Building Integration System

Integrating OSS-SO offline locking systems

en User manual

Table of contents

1 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.
In this documentation, we reference the OSS-SO implementation from the Uhlmann & Zacher company (U&Z), along with the hardware and software it provides.

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

2 System overview

Prerequisites

- AMS 4.0 or later, or BIS ACE 4.9.1 or later
- Uhlmann & Zacher OSS-SO hardware and software tools
- 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
- Defining an OSS-SO site using software and hardware from U&Z
- Importing the U&Z definition and configuring an OSS-SO locking system in the Bosch OSO Configurator tool

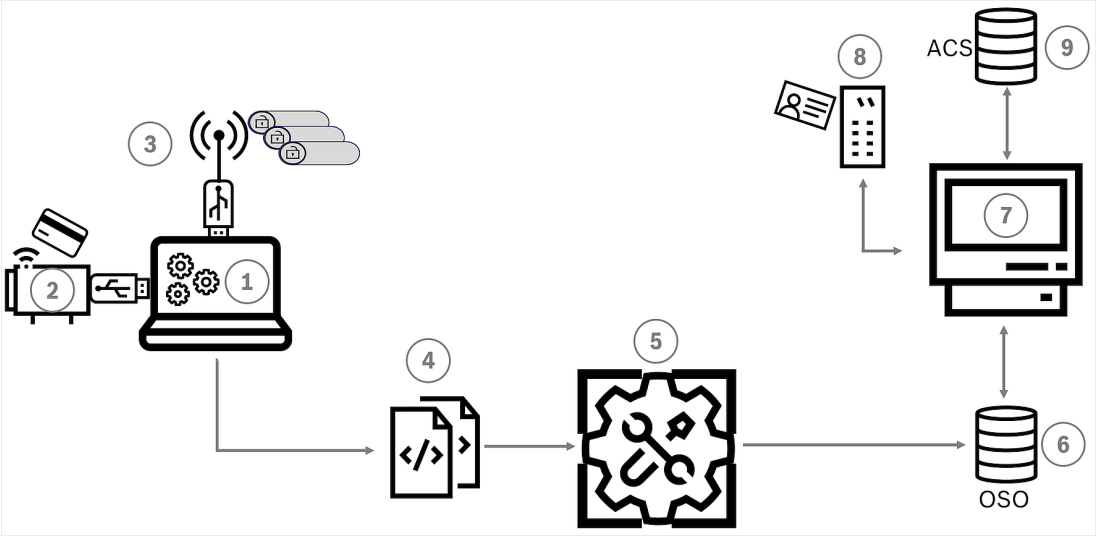


Figure 2.1: Overview of the OSS-SO configuration process

		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.

3 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.

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

Connecting a WUT 58661 converter to a LECTUS secure reader

The pin mapping is as follows.

	From the WUT 58661	To the LECTUS Secure 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.

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

Overview

Before they can be mapped into a Bosch access control system (ACS), the main parameters of an OSS-SO locking system (also known as an OSS-SO "site") must be defined in the manufacturer's own configuration tool. For the purposes of this document, we use the U&Z **ClexSCT tool**.

- This tool exports a configuration in the form of an XML file, to form the foundation of the Bosch OSS-SO configuration.
- The person responsible for configuring OSO in the Bosch ACS imports the XML file into the Bosch OSO Configurator tool, and adds to it those details that the Bosch ACS requires.

The OSS-SO Concept Card

The manufacturer of the locking system provides a Concept Card, the equivalent of a Bosch Facility Card. The Concept Card identifies the site owner and is required in the following circumstances:

- To create a new definition of a locking system in the third-party tool:
  - Present the concept card to the programming station when prompted by the tool.
- To initialize a locking unit (cylinder) for use in a particular locking system.
  - Present the concept card to the cylinder and wait for green LEDs on cylinder.

OSS-SO access cards

Order cards of type MIFARE DESFire from the card manufacturer of your choice. OSS-SO cards require the following specifications:

- Bosch code
  - Application ID (AID) consisting of 6 hexadecimal characters
  - Files
- OSS-SO Permissions
  - Applications ID (AID)
  - A DESFire key1 that the purchaser of the cards specifies and orders from the card manufacturer.
  - File 0: 32 bytes, for holding the Bosch code
  - File 1: 288 bytes for holding permissions

Prerequisite hardware and software from U&Z

- The ClexSCT tool
- USB radio stick in a USB port of the computer where the ClexSCT tool is running.
- Programming station, a small table-top device, connected via USB to the computer where the ClexSCT tool and the Clex database reside

Functions of the programming station

The programming station reads:

- U&Z Concept Card

  The Concept Card is equivalent to a Bosch Facility card and authorizes one site operator. It is required to initialize the database that will contain the site definition. That database resides on the computer where ClexSCT is running.

