

proxSafe Commander software

Features:

proxSafe Commander:

- No terminal limit.
- No cabinet limit (max. 64 per terminal).
- No keyTag limit (up to 2048 per terminal).
- No user limit (up to 4096 per terminal).
- Identification: Pin, Card, or a combination of Pin+Card can be used at the terminal.
- keyTag limit per person definable.
- User expiry date: define time range when a user is valid in the system.
- User time profile: time profiles can be created for a user, they define the time a user is allowed to take keyTags.
- keyTag remote release: keyTags can be released via the software.
- keyTag groups: keyTags can be combined in groups.
- Learn new cards via webinterface: new card data for users can be directly entered in the webinterface.
- Items: special data for a keyTag can be stored in an item, this can be attached to a keyTag.
- Standard reports: reports list all events of the system (e.g. keyTag taken by which user at which time...), own reports can be defined.
- Email reports: reports can be send per email.
- pdf/html export of reports: reports can be stored as a html file (for printing) or as a pdf.
- Graphic view of system: the current status of the system can be seen in a graphic view.
- log files: all changes in the webinterface are recorded and displayed in the log files
- proxSafe mobile: login for terminal users, they can see and change their own data and pin for the terminal.

Additional Features:

FLM (Fleet Management feature):

- License monitoring: License validity is stored for each user, if the expiry date is upcoming, users get an email for notification in advance, if license is expired users can not take any keyTags anymore.
- Mileage logging: When returning a keyTag, a mileage value can be entered, this value is shown in the reports.
- Fault Code logging: When returning a keyTag, a fault code can be entered, this value is shown in the reports. A description for this code can be entered in the proxSafe Commander, which will be also shown in the reports.
- Simple reservation: keyTags can be reserved for a defined time span for a user.
- Issue code logging: A code defining the reason for taking the keyTag can be entered at takeout, this will be shown in the reports. A description for this code can be entered in the proxSafe Commander, which will be also shown in the reports.

KRV (keyTag Reservation feature):

- Reservation of keyTags: keyTags can be reserved for a defined time span for a user (more options than FLM).
- Graphic overview of all reservations: In a daily, weekly and a monthly view all reservations can be seen at a time, the view can also be filtered for particular keyTags.
- Reservations via proxSafe mobile: Terminal users can make their own reservations with this login. The reservations have to be acknowledged by a system administrator before they will be active.
- Email notifications for reservations: User will be informed by email, if reservations of keys are not possible.

CSO (Security (Casino) feature):

- 4+ 6 eyes principle: keyTags can only be taken at the presence of one or two authorized users which have to confirm the withdrawal of the key.
- User groups: users can be combined in groups (for department release mode only, see also below).
- Department release mode: keyTags can only be taken, if one or two authorized users, which have to be in different groups and confirm the withdrawal of the key.
- keyTag time profiles: time profiles can be created for the combination of a keyTag and a user. A time span defines, when a keyTag is allowed to be taken (e.g. the day and the duration).
- Alarmer: additional tool and a special report in proxSafe Commander showing all active alarms in the system with the possibility to start an external software or to send emails in case of a defined alarm.

EXO (keyTag single assignment):

- keyTag single assignment: keyTags are attributed to a particular user, after return of the keyTag access to the keyTag is denied.
- keyTag single user assignment: one keyTag only can be allocate to one user.
- keyTag group withdrawal: several keyTags can be assigned to one group, which can be withdrawn.

Interfaces:

WBS (Webservice):

- proxSafe webservice: all functions possible in the webinterface can be accessed via external software.

IEP (Im-/Export feature):

- Importer: can import user data out of csv file.
- csv export: can export report data or user data into an csv file.

OPC (OPC-Server):

- OPC server: event and alarm transmission in real-time to OPC server.

Lenel (OnGuard System):

- Interface to Lenel OnGuard Access Control. proxSafe functions are integrated in Lenel.

Johanniter (Johanniter-Unfall-Hilfe):

- Interface with real-time transmission after incoming emergency call.

Installation & update of proxSafe Commander:

A product key (PK) in the database activates the features of proxSafe Commander. This PK is saved encrypted in the terminal settings in the database and is only valid for one terminal serial number. For every terminal which runs via the proxSafe Commander and dataCommEngine an **own** PK is needed.

- **Existing installation:** Terminal in database, no PK, - a new PK will be generated with all in this installation existing features (classic features)
- **Activating features:** Enter the new PK in the dataCommEngine, logoff and login. The new features will be shown in the webinterface.
- **Terminal is changed/replaced:** Standard PK is generated, additional features have to be activated with a new PK.