

AccessOne

Access Control Software



System description and manual

English Version VA1 BRO2262

Table of Content

1. About thi	s manual	4			
1.1 Man	ufacturer and service	5			
1.2 Targ	et groups of this manual	5			
о г		<i>_</i>			
2. For your s	arety	6			
2.1 Sale	Ly Information	6			
2.2 Lega	n mornation				
2.5 Syste 2.4 Data	anotection in AccessOne	6			
2.4 Data		0			
3. About Aco	cessOne	8			
3.1 Fund	tion extensions	9			
3.2 Recc	ommended procedure for initial setup of AccessOne				
4. Working	with dialogues				
4.1 View	v mode – change mode				
4.2 Tool	bar				
5. Logging o	n	16			
6. Configuri	ng AccessOne				
6.1 Cont	figuring the system				
6.1.1	Parameter				
6.1.2	Areas				
6.1.3	Parking groups				
6.1.4	Workstations				
6.1.5	Reader formats				
6.1.6	Card analysis	21			
6.1.7	Licences	22			
6.1.8	Card formats	23			
6.2 User	data	27			
6.2.1	User groups	27			
6.2.2	User master data				
6.2.3	User ACL (ACL Client ability)	29			
6.2.4	Assigning datasets to access lists (ACL)				
6.2.5	Web user groups				
6.3 Loca	tion data				
6.3.1	Creating a location				
7. Configuri	ng devices				
7.1 Onli	ne device data				
7.1.1	Displaying the device overview				
7.1.2	Creating a master controller (MAC)				
7.1.3	7.1.3 Creating a door controller (LAC)				



	7.1.4	Creating a door	
	7.1.5	Displaying the device status	53
7.2	2 Offlin	ne device data (OSS-SO)	54
	7.2.1	Facility data	54
	7.2.2	Cylinders (and handle sets)	55
	7.2.3	Programming offline devices	56
	7.2.4	Authorisations	57
	7.2.5	Data import	58
	7.2.6	Time models	59
8.Co	onfigura	tion of authorisations	60
8.1	L Auth	orisations	60
	8.1.1	Authorisations in the overview	60
	8.1.2	General information on time and day models	61
	8.1.3	Day models	61
	8.1.4	Special and holidays	62
	8.1.5	Time models	65
	8.1.6	Access masks	67
8.2	2 Auth	orisation profiles	68
	8.2.1	Online authorisations in the overview	68
	8.2.2	Offline authorisations in the overview	69
9.Cr	eating p	erson data	70
9.1	L Perso	on data	
	9.1.1	Person data in the overview	70
	9.1.2	Master data	72
	9.1.3	Further master data	74
	9.1.4	ID cards (access media)	75
	9.1.5	Authorisations	77
	9.1.6	Capture picture	79
	9.1.7	Lockouts	
	9.1.8	OSS-SO	
	9.1.9	Instructions	
9.2	2 Grou	p changes	83
	9.2.1	Person data	83
	9.2.2	Adding or deleting person lockouts	83
	9.2.3	Modifying person authorisations	
10	System	n documentation	
10	.1 Repo	rts	85
10	.2 Logb	ook	
	10.2.1	Messages	
	10.2.2	Filters	
11	Trouble	eshooting	

1 About this manual

This manual contains basic information on the setup and administration of an access control system using the AccessOne access control system.

The manual must be regarded as a part of the product and should be kept for the entire service life of the product. The manual must be passed on to any subsequent user of the product.

Other applicable documents

Licence activation >	${\sf BRO2307_EN_Manual_Activating-Licence-Module-AccessOne}$
Installation >	BRO2313_EN_Instructions_Installation-of-AccessOne

Symbol conventions



Refers to other documents.



Indicates additional information and tips.



Indicates warnings in step-by-step instructions and particularly important information.

Writing conventions

In this document, control elements in the dialogue interface, such as buttons, are

highlighted in a bold font (example: Click on Create user. Toolbar buttons

are also indicated by capital letters (example: Click CANCEL). Names of data objects, selection and text fields and checkboxes are shown in quotation marks (example: Enter additional information in the 'Remarks' field).

Illustrations

The dialogues shown in this manual do not include all of the options available to the system. Depending on the licence held and the options activated, screenshots and descriptions may differ.

Notes on trademark protection

MIFARE, MIFARE Classic and MIFARE DESFire are registered trademarks of NXP B.V. and are used under licence.

All of the information and data contained in these documents are subject to change or further technical development without prior notice. No part of this document may be copied or distributed for any purpose without the express written consent of C.Ed.Schulte GmbH Zylinderschlossfabrik.

© 2021 C.Ed. Schulte GmbH Zylinderschlossfabrik, Velbert/Germany

BRO2316-1 Version: VA1



Always use the latest version of this manual. Updated versions are available free of charge from www.ces.eu.

CEStronics

1.1 Manufacturer and service

The copyrights to AccessOne are held by ACcesstronic GmbH. Service and support are provided by C.Ed. Schulte GmbH, Velbert. For service assistance, please contact CES Service. CES Service can be contacted at +49(0)2051 204 222 or by e-mail: hotline@ces.eu

Manufacturer	Service and Support	
ACcesstronic GmbH	C.Ed. Schulte GmbH	Tel: +49 (0) 2051-204-0
Gartenstr. 38	Zylinderschlossfabrik	Fax: +49 (0) 2051-204-229
52249 Eschweiler	Friedrichstr. 243	www.ces.eu
	42551 Velbert	info@ces.eu

1.2 Target groups of this manual

Setting up of AccessOne is commissioned by the system operator and is carried out by its own specialists or by service providers from the IT/administration sector. The access control system may only be operated by personnel with product training. The information contained in this manual is therefore intended for different target groups. The relevant target groups are indicated at the start of each main section. Observe our recommendations on the procedures for installation, setup and operation of AccessOne (see the general information on the next page).

Target group	Skills
IT/administration	have many years of professional experience in the fields of IT structures, administ-
specialists	ration and networks.
	Particular characteristics of this target group:
	Knowledge of specialist IT terminology
	Knowledge of the structure and maintenance of networks, particularly knowledge
	of the network that they maintain
System operators	are experienced in the management of master key systems. This could be either
	knowledge of a number of such systems or an in-depth knowledge of a single
	master key system.
	Particular characteristics of this target group:
	Knowledge of the specialist terminology related to master key systems
	Skilled in the use of PCs and software
Product-trained	have been given product training by CES or a CEStronics partner. These personnel
personnel	are given detailed and specific information to prepare them for the required task.
	Particular characteristics of this target group:
	Knowledge of CEStronics products and experience in handling them (assembly,
	operation, etc.)

2 For your safety

2.1 Safety information

The AccessOne access control system described in this manual may only be operated by persons who are competent and qualified to do so. Qualified personnel have many years of professional experience in IT structures, administration and networks, and thanks to their experience in the management of master key systems or in-depth knowledge of a single master key system, are able to recognise risks and prevent potential hazards.



A blocked door can prevent help getting through or result in damage

Incorrectly programmed components can cause access to be blocked unintentionally. C.Ed. Schulte Zylinderschlossfabrik GmbH accepts no liability in the event that access to persons in need of help is prevented or material damage or any other damage occurs as a result of a blocked door.

2.2 Legal information

The purchaser is hereby explicitly advised that the use of the AccessOne access control system can be subject to legal and in particular data protection authorisation requirements and to the co-determination rights of the workforce. The purchaser and end user are responsible for the legally compliant use of the product.

2.3 System requirements

The minimum system requirements for AccessOne are based on the recommended system requirements for the Microsoft SQL Server.

- Operating system (server): Windows Server 2016 or later
- Operating system (PC): Windows 10 Professional or later
- RAM: at least 8 GB
- SQL Server: MS SQL Server 2016 or later; Express version can be used
- Hard disk: min. 1x 500 GB; 2x 500 GB recommended
- Network card

2.4 Data protection in AccessOne

Compliance with deletion periods

AccessOne features a parametrisable deletion process that starts shortly after midnight each day and erases data for which the deletion period has expired from the system. In particular, this includes movement data. The parameters can be set by the system user.



The deletion of personal logbook messages can be configured to comply with the General Data Protection Regulation (GDPR). The 'LogbookRewriteOffset' parameter specifies the number of days after which such messages are deleted.



Parameter	Description	Default setting
DateDeletedOffset	Delay period after which person datasets with a	3 days
	specified 'dateDeleted' date are finally deleted	
	from the database.	
VistorDeleteOffset	Delay period after which visitors are deleted.	183 days
EventDeleteOffset	Delay period after which completed events are	183 days
	deleted.	
AppointmentDelOffset	Number of days after which appointments and all	365 days
	dependent data are deleted.	
LogbookRewriteOffset	Number of days after which personal logbook	0 (not deleted)
	messages are deleted from logbooks.	
LogbookDelMessages	The number of the personal logbook messages	All access messages
	that should be deleted. Either individual numbers	
	or number ranges can be specified.	
LogbookLastRunTime	Date when the last deletion process was comple- Date of last executi	
	ted successfully.	

Data minimisation

The data required for operation and to perform the tasks is specified by the user. For everyday use of AccessOne, only the surname and a personnel classification (internal/external/visitor) are required for each person. The surname does not need to be the actual surname of the ID card holder. A pseudonymised name (e.g. 'MA_001') can also be used. The use of the surname is normally regarded as non-critical in terms of the GDPR.

Input control

AccessOne logs every data modification together with the workstation, user and timestamp plus the old and new value of the relevant data field.

Access control – data access control – system access control

In accordance with DIN EN 50133-1 access is defined as the action of a person entering or leaving a secure area. Control and regulation of such access is performed by AccessOne. Data access designates the logical processing of data in computers in terms of reading, writing, changing and deleting. System access is the logical introduction to using an information system or communication network. System access control is thus the automated checking of the access authorisation to an information system or network.

To enable the required monitoring and control, suitable technical and organisational measures must be taken by the client in terms of creating and maintaining the IT infrastructure (USB port, password guidelines, LDAP, etc.). AccessOne supports this with the option of assigning relevant user authorisations in the user interface.

3 About AccessOne

In its full version, the AccessOne access control system is a flexibly scalable access control management software suite for large premises with up to 200,000 users, 16,000 ID card readers and up to 100,000 offline locking devices. A version for small and medium-sized businesses is available with the AccessOne KMU licence. The access control system controls doors, barriers and other locking devices. The heart of the software is a user and authorisation management module that records all of the activities on the connected devices and monitors current processes. AccessOne is designed as an open system and can manage and control both online and offline devices. Communication is 128-bit end-to-end AES encrypted. Optional UPS and server redundancy concepts offer high levels of reliability and system security.



Offline locking devices



3.1 Function extensions

The following function extension	ons to the basic licence version of AccessOne are available:
ID card creation	AccessOne extension allowing custom card layout design using a graphics
Art. no. 348120V	editor.
Multi-Client function	The Multi-Client function enables defined parts of the system, such as doors
Art. no. 348121V	or persons, to be logically assigned to different, independent clients. These
	clients can manage the system parts assigned to them independently, but
	have no influence on the system parts assigned to a different client. Howe-
	ver, it is also possible for system parts, such as entrance doors, to be used by
	multiple clients.
Visitor administration	AccessOne extension enabling visitors to be logged into the system and
Art. no. 348122V	day passes with limited access to be issued. Visitors are logged in via a web
	browser.
Parking area management	AccessOne extension allowing the management of parking areas. Allows a
Art. no. 348123V	number 'n' of rented parking spaces to be assigned to specific tenants, while
	the remaining spaces are counted but are available for all other authorised
	users to use. Counting the number of parking spaces that are currently in
	use, with entry and exit readers, is mandatory for this function.
Time registration	AccessOne extension allowing the logging of arrivals and departures on
Art. no. 348124V	access readers and/or separate time registration readers and daily export in
	CSV format to a higher-level working hours management system.
Server redundancy	Adds a hot standby function to AccessOne.
Art. no. 348125V	
Third-party supplier admi-	AccessOne extension module for managing master data of external com-
nistration	pany employees without accessing the master data of in-house personnel.
Art. no. 348126V	This module enables clearance to be given to tradespeople working in the

electronic signature pad.

building and who require materials and/or an ID card for this purpose. Special approvals or necessary instructions can be stored and checked together with the validities. The external company employee confirms receipt of materials and knowledge of documents given to them by signing on an



3.2 Recommended procedure for initial setup of AccessOne

To reduce the burden for you as the user of entering large volumes of data when setting up the AccessOne access control system for the first time, we recommend that you perform the individual steps in a specific sequence. We make the distinction here between the system configuration of AccessOne by the system operator and/or a commissioned IT/administration specialist and that of creating devices, authorisations and person data by product-trained personnel.

The first steps must be performed by the system operator and/or commissioned specialist from the IT/administration sector:

Step	No.	Action
Configuration of AccessOne		Start the application and log in as the user (see 'Logging on' on
	(1)	page 16)
		Before you start to set up your AccessOne system, you must
	(2)	activate your licence within the system settings (see 'Configuring
		the system' on page 17).
		Once the system configuration is complete, create the different
	(3)	users so that each AccessOne user can later set up the system
		with their own allocation rights (see 'User data' on page 27).
		Define the location data of your AccessOne system. Then the lo-
	(4)	cation data can be allocated directly when setting up the devices
		(see 'Location data' on page 32).



Step	No.	Action
Create devices	(1)	First, create your online devices such as door controllers and
		readers. All of the readers can also be used as updaters for access
		media. This is a precondition for setting up offline devices (see
		'Online device data' on page 34).
		Once the online devices are set up, create the offline devices.
	(2)	This step is necessary so that you can subsequently define the
		authorisations with all of the created devices (see 'Offline device
		data (OSS-SO)' on page 54).
Create authorisation groups		First, set up the authorisation groups for the online and offline
and profiles	(3)	devices (see 'Authorisations' on page 60).
	4	The authorisation groups are integrated into authorisation profi-
		les. Now all of the necessary steps for your authorisation concept
		have been completed (see 'Authorisation profiles' on page 68).
Create person data	F	The authorisations that have already been configured for the on-
	(5)	line/offline devices can now be allocated directly to the persons
		(see 'Person data' on page 70).
		Use the card designer to print ID cards. This ensures that the
	(6)	card layouts are allocated to the person (AccessOne extension
		allowing custom card layout design using a graphics
		editor).
		You can also assign a company to the person (AccessOne exten-
	()	sion module for managing master data of external company
		employees without accessing the master data of in-house per-
		sonnel).
Subsequent modifications	>	All of the created data can simply be modified if changes are
		required (see 'Group changes' on page 83).

The following steps can be carried out by product-trained personnel:

4 Working with dialogues

Target group of this section:

- Personnel with product training
- IT/administration specialists
- System operators

AccessOne is operated via a dialogue interface with a consistent operating concept. All of the dialogues have the same structure so that a new user will quickly understand the system.

The dialogue interface has the same design as familiar Microsoft Office products. The buttons to select a dialogue (1) are located at the bottom left. Above this is the object selection (2), which lists the available data objects and varies depending on the selected dialogue. When an item is selected from the dialogue selection (1), the dialogue window (4) displays the details of this element on a tab in one or more areas (5). The data relating to a given data object (e.g. persons or devices) is summarised on a number of tabs, depending on the contents. Buttons in the toolbar (3) offer basic functions for the tab currently being displayed.



For every dialogue it can be defined whether a user has access to it and the level of authorisation (read, write, delete). If a user has no authorisation for a dialogue, the relevant button is not visible in the display. The same also applies for tab pages in the dialogue window.

Annothe - Jan Ada	(3)	toolbar				~
Champe New Copy Delete	Related Assignment)			-	
in t	See master data (15av 551) V	Weiking Designing Wildow	- 170 str. (4) d	ialogue windo	w)	
ball	t selection		name Gerner Inden			
Mulahi Web	The same		11 mains 			
(1) dialog	gue) "			(area	
Logbook	Automate Terrinit		Charter prevents to real that			
📄 Reports	Renter to part graph					
🥓 Device data	Asia Bahra		User provo		-	
ST OSS		cc		(P	
OSS Blacklist				(Jarea	
Luser data		>>				
/ Card designer						
ACLs	Nutif(coldine) of earth's		-			
1 Visitor / Appointments		<<		(
🗽 External employee				(j area	
O Workflow		35			-	
# Group changes						
System configuration						
Location data	User mailers		Wavestow PdJ-11517	All the set like setting	Events 0	Tenenut not active



Empty fields that are mandatory are highlighted red when saved. Tool tips provide additional information on the relevant element when the mouse is moved over it.