The programming station writes the various cards that an OSS-SO system requires, for example:

- Service card: to put a lock unit into service mode, so that it can communicate with the Radio stick.
- Battery-change card
- Disassembly card

Identifying USB ports

Use Windows Device Manager identify the COM ports used by the radio stick and the programming station. These will be required when you configure the ClexSCT software.

4.1 Defining an OSS-SO locking system with the ClexSCT tool

Introduction

For the purposes of this documentation, we use the ClexSCT application from Ulmann&Zacher to define a basic OSS-SO locking system (also known as a "site") and export it in an XML file for further processing in the Bosch OSO Configurator tool.

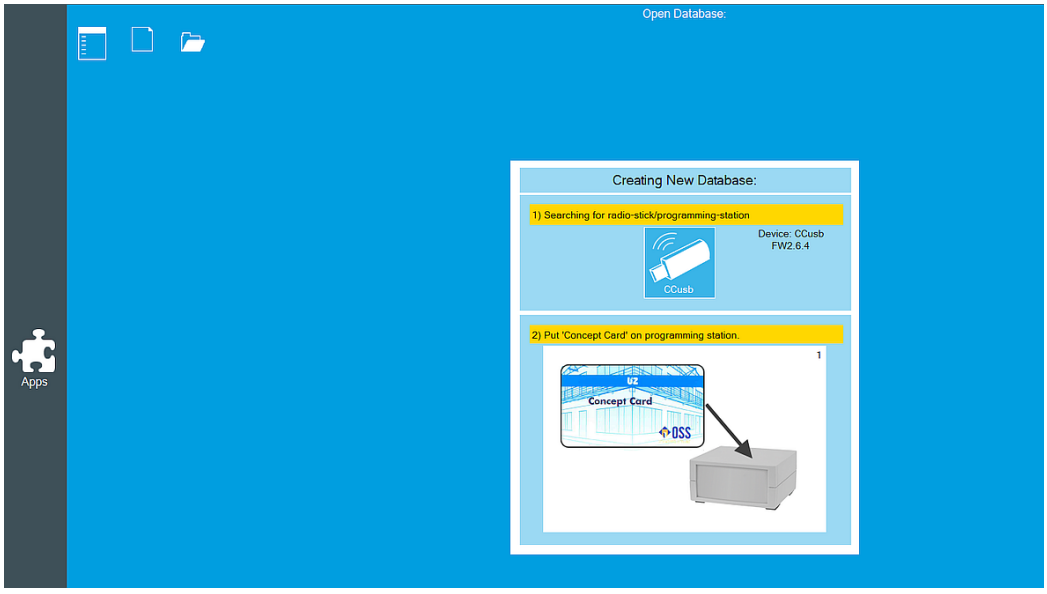
Prerequisites

- The ClexSCT application is installed on your computer
- The USB radio stick and USB programming station are connected.

Procedure

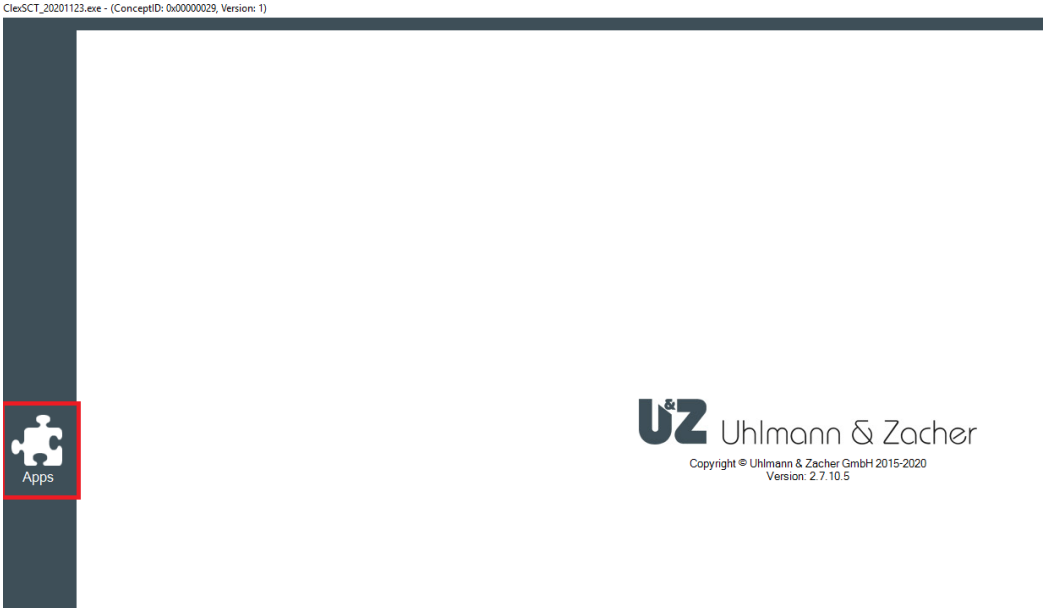
1. Double click the executable *ClexSCT_*.exe* to start the application.

