

# **Access Management System V5.2**

Integrating OSS-SO offline locking systems



## Table of contents

1	<b>Security</b>	<b>4</b>
2	<b>Introduction</b>	<b>5</b>
3	<b>System overview</b>	<b>6</b>
4	<b>Configuring a reader as an OSS-SO updater</b>	<b>8</b>
5	<b>Defining an OSS-SO site in a third-party configuration tool</b>	<b>10</b>
6	<b>Importing and configuring an OSS-SO-site in the Bosch OSS-SO configurator</b>	<b>11</b>
6.1	Basic adding, modifying and deleting	12
6.2	Starting the OSS-SO configurator	12
6.3	Setting the card technology	13
6.4	Importing an XML configuration file	14
6.5	Completing the configuration of the OSS-SO system	14
6.6	Configuring the updater	14
6.7	Editing locks in the locking system	15
6.8	Editing lock groups in the locking system	16
6.9	Adding time models to the locking system	17
6.10	Adding authorizations to the locking system	18
6.11	Supervisory dialogs and printed reports	19
7	<b>Assigning OSS-SO authorizations in the ACS</b>	<b>20</b>
	<b>Glossary</b>	<b>22</b>

# 1 Security

## Use latest software

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. For consistent functionality, compatibility, performance, and security, regularly update the software throughout the operational life of the device. Follow the instructions in the product documentation regarding software updates.

The following links provide more information:

- General information: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Security advisories, that is a list of identified vulnerabilities and proposed solutions: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch assumes no liability whatsoever for any damage caused by operating its products with outdated software components.

---

## 2 Introduction

OSS-SO is an industrial standard defined by the OSS Association to improve the interoperability of offline locking systems from different manufacturers. If an offline locking system is implemented to the OSS-SO standard, then locks from different manufacturers can interpret identically the access rights on the same smart card.

### **Intended audience**

Installers, configurators and system administrators involved in the implementation of OSS-SO offline locking systems within access control systems from Bosch.

### 3 System overview

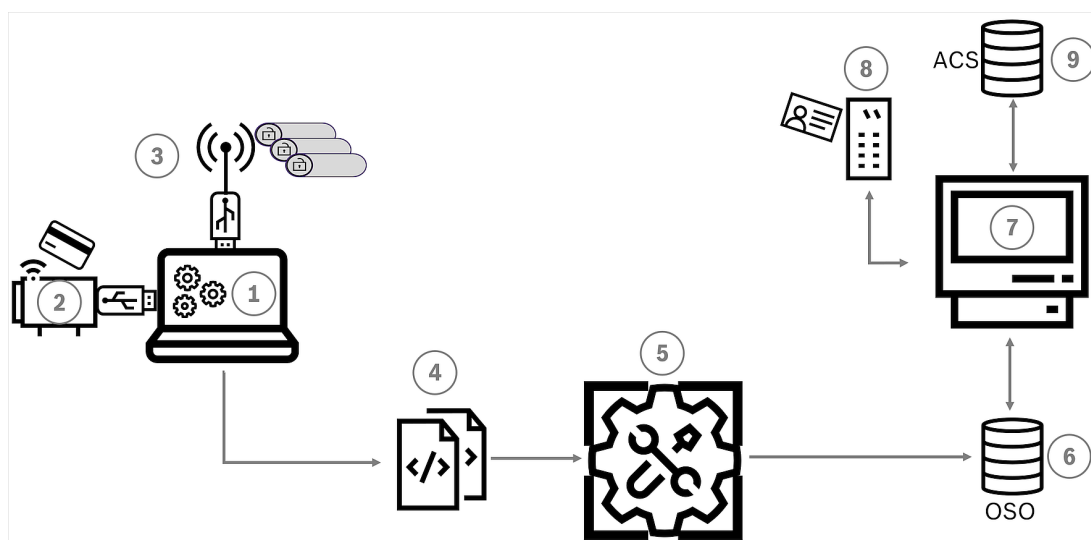
#### Prerequisites

- Originally implemented for AMS 4.0 and BIS ACE 4.9.1.  
Later implementations have additional OSS-SO manufacturers and features.
- License for the OSS-SO feature in your ACS (access control system).
- OSS-SO-standard door locks

#### Configuration tasks overview

In order to configure an OSS-SO locking system within an access control system (ACS) from Bosch, the following tasks are required. The tasks are described in detail in the rest of this document.