User master data	User ACL	Workflow	User groups	Web user groups	
User data					
Logon name:				Windows- User name:	
Person:				Auth. level:	+
Valid from:	Select a da	15 until:	Select a da 15	Languages	-
Web user:					is locked
LDAP login:					may approve authorizations 4-eye principle for the evaluation of logbooks

4.1 View mode – change mode

AccessOne distinguishes between view mode and change mode. In view mode, data can only be viewed but not changed, and are greyed out. In change mode, all buttons and input fields in a dialogue window are enabled. While in change mode, the selected dataset is internally locked to all other dialogue users.

4.2 Toolbar

Search

The input field for searches is situated at the left-hand end of the toolbar, above the object selection.



The SEARCH button in the menu bar is only active when the 'Person data' dialogue is selected.

Clicking the SEARCH button opens the 'Person Search' tab in the dialogue window. Additional search criteria are also available here (e.g. surname, name, company, personnel number, authorisation, authorisation profile, card number). The selection list in the input field is updated with each subsequent character entered.



AccessOne - Person data			- D X
Home			
Clear Execute Cancel			
No et la	Person search		
Last name First name Person	Person data		
Megolat 1	Last name:	First name:	
Mob RF- Stick	Company	Company 2:	(Description)
Mobelschloss System - M. Mustermann Max	Personnel no :	Number plate:	
2 Person data	Card no.	Version:	(only with sard no.)
Authorizations	Remark		
Authorization profiles	Further	055 Authorization	
🚡 Company data	Access mask:	COS Revisionarios	
Logbook	Authorization profile:		
🕒 Reports			

For the 'Person Search' tab, only the CLEAR, EXECUTE and CANCEL buttons of the search function are available.

Clicking EXECUTE refreshes the filtered selection list. Datasets can be selected and edited individually. Search terms remain active until you click CANCEL. Therefore if you have, for example, preselected a company in the Search dialogue, the selection list will only display persons linked to this company, irrespective of any further terms you may have entered in the search field above the selection list. This search criterion is only removed again by selecting the Search dialogue again and then cancelling the search. CLEAR deletes any content in the search dialogue and you can enter new search criteria.

	Home								
(ancel	T	P	New	Corry Corry		X	C) Reload	Assign	ment
H		chunge	1121	copy		June		AC	Ls
10 of 10					X	Orview	Mast	er data	Furthe

In the example shown here there are exactly two datasets with 'T' as the first letter. If no search criteria are entered, the display is limited to a maximum of 150 entries. This value can be adjusted in the AccessOne system parameters. You can temporarily suspend this restriction using the small button in the bottom right-hand corner of the search window. Then all of the datasets matching the search criterion are loaded into the selection list. If you do not enter a search term, all datasets in the database are loaded.

Change

Clicking CHANGE or double-clicking on the dataset in the selection list activates the input fields and buttons in the dialogue window on the right. The selected dataset is internally locked for all other dialogue users.

New

Creates a new, empty dataset.

Сору

Duplicates an existing dataset. Fields that must be unique to each dataset are automatically cleared.



Save

Saves and updates the dataset in the database. The database is then released for editing by other dialogue users again.



The current dialogue is automatically saved when you leave the dialogue page.

Delete

Deletes the currently selected dataset (highlighted blue). The action is performed following confirmation of a security prompt.

Refresh

Loads current data from the database and refreshes the view.

Assignment

Allocates the current dataset to a client. Only active if the client function is enabled.

5 Logging on

Once the software is successfully installed, you can log on as a user. To start the program, double-click the symbol on your desktop that was created automatically during installation.

Ð	Benutzername: Kennwort:	

For the first logon after installation, the following logon data should be used:

<u>User name</u>: admin

Password: admin

For security reasons, change the password as soon as you have logged on. To do so, go to the 'User Data' dialogue.

AccessOne - User data									0	×
Change New Copy Del	ete Reload Assignment									
dê.	User master data	User ACL	Workflow	User groups	Web user group					
admin Maju	ser data	admin			Windows- U	es næme:				
MaikEN	Persan:			1.00	'Auth-level					
MaikNL	Valid from:	Smieli	until:	Secto its (Language					
Web	Web user:						is locked	ulhonzations.		
	LDAP logini	(Fe					4-eye principle	for the evaluation of	logbooks	
📕 Logbook	Password data									
Reports	Password:	****			Dortfirmation					
/ Device data	Validity: Valid unbi date:	Days				- Ch	inge password at next	log in		
CSS	Member in user a	oups.								
SS Blacklist	User group				Use	r group	1	1		
😫 User data				<<	Aar	Internation of Con-	-			
/ Card designer	H				_					
ACLs				>>						
			_							

In the object search, select the logon name 'admin', then click the CHANGE button on top left of the toolbar. Create your own password. For best security, a password should be as long as possible and should include both letters and digits. You can use a password of any length. Re-enter the password to confirm it in the 'Confirmation' field.

If you wish to create a password that will be valid for a limited time, you have the option of doing so here. Confirm your change by clicking SAVE.

Creating additional users (see 'User data' on page 27) is described in detail later in this manual.



6 Configuring AccessOne

Target group of this section:

- IT/administration specialists
- System operators

To meet the requirements for setting up the access control system, you will have to modify a number of system parameters. You will specify areas and set up workstations. Additionally, you will define the reader and card formats to be used. Once you enter the user and location data, you have satisfied the requirements for configuring the devices and authorisations.

6.1 Configuring the system

6.1.1 Parameter

Shows the system parameters for your system.

AccessOne - System co	infiguration	2.0									-		x
Home													0
Change New	Copy Delete	O Reload											
ef adde (Parameter	Areas	Parking groups	Workstations	Reader formats	Catol analyse	Licensei	Card formats	Personnel classes			
Name	Category	Parameter											
EventBufferFileSize	AcMasterCom	Name-											
MacDataExpireTimespar	AcMasterCom	The second second											
MacEncryptionAlgorithm	AcMasterCom	Entegorya											
OfflineAuthRefreshPerio	AcMasterCom	Determine											
DateDeletedOffset	DeleteProcess	1 Desciptor											
VisitorDeleteOffset	DeleteProcess												
EventDeleteOlfset	DeleteProcess												
AppaintmentDelOffset	DeleteProcess	Value											
LdapDirectoryldentifier	Master	11											
LdapDistinguishedName	Master	10											
LogonTimeout	Master												
LockingTimeout	Master	12											
-D Workflow		1											
# Group chai	nges	1											
System cor	figuration	\mathbb{D}											
9 Location d	ata	Usen maiken	-	No describer	Work	station: INV-11537	All Lar and Mar	contine-	Events: 0	Timepu	t not a	cive	_

Explanation of parameters

Name	Explanation
EventBufferFileSize	Size of buffer file (MB) to store events for an individual
	MAC.
MacDataExpireTimespan	The time in minutes without a connection to the MAC
	after which the event buffer data becomes invalid.
MacEncryptionAlgorithm	Encryption algorithm for communication between Acces-
	sOne and MACs (default setting: none).
DateDeletedOffset	Time in days after which person datasets deleted via the
	dialogue are finally deleted from the database.
EventDeleteOffset	Number of days after which events are deleted from the
	database.
VisitorDeleteOffset	Number of days after which deleted visitors are deleted
	from the database.
LastRunTime	Time of the last process execution
(LastAccessProcess)	



Name		Explanation
LastRunTime		Time of the last process execution
(LockProcess)		
CardNoRecyling	Kartennummern	1= Reissue card numbers by searching for gaps left by
	wiederverwenden	deleted cards.
		0 = Issue card numbers consecutively.
DatabaseNumber		Identifier in dataset if more than one database is in use
		(00 until that is the case)
LockingTimeout		Time in seconds for which datasets currently being edited
		are locked. If the lockout is not renewed by the client wit-
		hin this period, the lock is lifted by the master process.
LogonTimeout		Time in seconds within which a client must renew their lo-
		gon with the master before they are automatically logged
		off.
NumberLogonFailures		Maximum number of unsuccessful logon attempts
ProcessLogfileAge		Maximum age in days of debug log files
ProcessLogfileSize		Maximum size in MB of debug log files
XmlDoorDataDir		Directory for OSS door data exchange
CardNoZeroes		Fill printed card numbers with zeros up to specified overall
		length.
CardToCodeAlgorithm		Algorithm for determining card numbers from code data.
		Standard: 0 = card number matches code data.
DialogTimeout		Standard timeout in seconds during which the dialogue is
		not used. If this time is exceeded, the user is automatically
		logged out.
EntitiesToTake		Number of datasets displayed in the selection list.
MaxPinLength		Maximum length of PINs (PIN, EMA1, EMA2)
MaxPinValidity		Maximum validity period of PINs in days
OfflineValidityTime	Offline-	Standard validity of an offline card in hours, minutes
	Gültigkeitszeit	(standard: 24.0).



6.1.2 Areas

AccessOne - System configuration									- 0	×
Home Home										0
Change New Copy	Delete Reload	_								
	Para eter Areas	Parkin groups	Workstations	Reader formata	Card analyse	Licenses	Card formats	Personnel classes	1	
4274										
Name	Area									
AW	Names									
IH										
<u>K1</u>	Detalphoe									
10	Fattlers									
124	Settingh									
Neutral	Parent.antim			- Qpt	ions:					
NV	Erre			CHE	ine men code:		nes saute			
055.2	- Chier			011	int area court		Generality (Mr.			
OSS Test	Company			Extra	im references					
\$1	100 million									
SV1	winz persona			0430	r bearing					
Tiefgerage	Max. stay time (h):					Revel area	counter at midnight			
Unbekannt										
				3rwf	tic light control via:					
				Ebr	tact bumber					
	2									

Every door in AccessOne leads from an origin area to a destination area. These areas need not necessarily be different. If your building is divided into a number of secured areas, an entrance might lead, for example, from an external secured area (ASB) to an internal secured area (ISB). However, a connecting door can also lead from one ISB to another ISB.

You select the origin and destination areas with 'Area entrance' and 'Area exit' respectively.

Settings

An area can be further subdivided under 'Settings'. For a 'Normal area', a minimum and a maximum permissible number of persons within the area can be specified. The maximum number of available parking spaces can be specified for a 'Parking area', for example.

6.1.3 Parking groups

(Only enabled if you are using the optional parking area management module, art. no. 348123V) Allows persons to be linked to a parking group. This group can then be assigned to a specific parking area.



6.1.4 Workstations

AccessOne - System configuration						- ø ×
Change New Copy Delete	Reload Assignment	_	_			
ef1	Parameter Areas	Parking grou, Workst	ations Ruder formats	Card analyse Lici	enses Card formats	Personnel classes
Name INV-11537	Warkstation Name:	_	_			
	Description Location, Room:					
	Configuration	[3e	conds)			
	Dialog reader:					
	Pinter code name		Keader Baudrate.			
	Printer coder driver:					
Workflow	Coder interface:		Encoder Baudrate:		-	
Group changes	Ennell biometric data:					
System configuration	UZ Rfsbck interface:		DS Ble stuck interface:			
Location data	Usen maiken	No sising reviser connected	Workstation: INV-11537	All Lac and Mac online	Events: 0	Timeput n

The various AccessOne clients and their exact Windows computer names are created in the 'Workstations' tab. This is used to define locally for each workstation whether a dialogue reader (e.g. an IdentBox) or a card printer with coding station is installed. The correct com ports must be set up for the end device in each case. You can read the com ports from your Windows Device Manager.

6.1.5 Reader formats

AccessOne - System configuration							- 0 X
Home	100						0
Change New Copy Delete	P Reload						
142	Parameter Areas	Parlong groups V	Vorkstation	Reader formats	ard analyse	Licenses Card for	mats Personnel classes
Name	Reader foresat			\square	-		
OSS-Desfine	Name: QS	S-Destine			et active formie	t	
cos-tege	Description: OS	S+Desfine					
	for protocal						
	Configuration						
	Card technology:	Mifare Desfire Ev1		Customer number: 0	ak Ø		
		Use MAD		User AlD: 0	h.		
	Mitaré MAD key Ac		-	Mitare MAD key B:			
	Mifare sector number.						
	Mitare key A /			Mitare key B /			
	Destine file read key: Destine application (D)	0x F75000		Destire foe write Key: Destire application key			
	Deshre key no:	+		Desfire file not	Ū.		
		Desfine key encryp	pted		Desfire key o	diversified	
- Workflow	Legicistamp			Legic stamp length			
🛃 Group changes		Serial as code nur	nber				
System configuration	Code number start:	72.		Length:	32	Formati	Big endian
	Version start:		_	Length:	-	Formatt	
Y Location data	W User: maiken	No dialog reader com	ected World	estation: INV-11537	All Lac and Mac	online Events: 0	Timeout not activ

Here you specify the reader formats to be read by the card reader of the door controller.



6.1.6 Card analysis

AccessOne - System configuration				- 0 ×
Home Home				0
R D D D H X	C) Reload			
1.91	Parameter Areas Parking gro	ups Workstations Reader form	m; ; Card analyse L enses. Card	formats Personnel classes
Name	Configuration		\square	
Dialog reader	Master tards: B	and the second se		
	Current card:	Refe		
	Analyse			
	Current card:	ayse		
	Description	Value		
 Workflow 				
# Group changes				
System configuration				
9 Location data	Usen maiken Ale dillog n	Workstation: INV-1153	7 All Lac and Mac online Events	0 Timeout: not ad

Master cards (e.g. LEGIC, IAM cards) that are important for using the write function of your dialogue reader (IdentBox) can be read in or deleted in the 'Card analyse' tab.

When the 'Analyse' button is pressed, locking medium cards of a previously defined card format are read out in detail via the connected dialogue reader.

In the 'Replacement cards' area, a defined number of replacement cards can be created in the database within the corresponding card number range.



6.1.7 Licences

AccessOne - System configuration					- 0 X
Home	1000				
BOBHX	D Releas				
	Pacameter Annus Parking ge	oups Workstations Reader formuts Card an rs	E Licenses	a lormate Personnel.c	haire
				/	
Loome	Activation				
	Please contact your distributor. You n	eed the name of the licenses to be activated and the signature of th	e target machine		
	Computer	signature 6499 6694 0461 1C/C 6386 /11D 15C3 3675			
	The received keys can be entered in t	he field 'Activation key' or being read as file by the 'Import' butto	n :		
	Activation	key.			
				- Import	
		1		- Income Constrained	
		Activate			
	Mifare syst	tem keys import.			
	License type: Pus flaved	highnight -			
	Id Paket name	Paket description	Available Acti	vated Expiring date	
	1 Base	1000 cards 50 readers, 50 offline locking devices, 2 workstations	0 1		
	2 Extension cartis	15.5 other readers (max, 200,00)	627 1		
	4 Extension readers	25 hurther readers (mail: 10000) 25 hurther offline locking devices (mail: 10000)	3798 270		
	5 Extension workstations	1 further workstation (max, 100)	97 1		
	6 Extension software updates	Software Updates for 1 more year (max: 100)	100 0		
	7 Extension card layout	Card and form layout creation	0 1		
	8 Extension clients	ACL Client ability	0 1		
	9 Extension visitor	Visitor dialogs	0 1		
	10 Extension parking area	Administrate parking places	0 1		
No. Contraction of the second s	11 Extension time recording	Administrate coming/leaving bookings	0 1		
La External employee	12 Extension workflow	Authorization workflow dialogs	0 1		
Part and a state of the state o	13 Extension server redundancy	Hot standby with 2. server	0 1		
• Workflow	14 Extension person import	Person data import from CSV file	0 1	1	
😤 Group changes	Limits: 11000 Cards, 7 Time recording	15 Reader, 5050 Offline lacking devices. 3 Workstations, 1 Card layou g. 1 Workflow, 1 Server redundancy, 1 Person import	d, 1 Clients, 1 Visitor, 1	Parking area, 1	
System configuration	Customer no.: 9999	Software updates until: 16.06.2022			
Location data	liese makes	Washiston IN/,11927 All	and Mar poling	Frank D	Tenanut est activa

The 'Licences' tab shows a list of program licences and their content.