- When prompted, place your Concept card on the Programing station as illustrated:



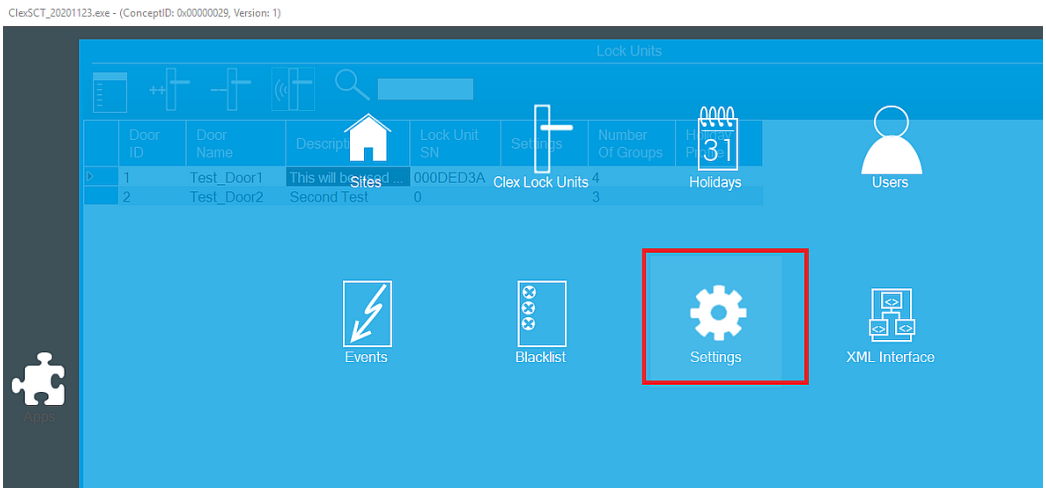
- The new database is created.

– The main window changes and presents the **Apps** icon.



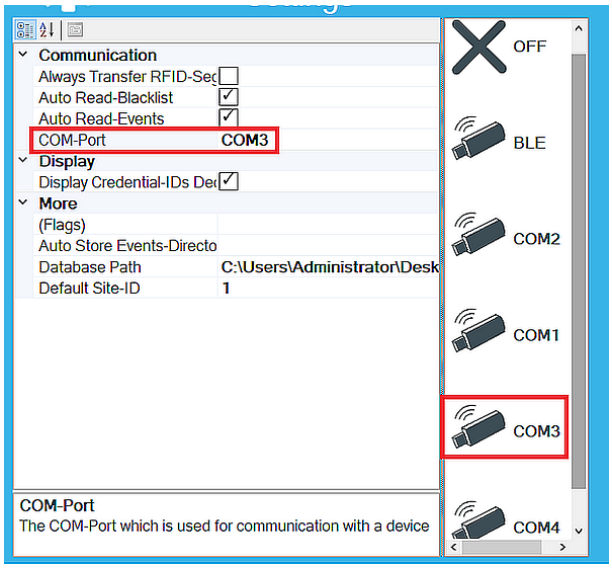
2. Click **Apps**

– the main screen appears:

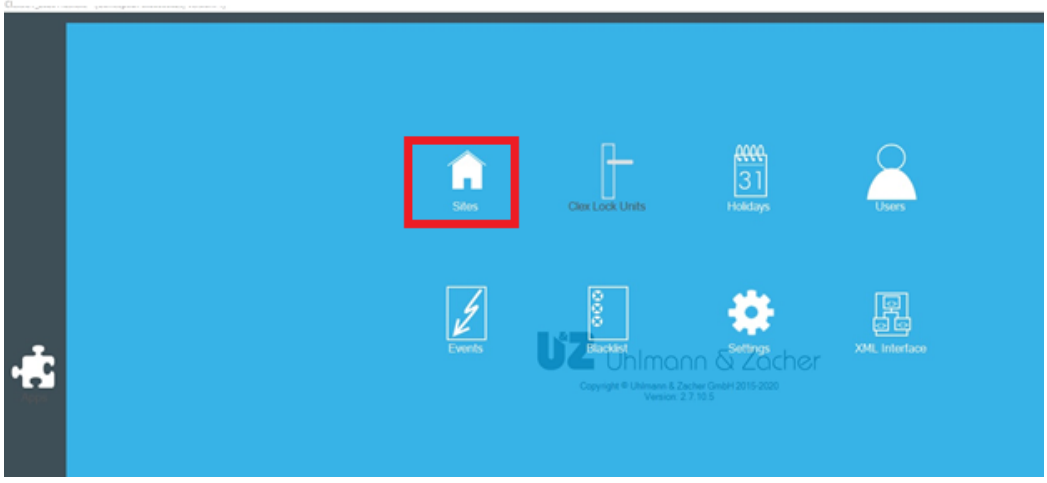


3. Click **Settings** and set the COM port of the USB radio stick

– Use the Windows device manager to identify the stick's USB port, if necessary. Your configuration will differ somewhat from the following example:

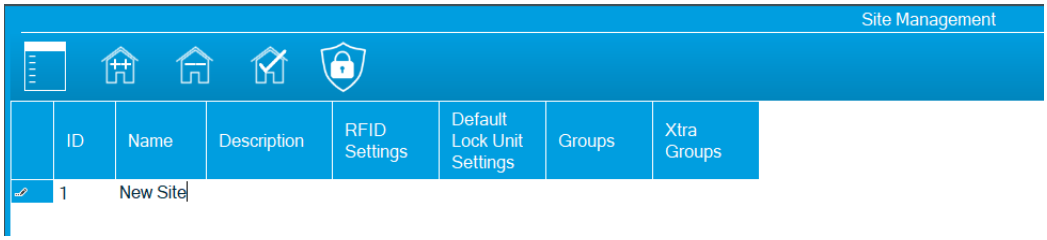


4. Click **Sites** on the main screen.



– The **Site Management** dialog opens.

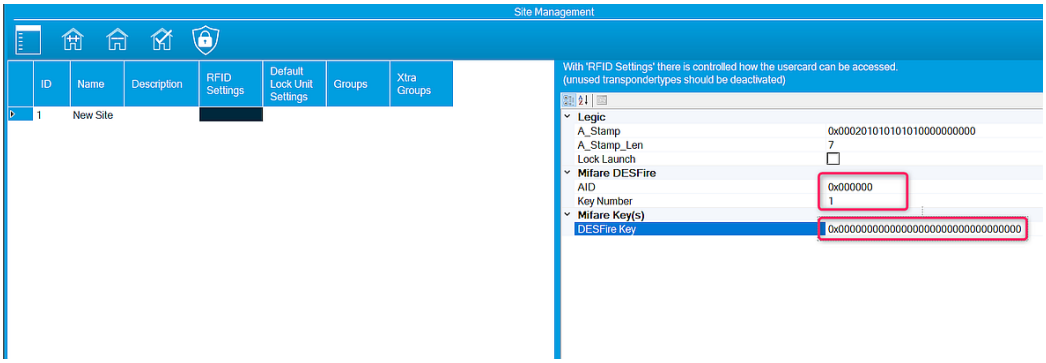
5. To add a site, select the ribbon icon with the **++** characters.