- Configuring a reader as an OSS-SO update reader
- Creating an XML definition of a site using software and hardware from an OSS-SO manufacturer
- Importing the manufacturer's XML definition and configuring an OSS-SO locking system in the Bosch OSO Configurator too
- Assigning the necessary OSS-SO authorizations in the ACS.



**Figure 3.1:** Overview of the OSS-SO configuration process

		Description
1	3rd party OSS-SO configuration tool	Usually on a portable computer. Creates initial definitions of the OSS-SO systems, including locks and lock groups.
2	USB programming station	Reads and writes OSS-SO control cards.
3	USB radio stick	Transmits configuration data to locking units
4	XML file	Contains top-level locking-system information, locks and lock groups
5	Bosch OSO Configurator tool	Imports XML. Adds more locking-system information, time models and validity periods to the OSS-SO configuration.

6	OSO database	Makes OSO information available to the ACS
7	Bosch access control system	The ACS (AMS or BIS-ACE)
8	Updater	Also known as an "Update Reader" Device for writing authorizations to OSS-SO cards.
9	ACS main database	Contains the cardholder data

**Operation tasks overview**

Operation of the OSS-SO system consists in assigning temporary OSS-SO authorizations to cardholders in the Bosch ACS.

In day-to-day use, cardholders receive updated authorizations on their cards whenever they present the cards to an OSS-SO updater.

## 4 Configuring a reader as an OSS-SO updater

### Introduction

Communication between the main access control system (ACS) and the OSS-SO updater runs through an Ethernet-to-serial converter. In the following example, we use a WUT 58661 converter device from the Wiesemann and Theis company.



### Notice!

#### Data security

Bosch urgently recommends that you select converter hardware according to current data-security standards. Our use of the WUT 58661 converter in this example is in **no way** an endorsement of the device from a data-security perspective.

### Settings on the converter

- RS-485 2-wire mode
- UART : 9600, 8, n, 1 (9600 baud, 8 bit, no parity bit, 1 stop bit)
- An IP address that the ACS can reach
  - If the converter is used externally, define the port in the firewall of the ACS server.
- Default TCP port 8000 for reader data

For example, to set 2-wire mode for RS-485 on a WUT 58661 device:

- Set the DIL switches SW1 and SW2 to ON
- Set the DIL switches SW3 through SW8 to OFF
- 

### Reader firmware

The firmware on the LECTUS select reader must be version 1.20 or later.

### Connecting a WUT 58661 converter to a LECTUS select reader

The pin mapping is as follows.

	From the WUT 58661	To the LECTUS select reader
	Data Out A, pin 1	Pin 2: RS485 data "B"
	Data In A, pin 2	
	Data Out B, pin 6	Pin 1: RS485 data "A"
	Data In B, pin 7	

### Reader power supply

- Pin 7 DC- (0V)
- Pin 8 DC+ (from 8V to 30V)

### Reader Address 1

- Set DIL switch 1 to ON.
- Set all other DIL switches to OFF)



**Notice!**

## Recommissioning an updater

If you remove an updater from an OSS-SO configuration in order to use it elsewhere, reset the reader to its factory defaults according to the manufacturer's instructions. Failure to do this will prevent the reader from reconnecting to the same system or to a different system.

---

## 5 Defining an OSS-SO site in a third-party configuration tool

### Overview

To map your OSS-SO locking system into a Bosch access control system (ACS), the following preparatory steps are required:

1. Depending on the manufacturer of your OSS-SO locks, define the main parameters of your locking system (also known as an OSS-SO "site") in the manufacturer's proprietary configuration tool.
2. Export the basic configuration from the proprietary tool in the form of an OSS-SO-standard XML file.
3. Import this XML file into the Bosch OSO Configurator tool. In that tool, add to the configuration those details that the Bosch ACS requires.

### Separate documentation for manufacturers' configuration tools

The configuration tools of the various OSS-SO manufacturers differ substantially from one another. We have therefore created separate documents for each of them.

In the same folder where this document is located, look for PDF files with the following naming structure:

– OSS-SO\_3rd\_Party\_Config\_<NameOfManufacturer>.pdf

After creating the XML configuration file in the manufacturer-specific tool, proceed to the next chapter for instructions to import the XML file into the Bosch OSO Configurator tool, and add those details that the Bosch ACS requires.