The computer signature of your AccessOne server PC is required to activate a licence. Without licence activation, your AccessOne installation can only be used as a demo licence with restrictions.

There are three types of licence:

- A test licence with minimum system features, which is active as soon as the AccessOne software is installed.
- A demo licence that is time-limited and created on the basis of customer requirements. This licence type can be renewed twice. On expiry of this period, the demo licence automatically converts to a test licence.
- The purchased licence offers all standard functions.



6.1.8 Card formats

The formats required to describe a card at a dialogue reader, coding station (such as in the card printer) or an access control wall terminal (updater for access media) are defined on the 'Card formats' tab.

Only one card format may be active for each card technology (Mifare, LEGIC, etc.). Nevertheless, other inactive card formats for the same card technology can be created.

To correctly define a card format, it is essential that the AccessOne user is familiar with the possible settings of the relevant card technology. Since Mifare-DESFire, in particular, gives the user a lot of freedom to define the access rights, it is possible for cards to be created that cannot be used if the settings are contradictory. The following text indicates which parameters affect which properties of the card. It does not, however, replace the need to read the relevant NXP and LEGIC documentation.

AccessOne - System configuration		- 0 7
Home Home		
Change New Copy Detet	Retoal Assignment	
	Parameter Arese Parking groups Worksantions Reader formats Card analyse Licen s Card formats Pe annel classes	
Name	Tard Issued	
CFS.Master Ratteriell epict	solution and the second s	
CES-Master Battery Desfire)	Name: USS-Desfine assigned to personnel cleas	
CES-Master Spind (Legic)	Description: OSS-Format Milare Desfine Sea active format	
CES-Master Spind(Desfire)		
CES-RF-Master (Desfire)	Configuration	
CES-RF-Master (Legic)	Card states of the Darte Did - Hilling MAD Manager States	
CES-RF-Master Zeit (Desfire)	Land biornauge minare previe ov Di pre revez indiminister approaches	
CES-RF-Master Zeit (Legic)	Mittare MAD key 8 Proc Master key:	
OSS-Blacklist-Desfire	Participation Protocology Protocology 2007 Destructure Dr. F.	
OSS-Blacklist-Legic	Decise of architect Decise et all and the count of a co	
OSS-Desire	Applications: No. Name Description	
OSS-Desfire - Intervention	1 OSS-Applicati OSS-Application (Demo Keys)	
OSS-Destire Test Markus		
USS-Legic		
U&Z-Batteriewechsel	X Petrassion	
UK2-Battenewechsel (Legic)		
U87-Demontage	Numbern Mame: Description	
1187-Surfam	Key settings I Av Key settings 2 Bv Application ID: On	
U&Z-System (Legic)	Number Hants Number Party and Number	
	Key 4 Key 5 Key 5 Key 5 Key 6 Key 7 Key 7	
2	Key 8. Key 9. Key 9. Key 10 Key 11 Man	
External employee		
-	Key 12 Key 13	
Workflow	Segments: No. Name Description	
Group changes	hereagened	
System configuration	X Delar square	
A second second	Number Name Description	
P Location data	Un Function Length	

The parameters are set up at different structure levels:

- Parameters at card level
- Parameters at application level
- Parameters at file level

6.1.8.1 Parameters at card level

When a new card is created, the PICC master key is first changed from the standard value to the value defined here. Next, the properties that relate to the use of this PICC master key are set up. The settings are stored as the 'Desfire Config Byte' value.

This value is bit-coded and is interpreted as follows:

Bits 4 to 7 must be 0.

Bit 3 specifies whether this configuration can ever be changed in the future (even not by formatting the card).

- 0: The configuration can never be changed.
- 1: The configuration can be changed if the user has first been authenticated with the PICC master key.

Bit 2 specifies whether the PICC master key is required for creating or deleting an application or not.

- 0: An app can only be created or deleted with the PICC master key.
- 1: Creating an app does not require the key; deleting an app is possible with the PICC master key or appli-



cation master key.

Bit 1 specifies whether the PICC master key is required to query the contents of the card or not.

- 0: Query is only possible with the PICC master key.
- 1: No PICC master key required for query.

Do not pass the PICC master key to a third party. If you wish to allow third parties to create their own applications, a suitable setting for the 'Desfire Config Byte' would be 0x0f, for example. With this definition there is no need to disclose the PICC master key.

6.1.8.2 Parameters at application level

In accordance with the DESFire standard, key 0 is always the application master key (APMK). All other keys can be defined, but this is not necessary. It is recommended that you define at least one additional key so that a third party can gain access if necessary, without having to disclose the APMK.

Key settings 1 specifies what is controlled by the application master key. 0xE1 is an example of a useful value. **APMK application settings:**

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	BitO	
Change key access rights				Configuration changeable	Create/delete freely wit-	Free access to directory	Allow change to APMK	
Bit3	Bit2	Bit1	BitO		nout APMK	APMK		

At application level, the coding is interpreted as (selected AID is not 0x00):

Bit 7 to bit 4	Specify the access rights for making changes to application keys (ChangeKey command).
	0x0: Authentication of the APMK is required to change any key (standard setting).
	0x10xD: Authentication with the specified key is necessary to change any key. A change
	key and a PICC master key can only be changed after authentication with the APMK. For
	other keys, authentication with the same key is required.
	0xE: Authentication with the key to be changed (same KeyNo) is necessary to change a key.
	0xF: All keys (except APMK, see Bit 0) within this application are frozen.
Bit 3	Specifies whether a change to the APMK settings is permissible:
	0: Configuration can no longer be changed (frozen)
	1: This configuration can be changed following authentication with the APMK (standard
	setting).
Bit 2	Specifies whether authentication of the APMK is necessary before Create file/Delete file.
	0: Create file/Delete file is only permitted with APMK authentication.
	1: Create file/Delete file is also permitted without APMK authentication.
Bit 1	Specifies whether master key authentication is required to access the file directory:
	0: Master key authentication is required for execution of the GetFileIDs, GetFileSettings and
	GetKeySettings commands.
	1: The GetFileIDs, GetISOFileIDs, GetFileSettings and GetKeySettings commands can be
	executed independently of a prior master key authentication (standard setting).



Bit 0Specifies whether the APMK can be changed:0: The APMK can no longer be changed (frozen).

1: The APMK can be changed (authentication with the current APMK required) (standard setting).

'Key settings 2' is used to define the number of keys valid for this application and the type of encryption used for access to this application.

The 'Key settings 2' parameter defines a group of settings:

Bits 03	The number of keys that can be stored within the application for cryptographic purposes.
	A maximum of 14 keys can be stored within a MIFARE DESFire EV1 application. An applica-
	tion can also be created without keys.
Bit 4	Reconfigurable function unit (RFU) must be set to 0.
Bit 5	Specifies the use of 2-byte ISO/IEC 7816-4 file numbers for files within the application:
	0: No 2-byte file numbers are supported within the application.
	1: 2-byte file numbers are supported within the application.
Bits 67	Specifies the cryptographical method of the application:
	00: specifies DES and 2K3DES operations for the entire application.
	01: specifies 3K3DES operations for the entire application.
	10: specifies AES operations for the entire application.
	An example of a valid value is 0x82 where two keys have been entered for the application.
	ISO/IEC 7816-4 is not supported. Bits 4 and 5 must therefore be 0. AES is normally used for
	the encryption.

6.1.8.3 Parameters at file level

For the comm and file settings, convenient selection boxes are provided accordingly. As regards to the access rights, you must specify which of the application keys has read or write access for each file and which key can, if appropriate, change this particular (access rights) setting (see table).

If, for example, you wish to allow reading and writing with key 1, but that these settings can only be changed with key 0 (APMK), the value for these rights would appear as follows: 0x1110.

Setting a value to 0xe will cause the communication to change from 'encrypted' to 'unencrypted'. This may in turn conflict with the application settings.

MSBit												LSBit
b15		b12	b11		b8	b7			b4	b3		ь0
	R			Ŵ			R	&W			Ċ	
	\sim			\leq				, · · · ·			\sum	
					3	1						
				H	ex	K	еу]				
				0:	x0	0)					
				0:	x1	1						
				0:	x2	2	2					
				0	x3	3	3					
				0	x4	4	1]				
				0:	x5	5	5					
				0:	x6	6	5]				
				0	x7	7	7]				
				0	x8	8	3					
				0	x9	9)]				
				0	xa	1	0]				
				0:	xb	1	1					
				0	хс	1	2					
				0	xd	1	3					
				0	xe	"fre	e"	←	1			
				0:	xf	ne	ver	←	2			

 $^{\scriptscriptstyle 1}$ no authentication possible

² no access



6.2 User data

In the first step, you create different user groups as required, with individual dialogue authorisations. The created user groups are then assigned to individual users on the 'User Master Data' tab.

6.2.1 User groups

Dialogue rights in groups are created and summarised on the 'User Groups' tab. The dialogue rights in the Read – Change – Save – ACL (optional) columns can be enabled/disabled simply by clicking them.

To facilitate the process you can select and click multiple cells at the same time by pressing and holding the mouse button. The individual entries in each cell are then reversed (Yes>No and No>Yes).

You should use a meaningful name and provide a description for the group.

Clicking the CHANGE button selects the relevant function and highlights it green. Clicking the SAVE button saves the specified authorisations in the system.

In the following example, the 'Reception staff' user group is created and the rights of an employee at the reception of the main building are restricted to creating and modifying person data. The employee can, for example, change person master data and use the ID card and lockout functions in the overview dialogue.

ar New Copy Delete	Reload Assignment									
		6								
	Liser master data User AC	1 World w User groups	W/ USET GT	oupe						
				-					_	
	Group data									
mployee	11	(married								
yet reception										
istrator	Courses Probati	and the second se								
	Diakua riahts									
	through the second second			_				-		
	Dialog function	Dialog page	Read	Change	Delete	ACL				
	ACLs	ACL Stammdaten	-	-	Alte	Nai		-		
	ACLs.	ACI, Einträge	1.0	A	No	Ne				
	Benutzerdaken	Benutzerstammdatzn	-	200	Ne	file				
	Benutzendalien	Benutzer ACI		in the	(des)	No				
	Benutzentlähen	Workflow	1.0		169	310-	_			
	Benutzentlaken	Benutzergruppen	100	1 mar	Thu:	No.				
	Benutzerdalen	Web-Benulbergruppen	1.0		THE .	No				
	Berechtigungen	Berechtigungen	-	No	1.64	No				
	Berechtigungen	Zeitmodelle	-	No.	tio.	No				
	Berechtigungen	Tagesmodelle	-	No	No	No	_			
	Berechtigungen	Sonder- und Feiertage		No -	230	No				
CC BlackEat	Berechtigungen	Zutrittsmasken		PL0	240	No				
755 Blacklist	Berechtigungsprofile	Online	100	140	Piler	No				
	Berechtigungsprofile	CSS		No	Na	No				
lser data	Berechtigungsprofile	Zutrittamasken		100	940	har				
	Berichte	Berichte	100	1	him	No				
ard designer	Berichte	Personen	1.00		NE	No		1		
and assigned	Berichte	Personenbarechtigungen	100	100	IND.	Ne				
Cl.	Berichte	Berechtigungen in Profilen	-		Ne	No				
CLS.										

Members of the 'Reception staff' group should not be granted access to the ACL here to ensure that they cannot add persons to other access lists. The members of this group only have read access to all of the master data, enabling them to answer questions about ID cards and authorisations if necessary.



Management and/or administration employees should be authorised to access the person data of employees permitted to enter the building.



6.2.2 User master data

Home Change New Copy Delete	Relaat Assignment			×
	User master data Use ACL We	ondītaw User groups V	Vels user groups	
Name	Uier data			
admin	Lagon name		Windows- User name	
Maik	Person		Auth. level	
MaikFR.	Valid from: Getes b ou [15]	until: [massade [1]]	Language	
Web	Web user:			is locked
	(DAP login:			may approve authorizations 4-eve principle for the evaluation of logbook
	Password data			
	Password: ****		Confirmation:	
	Validity: Days			
Reports	* Valid until date: Sever and T		() ()	unge pansword at next log in
/ Device data	Member in user groups			
🖌 OSS	User group		User group	
St OSS Blacklist		<<		
🤽 User data				
📝 Card designer		>>		
👔 ACLs	Notifications of events			
Le Visitor / Appointments	Event type		Event type	
🗽 External employee		<<		
-🌣 Workflow			1	
😤 Group changes		>>		
System configuration	Ilser MaivEN	Workstati	og INV-11537	Evente 0

Now create users who are permitted to log onto AccessOne.

User data

Assign a logon name. If the Windows user name is specified, the AccessOne software uses this for automatic logon (single sign-on). The person can be selected from a list. If the user profile should have only restricted validity, a from/until date can be specified. The user is automatically locked out when this validity expires. A user can also be manually locked out at any time with immediate effect (to do this, enable the checkbox).

In this screen the user can also be assigned the '4-eye principle for the evaluation of logbooks' attribute, which means that in order for detailed information from the logbook to be displayed, another user with this authorisation must also be logged in.

Similarly, the 'Approve authorisations' right can be assigned to the user. This right is required for certain authorisations that call for self-activation.

Password data

Assign a password to the user. You can specify a restricted validity for a particular period of time or simply state a 'Valid until date'.

Enable 'Change password at next log in': Once the user has entered their logon name and assigned password in the input mask for the first time, they will be asked to enter a new password and to confirm it. You can enter a password with any number of characters. The maximum password length can be set in the system. Member in user groups

Allocate the dialogue pages and functions that the AccessOne user is permitted to see or edit after logging on. These dialogue rights are defined in advance for so-called user groups. Further information is available in section 6.2 'User data' on page 28.



Authorisations for events

Allocate the events that the AccessOne user is permitted to see or edit after logging on.

6.2.3 User ACL (ACL Client ability)

(Only available if data separation is implemented.)

Access control lists (ACLs) can be allocated to dialogue users here. The ACLs can be set up and modified. This requires that the ACL function has been enabled by the administrator.

AccessOne - User data		- 🗆 ×
Home Home	c	
Change New Copy Delete	Reload Assignment	
	User master ata User ACL Wor low User groups Web user groups	
Hame		
admin	Logon name Maile	
MaikEN	Person	
Maik#R		
Markki. Web	Assigned ACIs	
	ACL ACL	
	Velbert << Kolm	
	Address Contary Di	
Reports	and include ()	
and the property of	i 🗟 Gets right to read	
Device data	Girds right to write	
220 4	Ciety agent to device	
8 033	adzimatically in the ALL	
St OSS Blacklist		
👪 User data	25	
/ Card designer		
9		
JI ACLS		
-🌣 Workflow		
# Group changes		
System configuration	User-MakEN Wholehalterer 90/v21527	Events 0 Timenational active

The ACL Client ability function is recommended if one AccessOne installation/database serves multiple customers (clients) and each customer can only view and edit their own data. Datasets that are not allocated to a specific client remain available to users from all clients. These parameters must be edited by a higher level person (system administrator). The management and system administrator should always be given master rights or additional rights. Employees, such as those at reception, should have their own sub-system for the access control system set up so that they can view, edit and delete master data. Users of a sub-system, such as the 'Reception staff' group, should, for example, not have access to the ACL function, as they could otherwise add persons to other access lists. Authorisation to read out master data is sufficient for users of this sub-system.

Where an AccessOne user only has one access list (ACL) assigned to them, they can only allocate the authorisations that are contained in that particular ACL. The AccessOne user can thus only issue authorisations to members of the 'Reception staff' group for doors allocated to the reception area of the building. Other doors are not displayed in the selection list.

Members of the 'Reception staff' group can view, edit and delete these authorisations but cannot add them again. They can only be added by the system administrator or another person with the relevant access or allocation right. It is at the discretion of the user to divide the data up in a way that is practical and in accordance with their specific (security) requirements.

Workflow

The 'Workflow' tab allows workflows to be created for certain actions that must be performed, e.g. where approval from a superior is required.