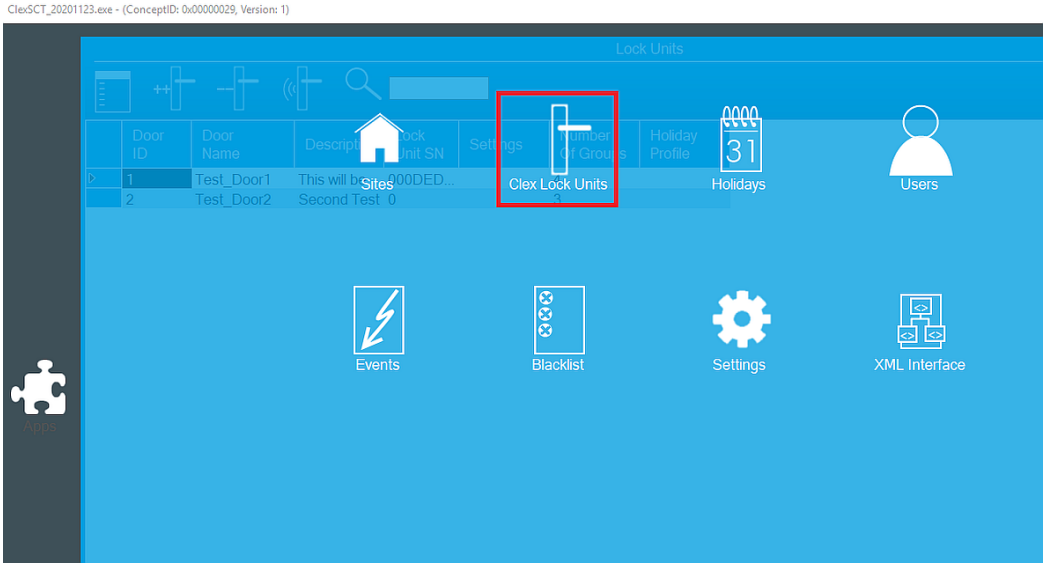
6. Enter a unique name and a description of the site. The ID is automatically set but can be edited. **IMPORTANT:** Do not use *0* (zero) as this is prohibited by the OSS-SO standard.
7. You can leave the **RFID Settings** at their defaults, but they can be edited if desired.

– **AID** (provided by your card manufacturer)
– **Key Number:** *1*

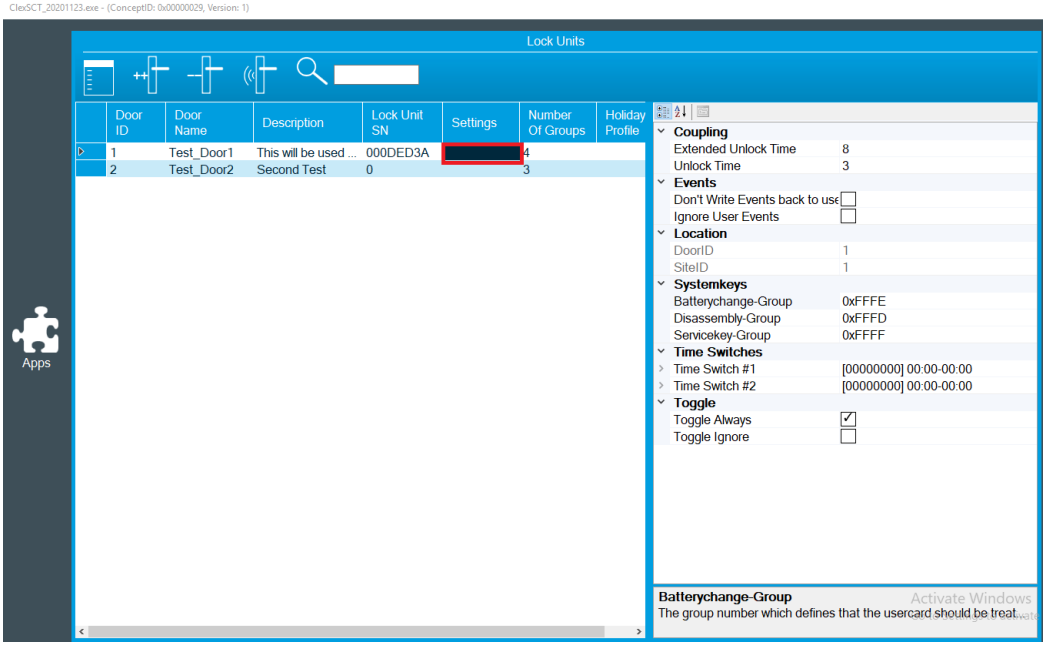
– **DESFire key** (provided by your card manufacturer)



