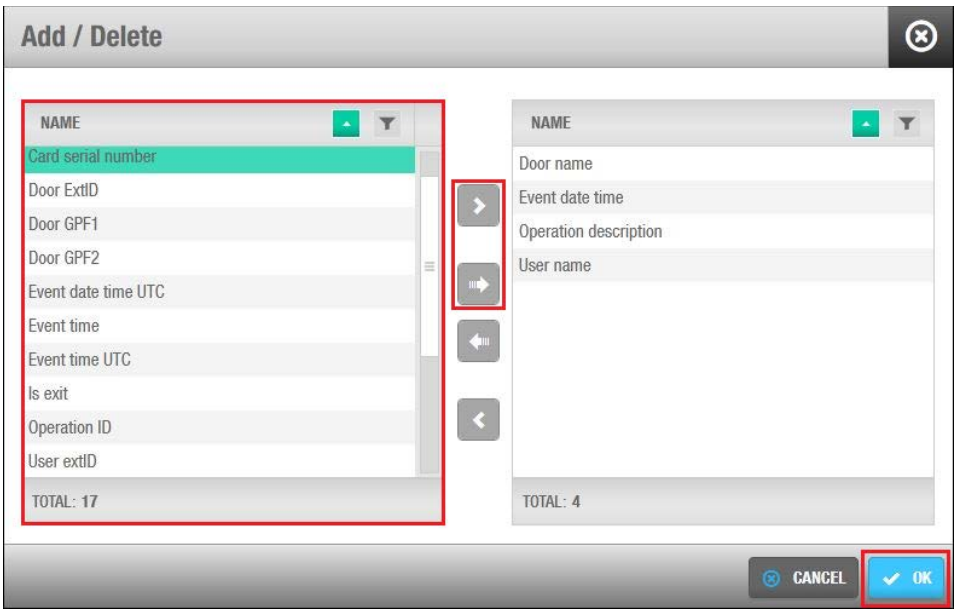


Figure 214: Select fields dialog box

135. Select the data fields that will be sent as part of the events stream.

The fields listed here match the information passed by keys to the SALTO SQL DB and to the third-party systems.

136. Click the chevron to transfer the selected fields to the right side of the dialog box.

137. Click **Ok**. The fields you selected are displayed. Note that if you want to have a specific order in the list, you must select them one at a time. When the fields are added to the list, you cannot change the order.