## 6 Importing and configuring an OSS-SO-site in the Bosch OSS-SO configurator

### Introduction

The OSS-SO configurator is a web application that is installed automatically with the Bosch ACS. It requires its own license to read or store data.

The tool imports OSS-SO offline door configurations in the form of XML files. These XML configuration files are generated initially in the configuration software of OSS manufacturers. The purpose of the Bosch OSS-SO configurator is to create and maintain data structures to which the Bosch ACS has read-access. The data structures define the locks, updater devices, authorizations and time models of the offline locking system. The cardholder records are stored in the database of the ACS itself.

### The card-update process in the ACS

When someone presents a card to the updater device, the ACS performs the following process:

1. Use the personal data on the card to identify a person in the ACS database.
2. Use the person's ID to retrieve the current, temporary authorizations for that person from the OSS-SO database.
3. Cause the updater device to write the person's current, temporary authorizations to the card.

### Prerequisites

- Originally implemented for AMS 4.0 and BIS ACE 4.9.1.  
Later implementations have additional OSS-SO manufacturers and features.
- License for the OSS-SO feature in your ACS (access control system).
- OSS-SO-standard door locks
- The supported browsers: Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based)

Web Browser	Version
Google Chrome	116 or higher
Microsoft Edge	116 or higher
Mozilla Firefox	102 or higher

### Top-level procedure

1. Start the OSS-SO configurator
2. Set the card technology to be used, and the parameters that it requires
3. Import an XML configuration file
4. Complete the configuration of the overall locking system
5. Configure one or more updaters
6. Edit locks and lock groups within the locking system, if required
7. Define OSS-SO-specific time models. These determine the time-periods in which the cards can operate the offline locks.
8. Define authorizations that can be assigned to cardholders in the ACS.

The individual steps of this top-level procedure are described in detail in the following sections, beginning with generic editing procedures:

## 6.1 Basic adding, modifying and deleting

### Elements of the configuration








Configuration of an OSS-SO system consists in adding, modifying and deleting the following elements:

- **Locking systems**, also known as OSS-SO "Sites"
- **Time models**
- **Authorizations**
- **Update readers**

Although it is possible to edit locks and lock groups, these are typically defined in the 3rd party configuration tool and imported without alteration.

### Editing procedures

The basic procedures are the same on each dialog:

- To add an element, click  in the dialog for that element
- To delete an element, select it and click 
- To modify an element, double-click the element, or click 
- To do an incremental text search on a list of elements, click 
- To use predefined filters on a list of elements, click 
  - Regular-expression (regex) syntax is allowed in searches, for example:  
`North.*Entrance` matches both `North East Entrance` and `North West Entrance`
- To assign an element to a group, move it from the list of available items to the list of assigned items. There are 3 possibilities:
  - Double-click the element
  - Drag and drop the element
  - Click  to assign and  to unassign

## 6.2 Starting the OSS-SO configurator

1. Launch the OSS-SO configurator tool from the main menu of the dialog manager of your ACS,  
**System data > OSSO-SO Configuration**  
 or  
 Open a supported browser with HTTPS, the hostname of your ACS server and port 63802
  - `https://<name of ACS server>:63802`
2. Log on as any operator who has OSS-SO authorizations.
- For details on how to assign OSS-SO authorizations in the ACS, refer to the section **Assigning OSS-SO authorizations in the ACS.**

**Refer to**

- *Assigning OSS-SO authorizations in the ACS, page 20*

**6.3****Setting the card technology**

The first task in the OSS-SO configurator tool, **before** importing an XML configuration file, is to set the card technology that your OSS-SO system will use, for example MIFARE DESFire or LEGIC advant. Each card technology will require that you enter its particular settings.

Enter these settings in the **Locking system** dialog.