8. On the main screen, click **Clex Lock Units**



9. On the **Lock Units** page, to add a lock unit, select the ribbon icon with the **++** characters.

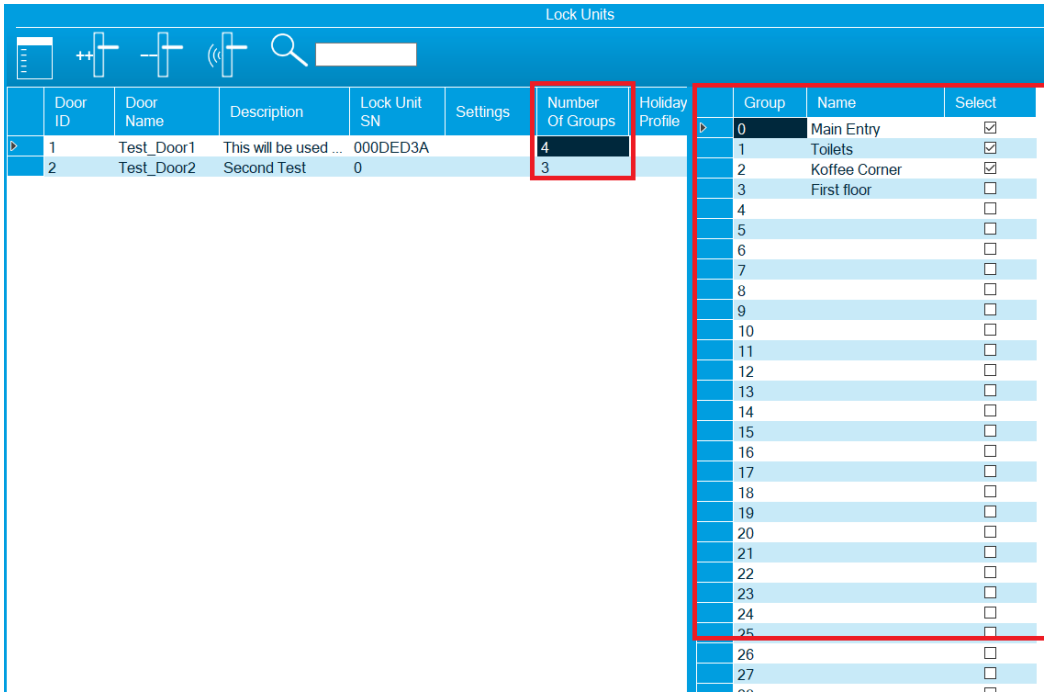


10. Add the following information:

– **Door ID**

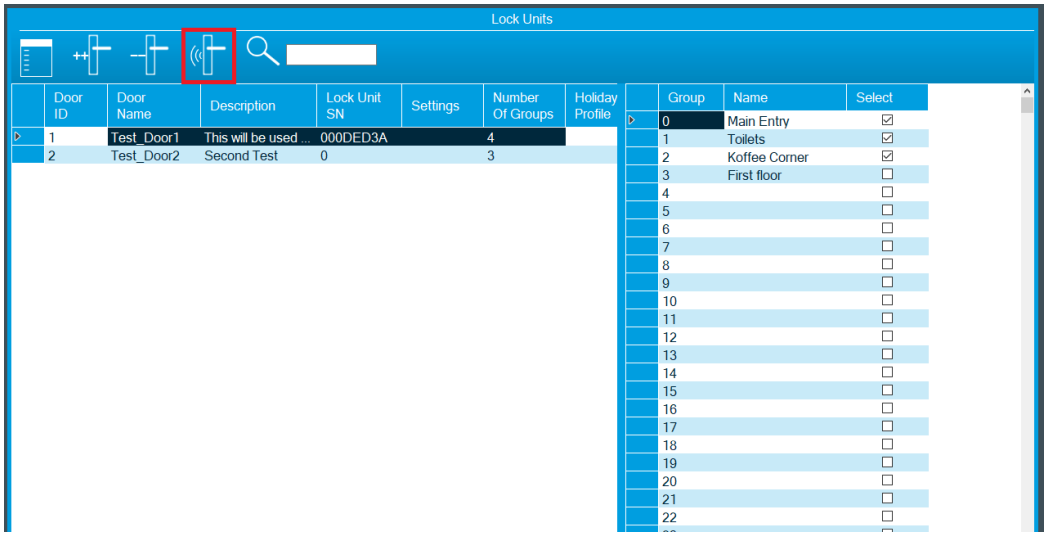
– **Door Name**

- **Description**
- The **Lock Unit SN** (serial number) is automatically read when the **service card** is presented to the lock unit.
- **Number Of Groups** (lock groups): A door can be part of zero, one or more groups. There are 1024 groups available.