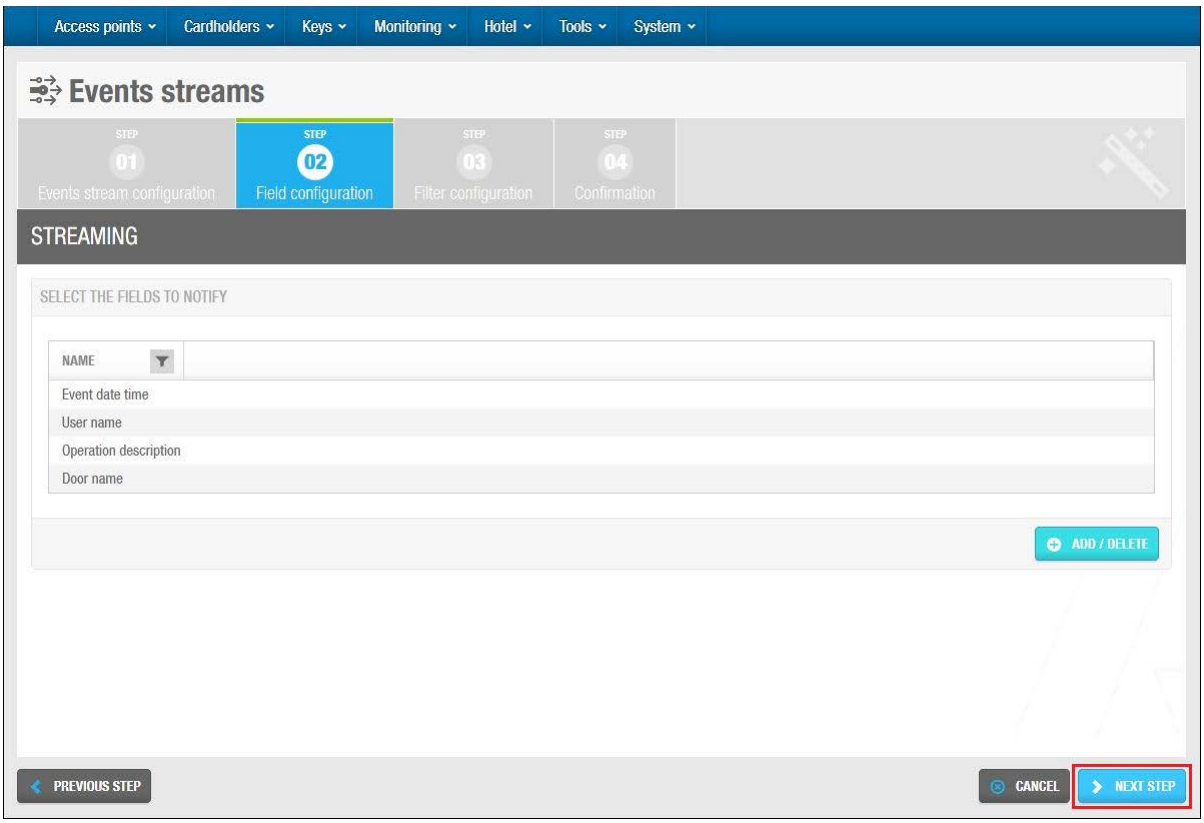


Figure 215: Selected fields displayed

138. Click **Delete** if you want to remove entries from this field.

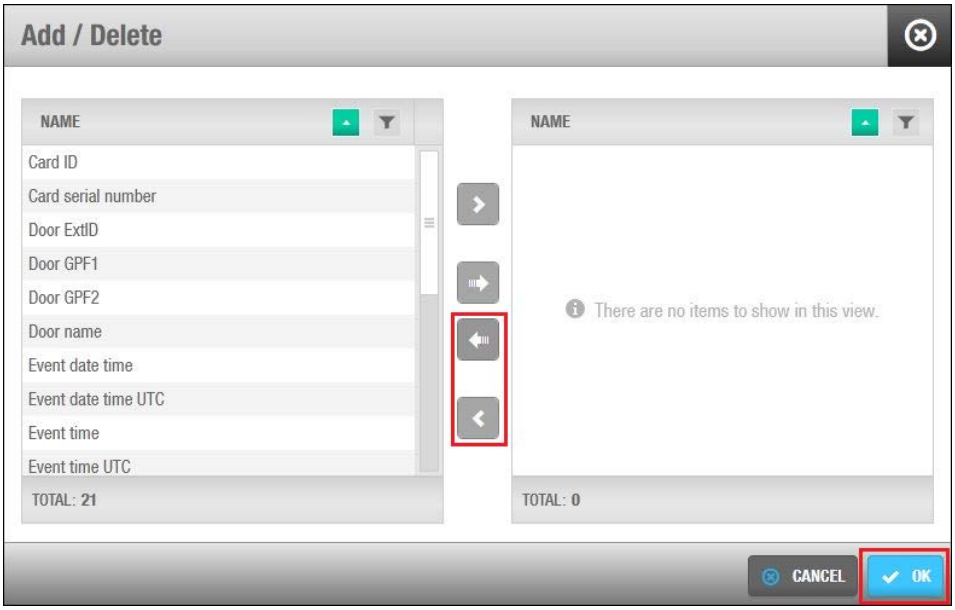


Figure 216: Deselecting fields displayed

139. Click **Next**. The **Who**, **Where**, **What**, and **When** panels and the **Real time window** fields are displayed.

14. 10. 3. Step 3: Specifying the Parameters

After you select the data fields for the events stream, you need to specify the parameters, for example, the location and type of event, for the events stream.

To specify the parameters, perform the following steps:

140. Select **Users** in the **Who** panel.

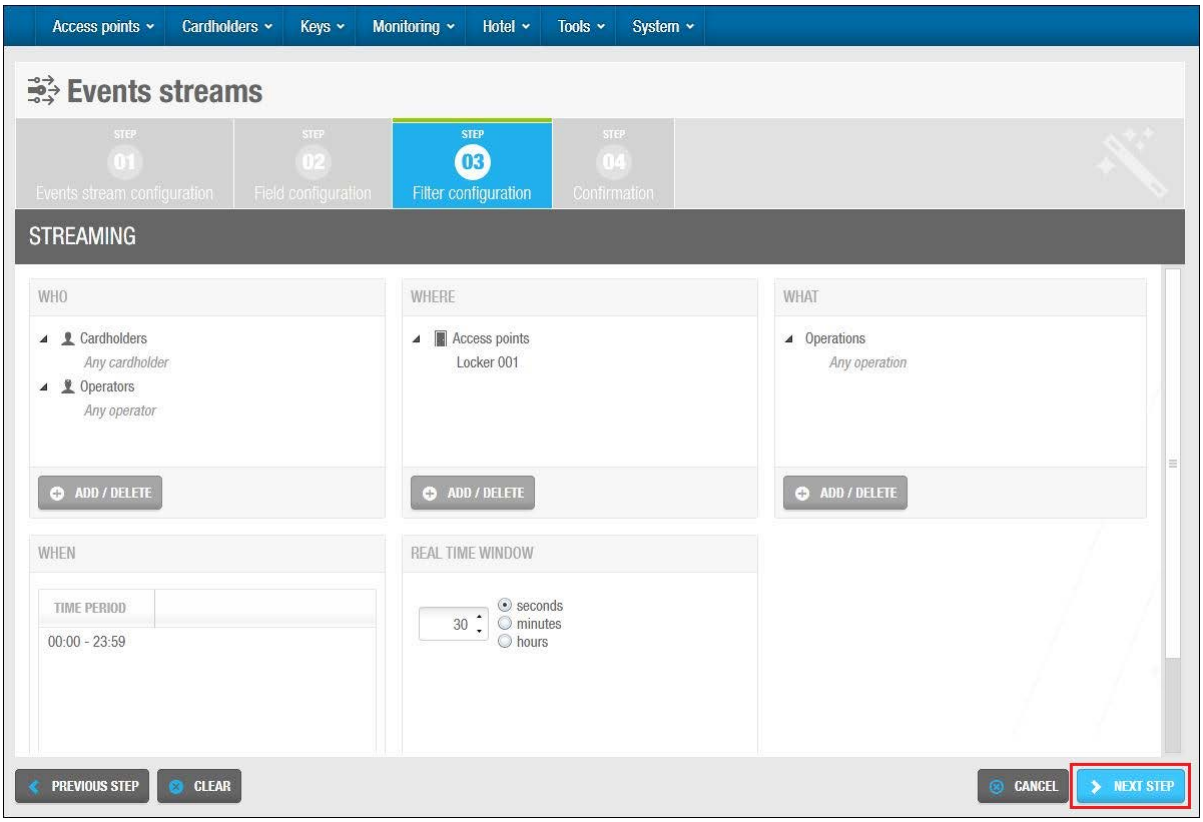


Figure 217: Panels and the Real time window

141. Click the **Add/remove items** button below the **Who** panel. The **Who** dialog box, showing a list of cardholders, is displayed.

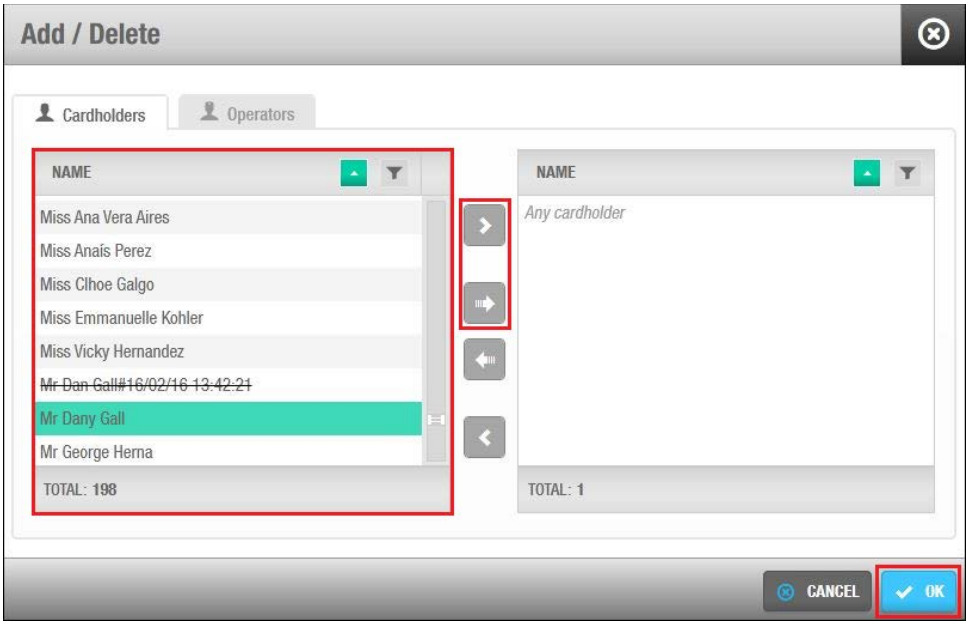


Figure 218: Who dialog box

142. Select the required user in the **Non-selected items** panel and click the arrow. The selected user is displayed in the **Selected items** panel.