6.2.4 Assigning datasets to access lists (ACL)

If access to data already entered into the system must subsequently be restricted, that data must be assigned to an ACL using the ASSIGNMENT button.

Important note: Data not assigned to an ACL is visible to everybody.

C AccessOne - Device data							- D ×
Home	54 - C						
Change New Copy Delete	Reload Assignment						
DMS Heal Mac	LAC master data	IO-Module Reads	er Access-Po	int		_	
Lat Main entrance	ACL Assignment					×	
D Em Side entrance	assigned ACLs			not assigned AC	Ls	and a second	
	Name	Description	**	Name Velbert Köln	Description Standort Velbert		
Authorizations							
Authorization profiles			1			111	
🚡 Company data			>>				
Logbook			_		1 203		
📄 Reports				29%6	Lancei		
Device data	D						
oss	1. pretnost	Datasec	Baudirate		Key		
SS Blacklist	2. protocol. 3. protocol:	CES-FastCrypt	Baudrate.	THEVIL	Key.		
🎎 User data	4, protocol.	CES-FastCrypt	Baudrate:		Key.	E.	
Card designer	User, admin	Normalog reader co	nnected Workst	ation: INV-11537	Lac D Mac offline	Events: 0	Timeout not active

Recommended procedure and sequence

Start with the doors in the 'Device Data' dialogue. To do so, click the ASSIGNMENT button in the toolbar. Select a door from the selection list on the left and assign it to the appropriate ACL. Next, click SAVE CHAN-GES. The selected object is now highlighted with a coloured bar.

Proceed in the same way for the 'Person data' and 'Authorisations' dialogues.



6.2.5 Web user groups

Search Change New Copy	Delete Reload Assignment	master data Cards. Authomitations	Capture pittur	e Lockouts	Access masks	OSS.
Last name First name Personnel Spind-Mast	Last name: Company: Department:	First name: Company 2: Date of birth	e.			
	Location Current area: Unknown Last entry: 29.06.2021 13:56 Packing area: Unknown	ACL Assignment assigned ACLs		not assigned ACL	i.	×
Person data	Inds	Name Description		Name Velbert	Varne Description (elbert Standort Velbert	
Authorizations	Identification at date of first card issue	-		Köin	-	
Authorization profiles	Number Version 100 0					
Company data			100			
Logbook	Lockouts		35			
Reports	Lockout Reason	4 L				
Device data				Save	Car	ncel
				~	Delete	

(Only available in conjunction with the Visitor Administration licence module, art. no. 348122V.)

This area links together web pages for web-based visitor registrations and the allocation of external company employees to web user groups.

Information about users and their group memberships can also be provided and added to the system via the lightweight directory access protocol (LDAP). LDAP enables information in an LDAP directory to be retrieved.



6.3 Location data

The location data allows you to map all of the object structures relevant to the access control system. The structures are displayed concisely in the form of a tree.



Enter the location data as completely and in as much detail as possible, as it is subsequently used to set up hardware components.

If multiple locations have been created, the 'Location Search' tab is helpful. Click on 'Locations' in the tree to display all of the created locations, sorted by type. Double-click a location in the list to open the location in the tree on the left.

6.3.1 Creating a location

AccessOne - Location data				-	a x
Home Home					
Change New Copy Delete Control Velbert Velbert Manu-Duilding	Relead		_		
Area 1 E123	Name - Velbert Service	Description Velbert Service	Type Object Area		
🛓 External employee	Area 1 E123	Main-Building Area 1. E123	Floor Room		
• Workflow	E123	E123	Door		_
🛃 Group changes					
System configuration					
Location data	User admin	Workstation: INV-11537	Events: 0	Timeout: not a	ctive

Select 'Location Data' in the dialogue selection. The 'Location Search' tab opens and the object, area, building, floor, room and door data are displayed hierarchically in the structure tree on the left.

An item can be entered or edited by clicking the NEW or CHANGE buttons on the relevant level.

Object

Define an object name for the location in which areas, buildings, doors, electronic cylinders, readers and offline devices are situated. More than one location can be created at the object level.

Area

Define names for areas within the object (e.g. 'Production', 'Development', 'Accounting', etc.).

Building

Define a name for the building in which all of the areas of the object are located (e.g. 'Building 3.1') and specify the address and contact details.

Floor

Enter the floor name and floor number in which the doors, electronic cylinders, readers and offline devices of the main building of your object are situated, e.g. 'Ground floor'.

Room

Assign names for the rooms on the same floor, e.g. '0.12' and configure the rooms on the basis of responsible persons, usage and trade.

Door

Enter the name of the door of the room, e.g. 'Door 0.12 external'.

7 Configuring devices

Target group of this section:

• Personnel with product training

Setup of devices begins with the master controllers on level 2. After this the door controllers on level 3 are configured and the I/O modules are created. Finally, the connected online and offline devices are set up on level 4.

AccessOne – the 4-level concept



In hardware terms, AccessOne is based on a four-level concept that forms the basis for practically unlimited scalability. The application and database server processes run on Windows Server operating systems and on an installed SQL server. In most cases, the server software runs in a virtual environment (level 1). The master controller distributes the data to the door controllers and provides all functions at the levels above the individual door controllers (level 2). The master controller does not need not be physically present as a standalone component; it can also be virtualised just like the server software. The master controller is linked locally to the door controllers via a network (level 3). Each of the connected door controllers is autonomous and, once the data has been loaded, it has access to all of the authorisation data for a person, including offline data. All of

the access decisions are thus made locally (level 3). The readers are connected via a RS485 interface (level 4). All of the readers can also be used as updaters for offline devices.

CEStronics

7.1 Online device data

7.1.1 Displaying the device overview

Accessione - Device data									L	_
Home										
Change New Copy Delete	Reload			_	_	_	_	_		
CES Terminal			Ali	×.						
PM	Device	Type	State	Program	Power	Sabotage	Mode	State		
PHG Terminal	Mac	MAC	Online	Unknown	1	1	1			
D EM SOC	- Aufzug 1	LAC	Unknown	Unknown	Unknown	Unknown				1
Side entrance	+ IO Modul: 6	IO-Module	Unknown		Unknown	1	1	1		1
	- Main entrance	LAC	Utilities	Unknown	Unknown	Unknown				7
	- CES Terminal	Door	Diffines			1	Unknown	Unknow		7
	- CES Leser 1	Reader	Unknown		Unknown	Unknown				-
	- PHG Terminal	Door	Linknown				Unknown	Unknow		-
	- Infoterminal	Reader	Uningwn		Unknown	Unknown				1
	- PM	Door	Olline			1	Unknown	Unknow		7
	- Eingangsleser	Reader	Uningwa		Unknown	Unknown		10000		7
	- CES Leser Modul	IO-Module	Unknown		Unknown					7
	- IO Modul: 1	IO-Module	Unknown		Unknown					-
Reports	- CES URC	Access-Point	Disknown		Unknown					-
	- SDC	LAC	Unknown	Unknown	Unknown	Unknown				1
Device data	- test1	Door	Unknown				Unknown	Unknow		1
a solve a summer	- Test CES	Reader	Unknown		Unknown	Unknown				1
			A company of the second se							

AccessOne provides a device data editor for the creation and parametrisation of devices. This shows the devices in a tree structure in the object selection on the left. The top entry is the Data Management System (DMS), and the devices are arranged beneath this. All of the data changes and all of the messages from door controllers (TSG1, TSG8, AMC or LAC*) are completed here. This is therefore also where the status messages are interpreted, stored in the memory and displayed.

Click on 'DMS' entry to view the status of all the devices in the overview. The 'DMS' entry cannot be deleted and a second one cannot be created.

The status of an individual device (online or offline) is also displayed in the detailed view for the device.

The dialogue window shows the status of all the available devices in list form. This view is not refreshed automatically. To refresh the list, click the REFRESH button. A search window is situated to the left above the object selection. When letters are entered here, the list beneath is filtered by all of the devices that contain these letters. They do not have to start with these letters. To simplify the search, no distinction is made between capital and lower-case letters. The names of the devices are shown in a blue font, which in AccessOne generally means that double-clicking on the name will take you directly to the tab for that entry. In the centre there is a further filter option, by device status. If, for example, you wish only to view the devices that are currently online, you select 'Online' from the drop-down menu. Right-clicking on the name of a door shows the available control commands that are permitted for that door.

* TSG = door controller, AMC = access modular controller, LAC = local access controller



7.1.2 Creating a master controller (MAC)

To create a new master controller (MAC), select the 'DMS' entry in the tree structure and click the NEW button.

ccessOne - Device data					- 🗆 × -
Home					6
Corcel D D D R	0				
6	MAC master data				
	MAC				
	Narrez:				
	Description:				
	Location, Room:	E123 - E123			
	Ext. references				
	Settings				
		🗹 Active	Status:	200	
	Ip address:		Port	16100	
	lp addr. next MAC		Port next MAC:	16110	
	Debug level:	0 ~	Encrypt		
Reports	Firmware	MACVOUTIZIP	Offine system:	USS	
Device data	Mac address Inventory number:				
OSS	Date of installation	s Select a date 15			
	Serial number:		Options:		
OSS Blacklist					
User data					
Card designer	User admin	No date made and Workstation INV-115	37 1 Lac It Mac eff	Events: 0	Timeout: not active

7.1.2.1 MAC master data

An empty MAC tab now appears on the right, into which you can enter the required data. Each MAC requires a name; this should be chosen so that it describes the area of responsibility of this device. One MAC is normally sufficient for a small installation. For larger installations, one MAC per building complex is common. It therefore makes sense to name the master controller after the building it serves. An individual MAC can manage up to 32 access modular controllers (AMC).

You can also add a further 'Description', e.g. the exact installation location. The 'Location' selection box provides a list of the locations configured thus far. In a new system, only the location 'Unknown' is available. You can complete this list with additional locations using the 'System Configuration' > 'Locations' dialogue (see 'Configuring the system' on page 17). For applications in which the access control system is distributed over multiple locations, we recommend that you create these locations beforehand and then simply select them from the list when creating devices. Depending on the type, the location data contains additional information, such as the address of a contact person and telephone number, which is useful in the event of a malfunction.

An IP address and a port number must be specified for every MAC address. The IP address of the MAC is detailed in the network configuration on the MAC. You can also open a command window (cmd. exe) on the master controller and enter the 'ipconfig' command. The IP4 address shown for the LAN adapter is the IP address of the MAC. If you have any questions, please contact your network system administrator.

On newly installed master controllers, the port address is set to 50100. This address can be freely modified, but must be identical in the MAC configuration (Datasec\Mac\config\MacConfig.ini) and in this device data, as no communication can otherwise be set up.

The 'Debug Level' field is an aid for the manufacturer to generate detailed error logs in the event of a malfunction. The higher the debug level, the more extensive are the log entries that the master controller records for all of the actions. Ensure that the value is not higher than 1, as this may impact the performance of the



device.

The 'Encrypt' checkbox lets you specify whether or not the communication between the DMS and the MAC AES is encrypted. Encrypting the data slows the speed of establishing connections and then has a minimal effect on the throughput when exchanging data.

The 'Firmware' field allows the new software version to be entered if an upgrade is performed. This is automatically distributed to all master controllers and activated. Important: Each MAC has its own firmware.



You should only change the preset value if you have received an appropriate update from CES. If card readers with the update function for offline systems are operated from your MAC, you must set this up when creating the MAC. In this case the choice of firmware(s) for use with the MAC will change. Any **subsequent** change to this MAC function is **not possible**. In such cases a new MAC must be created in the DMS and the LACs that have already been assigned must be ported to the newly created MAC.

You can also, optionally, add the MAC address, an inventory number and the installation date to the device. Please note that the MAC address can be important if your network only serves configured MAC addresses to prevent unauthorised persons connecting to your network.



A checkbox is provided for every device and every door, by means of which the device is activated. Only when this checkbox is selected will the device be loaded with data and started. The devices can thus already be configured and then only set as active following installation. Advantage: non-activated devices are not monitored by the system. Pre-configured but not activated devices are therefore also not reported as faulty devices. Overall, up to 32 local door controllers can be connected per MAC.


7.1.3 Creating a door controller (LAC)

7.1.3.1 LAC master data

AccessOne - Device data								-	×
Home Home									
B D B H X									
Change New Copy Dele	te Reload Assignment								
ES I	1								
MET Mar	LAC master data	IO-Module	Reader	Access-	Point				
E Aufzug 1	LAC								
	Name	Main entrance							
D Side entrance	Description.	Musterholfer Pl	w:						
	Locetion, Room:								
	MAC-	Wac							
	Ed. reférence:								
	Settings	The					-		
		M ACINE				Statut-			
	LAC type:	156 8/Compac	1			Dest	10003		
	Debus looth	0				Farmet	i uuui		
керопс	Firmware:	756V1922.6IN				Offline system	2		
Device data	Mat address.					Offline area	1 - OSS Test		
beriet data	Inventory number					Date of installatio	ne 08. (d. 100.000		
• OSS	Senial number	26280029				Options:			
OSS Blacklist	Bus								
	1. protocol	Datases	Ba	audrate:		Ney:			
User data	2. protocos	PHS CAPI	Ba	audrate	19200	Key:			
Card designer	ä, protocok	CES-FastCrypt	Ba	sudrate:		Keyt			
ACLe	4. protocol.	CES-FastCrypt	Ba	sudrate:		- Kinje			
ACLS	Contacts	-	_		and the second second		Marca and	 - Contractor	 _

Local door controllers (local access controllers, LACs) are each created under the MAC to which they are also connected. Select the required master controller with the mouse and click

New.

The dialogue window now displays the tab for a door controller.

Each LAC requires a name and a description. Proceed here in the same way as for the master controller (MAC). In this case it is also sensible to choose a name that gives an indication of the scope of responsibility. The description further enables you to state the exact installation location.

tungs	Active	Status:	Offline
LAC type:	TSG 8/Compact		
lp address:	TSG 8/Compact	Port:	10001
Debug level:	TSG 8/Elevator TSG 1/SDC	Encrypt:	
Firmware:	AMC2_4R4 (Bosch)	Offline system:	~
Mac address:	AMC2_WIE (Bosch)	Offline area:	1 - OSS Test 🔍
Inventory numbe	n	Date of installation:	03.12.2020 15
Serial number:	26280029	Options:	

AccessOne supports door controllers from various manufacturers. Under 'LAC type', select the hardware you are using. A mixture of controllers can be used within the same installation.

- TSG 8/Compact (Art. no. 348007V) central access controller for up to 8 doors with up to 16 readers
- TSG 1/SDC (Art. no. 348008V) central access controller for 1 door with up to 2 readers
- AMC2_4R4 with 4 RS485 connectors for up to 8 doors
- AMC2_WIE with 4 Wiegand interfaces for up to 8 doors

Specify an IP address for the LAC that can be reached from the MAC. The port address is preset to

10001 and should not be changed. To set the IP address on the door controller, select the appropriate configuration for the door controller.

CEStronics

You can also, optionally, add the MAC address, an inventory number and the installation date to the device.

The 'Encrypt' checkbox lets you specify whether or not the communication is AES encrypted. Encrypting the data slows the speed of establishing connections and then has a minimal effect on the throughput when exchanging data.

The 'Offline system' checkbox means that the AMC detects when offline systems are being operated and an updater is available.

The relevant protocols, depending on the hardware and interface, can be specified here.

er: admin	Wiegand	connected Wor	kstation: INV-11537	1 Lac. 0 Mac offline	Events: 0
1. Firmware:	Datasec Nedap	2, Firmware:	a l	3. Firmware:	ų
Logic OS Eirmungen	CES-FastCrypt				
Special function:	PHG Crypt	*	8	Contact number:	
Fault:	V-Bus Aperio			Contact number:	
Sabotage:	L-Bus	~		Contact number:	
Contacts	DE-Bus			A DESCRIPTION TO	
4. protocol:	CES-FastCrypt *	Baudrate:		Key:	396
3. protocol:	CES-FastCrypt **	Baudrate:	*	Key:	
2. protocol:	PHG Crypt ~	Baudrate:	19200	Key:	jas
1. protocol:	Datasec ~	Baudrate:	1.99	Key:	
Bus					

A checkbox is provided for every device and every door, by means of which the device is activated. Only when this checkbox is selected will the device be loaded with data and started. The devices can thus already be configured and then only set as active following installation. Advantage: non-activated devices are not monitored by the system. Pre-configured but not activated devices are therefore also not reported as faulty devices. Overall, up to 32 local door controllers can be connected per MAC.