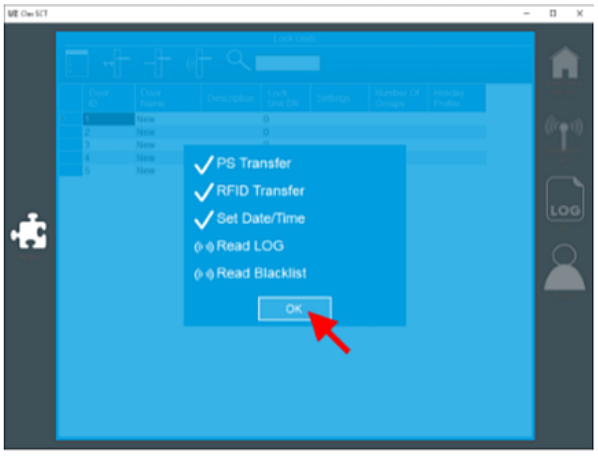


Transmitting the configuration to the lock unit hardware,

1. Make sure that the lock unit is within range of the radio stick.
2. Hold the service card in front of the lock unit hardware.
3. On the Lock Units screen, select the lock unit icon with the radio waves, framed in the following illustration.



– Progress is displayed as in the following illustration



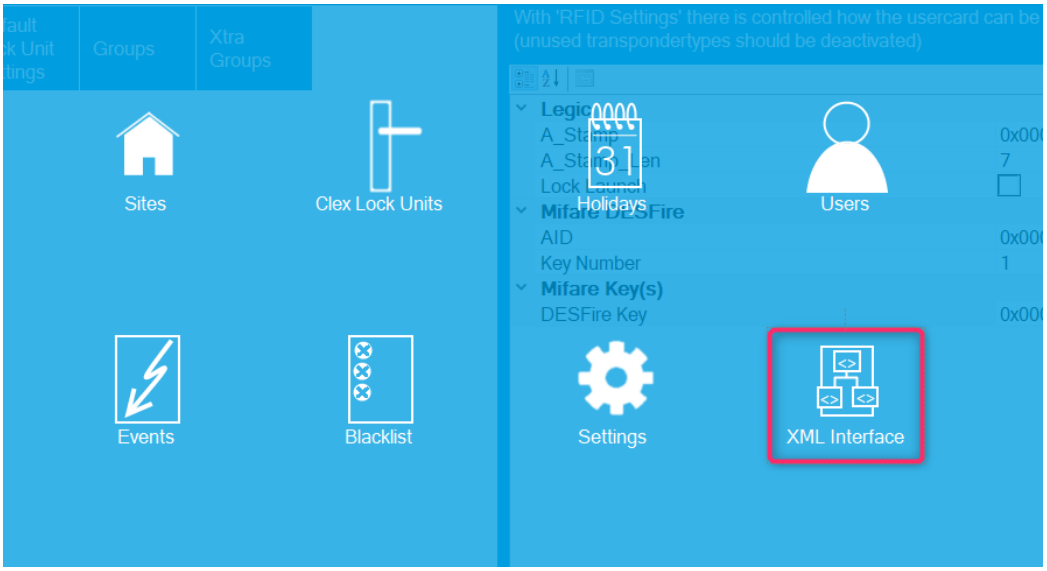
4. Click **OK** when the transfer process is complete.

– The Lock unit is now ready to read OSS-SO access cards.

Exporting the OSS-SO configuration to an XML file

After all locks are configured, the configuration needs to exported for further processing in the Bosch OSO Configurator tool

1. On the main screen, click **XML Interface**



– A file explorer window appears.

2. Save the XML file in a location to which the Bosch OSO Configurator tool has access.
3. Proceed to the next chapter for instructions on using the Bosch OSO Configurator tool.

Refer to

– *Importing and configuring an OSS-SO-site in the Bosch OSS-SO Configurator tool, page 15*

5 Importing and configuring an OSS-SO-site in the Bosch OSS-SO Configurator tool

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, such as Uhlmann & Zacher.

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

– License for the OSSO-SO feature
– ACS: BIS-ACE version 4.9.1 or later; or AMS version 4.0 or later
– The supported browsers: Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based)

Web Browser	Version
Google Chrome	90 or higher
Microsoft Edge	90 or higher
Mozilla Firefox	88 or higher

Top-level procedure

1. Start the OSS-SO configurator
2. Import an XML configuration file
3. Complete the configuration of the overall locking system
4. Configure one or more updaters
5. Edit locks and lock groups within the locking system, if required
6. Define OSS-SO-specific time models. These determine the time-periods in which the cards can operate the offline locks.
7. 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.