By default, **Any cardholder** is displayed in the **Selected items** panel. This means that all users are included in the events stream. To remove this value, select **Any cardholder**

in the **Selected items** panel and click the inverted arrow. **Any cardholder** is displayed in the **Non-selected items** panel. You must repeat these steps if you want to remove **Any operator** from **Operators**, **Any door** from **Doors**, and **Any operation** from **Operations**, as applicable.

143. Click **Ok**.
144. Click the **Operators** tab.
145. Repeat the above steps for operators.
146. Click **Ok**.

The selected users and operators are displayed in the **Who** panel.

147. Repeat the above steps to select the required doors in the **Where** panel.
148. Repeat the above steps to select the required operations in the **What** panel.
149. Click **Add** below the **When** panel. The **Select period** dialog box is displayed.

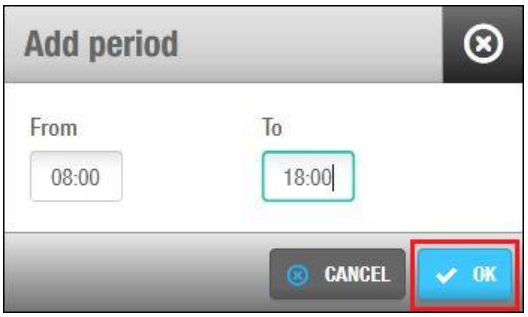


Figure 219: Select period dialog box

150. Select the applicable time interval using the arrows in the **From** and **To** fields.

This specifies the active period for the events stream. In the above example, the system only sends events during the period 08:00 to 18:00.

151. Click **Ok**. The selected time interval is displayed in the **When** panel.
152. Specify the frequency of events stream notifications by typing the applicable number in the **Real time window** field and selecting either **seconds**, **minutes**, or **hours**, as applicable.

For example, if you specify 30 seconds, the system only sends events created 30 seconds ago or less.

14. 10. 4. Confirming the Configuration Settings

After you specify the parameters for the events stream, you need to confirm the configuration settings.

To do this, perform the following steps:

153. Click **Next**. The events stream configuration settings are displayed.

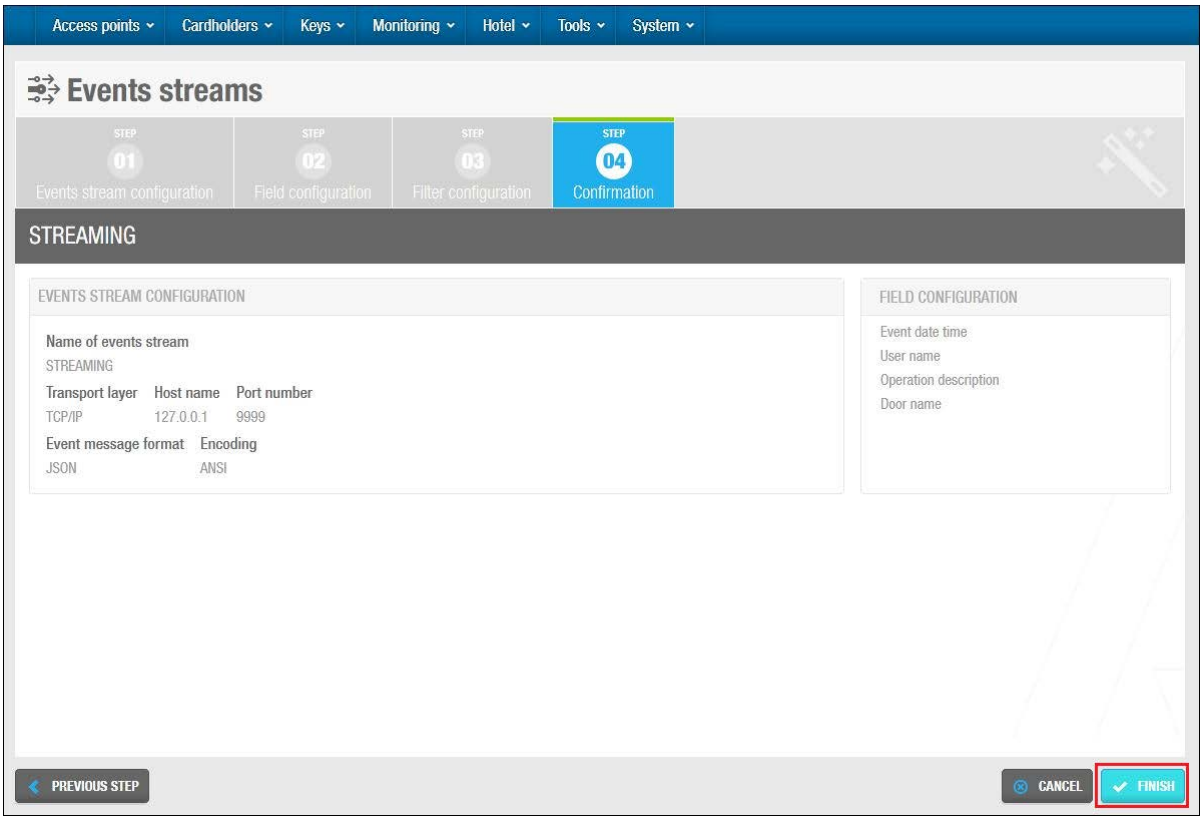


Figure 220: Select period dialog box

154. Click **Finish**. A message is displayed confirming that the changes will not take effect until you restart the SALTO Service.

The events stream you created is displayed in the **Events streams list** dialog box.