The 'Reports' dialogue selection contains a device list that provides the relevant hardware documentation data for all of the devices. If all of the data is entered, the system can provide complete system documentation at all times.

7.1.3.2 IO modules

The door controller properties section also includes a tab for IO modules. Each local door controller requires hardware components to monitor input signals (e.g. door status signals) and to issue control commands. These are known as the input-output (IO) modules of the LAC. An IO module has several input circuits to check whether an external contact is open or closed.

AccessOne treats IO modules as separate modules, even if the relevant hardware is in fact contained in the door controller or ID card reader. This makes it possible to freely allocate signals across all available IO modules.

AccessOne can determine whether the IO module concerned is an onboard module of the LAC or a separate IO module. The IO module provided onboard is set up by default when the LAC is created. Separate IO



modules must be added manually with their relevant bus address. Signal programming of the IO modules is performed individually at a later stage when the respective doors are configured.

Go to the 'IO modules' tab to configure the hardware for the inputs and outputs of the door controller.

🐔 AccessOne - Device data					- 🗆 X
Home					U
Change New Copy Delete	Reload Assignment				
DMS Imma Mac The Aufron 1	LAC master di a IC	-Module Fader Access-Point			
CES Terminal	LAC:	Main entrance			
PHG Terminal	Name	Description		Address	
Side entrance	IO Modul: 1	Onboard Konlakte		0	1
	CES Leser Modul	CES Leser Middul		3	
					New IG-Mothie
					X Deste O Massa
	10-Module				
	Name	10 Modul: 1	Status-	-	1
E Reports	Descriptions	Onboard Kontakte		_	
Device data	Location Room:				
1 055	Settings				
a 033	Modul address:	0	Gid / Did:	D	
SS Blacklist	Type;	AMEIO	Debug level:	0.	
Se Licor data	Number entrances:	8	Number evits:	10	
Ser uata	Serial number:		Encrypt		
/ Card designer	External reference		Firmwares		
18 ACLs	. User admin	No dialog reader connected Workstatio	n: INV-11537	fac offine Eve	ents: 0 Tin

If you have selected a door controller that already has inputs and outputs integrated in the device, this IO module is automatically created when you move to this tab.

To create a new IO module, click the 'New IO Module' button and complete the relevant input fields. The module address for internal contacts is 0.

Select 'AMC-IO' as the type if you have chosen an AMC as the door controller. If you are using a TSG central access controller, select 'TS2' as the type for a door controller module with four inputs and outputs and two reader interfaces, or 'IO8' for a relay board with eight inputs and outputs. For separate door controller modules that are connected to the reader bus, enter the bus address that has been set and select the type 'TSM'. TSM door controller modules have two inputs and two outputs (note: this varies depending on the version/ type). You should enter only the actual number of inputs and outputs that are available, otherwise control commands issued for relays that do not exist may result in error messages.

1

Up to 64 input signals and 64 output signals can be controlled by each door controller. The distribution to IO modules has no relevance, provided that the address range of the reader bus, with a maximum of 16 subscribers, is not exceeded.

CEStronics

7.1.4 Creating a door

7.1.4.1 Door master data

To create a door on a door controller (LAC), select the appropriate door controller from the selection list on the left and click the NEW button. The window now displays the properties page for a door controller on the right.

VIS	Door master data Reader 1	Pacameter P	Farameter I	Parameter O			
INCO Mac	New						
A Em Main entrance	Depr						
	Description CES Terminal						
PHG Terminal	Location Room: E123 - E123						
5 Em Side entrance	LACI Main entrace						
	Esti réference:						
	Settings						
	Type:	R Active	with an induction of a	adar field one direction			
	Dournumber:	3	and engance in	ton control over one could			
	Door smith time:	40	(0,1 s)	Door strike time min	10	par (a)	
	Door inertita timie:		10.1 st	Door pini		them.	
Reports	Betweistmodus	Normal mode					
	Debug level:	0					
Device data	Alexa						
OSS	Max door open hote before alarmi	200	ints.	Door incealarm!	100	milei	
OSS Blacklist	Alam suppression time	0.	(a) (a)	and the second			
	Suppress Octor open too long			Suppress (Doprintrusion)			
User data	Time models						
Card designer	Time model without PIN.			Time model permanent open:			
				- I - and the later is a second			

The general properties of a door are defined in this tab. In addition to a meaningful name and the location, the type of the required door is also specified. The type determines how the access sequence is arranged and which input and output signals are used.

AccessOne provides pre-configured door models that cover all of the standard tasks performed by a door. Additional, special door models that meet customer-specific requirements can be added if required. Select the appropriate type for your application. In the following example, a simple entrance door used in only one direction is selected.

AccessOne - Device data			- 🗆 X
Home Rome	OR		U.
Cancel Save	- Ale		
DAS Mar Mar Mar Mar Mar Mar Mar Cas Mar Cas Mar Cas Por Cas Por Cas Por Cas Soc Ext Soc Ext Soc Ext Soc	Deor master data Reader 1 Deor Name: CES Terminal Description. CES Terminal Location. Room: E123 E123 LAC: Main entrance Ext. reference:	Paraméter P Paraméter 1 Paraméter 0	
	Settings Type: Door number: Door strike time: Door verta time: Betnebenodar:	Active Door/turnstile with entrance reader. Only one direction Atam anning (PRG/F6) Door type Kone call reader Door with input and a styper reader. Both directions Door with vinuut office mode Doorkunstile with entrance reader. Only one direction Exercise of a conder	
це керопз	Debug level:	Entrance foyer	
🖌 Device data		Info terminal with display reader. (One direction) Input with arming without keypad(hold card in front for 3 seconds)	
🖌 OSS	Alarm	Parking entrance (Pool/Fix Parker) Parking interance with count	
OSS Blacklist	Max door open time before alan Alarm suppression time: Suppress 'Door open too long':	Panding for extended with count Panding for extended with count Permanent facking or release (Loggle function) Stude with 2 doors Both directions	
🎎 User data	Time models	Time recording with function reader. (control booth, eppointments) Turnstile with inout and output reader. Both directions	
Z Card designer	Time model without PIN:		
1 ACLs	Time model without motor lock: Time model door pin active:	Time model no door alarms: v	
Visitor / Appointments			
External organization	👷 User: admin 👘 Nor dual o	og reader provided Workstation: INV-11587 11 Lac # Maic office Events: 0	Timeout: not active

After selecting the door type, the basic parameters of this access can be set in the input fields.

'Settings' area

Each device has an 'Active' checkbox that is used to activate the device. Only when this checkbox is selected will the device be loaded with data and started. The devices can thus already be configured and then only set as active following installation. Advantage: non-activated devices are not monitored by the system. Pre-configured but not activated devices are therefore also not reported as faulty devices.

You select the origin and destination areas with 'Area entrance' and 'Area exit' respectively. Every door in AccessOne leads from an origin area to a destination area. These areas may be different but do not have to be so.

Example: If your building is divided into a number of secured areas, an entrance might lead, for example, from an external secured area (ASB) to an internal secured area (ISB). However, a connecting door can also lead from one ISB to another ISB.

The areas are created in the 'System Configuration' dialogue selection in the 'Areas' tab. For a particular area in the building, the system can count how many persons are currently present there and can, for example, check whether the maximum number of persons has been reached. If this is the case, no further access is permitted. The requirement for this is that a person without an ID card cannot enter the area in question and the entrances and exits are fitted with access control devices, such as turnstiles, so that it is not possible for multiple people with access authorisation to enter the area at the same time.

Each door requires a unique door number in the door controller. This number must be between 1 and 8 since a maximum of eight doors are supported per door controller.

The value in the 'Door strike time' field defines the maximum amount of time for which the door opener remains actuated when an authorised access medium is presented. This value is entered in tenths of a second. Thus, entering 40 in this example means $40 \times 0.1 \text{ s} = 4$ seconds. If the door has a door contact, the door cont-

CEStronics

roller can determine whether the door was opened. In this case, the release is cancelled as soon as it is detected that the door is open. In this case, the value in the 'Door strike time min.' field makes it possible to ensure that the door opener remains actuated for enough time to guarantee that the door can be opened safely.

CEStronics

There are door opening contacts that are integrated into the lock or the magnetic closure device that signal that the door is already open even if it has been moved only a few millimetres. In this case, if no minimum opening time were specified, the door would be locked again immediately and in some circumstances no access would then be possible.

The value in the 'Door inertia time' field specifies how long the AMC should wait after a door has been accessed and after detecting that a door has been closed again before reactivating the intruder monitoring system of the door. With heavy doors it may be the case that when the door returns to the closed position in the door frame, it may vibrate briefly, such that the door controller briefly detects that the door is closed and then momentarily senses it open again, before a steady closed state is detected. Without this inertia time, accessing a door could always be followed by a message reporting that the door had been forced.

In operating mode, the following alternatives can be selected:

Settings	Active					
Туре:	Door/turnstile with e	ntrance rea	der. Only one direction		~	
Door number:	3					
Door strike time:	40	[0,1 s]	Door strike time min:	10	[0,1 s]	
Door inertia time:	-	1.01.1	n		New	
Betriebsmodus:	Normal mode				~	
Debug level:	Normal mode					
Alarm	Permanent open, ent Permanent open, exit Permanent open with	trance t	odel, normal mode ouside			
	Permanent open with	hin time mo	odel, normal mode ouside			
wax, door open time before alarm:	Permanet opened wi	thin time m	nodel, normal mode outside tin	ne model after first acc	cess I SI	
Alarm suppression time:	Permanent closed, er	ntrance				
Suppress 'Door open too long':	Permanet closed, exit	t .	subbless noor managou:	<u>ш</u>		
Time models						
Time model without PIN:	×	T	ime model permanent open:		*	
Time model without mator lock:	*	1	îme model no door alarms:		*	
The stand of the stand of the stand		T				

Normal mode (default): In this mode the door can only be accessed only with the appropriate authorisation and a valid ID card.

Permanent open: The door opener is constantly active; the green LED on the ID card reader is on permanently and anybody can open this door without an ID card.

Permanent open within time model, normal mode outside: The door can be opened during office hours without an ID card, but outside these (freely definable) times, only authorised persons should have access.

Permanent open within time model, normal mode outside time model after first access: Following the first authorised opening, the door remains open. During the selected time model the door changes to the 'Permanent open' state. This ensures that at least one authorised employee is present.

Normal mode within time model, locked outside: Outside the assigned time model, this door cannot be used, even with an authorised ID card. Within the time model, a valid ID card and the appropriate authorisation are required to open the door.



Alarm

The parameters for the door alarm are set in the 'Alarm' section.

Alarm							
Max. door op	en time before alarm:	200	[0,1 s]	Door prealarm:	100	[0,1 s]	
Alarm suppr	ession time:	0	[0,1 s]				
Suppress 'Do	or open too long':			Suppress 'Door intrusion':			

Max. door open time before alarm: Defines how long the system should wait for the door to be closed again before an alarm is issued. This value is specified in tenths of a second. If the specified time is exceeded, the system generates a log entry with the text 'Door open too long'.

Door prealarm: The value in this field should be smaller than that in the previous field. It specifies when an attention signal should be generated on the reader. This means that the person can close the door before an alarm is issued. If the door remains open longer than this specified value, the ID card reader mounted on the door repeats an acoustic signal until the door is closed again or an alarm is issued.

Time alarm suppression: This value is necessary for doors that are constantly monitored by an additional intruder alarm system. Here it may be necessary to inform that system, by means of an output signal, that the door is now being opened for an authorised purpose. The signal is cancelled soon after the door has been closed again, but no later than after the time specified by the value in this field.

Suppress 'Door open too long': Here you determine whether the system should trigger an intruder alarm or not if the door is opened without an ID card.

Suppress 'Door intrusion': With this checkbox you can control the alarm signal on site.

The system does not generate separate door status messages. The information of whether the door was opened or not is obtained from the relevant access log entry. Log entries:

'Access permitted': The door was opened following an authorised activation.

'Access not permitted': The door was not opened, even though it was released.

Time models

In this section the time models that may be required for general behaviour can be selected:

Time models			
Time model without PIN:	¥	Time model permanent open:	Ŷ
Time model without motor lock:	~	Time model no door alarms:	.*
Time model door pin active:			

A total of four time models are available:

Time model without motor lock: If the door has a motor lock, the mechanical load is reduced by only enabling the motor lock before and after the specified time model is activated.

Time model without PIN: The requirement for entering a PIN into the ID card reader is restricted to times outside the specified time model.

Permanent open: The door opener is always active and the door can be opened without an ID card (this setting is the same as the 'Permanent open' time model).

Time model no door alarm: Door alarms are issued only outside the specified time model.



7.1.4.2 Readers

Home						
B D D D H X	0					
Change New Copy Delete	Reload Assignment					
MIS = INCA Mec = Main Auforg 1 = En Main Auforance CES Terminal	LAC maxim data 40	Mod Reader A esu-Fo	mi			
PMS PHG Terminal	Name	Description		Position Address		
Em Side entrance	Empanyateset Infoterminal	Eingangsleser Infoterminal		Entrance 1 1 Entrance 1 2	-	
	Funko-1 CES-Leser 1	Funk-1 C25 Leser		Entrance 1 3	I Norlaco I	
					× Dara tarta	
	Redder					
	Name.	Eingangsleser	Stat	1.12 No.00	1 C	
	Description	Engenetiese				
	Location Short					
	Workflow:			activitie by approver		
	Settings					
Reports	* Modul address	1		Usage teamer:		
Device data	Seriel number.	17496478		Tunnel mode		
OSS	Address	Gd/Did	-	Encypt		
OSS Blacklist	Area entrance:	Uniations:	Area pric	Unbelwere		
Out Direction	Date of installation:	in taken In	Éxtemal referenze			
User data	Antipaviback group		Options	9		
Card designer	Repboard prevent		Reader can write:	les		
ACLs	With skiden		Tide tornal	Settings -		
	Battery state	ramount	Date of Dattery state:	Interview To		
Visitor / Appointments	and a second second					
Visitor / Appointments	Battery change date:	Lessa presi 🔯		Change bettery data		

The ID card readers associated with the door are defined on the 'Reader' tab.

To create a new reader, click the 'New Reader' button. The system then adds a new line to the overview list and allows you to enter the parameters associated with the reader in the fields below it.

'Reader' area

In the 'Reader' area you can specify the name, description, location, authorisation level and workflow.

Name:	Entrance-Terminal	Status:	Unkrjown
Description	Entrance-Terminal		
Location, door:			
		activate	by approver
Auth. level:			

Authorisation level

Five authorisation levels ranging from 'very low' to 'very high' can be selected. This reader can only be entered into an authorisation or for a person if the user at the dialogue station has at least the same or a higher authorisation level. You can use the authorisation levels to ensure that not every AccessOne user can issue access authorisation to sensitive areas.

The 'Activate by approver' checkbox ensures a further activation is required by a user with suitable authorisation.

Workflow

Here you can create specific work steps that must be approved by a superior, such as the allocation of authorisations for a particular area.

'Settings' area

In the 'Settings' area, you specify the technical properties of the ID card reader.



Modul address:	1			Usage counter:	1.1
Serial number:	17498478			Tunnel mode:	
Address:	1	Gid / Did:		Encrypt	
Firmware:	MRS_0292.BIN	-	Protocol:	Datasec	
Area entrance:	Unbekannt		Area exit:	Unbekannt	
Date of installation:	03/12/2020	2	External reference:		
Antipassback group:			Options:	Q	
Keyboard present:		-	Reader can write:	Yes -	
Display present:					
With slider:			Slider control:	Settings	
Battery state:	Unknown		Date of battery state:	Select a date 15	
Battery change date:	Select a date	5		Change battery data	in i

Module address

The first field is read-only and indicates the internal reader index allocated by the system. This is used to compile the authorisations and cannot be changed.