- **Dialog path:** OSS-SO Configurator tool > **Locking systems**
  - ▶ In the **Card technology** picklist, select the desired technology

**MIFARE DESFire**

- For **MIFARE DESFire**, enter the following parameters. The parameters marked with an asterisk (\*) are mandatory:

<b>Site ID</b>	Integer: Default value is 1	Free text
<b>Name</b>	String: a name for the locking system	Free text
<b>File size (byte)</b>	Integer: The size of files on the card. Default 288. This information available from the manufacturer of your access cards.	This information is available from the manufacturer of your access cards.
<b>Application ID (HEX)</b>	6 hexadecimal digits: The ID of the application area on the cards that will be used for OSS-SO.	
<b>RW key number</b>	32 hexadecimal digits: the read/write key	
<b>Default validity period*</b>	Select from pick list: The default duration of the validity of the card, after the update reader has initialized it.	Pick-list.
<b>Number of events*</b>	Integer: Default value is 8	Number picker

**LEGIC advant**

- For **LEGIC advant**, enter the following parameters. The parameters marked with an asterisk (\*) are mandatory:

<b>Site ID*</b>	Integer: Default value is 1	Free text
<b>Name*</b>	String: a name for the locking system	Free text
<b>Stamp (hex)*</b>	An even number (4-32) of hexadecimal characters, for example: ab2c or dc443f	This information is available from the manufacturer of your access cards.
<b>Default validity period*</b>	Select from pick list: The default duration of the validity of the card, after the update reader has initialized it.	Pick-list.

<b>Number of events*</b>	Integer: Default value is 8	Number picker
--------------------------	-----------------------------	---------------

**NOTE:** In order to use LEGIC advert card technology you will need to order from the PHG company:

- An OSS-SO updater
- A SAM63 card with your company's unique LEGIC stamp. The SAM63 card initializes the updater so that it can write to LEGIC cards.
- LEGIC user cards with your company's LEGIC stamp
- Click **Save** to save the data or **Cancel** to discard your changes.


## 6.4 Importing an XML configuration file

### Initial use

If you start the OSS-SO configuration tool, and no locks have yet been defined, it will prompt you for an XML configuration file. Select an XML file that was prepared in the OSS-SO configuration tool of a recognized OSS-SO manufacturer.

### Loading more XML files



On the **Locks** dialog, click  to load another XML file.

Note that the load procedure adds elements from the XML file, but does not delete elements that have already been defined in the tool. To delete elements, go to the appropriate dialog and delete the elements explicitly, using the icon.

## 6.5 Completing the configuration of the OSS-SO system

After importing the XML configuration file from the manufacturer's configuration tool, add the data that the Bosch ACS requires.

### Manufacturer

Dialog path: OSS-SO Configurator tool > **Manufacturers**

- ▶ Select the manufacturer of the OSS-SO locking system from the list.
- Click **Save** to save the data or **Cancel** to discard your changes.



## 6.6 Configuring the updater

The updater, also known as an update reader, is a device that for the reading and writing of data from and to OSS-SO-compatible credentials. The configuration of the updater is not part of the initial XML configuration file as exported from the manufacturer's configuration tool.

### Dialog path

OSS-SO Configurator tool > **Updater**

### Procedure

1. To create a new element, click 
2. To edit an existing element, double-click the record or click 
3. Enter the following parameters:

<b>Reader name</b>	String: a name for the updater device	Free text
<b>IP Address (IP-V4)</b>	The IP (version 4) address of an OSS-SO-compatible updater on the network	
<b>Port</b>	The network port for OSS-SO communication.	Consult the manufacturer's instructions.
<b>Description</b>	Recommended: a clear description of the updater type and its physical location.	Free text

- Click **Save** to save the data or **Cancel** to discard your changes.

## 6.7



### Editing locks in the locking system

A lock is an individual OSS-SO-compatible locking unit, or "cylinder" as found in a single door. Definitions of locks and lock groups are already defined in the imported XML file, and it is usual to leave those definitions unchanged.

#### Dialog path

OSS-SO Configurator tool > **Locks**

#### Procedure

1. To create a new element, click 
2. To edit an existing element, double-click the record or click 
3. Enter the following parameters:

<b>Name*</b>	Recommended: follow a systematic naming convention for clear identification, even when the system contains hundreds of locks.	Free text
<b>Manufacturer*</b>	The name of the manufacturer of the lock	Drop-down list
<b>Locking system*</b>	The name of the offline locking system	Drop-down list
<b>Lock ID*</b>	Unique integer within the locking system	Unique integer within the locking system.
<b>Description</b>	Recommended: a clear description of the door and its physical location.	Free text
<b>Default unlock time (sec)*</b>	The number of seconds of the standard unlock pulse	Integer
<b>Extended time</b>	If enabled, use of a valid credential at this lock sends an extended unlock pulse to the lock, to allow more time to open the door.	On/off toggle
<b>Extended unlock time (sec)*</b>	The number of seconds added to a standard unlock pulse for extended unlock time.	Integer

- Click **Save** to save the data or **Cancel** to discard your changes.