5.1 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.

5.1.1 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 
  – 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

5.2 Import 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 an OSS-SO configuration tool, such as the ClexSCT tool from Uhlmann & Zacher.

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.

5.3 Complete the configuration of the offline locking system

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

Dialog path
OSS-SO Configurator tool > **Locking systems**

Procedure

1. To edit the existing locking system, double-click the record or click 
2. Enter the following parameters:

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

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

5.4 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:

Reader name	String: a name for the updater device	Free text
IP Address (IP-V4)	The IP (version 4) address of an OSS-SO-compatible updater on the network	
Port	The network port for OSS-SO communication.	Consult the manufacturer's instructions.
Description	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.

5.5 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:

Name*	Recommended: follow a systematic naming convention for clear identification, even when the system contains hundreds of locks.	Free text
Manufacturer*	The name of the manufacturer of the lock	Drop-down list
Locking system*	The name of the offline locking system	Drop-down list
Lock ID*	Unique integer within the locking system	Unique integer within the locking system.
Description	Recommended: a clear description of the door and its physical location.	Free text

Default unlock time (sec)*	The number of seconds of the standard unlock pulse	Integer
Extended time	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
Extended unlock time (sec)*	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.

5.6 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:

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

		Click  to select all members of a list.

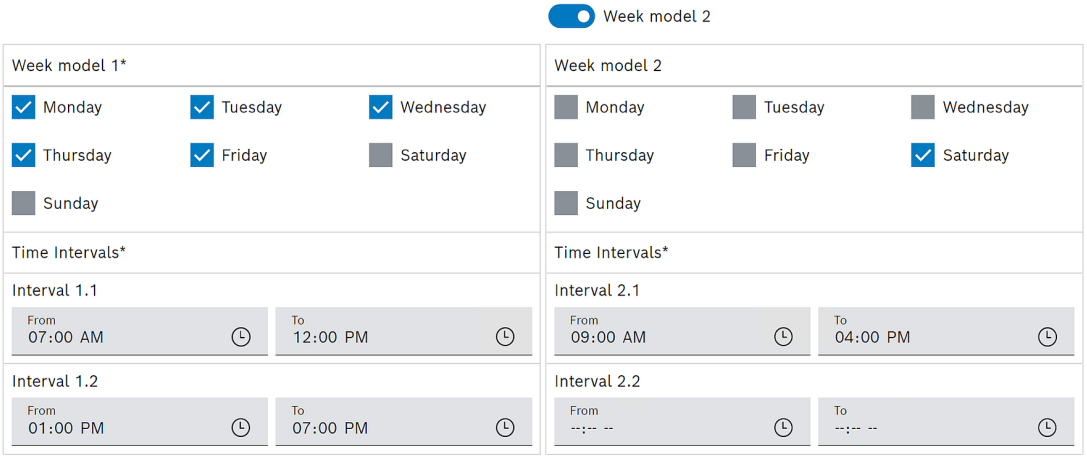
– Regular-expression (regex) syntax is allowed in searches, for example:
*North.*Entrance* matches both *North East Entrance* and *North West Entrance*

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

5.7 Add 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



*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:

Name*	Recommended: follow a systematic naming convention for clear identification.	Free text
Description	Recommended: a clear description of the time model and the authorizations or persons to whom it applies.	Free text

Week model 1*	Days of the week	Select the check boxes of the days of the week model.
(Optional) Week model 2		
Time interval 1.1*	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.
(Optional) Time intervals 1.2, 2.1, 2.2		

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

5.8 Add 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:

Name*	Recommended: follow a systematic naming convention for clear identification.	Free text
Description	Recommended: a clear description of the authorization and the locks that it contains.	Free text
Assigned locks and lock groups	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. Click  to do an incremental search on long lists. Click  to select all members of a list.
Available locks	A list of the names of the locks that are eligible for this authorization.	
Available lock groups	A list of the names of the locks groups that are eligible for this authorization	

– 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:

Office mode / toggle door	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. Each presentation of the card at this lock unit toggles the state from locked to unlocked or vice versa.	On/Off toggle
Time model	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 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.

Valid from	The earliest date and time when the updater may transfer the assigned authorizations to the card.
Valid until (optional)	The latest date and time when the updater may transfer the assigned authorizations to the card.
Validity time	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 7*

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.

Uhlmann & Zacher company (U&Z)

https://www.git-security.com/companies/uhlmann-zacher-gmbh

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202112091633