Card reader serial number

The serial number of the reader is required to implement the internal bus addressing of the reader. With these readers, the bus address cannot be set using DIP switches but is controlled by a configuration software. AccessOne automatically allocates the address when the serial number of the reader is entered. If, for example, a reader configured to address 3 fails to issue a signal, the door controller will try to identify that reader using the serial number. If identification is successful, the relevant address, in this case 3, is assigned to it.

Address (manual entry)

Each reader must have a bus address between 1 and 8.

Depending on the reader protocol, another fixed numerical value is added to the bus address, as in some reader protocols the addresses A to H are issued. This occurs automatically, since the conventions of the different reader protocols are stored in the door controller.

Firmware

Selection field for the firmware version. The current version is displayed at all times.

GID/DID

If readers with an old V-protocol or 9-way protocol are connected to the door controller, a group ID (GID) and a device ID (DID) must be specified in addition to the logical bus address. The GID forms the tens digit and the DID the units digit. Both values must be between 1 and 8. Example: The value '12' describes a reader address with a GID of 1 and DID of 2.

Usage counter

The reader checks whether the ID card has reached the maximum number of uses for the current day. **Tunnel mode**

Relevant only for LEGIC readers with DE bus. Like most other card readers, Deister ID card readers can only evaluate one stamp in the case of LEGIC cards. If the card has more than one segment and if all of the segments have to be evaluated, the intelligence of the reader must therefore be disabled and 'Tunnel mode' employed. In this mode, the commands to the LEGIC chip for searching and reading a segment are passed from the reader to the master controller. The AMC firmware can then read the segments that are

activated in the AccessOne reader formats successively.

With the DE bus and Datasec bus, communications with the ID card reader can also be AES encrypted. **Encrypt**

The link between the MAC and controller is additionally encrypted.

Date of installation

Automatically pre-filled when the reader is set up with the current day, but can be changed as desired. The date of installation is part of the system documentation.

CEStronics

External reference number

For internal labelling by the customer.

Options

For internal labelling by the customer.

Antipassback group (time-based)

Disables an access medium from being passed to another person after being used and thus allowing them to also gain access with the same medium. In order to treat adjacent doors equally, these doors can be combined in a group. Readers in the same antipassback group are treated as if they were mounted side by side and serve the same access. An access medium that has been used on a reader in this group is locked for all other readers of the same group for a set period (this period can be set in the door parameters). The value entered is a number between 1 and 99. Up to 99 door groups can be created.

Reader position

In AccessOne a door can be equipped with up to four readers – two for the entry direction and two for the exit direction. Example: at vehicle entrances it can be useful to fit a second reader for use by commercial vehicles above the reader used by cars.

Reader can write

The reader can write to cards. Example: updating access rights on offline locking devices. With some readers, the software can detect this automatically, while with others it must be specified explicitly. If no value is specified, any write function available in the reader is not used.

Keypad available

At some access points it is necessary to enter a PIN to arm the intruder alarm or as an addition to a biometric to gain access. Since on some of the readers, the keypad must be activated by a control command from the door controller, there is an option here to specify this explicitly. In most cases, however, the door controller detects the presence of a keypad automatically.

Display available

A display on the reader is only actuated if a suitable entry is provided here.

With slider

Here you can specify whether the reader is equipped with a motorised card slider.

With slider:		Slider control:	Settings
Battery state:	No	Data of hattany states	Salact a data
	Yes (with LEDs)	Date of battery state:	Select a date [15]
Battery change date:	Yes (without LEDs)		Change battery data
	Automatically		

If the slider slot is fitted with LEDs, these must be actuated instead of the LEDs on the reader. In this case select 'Yes (with LEDs)'. If you select 'Yes (without LEDs)', the LEDs of the reader are actuated.



Slider control

If a motorised slider is present, this section is used to specify whether the card is returned after being read and the conditions under which it should be retained.

Settings			Card collection X
Modul address:	T		-
Serial number:	17498478		Collect card, when
Address:	1 Gid / Did:		always
Firmware:	MRS_0292.BIN *	Protocol:	card unknown
Area entrance:	Unbekannt *	Area exit:	manually locked
Date of installation:	03.12.2020	External reference:	locked due to invalid PIN
Antipassback group:	-	Options:	no access authorization
Keyboard present:		Reader can write:	access denied, outside user time model
Display present:			wrong card version
With slider:	Yes (with LEDs)	Slider control:	Analy Count
Battery state:	Unknown	Date of battery state:	Appiy Cancei
Battery change date:	Select a date 15		Change battery data



7.1.4.3 Parameter P

ant name	ES Tarmina		
contrante. c	c.s remains	a1	
mmon parameter			
Parameter	Direction	Value	_
Options	Entrance	10	1
Tailgating	Entrance	No	
Random generator rate	Entrance	0	T
AntiPassBack time	Entrance	0	
Area checking	Entrance	0	
Companion required	Entrance	No	
Group access	Entrance		
Usage counter	Entrance	No.	
Ignore offline write errors	Entrance	No	
Always update offline data	Entrance	Ves	
Pincode required	Entrance	No.	
Pulse time arming	Entrance	0	
Automatic arming	Entrance	0	
Generate time registration message	Entrance	0	
Time for threat alarm	Entrance	0	
Threat alarm button	Entrance	0	

This tab contains the parameters that affect the sequence control of the door. The number of parameters listed on this page is dependent on the complexity of the selected door type. The following example is based on a standard door with one direction of passage. For doors used in both directions, the parameters are provided for each of the entry and exit directions.

Options	The options are used to enable customer-specific actions to be implemented.
	On all door types, the value 1 determines that the authorisation time model
	for is ignored on this door. A good application for this is the exit reader, for
	example.
	Example: a person should no longer be allowed to enter the building after
	17:00 but is free to leave. After 17:00 the entry reader will reject the person
	with the message 'Not permitted, outside time model'.
	If option 1 is set, the exit reader checks only whether an authorisation exists for
	this reader and ignores the time model.
	This specifies whether the controller requires the door to be closed again after
Tailgating	each authorised entry before the next card is accepted.
- · · · ·	If a random bag check is desired, the percentage rate can be set here with a
Random generator rate	value between 0 and 100. The software uses a random generator.
in %	Example: a value of 50 means that for every 100 passes, exactly 50 persons are
	denied access with the message 'Authorised for check'. A lockout is then set for
	this person that must then be deleted by security personnel once the check has
	taken place. This lockout also acts to prevent access at other access points.
AntiDaceDacktime	Specifies how long, after being successfully used, a card is locked on readers in
AntiPassback time	the same AntiPassBack group (time in seconds).



Area checking	The current location of a person (= area) is monitored by AccessOne with each
Area checking	use of their ID card on a reader. The door controller is therefore also able to
	check whether the person who has just held their card up to the reader is in
	fact registered in the same area in which the reader is located. If this is not the
	case, then either the person has passed through an open door without pre-
	senting their card to a reader, or the card has been stolen. If the area checking
	function is enabled, a door can then only be passed through if the person's
	location is the same as the location of the ID card reader. The requirement for
	this is a clear separation of the access areas and a constant monitoring of entry
	and exit movements by the access control system.
	Visitors may not enter particular areas unsupervised. On detecting a visitor
Companion required	card, therefore, the door controller waits for up to 10 seconds for a second card
	to be presented, which must be for a member of staff. Only when this occurs
	and the accompanying person has the required authorisation for this door will
	the door be released. During the waiting period, the green LED on the reader
	flashes to indicate that while one authorisation has been granted, another card
	is required.
	Where an area should only be entered by more than one person at a time,
Group access	this situation can be set up using this parameter. If, for example, the value 3 is
	entered, at least three cards for different authorised persons must be held up to
	the reader in succession before the door will be released.
	AccessOne allows an ID card to be created with a fixed maximum number of
Usage counter	uses. If this value is set to 1, the ID card is comparable to a single-use admission
	ticket. Every reader, that has this parameter set, checks whether the maximum
	usage of the ID card is still greater than zero. If yes, and if the person has the
	necessary authorisation, the door is released and the usage counter counts
	down by one. If the counter has reached zero, no further door for which this
	parameter is also set will open. If this parameter is set on the reader at the
	building entrance, the situation will be that the visitor can enter the building
	exactly once. The counter is not checked within the building and the visitor is
	not restricted while there.
Ignore offline write errors	This parameter is only useful if an offline locking system is in use. It controls
ignorieren	whether access should also be granted if the process of writing the access
Ũ	authorisation for the offline doors was performed without errors. Normally,
	the door opens only if the card holder holds their card in front of the reader for
	sufficient time that it could be successfully written to.
Always update offline data	To avoid too many write operations, the door controller updates the card only
aktualisieren	when at least half of its validity has expired. This update, however, only takes
	place in offline locking systems.
PIN code required	This value specifies whether a PIN must be entered to gain access. It requires
	that the reader has a keypad.

7.1.4.4 Parameter I

On this page the inputs are specified, i.e. which input on the respective IO board is connected to the monitoring contacts of the connected peripherals.

or master data	Reader	Parameter P	Parameter I	Parameter O	
Door name:		CES Termina	L.		
aput parameter					
Parameter		Direction	Value	Lac	
Door contact IoMe	odule	Entrance	1		. r.
Door contact, con	tact no	Entrance	(D)		- 0
Door switch IoMo	dule	Entrance	IO Modul: 1		
Door button conta	act no	Entrance	2	1	
Bolt contact IoMo	dule	Entrance			
Bolt contact, conta	act no	Entrance		· · · · · · · · · · · · · · · · · · ·	
Lock input loMod	ule	Entrance			
Lock input contact	t no	Entrance	1	4	
Sabotage contact	loModule	Entrance	1		
Sabotage contact,	contact no	Entrance			
Reader activation	laModule	Entrance			
Reader activation	contact noconta	ect Entrance			
IoModule for EMA	arm ready	Entrance	1		
EMA arm ready co	intact no	Entrance	1		
loModule to arm I	EMA	Entrance	IO Modul: 1		
Contact no to arm	EMA	Entrance	3		
Key switch alarm I	oModule	Entrance			
Key switch alarm o	contact no	Entrance	1		
The Million of the	March 14	0.34			- P.

Meaning of the individual input signals, regardless of door type:

Door contact IoModule	The IO module to which the door contact is connected (input).
Door contact	Number of the contact on this module.
Door switch IoModule	The IO module to which the request-to-exit contact is connected.
Bolt contact IoModule	An additional signal that states whether the door should not only be closed
	but that the locking bolt should also be extended.
Lock input IoModule	The IO module to which the contact for blocking passage is connected.
Sabotage contact IoModule	If this signal is detected, a tamper message is generated and the tamper
	relay is actuated.
Group access	Where an area should only be entered by more than one person at a time,
	this situation can be set up using this parameter. If, for example, the value 3
	is entered, at least three cards for different authorised persons must be held
	up to the reader in succession before the door will be released.
Reader activation IoModule	The IO module to which the slider contact/light barrier is connected.
IoModule for EMA arm ready	The IO module to which the 'Alarm system ready' contact is connected.
IoModule to arm EMA	The IO module to which the 'Alarm system armed' contact is connected.
Key switch alarm IoModule	The IO module to which the (key) contact 'Please arm the alarm system' is
	connected.



Handle contact IoModule	Triggered if the lever handle (door handle) of a door that has no ID card rea-
	der is actuated from the inside. This prevents an intruder alarm being issued
	when the door is opened with the lever handle.
Key contact IoModule	Similarly to the handle contact, a signal here indicates that the door is being
	opened using a key.



7.1.4.5 Parameter O

On this page, the output signals are specified, i.e. which relay output on the respective IO board is connected to the actuators of the connected peripherals.

Door name:	CES Termina	រវ		
Output parameter				
Parameter	Direction	Value	Lac	
Door opener loModule	Entrance	IO Modul: 1	1	1
Door opener relay no	Entrance	1		
Alarm suppression loModule	Entrance	1	1	
Alarm suppression relay no	Entrance	1	1.	
Motor lock loModule	Entrance			
Motor lock relay no	Entrance	111		
Door alarm IoModule	Entrance	IO Modul: 1		
Door alarm relay no	Entrance	7		
Pre alarm loModule	Entrance			
Pre alarm relay no	Entrance			
EMA arming loModule	Entrance	IO Modul: 1		
EMA arm relay no	Entrance	3		
Additional relay 1 loModule	Entrance			
Additional relay 1 relay no	Entrance			- 11.2
Additional relay 2 loModule	Entrance	1		11.2
Additional relay 2 relay no	Entrance			
Light IoModule	Entrance			
Light relay no	Entrance		11.14	
A	E I	10 M		100

Meaning of the individual output signals:

Door opener loModule	The IO module to which the door opener relay is connected (output).
Alarm suppression IoModule	The IO module to which the alarm suppression relay is connected (out-
	put).
Motor lock IoModule	On self-locking doors, the motor lock must be actuated in addition to
	the door opener to retract the deadbolt. This output signal can be com-
	bined with a time model. If the door is in the 'Permanent open' state,
	this signal is constantly set.
Door alarm IoModule	Output signal for the intruder alarm. This is always set if a door has been
	opened without authorisation or is open for too long. The setting of this
	signal can be suppressed in the parameter settings.
Pre alarm IoModule	If a pre-alarm time has been set for a door, this signal is set once the
	door has been opened and the set time has expired.
EMA arming IoModule	The IO module to which the relay for arming the alarm is connected
	(output).
Additional relay 1 IoModule	The IO module to which the relay for special function 1 is connected
	(output).
Additional relay 2 IoModule	The IO module to which the relay for special function 2 is connected
	(output).



7.1.5 Displaying the device status

AccessOne - Device data									- 0
Home	and the second								
Change New Copy Delete	Reload Device status								
🚟 Aufzug 1	Device status								
Main entrance	M	_	Au	V					
Side entrance	Device	Type	State	Program	Power	Sabotane	Made	State	Alarm system
	Mac	IMAC	Online	Unknown	1		1		1
	- IO Modul: 6	IO-Module	Linknown	-	Unknown		1	1	-
	- Main entrance	LAC	Offine	Unknown	Unknown	Unknown	-		
	- CES Terminal	Door	Offine			1	Unknown	Unknown	Unknown
	- PHG Terminal	Door	Unknown				Unknown	Unknown	Unknown
Papatr	- Infoterminal	Reader	Unknown		Unknown	Unknown			
E Reports	- PM	Door	Coffine				Unknown	Unknown	Unknown
	- Entrance-Terminal	Reader	Unknown		Unknown	Unknown		1 1 1	
Device data	- CES Leser Modul	10-Module	Unknown	1	Unknown		·		
	- IO Modult 1	IO-Module	Unknown		Unknown				
		10.11.1.1	CONTRACTOR OF		Mahannin				
COSS COSS	- IO Modult 5	IO-Module	Shiemawn		Unenown		-	test -	1

Click on 'DMS' in the tree structure with the left mouse button to view the status of all devices in the overview. The status of an individual device (online or offline) is displayed in the detailed view for the device. This entry cannot be deleted and a second one cannot be created.

Right-click on DMS to view a further range of choices. Here you can create a new MAC, a new EMC or a new PS-Online (key cabinet).



7.2 Offline device data (OSS-SO)

Facility data must be created for every installation of OSS Standard Offline. Basic data for the offline devices, such as electronic cylinders and handle sets, are entered here. This and other data are used to determine the size of the memory on the locking medium for offline data and how much space should be reserved for events and lockout list entries. With MIFARE, the facility data contains the access keys to offline segments of the card and application ID. For LEGIC this is where the stamp is stored.

7.2.1 Facility data

Facility data are normally pre-installed by CES but can also be added or changed by the user. There is one dataset per system. To create a new entry, click New in the toolbar.