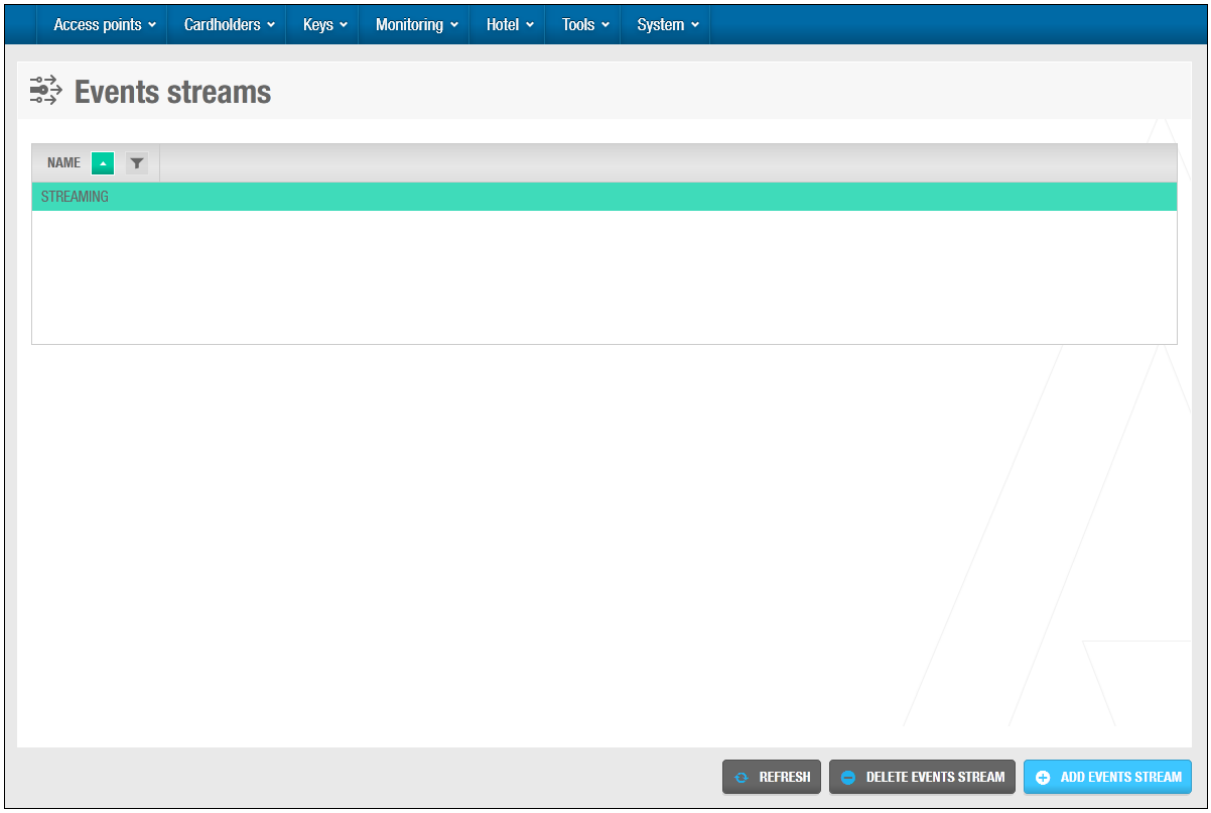


Figure 221: Created event stream

155. Click **Close**.

14. 11. Card printing

You can create badge templates within ProAccess SPACE and print these templates as user cards (keys). You can create card templates for different users in your organization. For example, you can create one template for day staff and a different template for night staff.

To create a badge template, perform the following steps:

156. Select **Tools** > **Card template list**. The **Card template list** screen is displayed.

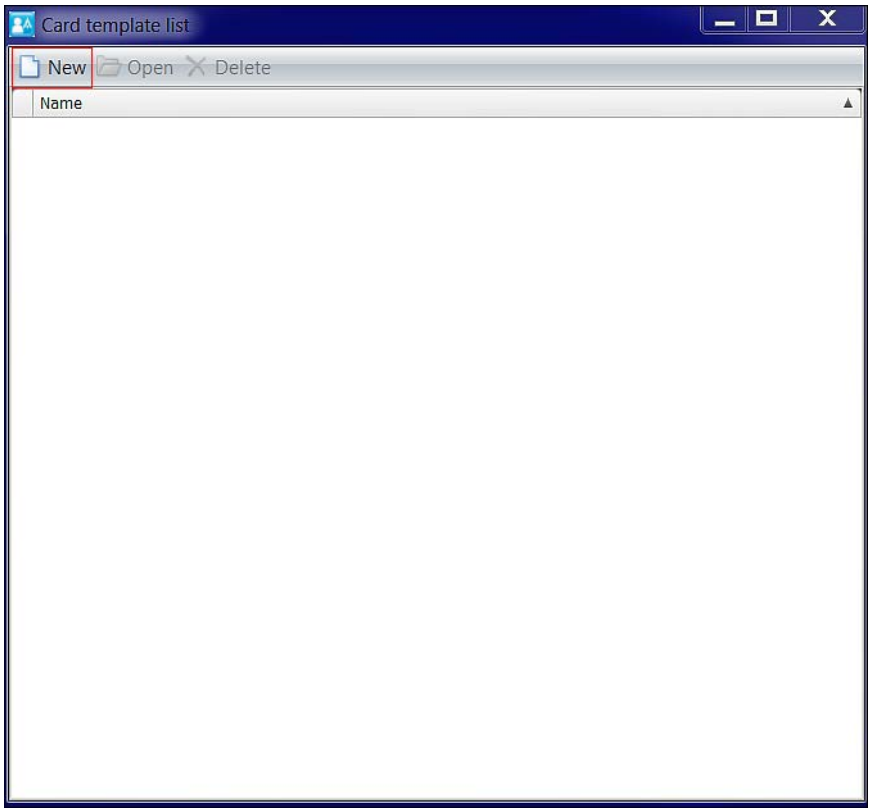


Figure 222: Card template list screen

157. Click **New**. The **New** dialog box is displayed.

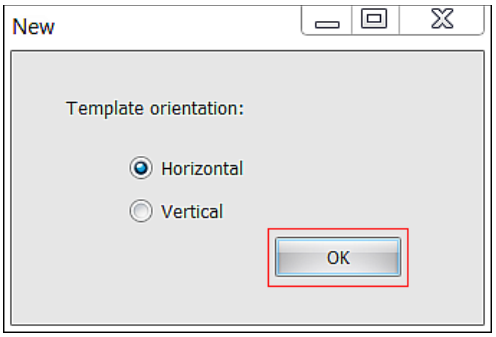


Figure 223: New dialog box

158. Select either **Horizontal** or **Vertical** as your template orientation and click **OK**. The **Card template design** screen is displayed.