## 6.8 Editing lock groups in the locking system



A lock group is an abstract container object to make configuration of the locking system easier. It is a set of locks with something in common. For example, the locks of one floor of a building; or the locks used by a particular type of cardholder, such as kitchen staff or sales assistants.



Definitions of locks and lock groups are already defined in the imported XML file, and it is usual to leave those definitions unchanged.

### Dialog path

OSS-SO Configurator tool > **Lock groups**

### Procedure

1. To create a new element, click 
2. To edit an existing element, double-click the record or click 
3. Enter the following parameters:

<b>Name*</b>	Recommended: follow a systematic naming convention for clear identification, even when the system contains hundreds of locks.	Free text
<b>Locking system*</b>	The name of the offline locking system	Drop-down list
<b>Group ID*</b>	Unique integer within the groups of the locking system	Integer
<b>Description</b>	Recommended: a clear description of the group and the locks that it contains.	Free text
<b>Assigned locks</b>	A list of the names of the locks in this group.	Move locks from one list to the other to assign and unassign.
<b>Available locks</b>	A list of the names of the locks that are eligible for this group.	Click  to do an incremental search on long lists.  Click  to select all members of a list.

- Regular-expression (regex) syntax is allowed in searches, for example:  
North.\*Entrance matches both North East Entrance and North West Entrance
- Click **Save** to save the data or **Cancel** to discard your changes.



## 6.9 Adding time models to the locking system

Time models are a way of limiting authorizations to certain periods on certain days of the week. The OSS-SO Configurator allows you to create any number of time models for later inclusion in authorizations.

- Each time model can contain one or two week models to govern different days, for example weekdays and weekends.
- Each week model can contain one or two time intervals

Week model 2

<b>Week model 1*</b> <input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday	<b>Week model 2</b> <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input type="checkbox"/> Sunday
<b>Time Intervals*</b>	<b>Time Intervals*</b>
<b>Interval 1.1</b> From 07:00 AM <input type="text"/> To 12:00 PM <input type="text"/>	<b>Interval 2.1</b> From 09:00 AM <input type="text"/> To 04:00 PM <input type="text"/>
<b>Interval 1.2</b> From 01:00 PM <input type="text"/> To 07:00 PM <input type="text"/>	<b>Interval 2.2</b> From --:-- -- <input type="text"/> To --:-- -- <input type="text"/>

\*Mandatory

### Dialog path

OSS-SO Configurator tool > **Time models**

### Procedure

1. To create a new element, click
2. To edit an existing element, double-click the record or click
3. Enter the following parameters:

<b>Name*</b>	Recommended: follow a systematic naming convention for clear identification.	Free text
<b>Description</b>	Recommended: a clear description of the time model and the authorizations or persons to whom it applies.	Free text
<b>Week model 1*</b> <b>(Optional) Week model 2</b>	Days of the week	Select the check boxes of the days of the week model.
<b>Time interval 1.1*</b> <b>(Optional) Time intervals 1.2, 2.1, 2.2</b>	Starting time and finishing time (From/To)	Use the time picker widget to select times. The time format depends on the settings of your operating system.

- Click **Save** to save the data or **Cancel** to discard your changes.



## 6.10 Adding authorizations to the locking system



OSS-SO authorizations are convenient bundles of access rights for assignment to OSS-SO cardholders. They describe which doors the cardholders can use, and when. Although the principle is similar, OSS-SO authorizations are separate from the authorizations in the ACS. Authorizations consist of locks, lock groups and time models. Therefore, you must create these before you can create authorizations. Locks and lock groups are usually imported with the XML file from the 3rd party configuration tool.

### Dialog path

OSS-SO Configurator tool > **Authorizations**

### Procedure

1. To create a new element, click 
2. To edit an existing element, double-click the record or click 
3. Enter the following parameters:

<b>Name*</b>	Recommended: follow a systematic naming convention for clear identification.	Free text
<b>Description</b>	Recommended: a clear description of the authorization and the locks that it contains.	Free text
<b>Assigned locks and lock groups</b>	A list of the names of the locks in this group. See the additional parameters in the following table.	Move locks from one list to the other to assign and unassign.
<b>Available locks</b>	A list of the names of the locks that are eligible for this authorization.	Click  to do an incremental search on long lists.
<b>Available lock groups</b>	A list of the names of the locks groups that are eligible for this authorization	Click  to select all members of a list.