AccessOne - OSS					- 0	×
Home	Ends.					
Change New Copy Dele	ete Reload					
1.41	Cylinder Authoriza	tions Time models	Facility data Data import			
Name						
Facility_Legic	Name.	Facility_Legic				
Facility-Desfire	Data type:	Legic Advant				
	Main version:	1	Minor version	T		
	Mar puests par carts	3	Max blacklist untrust net care	3		
	mar crois po cara	12 4 10 10 10	that adding concepts one			
	Event configuration:	Failed to unlock	Tamper detect	lacidist card	Blacklist full	
Raport	Legic Advant stamp:	-	Stamp lengtfr	12	Segment length:	640
IE Reports	Write protected length	e 13				
✓ Device data						
1 055	Mifare Classic/Desfire	key:	Desfire application ID:	0x	Start into block no.:	
g 055	Desfire data file length	<u>k</u>				
SS Blacklist						
🎎 User data						
📝 Card designer						
9	User: admin	No dialog teader connecte	Workstation: INV-11537	Lac, O Mac offine	Events: 0	

Specify a name and choose the data type. Enter the main and sub-version number (e.g. the digits 1 and 0 for version 1.0). The version number is important as a distinguishing feature.

In the 'Event configuration' area, specify which events should be written on to the card by the electronic cylinder. These settings apply across the system; they are thus written on the updater in the same way for all of the locking media.

For a LEGIC advant system, enter the stamp and stamp length. To enter the stamp, click the button to the right of the input field. Both the stamp and key are normally entered in hexadecimal format, i.e. digits 0-9 and letters A-F are permitted. The total length of the key value for Mifare DESFire is 32 characters (Mifare Classic: 12 characters).



The access keys are encrypted and saved in the database. Once entered, for security reasons this value will NEVER again be displayed in clear text; it is only possible to enter a new value.

Click SAVE in the toolbar when the entries are complete.



If you change the key, the change is effective immediately. This may mean that from this time onwards no further locking medium can be updated.



7.2.2 Cylinders (and handle sets)

The offline components are created on this tab. Click NEW in the toolbar and enter the data for the cylinder.

In the 'Description' field, specify the exact installation location. Offline components are battery-powered. As standard offline components they are capable of writing the battery status back to the locking medium if the battery falls below a certain voltage level. The installation location must be known so that a low battery can be replaced.

Hom Andern	Neu Kopieren	Löschen	Aktualisieren Zuordnung					
në la		(Zylinder Belichtigu	ingen Zeitmodelle	Facilitydaten	Datenimport		
Name	Beschreibung	Status						
eschlag	Muster Beschlag	Geschneben	Name	CES Zwinder		Indec	8	Mitglied in Serechtigungen: 5
ES Zylinder	Test OSS Tool	Geschrieben						
Austerkoffer	Musterkoffer	Übertragen	Beschreibung	Test USA Tool				
est	Test	Geschrieben	Standort Tur-					
est 4	Test 4	Geschrieben	and a start of the					
est 5	Test 5	Geschneben	Sicherheitsstofe		durch Be	will ger aktivieren:		
est 6	Test 6	Geschneben	Warkflow					
est 7	Test 7	Geschrieben						
est 8	Test 8	Geschrieben	Eigenschaften					
est Tim		Geancert		an al al		Automatica .	10	Numero Antonio
est1	Testimport 1	Geschneben	Zylindentyp:	CES Zylinder		Offnungszeit (s.;	~	Verlangerte Offnungszeit (s.)
est2	Testimport 2	Geschrieben	Offline Bereich:	1 - DSS		Zeitmodellt		Intervalle 1 (1.) Intervalle 2 (1.)
est3	Testimport 3	Geschneben	Einstellungenet	I see from The school of		Transfer Line and		Contractor Parameterizat
Tim's Zylinber	1	Geschrieben	chaelanger	Benps Mailbox Modui		Beeps Zutritt verword	et	14D
			Leserrelans			Parik Zylinder		
			Lange auflion (nom):			Lange innen (mm):		Serienna
			Batteriestatus:	Useran		Batteriestatusdatum:	Different exceptions and	Firmware:
			Installationsdatum:	Decret Screeker [15]		Externer Transfer:		

Cylinders and handle sets are clearly distinguished by their number. AccessOne allocates the number automatically when a new electronic cylinder is set up and saved (it appears in the 'Index' field).

Properties area

Further information on the installed device is entered here.

Cylinder type

Choose between cylinder, handle set and wall terminal. These devices may require different batteries.

Open time

Specifies how long the cylinder remains coupled during an authorised access. A value of 5-10 seconds is normally sufficient (default setting: 5).

Extended open time

The standard open time can be extended for certain person groups.

Offline area

With Standard Offline, the offline area number (site ID) must always be specified. The value 0 is not permissible here. The area number allows an installation to be divided into several areas. In this case there are multiple cylinders with the number 1, i.e. one for each area. This means that the cylinder number is only unique in combination with the area number. When a person moves from one area to another, the updater deletes the data of the previous area and replaces it with that of the current area. By dividing it into multiple areas, the number of offline locking devices in an installation can in theory be unlimited.

Time model

Selection options for the time model. Function is dependent on the device type and manufacturer.

Intervals 1 and 2

Function is dependent on the device type and manufacturer.

Settings

Available settings are dependent on the device type and manufacturer.

Reader relay

Function is dependent on the device type and manufacturer.

Panic cylinder

Device type information.

Length

Information on internal and external length.

Serial number

Serial number is specified here.

Battery status

The 'Battery Status' field shows whether an offline device has signalled a low battery. The 'Date of battery state' indicates when this message was created. If the battery is replaced, the offline device generates a 'Battery changed' message the next time an activation occurs, which is returned to the system via the ID card updating the data accordingly. The 'Reader battery state' report can generate a list of devices with low batteries at any time.

CEStronics

Finally, transfer the data by clicking **Transfer**.

7.2.3 Programming offline devices

Programming the data onto offline devices is completed directly from the tab. The following items are required:

- RF-Stick
- System-Master
- RF-Stick-Master

Procedure:

- 1. Insert RF-Stick into the PC.
- 2. Click TRANSFER.

3. Import A-licence into AccessOne (a one-off procedure for the first device that is programmed)

4. Hold the RF-Stick-Master in front of the device.



7.2.4 Authorisations

Link several doors into a door group.

If you allocate a new authorisation to a cylinder, you must also transfer this data to the offline device.

1

Authorisations should be designed so that they only link rooms with the same authorisation level. If a room or corridor has multiple access points, the relevant electronic cylinders should be combined in a single authorisation. You can then link the door groups via the authorisation profiles based on the user profile.

AccessOne - OSS								- 11
Home Nome	and the second sec							
Andern Neu	Kapieren Losche	n Aktuelisieren Zusziden	ing					
81	ſ	Zylinder Berech	tigungen Zeitmod	elle Facilitydaten Da	tenimport.			
Name	Beschreibung							
Musterkoffer	Aller Contractor Ba	Marpe	Produktion			index	14	
Service	Offline Gerate in Service	Bestimeibung,	Offine Geräle in der Pro	dlubbion			ourso Berninser aktivitie	r .
		Öttine Bereych	1 - CSS	Scheme is stole		Workliber		
		Zageoritnete Zylin	der					
		Name	Beschreibung	Sicherheitsst.				
		CES Zylinder	Test OSS Tool	Ohne		Name	Beschreibung	Sicherheitist.
		Musterkoffer	Musterkoffer	Ohne		Beschlag	Muster Beschlag	Ohne
		Naum ±124	Kaum E124	Uhne		Raum E123	Raum E123	Ohne
		and the second				Raum E125	Raum E125	Ohne
						Test	Test	Ohne
					<<			
/ Kartendes	igner	5						
OSS					>>			
Besucher	/ Termine							
Fremdfirn	nen-MA							
9 Standorto	laten							
• Workflow								
OSS Black	list	Benutzer: maik	Terr Darbert In	Arbeitsstation: IN	V-11537	- office	Ereignisse: 0	Timeout: nicht aktivier



7.2.5 Data import

AccessOne - DSS		- 🗆 ×
Hame		
ROGHX	O Rebust	
4 5E0	Cylinder: Authorizations Time model: Facility da Data import	
Name	Office years 1. OFFICE 1	
	Minima di yee	
	Cylinder	The second second
	Halling reactioned change the were also over the reaction of t	Read
		Import
Reports		
Device data		
🕜 OSS		
SS Blacklist		
🎎 User data		
📝 Card designer		
JE ACLS	User admin Events: 0 1	Timeout not active

Allows the import of a *.csv door list. Select the required offline area and click **Read**. Choose the relevant door list from the directory folder.

 $(\mathbf{1})$

The door list is normally created by CES when the system is set up. The list can however also be edited by the customer.

Name	Beschreibung	Zylindertyp	Sicherheitsst.	Türöffnungszeit	Länge aussen	Länge innen	Verl. Türöffnungszeit
PM124	Eingangtür PM	CES Zylinder	Ohne	5	42	42	10
PM125	Spind PM	CES Möbelschloss	Ohne	5	42	42	10
PM126	Nebeneingang PM	CES Beschlag	Ohne	5	42	42	10

AccessOme - OSS										-		×
Be Home												9
BOPH	X D Record											
940	Cylinder Autho	inzations Time n	nodels Facility	dista Data	import							
Name	Offine area	1 - OSS Test	ū							_		2
	Name	Description	Cylinder type	Auth level.	Door open time	Length autside	Length insid	Ext. door open time	Status	Dana		
	PM125	Entrance door PM	CES cylinder	Without	5	42	42	10		now		
	PM126	Locker PM	CES escutcheon	Without	5	42	42	10		Immedi		
Reports			-)
🧨 Device data	3 of 3 records reed	d for import										
oss 🗸												
SS Blacklist			_					-		_		
The second second	Usen admin	The Design		Workstation	INV-11537	The run		Events: 0		Timenut not a	the	

You can now review the imported file again in the list view, in the 'Cylinder' field. Press the 'Import' button to import the list into the database. The confirmation is displayed in the text field beneath the field.

7.2.6 Time models

OSS Standard Offline uses a different time model format and is less flexible than AccessOne is for online components. As a result, the online time models cannot be used consistently throughout the installation; there is a separate tab for OSS Standard Offline time models.

In OSS Standard Offline, a time model consists of up to four intervals. For each interval group, days can be selected on which it is valid. If no time model is included in the authorisation for a particular person, the authorisation is valid for the whole day.

	Zylinder Bas	rechtigun	gen Zeitm	odelle Fac	oldydaten 13	Interimport					
Name											
vbeitszeit	liene Beschreibung	Arbe	iltzet atszer			indito:					
	Zeltinicovalle										
	Intervalle 1	ion.	07.50	bie:	70.00	gung	S Montag	J Diemtag	A Mittwoch	9-Disheritag of Helag	
		ware		bee) Semistar	Sprintag	Feetlag		
		VOID		bete							
		Vari		Bith							
	Intervalie 5	HONE!	07300	Bit	14:00	güllig	Montag	Dampag	Mitmanh	Desverved Pretag	
		von		the			(%) annatas	_ soundad	/itertaa		
		VOR		bic							
Logbuch	Intervalle 3	van		bus		9076	Mentag	Diemitag	L Millouth	Downerstag () Fordag	
Berichte		work.		hac			Semilar	Toonbag	C. Feedag		
A Constantine		urbre:		the state							
Geratedaten		- Port		urs.	-				-		
Benutzerdaten	Intervalie 4	legenti legenti		bin.		dm.2	- Montag	Diemtan	Venetar	Dichneistag / Frietag	
System-Konfiguration		Vaic		DRD							
ACLs		VER		bis							
Gruppenänderungen											
/ Kartandarianar											
Kantenuesigner											

In the example, access is granted Mondays to Fridays from 7:00 to 20:00 and on Saturdays from 7:00 to 14:00. No access is permitted on Sundays or public holidays.

8 Configuration of authorisations

Target group of this section:

• Personnel with product training

8.1 Authorisations

First, set up authorisation groups for online and offline devices. Then use day and time models to define further restrictions or door functions (e.g. opening functions at specific times of day), taking special days and holidays into account.

AccessOne - OSS 12.7 DBHX P 0 Berechtigungen Offline Geräte in der Pro te Zy Name CES Zylin Musteria est OSS Raum E124 Raum ET24 aum E12 Tim's Zylin < < / Kartendesigner / OSS Le Besucher / Termine 🛓 Fremdfirmen-MA Standortdaten - Workflow SS Blacklist

8.1.1 Authorisations in the overview

Selecting the 'Authorisations' dialogue opens multiple tabs in the dialogue window.

In the 'Authorisations' tab, multiple readers can be combined in one group. The readers are selected from the list of unassigned readers (right-hand list) and allocated to the current group with the '<<' button.

Authorisation groups consist of linked authorisations. The authorisations listed on the right-hand side of the window (unassigned) can themselves also be individual authorisations or group authorisations.



8.1.2 General information on time and day models

Time models are used at various places in AccessOne.

- To restrict access. A person-based time model can be created here, such as a time model for an employee. If no separate time model is specified in the authorisation, the person-based time model always applies.
- Time models are used for doors, e.g. to specify a 'permanent open' function at particular times of day.

In AccessOne, a time model either equates to a weekly plan, consisting of individual day models for each day of the week, or to additional day models for special or holidays.

Each day model can contain three intervals and specifies access times for exactly one day.

We recommend the following procedure when defining the plans:

- 1. Create time models
- 2. Combine special and holidays in groups
- 3. Create time models for doors

8.1.3 Day models

AccessOne - Authorizations					
Change New Copy Delete	Reload Assignmen	t			
r2	Authorizations	Time mode s	Day models	S ecial and holidays	Access masks
Name					
07-22	Name:	07-22			
13-14	Description:	07-22			
	Time intervals				
	from:	07:00	until:	22:00	
	frame		until:		
	in Gin.				

In the toolbar, click NEW. Enter a name for your day model. You can optionally add a description.

Enter at least 1 interval in the 'Time intervals' section. This must be defined with a 'from'/'until' time. Then click SAVE.

TIP Also create the 'No entry' time model. This model is, for example, useful for employees who are authorised on certain days but not on others. Holidays can thus easily be taken into account.



8.1.4 Special and holidays

Click NEW and enter a 'name' for the special day. The categories are used to arrange the special days into groups and thus to enable a day model to be created for such a group.

TIP Combine all of the national holidays in one category. The 'No access' day model then applies for these days. (Alternatively, no access in this category is equivalent to a day model with an interval from 0:00 to 0:00.). By sorting the holidays into appropriate categories, a situation can be reached in which the holidays that apply in the relevant region are taken into consideration for the time model, while the others are ignored.

AccessOne - Authorizations		
Home Home		
Cancel		
	Authorizations	Time models Day mot is Special and holidays Ac ass masks
Description		
Easter Sunday	Description:	Easter Sunday
1.000	Category:	1 *
	Valid for offline:	
	Calculation meth	od
	Туре:	depending on Easter
	Date:	0
	Priority:	1 - overwrites working day
	Valid from:	1 - overwrites working day
	Tano manin	2 - overwrites saturday 3 - overwrites sunday

The calculation method is selected below:

Most moveable festivals and holidays of the Christian year are determined by the date of Easter Sunday:

- Ash Wednesday = 46 days before Easter
- Palm Sunday = 7 days before Easter
- Maundy Thursday = 3 days before Easter
- Good Friday = 2 days before Easter
- Easter Monday = 1 day after Easter
- Ascension = 39 days after Easter (i.e. the 40th day)
- Whit Sunday = 49 days after Easter (i.e. the 50th day)

In the Catholic Church the following festivals also apply:

- Corpus Christi = 60 days after Easter
- Feast of the Sacred Heart = 68 days after Easter

The door controller calculates the date of Easter Sunday automatically and can therefore determine these Easter-dependent holidays if they are created in the system. For days that are calculated in relation to Easter, the number of days that must be added to the calculated date is entered in the date field.



Change New Copy Delete	Reload Assignmen	st			
T	Authorizations	Time models	Day models	Special and holidays	Access masks
Description Easter Sunday	Description: Category:	Easter Sunday)		
	Calculation met	hod depending on E	aster		
	Date: Priority:	0 1 - overwrites w	orking day		
	Valid from:	Seren a bate	untit s	eettadate Its	

In the example below, Easter Monday (= 1 day after Easter) is defined as follows:

If the holiday comes before Eater, a negative value can be entered. Example: for Good Friday (2 days before Easter), the entry is -2.

• Fixed date

Special days that must be created again every year, or one-off occasions such as company celebrations, are created with a fixed date. They are then valid exactly once.