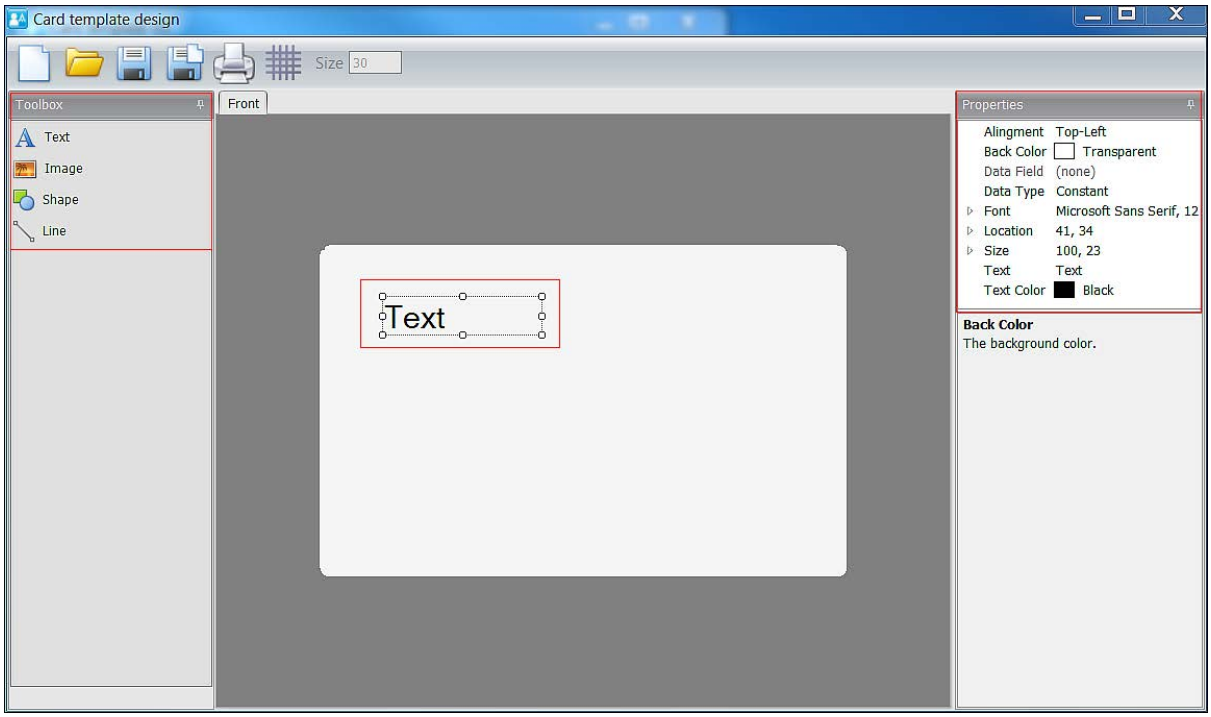


Figure 224: Card template design screen

The **Toolbox** section within the **Card template design** screen is comprised of four features:

- Text
- Image
- Shape
- Line

After you select any of the **Toolbox** features, you can customize it on the blank template in the centre of the screen. When you select the feature on the template, a **Properties** menu, specific to the feature, is displayed in the top right of the screen.

The four **Toolbox** feature menus are described in the following sections.

14. 11. 1. Text

The **Text** menu allows you to customize the text used in the template.

The options are described in the following table.

Table 41: Text menu options

Option	Description
Alignment	Arrangement of the text on the template, for example, **Top-Center**
Back Color	Background colour for the template
Data Field	Text field to include in the template, for example, **Title**, **First Name**, **User ID**, or **Passport**. This field is only enabled when **Dynamic** is selected for **Data Type**.
Data Type	Allows the text to be defined as **Constant** (static text) or **Dynamic** (variable text). If you want the fields in the printed card template to be automatically completed with user data, select **Dynamic**. When **Dynamic** is selected, the **Data Field** is activated.
Font	Text font on the template

Option	Description
Location	Location of the text on the template. You can specify the X and Y coordinates.
Size	Height and width of the text
Text	Text that appears on the template
Text Color	Colour of the text on the template

14. 11. 2. Image

The **Image** menu allows you to customize images imported into the template.

The options are described in the following table.

Table 42: Image menu options

Option	Description
Back Color	Background colour for the image
Data Field	Allows the selection of an image from the specific **User** information screen (in ProAccess SPACE). This field is only enabled when **Dynamic** is selected for **Data Type**.
Data Type	Allows the image to be defined as **Constant** (static image) or **Dynamic** (variable image). When **Dynamic** is selected, the **Data Field** is activated.
Image	Image for the template. Click the ellipsis icon to browse for an image to import.
Image Mode	Arrangement of the image on the template, for example, **Scaled**
Location	Location of the image on the template. You can specify the X and Y coordinates.
Size	Size of the image on the template. You can specify the height and width.

After you create a badge template, you can associate it with an individual user in ProAccess SPACE. See *Card Printing Templates* for more information.

14. 11. 3. Shape

The **Shape** menu allows you to customize shapes on the template.

The options are described in the following table.

Table 43: Shape menu options

Option	Description
Back Color	Background colour for the shape
Line Color	Line colour for the shape
Line Width	Line width of the shape
Location	Location of the shape on the template. You can specify the X and Y coordinates.
Size	Size of the shape on the template. You can specify the height and width.
Type	Shape can be a rectangle or an ellipse

14. 11. 4. Line

The **Line** menu allows you to customize lines on the template.

The options are described in the following table.

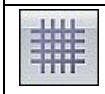
Table 44: Line menu options

Option	Description
Back Color	Background colour of the line
Direction	Direction of the line
Line Color	Colour of the line
Line Width	Width of the line
Location	Location of the line on the template. You can specify the X and Y coordinates.
Size	Size of the line on the template. You can specify the height and width.

14. 11. 5. Design Icons

There are six design icons on the top left of the **Card template design** screen. These icons are described in the following table.

Table 45: Design icons

Icon	Description
 New	Allows you to create a new card template
 Open	Allows you to select any templates you previously created
 Save	Allows you to save a card template
 Save As	Allows to you save card templates with different names, for example, in case you need to use the current design as a basis for another template design
 Print	Allows you to print your template
 Grid	Allows you to use a grid reference to place design elements accurately

14. 11. 6. Back Design

You can design the front and back of a card template.

To add information for the back of the card template, perform the following steps:

159. Right-click the **Front** tab. The **Add back side** option is displayed.

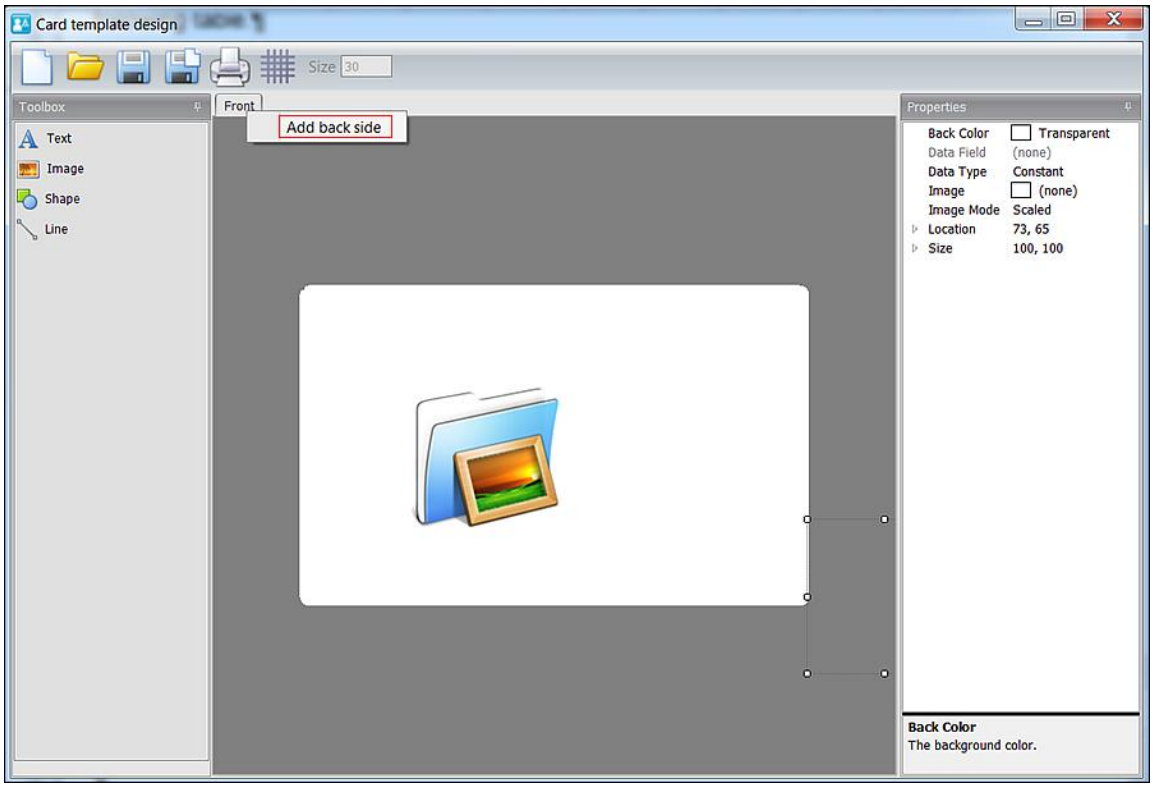


Figure 225: Add back side option

160. Click **Add back side**. A new **Back** tab is displayed.

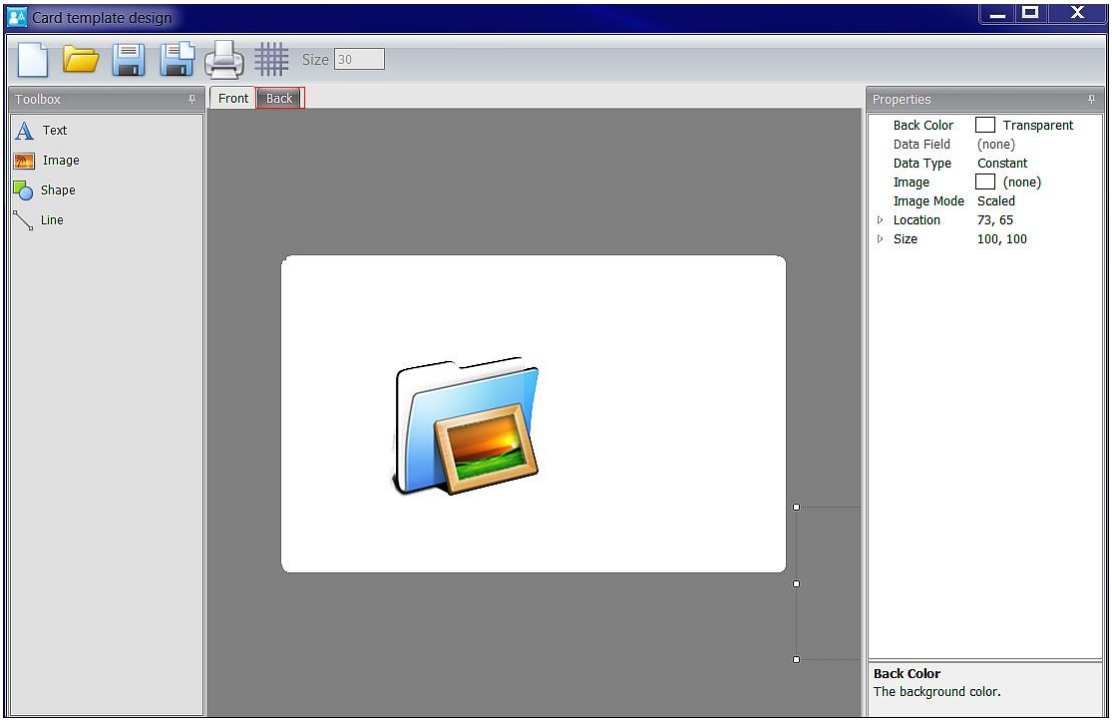


Figure 226: New Back tab

161. Click the **Back** tab to design the back of the card template.

14. 12. Using Card Printing Templates

After you create your badge templates, you can print these as user cards (keys) in ProAccess SPACE. The card printing functionality is license-dependent. See *Registering and Licensing SALTO Software* for more information.

NOTE: To print card templates, the template must contain dynamic fields with a specific data field in the user list.

To print card templates perform the following steps:

162. Select **Cardholders** > **Users**. Select the user associated with the card template to print. The **Print** button is visible in **Card Printing Template**.