- Regular-expression (regex) syntax is allowed in searches, for example:  
North.\*Entrance matches both North East Entrance and North West Entrance

For each assigned lock or lock group, two optional parameters are provided:

<b>Office mode / toggle door</b>	If enabled, this option allows the holder of the authorization to unlock or lock a door for a prolonged period, for example during office hours.	On/Off toggle
----------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------	---------------

	Each presentation of the card at this lock unit toggles the state from locked to unlocked or vice versa.	
<b>Time model</b>	The days and periods in which the holder of the authorization can operate the respective assigned lock or lock group.	Drop-down list


- Click **Save** to save the data or **Cancel** to discard your changes.

## 6.11 Supervisory dialogs and printed reports

The OSS-SO Configurator also provides supervisory dialogs so that users can obtain important details of the configuration for maintenance and administrative purposes. Users can then print this information for offline use.

- **Battery states:** Determine which offline locks require a change of battery.
- **Authorizations report:** Determine which cardholders from which companies are authorized for which locks and lock groups.

### Basic procedure

1. Use the search and filter functions to filter out elements of interest.
2. Click the  (print) icon on to send the filtered list to a printer or PDF file.

## 7 Assigning OSS-SO authorizations in the ACS

### Introduction

The main OSS-SO task of an operator of the main access control system (ACS) is to assign OSS-SO authorizations to cardholders. The authorizations have been written to the OSS-SO database by the Bosch OSS-SO Configurator tool. The ACS reads the authorizations from there and applies them to a person defined in the ACS database. Note that authorizations are assigned to a person, and not to a particular card.

Although OSS-SO authorizations are not the same as standard ACS access authorizations, the assignment procedure in the **Cards** dialog is identical.

### Dialog path

- In the ACE client menu select **Personnel data > Cards**
- In the AMS main client menu select **Personnel data > Cards**

### Procedure

1. In the Cards dialog, select the person to receive OSS-SO authorizations.
2. Select the OSS-SO tab.
3. Make the assignments:
  - All OSS-SO authorizations that are already assigned to the person appear in the list on the left.
  - All OSS-SO authorizations that are available for assignment appear in the list on the right.
 Select items and then click the buttons between the lists to move items from one list to the other.



assigns the selected item.



unassigns the selected item.



assigns all available items.



unassigns all assigned items.

1. Save the person record now, or first configure a time window, as described below.

### Configuring a time window for the transfer of authorizations to cards

The authorizations are normally transferred to a card the first time the card is presented to a reader that has been configured as an OSS-SO updater. See the chapter on configuring a reader as an OSS-SO updater.

The operator can set here in advance the period within which the cardholder may receive these authorizations from the system.

At the bottom of the OSS-SO tab, set the following parameters.

<b>Valid from</b>	The earliest date and time when the updater may transfer the assigned authorizations to the card.
<b>Valid until</b> (optional)	The latest date and time when the updater may transfer the assigned authorizations to the card.
<b>Validity time</b>	The duration of the authorizations from the moment they are transferred to the card.

The default value for this duration is set as a property of the locking system, but you can override that value here.

**Refer to**

- *Configuring a reader as an OSS-SO updater, page 8*

# Glossary

## ACS

---

generic term for a Bosch Access Control System, for example, AMS (Access Management System) or ACE (BIS Access Engine).

## offline locking

---

access control where the locks are not in constant electronic contact with the main system. Instead the locks receive their settings from smart cards that a human operator programs at a separate computer.

## OSS Association

---

The Open Security Standards Association. <https://www.oss-association.com>

## OSS-SO

---

the SO (Standard Offline) standard of the OSS Association. An industry standard to improve the interoperability of offline locking systems from different manufacturers.

## OSS-SO updater

---

an electronic device which writes, deletes and modifies authorization data on an OSO credential.

## UART

---

Universal asynchronous receiver-transmitter (UART) - a hardware device for asynchronous serial communication. Data format and transmission speeds are configurable.



**Building solutions for a better life.**

202309201124