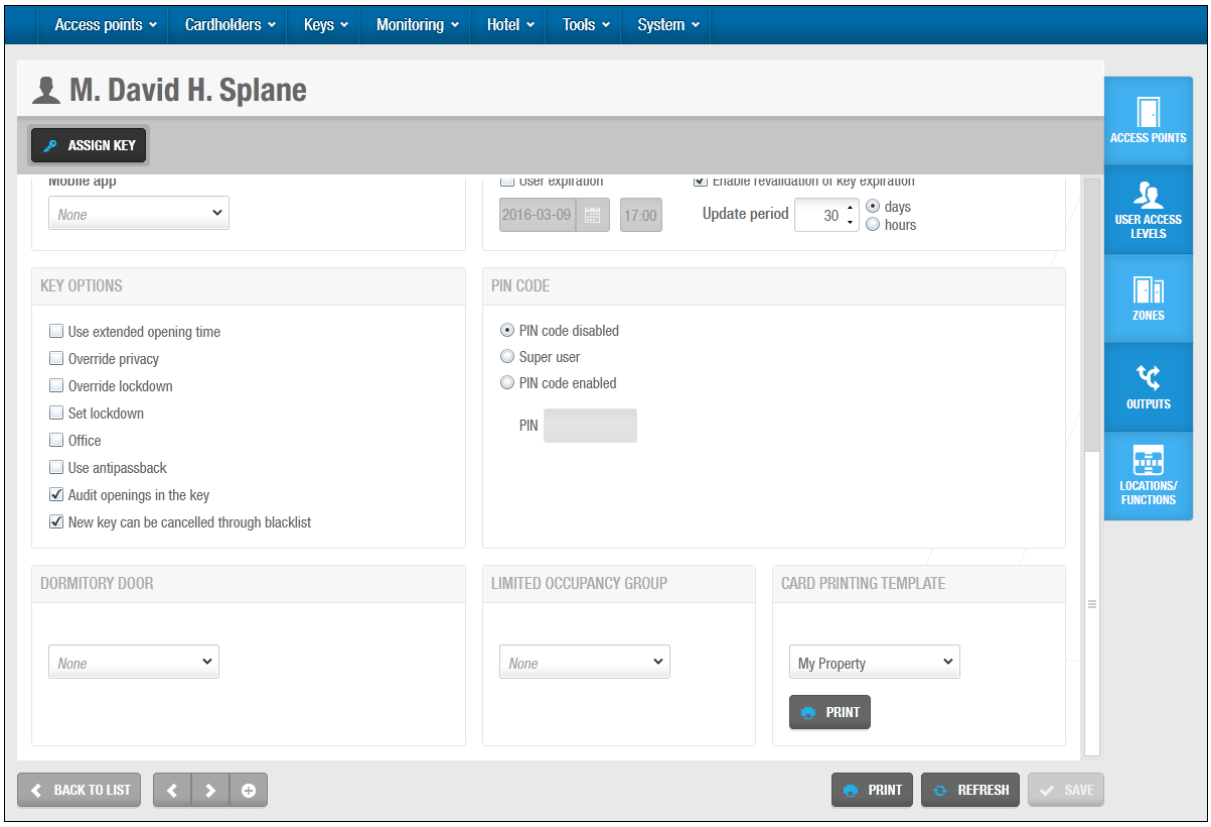


Figure 227: Print users cards screen

163. Click **Print**. The **Card Preview** screen is displayed.
164. Select the **Print** icon on the top left-hand side of the screen. The templates are then printed.

PROACCESS SPACE SYSTEM CONFIGURATION for more information. These devices can be monitored by using **Online Monitoring** in ProAccess SPACE Monitoring and updated by using SALTO Network in ProAccess SPACE System.

This chapter describes the different types of peripherals available and the tasks associated with them.

14. 12. 1. Peripheral Types

The functionality of each peripheral type is described in the following table.

Table 82: Peripheral types

Peripheral	Functionality
Encoder	Connects to the system either by a USB or serial connection, or by an Ethernet connection. The Local IO Bridge allows USB encoders to be used with ProAccess SPACE. See *Local IO Bridge* for more information. Encoders are used to: ▪ Read the information encoded on a key (user name, issuing date, expiry date, available memory, etc.) ▪ Allow the issuing and encoding of a key, assign access to a user, and edit the user card with up-to-date access data ▪ Delete all the information stored on a key, allowing the key to be reused ▪ Allow the updating of a key with new data and permissions
ESD	Reduces energy consumption by controlling the activation of electrical equipment in a room or an area. ESDs are used to: ▪ Activate electrical equipment in a room (lights, sockets, etc.) ▪ Indicate real-time presence of guests or staff in a room (online ESDs) in a hotel site. You can view whether or not a room is currently occupied by selecting **Hotel** > **Room status** and clicking **Show ESD**.

14. 13. Encoders

Encoders are used to read keys, and encode keys with access permission data. They are connected to the system either by a USB or serial connection, or by an Ethernet connection. You can add Ethernet encoders to the system by using the **SALTO Network** screen. See *Adding Ethernet Encoders* for more information.

You must specify how encoders connect to the system on the **Settings** screen in ProAccess SPACE. See *Encoder Settings* for more information. Note that you must address Ethernet encoders by using the **SALTO Network** screen in ProAccess SPACE before you select them on the **Settings** screen in ProAccess SPACE. See *SALTO Network* for more information.

14. 13. 1. Updating Encoder Firmware

You can update the firmware of an encoder that is plugged into your local PC using either a USB, Ethernet or serial connection in ProAccess SPACE. See *Updating Firmware* for more information.

Firmware updates are available when a new version of the SALTO software is downloaded. Your SALTO technical support contact may also recommend specific firmware updates if required.

NOTE: This software option can be used with EH, E7000, E8000 (Legic), and E9000 technology.

To update the firmware of an encoder, perform the following steps:

1. Click **admin** (or other appropriate operator login) on the top right-hand side of the home screen. The **Settings** screen is displayed.
2. Click **Show Firmware** in the **Encoder Settings** panel. The **Show firmware** dialog box, showing the available firmware files, is displayed.

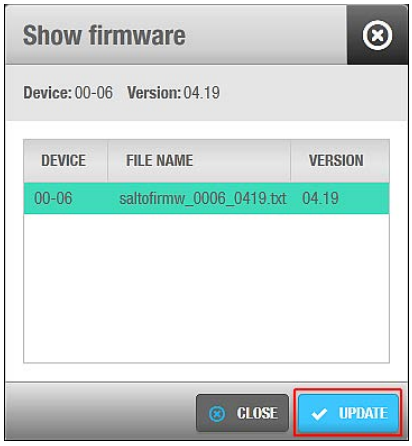


Figure 310: Show firmware dialog box

   The **Show Firmware** button is located on the right-hand side of the **Local** option. See *Encoder Settings* for more information about encoder settings.
3. Select the required file.
4. Click **Update**. The **Update encoder** progress screen is displayed.
5. Wait for the update to complete. A pop-up is displayed confirming that the operation was completed successfully.
6. Click **OK**.

14. 14. ESDs

ESDs are used to control the activation of electrical equipment in a room or area. They can be used in both hotel and non-hotel sites. However, the process for enabling and setting up ESDs on the system is different for both. The procedures for giving hotel guests and users access to ESDs also vary. See *Associated Device Lists*, *Checking ESD Status*, and *Configuring Associated Devices* for more information about using ESDs in hotel sites. See *Energy Saving Devices* for more information about using ESDs in non-hotel sites.

15. GLOSSARY

The following terms and acronyms are used throughout this manual.

Table 83: Glossary of terms

Term	Definition
Access level	A defined group of users with the same access permissions, for example, all staff in a department or all managerial staff
Access point	Any point in a site that has controlled access, for example, doors or lockers
Access point timed period	Defines the time interval in which an access point operates in a specified working mode, for example, Timed office mode or Automatic opening mode
Admin interface	A superset of menu options and screens within ProAccess SPACE. This refers specifically to the various options and quick-access tiles that are displayed to an operator with admin rights.
AID	Application Identifier
AMK	Application Master Key
AMOK lock	A type of lock that allows you to perform manual lockdowns for offline doors. These are commonly used in university sites, for example.
Antipassback	A security mechanism that prevents a person from using a key to enter an area a second time without first exiting (so that the card cannot be passed back to a second person who wants to enter)
Audit trail	A chronological list of access point events
Authorization list	A list of authorization numbers for zones, outputs, and associated devices in a hotel for which guest access is optional. You must create an authorization list if you are using PMS software with the SALTO software.
BAS	Building Automation System
Blacklist	A record of all cancelled keys. Once a key has been cancelled, the information is communicated from the system to the SVN wall readers. As users update their keys and present their keys to the lock, the new blacklist information is circulated to all access points.
BLE	Bluetooth Low Energy. Used in SALTO BLE readers to read data from JustIN Mobile application.
Calendar	Defines the workdays, holidays, and other special days for an organization
Cardholder	A generic term that covers all persons issued with a key. There can be various types of cardholders, for example, users, who are generally the staff of an organization.
Cardholder timetables	Define the time periods during which a cardholder's key is valid and can be used with a site's access points
Carrier	A generic term used to refer to any type of SALTO key
Connection type	Specified when adding a door or room to the system. There are five different connection types (online and offline) for doors in the SALTO system.
CU	Control unit - used to control access where a stand-alone lock cannot be fitted, for example, barriers
CU4200	A specific SALTO control unit model

Term	Definition
CU5000	A specific SALTO control unit model
Data-on-card	A term used to describe the saving of access permissions to a key (card) rather than a lock. Changes to a user's access permissions are retrieved from the SALTO system and written to a key through the SVN.
DHCP	Dynamic Host Configuration Protocol
Door	A door within the SALTO system that has controlled access. Doors can be either online or offline.
DST	Daylight Saving Time
Encoder	A peripheral that reads and updates keys with access information. Encoders can be enabled for USB or Ethernet.
ESD	Energy Saving Device – a peripheral mounted on the wall at an access point. It is used to activate the electrical devices in a room or area. The electrical devices only work if a valid SALTO key is inserted into the ESD. These are commonly used in hotels but can also be used in non-hotel sites.
Free assignment zone	An area where users are free to choose any locker. They do not have pre-assigned individual lockers.
Function	A category of permissions within a SALTO location that can be associated with users, for example, a maintenance function for electricians
Guest	A person who is given a key to allow access for the duration of their stay at a hotel
Guest profile	A system entry for guests that is automatically generated when a room or suite is created
Hotel interface	A subset of the overall ProAccess SPACE interface. It contains menu options, quick-access tiles, and screens specific to hotel sites. These options are related to guest activities such as check-in and check-out, and cancellation of guest keys.
Key	A carrier that controls access to an area, building, and/or site asset (for example, a cupboard or locker). Keys come in a wide variety of formats, including, bracelets, fobs, and keycards.
Limited occupancy	Defines specific limited access areas. For example, if a parking area contains 20 spaces, the system counts how many valid users have accessed the area. When 20 users have occupied a space, the next user will be denied access, even if they have a valid key.
Local IO Bridge	A Windows service that allows USB devices (like encoders or PPDs) to be used with ProAccess SPACE
Location	A large area of designated access points in the SALTO system, for example, all of the access points in the headquarters or regional offices of an organization
Lock	An electronic locking device. The lock can be mechanical, electrical, or magnetic. Data can be transferred to the lock by a key or a PPD.
Lockdown area	A defined area where all access points can be closed or opened in an emergency situation
Locker	A generic term used to describe lockers, cupboards, display cabinets, boxes, or cases fitted with an electronic device that controls the lock
MAC address	Media access control address
MAD	Mifare Application Directory
NFC	Near Field Communication

Term	Definition
Opening mode	Defines the working mode of a door, for example, Standard or Office opening mode
Opening time	Defines how long a door stays open after it is unlocked
Operator	A person who uses the ProAccess SPACE applications to control access within their site. The system has one default operator: admin. Different operators access different features, for example, when an admin operator logs in to ProAccess SPACE, they have full access to all of the menus and functionality. However, other types of operators, such as hotel front-desk staff, can have access only to a subset of menus and functionality, depending on the permissions set by the admin operator.
OTA	Over the Air
Output	A type of electrical permission or authorization used to activate relays for CUs or ESDs
Partition	Items within the system that are grouped together for ease of management. Partitions allow admin operators to separate a SALTO network into different 'parts' that are then individually managed by other operators.
Peripheral	An external hardware device such as an encoder or PPD that is used to perform routine system management tasks. This term can also refer to a device such as an ESD which is mounted on a wall and used to activate the electrical devices in a room or an area.
PMS	Property Management System
PPD	Portable Programming Device – a portable electronic device that can be physically connected to a lock. This device communicates information such as door identification and configuration details to the lock. It is used to initialize locks and update offline doors, as well as other maintenance tasks.
Re-rooming	Defines scenarios where the hotel operator assigns a different room to a guest. In the SALTO system, the guest does not have to go to the front desk to do this. The new information can be conveyed to the doors in two ways: ▪ **Manual**: The guest updates their key on an SVN wall reader. ▪ **Online**: The updated data is sent automatically to the new room door.
RF doors	Online doors within the SALTO network that are updated using radio frequency technology
RFID	Radio-frequency identification
Roll-call area	A list of how many and which users are in a specified area at a particular time
Room	A room assigned to one or more guests in a hotel site
ProAccess SPACE Configurator	A desktop application that is used to set up communication between the various components of the SALTO system. It is also used to start and stop the SALTO Service.
SALTO reader	A device that can read keys, for example, a wall reader or an encoder
SAM	SALTO Authorization Media
Scheduled job	A system task such as an audit trail purge that is set up to be performed automatically
SHIP	SALTO Host Interface Protocol
Suite	A series of rooms containing one or more rooms with individual entrance doors from the outside and a connecting door between

Term	Definition
SVN	SALTO Virtual Network – a technology that enables keys to be updated with the most current access data and permissions through the use of wall readers and CUs. These devices facilitate the communication of data between the various components of the SALTO system by transferring access data to keys and uploading information such as audit trail data from the keys back to the system.
System auditor	A chronological list of all system operator events
Thumbturn	A part of the lock that is used to unlock a device mechanically. It is designed to be turned by the thumb and finger.
UDP	User Datagram Protocol
UID	Unique Identifier
User	A member of staff in an organization who has a valid key
Visitor	A person requiring temporary access to a site for a specified time period, for example, to do site maintenance
Wall reader	An electronic device mounted on a wall that is connected directly to a CU. Wall readers are used to control access to a site's access points, for example, doors. They can also be configured to operate as updaters. In this case, they are termed SVN wall readers. When a user presents their key to an SVN wall reader, the latest up-to-date access information is automatically transferred to the key and the data on their key is transferred back to the system.
Zones	A specified group of doors or lockers that are grouped together to make them easier to manage in the system. For example, a zone could be the doors on the first floor, all the locker doors in the gym area, or all the doors in the financial services area.