• Annually recurring

There are dates for special and holidays that recur every year, such as 1 May and 24 December. For these, choose the date from the calendar. The year number is ignored during the check.

• Priority/category

The priority of a special day determines its relevance. A normal holiday has a priority of 1; if it falls on a working day, the day model for the working day does not apply, but rather the day model for the special day. Example 1: Christmas Eve is allocated to category 8, and all category 8 special days are entered in your time model with a day model of half a working day (07:00-12:00). Thus if Christmas Eve falls on a Monday, the secured areas can be entered between 07:00 and 12:00. Should it fall on a Saturday or a Sunday, however, no access should be granted. In this case, priority for Christmas Eve should be set to 1, since Saturday and Sunday have a higher level of priority.

Example 2: some employees require access for weekend stocktaking. For this special day, a priority 2 or even 3 must be set so that the ordinary Saturday or Sunday day model is overwritten.

CEStronics

Holiday	Regions applicable
New Year's Day	National
Epiphany	Baden-Württemberg, Bavaria, Saxony-Anhalt
Good Friday	National
Easter Sunday	National
Easter Monday	National
Labour Day/1 May	National
Ascension day	National
Whit Sunday	National
Whit Monday	National
Corpus Christi	Baden-Württemberg, Bavaria, Hesse, North Rhine-Westphalia,
	Rhineland-Palatinate, Saarland
Assumption Day	Bavaria (Catholic areas), Saarland
Day of German Unity	National
Reformation Day	Brandenburg, Mecklenburg-Western Pomerania, Saxony,
	Saxony-Anhalt, Thuringia
All Saints' Day	Baden-Württemberg, Bavaria, North Rhine-Westphalia, Rhine-
	land-Palatinate, Saarland
Day of Prayer and Repentance	Saxony
Christmas Day	National
Boxing Day	National

The following table gives an overview of holidays in Germany:

We recommend that you select the categories for special days such that holidays that apply in the same region are grouped together in the same category.

National holidays	Category 1
Epiphany	Category 2
Corpus Christi	Category 3
Assumption Day	Category 4
Reformation Day	Category 5
All Saints' Day	Category 6
Day of Prayer and Repentance	Category 7
Other category 8 special days	Category 8



8.1.5 Time models

Home Home Change New Copy Delete	Reload Assignmen	nt					
5an	Authorization	Time models	C y models	Special and ho	olidays	Access masks	
Name							
Mo-Fr. 7-22	Name: Description:	(Mo-Fr. 7-22		Inde	Bic .		1
	Day model, day	rs of week					
	Monday:	07-22		Saturday:	07-22		
	Tuesday:	07-22		Sunday:	07-22		
	Wednesday:	07-22					
	Thursday;	07-22					
	Friday:	07-22					
	Day model, spe	cial days and holidays					
	Category 1:			Category 5:			
	Category 2:			Category &			
Person data	Category 3			Category 7:			
Authorizations	Category 4:			Category 8:			
Authorization profiles							

If no special day is set up in the system, no access is granted on this date. Click NEW and enter the relevant information. Save the time model. If you navigate to another page without saving, in this case AccessOne will save the time model automatically.

The 'Description' input field is used for internal allocation within the company.

The entry in the 'Index' field is a sequential control number to indicate the order in which the time models were created.



Home							
Cancel	OR						
1	Authorizations	Time models	Day models	Special and h	olidays	Áccess masks	
Name Ma-Fr. 7-22	Name:	Mo-Fr. 7-22		Ind	ex:		1
	Description:						
	Day model, day	s of week					
	Monday:	07-22	u U	Saturday:	07-2	2	-
	Tuesday:	07-22	-	Sunday:	07-2	2	-
	Wednesday:	07-22	7				
	Thursday:	07-22	8				
	Friday:	07-22					
	Day model, spec	cial days and holid	ays				
	Category 1:	13-14	*	Category 5:			.9
a second and	Category 2:	07-22	.4	Category 6:			-
Person data	Category 3:		*	Category 7:			-
Authorizations	Category 4:		w]	Category 8:	-		-
Authorization profiles							

In this example, the same day model applies from Monday to Friday. Category 1 holidays are ignored in this time model, i.e. if the holiday is on a weekday, the usual weekday day model applies. For category 2 special days there is a corresponding day model. For all other special days, i.e. those in categories 3 to 8, no day model is entered and access is thus blocked.

AccessOne - Authorizations					
Home					
initiation and a second and a	40%		_		
- m3	Authorizations	Time models	Day models	Si scial and holidays	Access masks
Name			-	-	
Ignore special days	Name:	Ignore special	days		
13-14	Description:				
	Time intervals				
	from:		unfil:		
	from:		untik		
	from:		amhl:		

In order to override a special day so that the ordinary day model of the relevant working day applies, a special day model must be created, unless such a model was automatically created during installation (e.g. 'Ignore special days').



8.1.6 Access masks

	1	Authonizations Tir	ne models	Day models	Special and	olidays	Access mask	s)		
lame	Description					-		_		
est elevator 1	Test elevator 1	Name	Tesk elever	an t				280		
		Description	Test eleval	ar 1						
		Elevator Group (EGC)					50	ngle elevator (L	AC):	
		Mask type:	Man				LH.	na:		
						Au	itti leveti			
		Winkflow-					90	fivatic by appro	-	
		Augned floors								
		Floor name		Floo	Source front	Destination	Source rear	Destination		
		2. Etage		2	16- C	Rec.	No	No		 _
		1. Etage		1	1.1	No.	No	No		_
		1. Untergeschoss		-1	No	No	No	No		
		2 Unterneschoss		-2	No.	No	No	No.		

Access authorisations for a previously created elevator group can be created in the 'Access masks' dialogue. Click NEW to create a blank access mask. Enter the name and a description and select an elevator group to view the floors of this group. Next, define the mask type ('User' or 'Emergency'). To allow authorised access to the floors, switch or drag the 'Start' and 'Destination' doors from 'No' to 'Yes'. Save your entries.

8.2 Authorisation profiles

In the 'Authorisation profiles' dialogue the user can create an authorisation profile from multiple authorisation groups. This allows the authorisations for online and offline devices to be linked and thus be combined in a profile.

AccessOne - Authorization profiles				- 0
Change New Copy Delete	Recard Automment	_		
1	Online OSS Wrome made	_		_
ame Description offie 1 sitors onference vooms nployees service	Name: Instructory est provide Name: Instructory est provide Description: Values: Walding: 1	Warrittan		
A st	Autimeil authorizations			
	Name Description Time mode Auth-snet Service Group Online Gelices in service (Without)	<<	Name Deproton Dure And Time Dure And Time	Auto-evel vetricol
Authorizations Authorization profiles		>>		
Company data				
Reports				
	User admin Workstation/INV-11537	The Thee?	Events 0	Timeout not active

8.2.1 Online authorisations in the overview

In the 'Online' tab, authorisation groups can be combined in an authorisation profile. The groups are selected from the list of unassigned groups (right-hand list) and allocated to the current profile (left-hand list) with the '<<' button.



t New Copy Delete	Reload Assignment								
	Online OSS	court results							
		Jacob Contractor							
Description									
	Tsame	Employees service			100 mm				
ce rooms	Description					services by an	poe:		
rs service	Validativ	T Dave	Suits level		(WenkWaper)				
	Assigned authoriz	nthant / Cylliniters							
	Name	Description	Time model	Acts level. Off area no.					
	Service Gruppe		1	Without 3		-	Burnelster	A	0.00
				1		THE R. L.			
					11				
					>>				
					>>				
					>>				
thorizations	-				>>	Name	Description	Auto level	Off lates re-
thorizations					>>	Name Musteriother PM	Description	Auth level	Off pres. rc
thorizations	-				>>	Name Mudekidhe PM OSS Too' Tett	Descision	Auto level. Without Without	Defilestic re-
thorizations thorization profiles	-				>>	Name Mutaksiter PM OSS 500 Test Jahr	Description	Auth level Without Without	Off lines for 1 1
thorizations thorization profiles					>>	Name Mustewater PM OSS Stall Test Uster PM124	Description Engineering	Auth-Websut Without Without Without	05 Jest Ac 1 1
thorizations thorization profiles mpany data					>>	Kame Mutakwater PM OSS 100 PM PM124 PM124 PM124 PM125	Description Enganglia: PM Spin PM Spin PM	Autri leveli Without Without Without Without Without	Dff area.fc 1 1 1 1 1 1
thorizations thorization profiles mpany data					>>	Kame Mutekoter PM OSS 500 Test Jato MA124 TM125 Schrank 1	Description Engangtic RM Signed RM Neeelengang PM Sciencek 1	Auth Innel Without Without Without Without Without	D# aves. Ac 1 1 1 1 1 1 1
thorizations thorization profiles mpany data gbook					>>	None Nucleosate PM 055 100 PM 055	Description Engargur HM Spind PM Neter Intgang PM Schark 1	Auth-Iwell Without Without Without Without Without	00 bes.nc 1 1 1 1 1 1 1 1
thorizations thorization profiles mpany data jbook					>>	Name Muderister Pili dist Intila Intila Edmini 1 Edmini 1	Descention Engangtic RM Sond RM Networkings RM Schank 1	Auth Newl Without Without Without Without Without	

8.2.2 Offline authorisations in the overview

In the 'OSS' tab, offline devices can also be combined in the selected profile. From the right-hand list (unassigned groups and devices) you can allocate both an authorisation group and an individual offline device to the current profile using the '<<' button.

1

Before offline devices can be integrated, those offline devices must be set up (see 'Offline device data (OSS-SO)' on page 54).

9 Creating person data

Target group of this section:

• Personnel with product training

The 'Person data' dialogue allows you to assign authorisations and to record all of the necessary data about the person. You should allocate the previously configured authorisations for online and offline devices directly to the persons.

9.1 Person data

9.1.1 Person data in the overview

All significant data on the person is displayed in the first tab. It is also possible to delete a lockout or to assign a new ID card to a person who has forgotten theirs ('Change card' button). This deactivates the previously active ID card.

This overview is intended to quickly record properties that are assigned to a person (e.g. for security personnel).

×	Overview Masteridata Forther maxing alater Cando	Additionation: Capture pullate ()	actionally Accessionalis C	55/
Last same First name Personnel / Spind-Maet	Last name: Spind-Master Company:	First name: Company 2:		
	Department:	Date of birth:		
	Location Current area Unknown	SHOR -	• Change area	
	Parking area: Unknown	sinte: -	Change parking area	
	Conds identification at date of first card issue	Schlüsselausgebeformula	1.	
	Number Version Valid from Valid until 100 0	Status Wepl. card	Print form	
			Crange card	
	Lockouts			
	Lockout Reason	From Until		
Person data			X Delete	
Authorizations	Logbook Days 2 - Reload			Client
	Date LAC / WS Reader / Login Area / Prog	gram No. Message	Card	Client
Authorization profiles				
Authorization profiles Company data				
Authorization profiles Company data				

'Location' area

The Location area displays the 'Current area', 'Last entry' and 'Parking area'.

Current area

When a person with an authorised ID card passes through a door secured with AccessOne, the location is recorded. Every door has a definition specifying the adjacent areas. The area entered at the time of the activation is displayed here.

Last entry

Every day at midnight, the log book for the current day is read and the last entry is entered in the dataset for the respective person. This information is displayed under 'Last entry'. It can happen that an entry is several weeks ago. In this case the current location is not known. Nevertheless, the date of the last entry saved for the person is retained.

CEStronics

In AccessOne this date can also be used to automatically lock out persons who were not present for a definable period. This is controlled by means of the 'Absence time' lock type (see 'Lockouts' on page 80).

Cards

The list provides an overview of the access media assigned to a person. The current status and validity are stored. You can change a person's access medium by means of the 'Change card' button. If the person has lost their ID card, a replacement card must be activated.

Lockouts

Indicates whether a lockout has been entered for this person. Lockouts can also apply to the future and may in this case only become active from a later time. Lockouts that are currently active are highlighted orange. Lockouts can also be selected and deleted in this dialogue. If a lost ID card is then found again, the relevant lockout can be removed here. To do this, simply select the active lockout and then press the 'Delete' button.

Logbook

Clicking the 'Refresh' button shows the logbook messages about the person for the last two days. You can set the value between 2 and 7 days.

Example: a person is denied access and they inform the security personnel about this. The security service can then see at which door the person was refused entry and whether changes have been made to the person data, e.g. whether an authorisation has been taken away or a time model changed.



9.1.2 Master data

P P Dange New Copy	Delete Reload	Assignment						
	Overvier Mat	iter data Fi her masker o	lata Cards	Authentations Capture	e picture	Lockouty Access mask	g. 055	
Last name First name Personnel I	Ferrion data							
[Spind-Mast]	Lail isere:	Spind Midstor	Pipi name:		Further.			
	Title		Maden name:					
	Date of Cress	forest and	CIEVO/DADA		Country in	Bertro-		
	Unnder,	tempo sae	wants tiet/c		resources			
	Complete 7		Department.		Inho			
	Europeal so:		Destroyed Harr	E-Townstore	Estamain	Hearing		
	Organisation		Himasthy		Numbers	Lite		
	Bernerik		treasury.					
	Address / contrac	t date						
	Country							
	29 code				Street			
	Prose		ta:					
	Mobile		I year					
	Internal contact	distri						
	Phone internal		Office		Isableg			
- contract allow	Altendance							
Person data	Attrindant:		Department					
Authorizations	Approve visits		Accompany wa	ters	Control al	welds E		
Authorization profiles	Pin		-			-	-	
Company data	Aren DAAr		Vinnem EMA:		mad one	Compared the		
Logbook								
	-							

To create new person data, click NEW. The 'Master data' tab opens automatically. If you wish to leave this tab, you must first complete the two mandatory fields marked red, 'Name' and 'Personnel class'.

Person data

This area contains mandatory fields that must be completed for every person ('Name' and 'Personnel class'). AccessOne makes a distinction between the classes 'Staff', 'External staff' and 'Visitors'. Additional personnel classes can be created in the database by the administrator, but must be allocated to the three pre-defined classes – staff, external staff or visitors. Thus the user can divide external staff between, 'external companies with personnel leasing' or 'external companies', for example. Some lockouts are set based on the personnel class. Thus you can set a lockout following excessive absence to occur for staff after six weeks, but for external staff after just two weeks. Personnel class is also evaluated at the points of access.

Example: for bag checking purposes, the settings can be implemented in such a way that visitors are always checked, but in-company staff are checked only on the random check basis.

The personnel number is an external classification criterion that generally comes from an external personnel management system (e.g. SAP). This is used to assign persons in the access control system to the data held by the personnel department. The personnel number can also be used as a search criterion.

Define the company and department in the 'Company data' dialogue. It is defined here whether the company is an 'Own company' or an 'External company'. Only own companies can be entered into the 'Company' field; only external companies can be entered into 'Company 2'. The departments are predefined in the company data and can only be selected here. It is important therefore to enter the companies first and only then add the persons.

Address

Enter all of the relevant address data for the person here.

Contact data

Enter all of the relevant contact data for the person here.

Attendant

An attendant can be entered for external company employees. This must always be a member of in-company staff. The attendant is the responsible contact person for the persons entrusted to them.


PIN codes

AccessOne involves the use of three PIN codes. One PIN is the personal number code for the access control system. Certain doors can only be opened by entering this PIN code. The minimum length of the PIN can be set by a system parameter (standard length 4 characters, maximum 6 characters).

The PIN can be given a limited validity and can also be locked. If the wrong PIN code is entered three times, this PIN is automatically locked and must be changed in the system.

Two additional PINs are used in the system to arm and disarm the intruder alarm system. The PIN for arming and disarming can be identical, but must be different from the PIN used for access control.

It is a VDS*1 requirement that two different PIN codes are used. These PIN codes do not have a time-limited validity. Within the authorisation for a person at a door, there is an option to determine whether the person can arm the intruder alarm, disarm it or both. A PIN code can only be entered if this authorisation exists.

T even but even	
Pin code:	
Confirm pin code:	
Reset pin code:	
	OK Cancel

All PIN codes must be entered discreetly. The four- to six-digit PIN code must be entered twice and must include at least three different numbers. They are entered by the relevant ID card holder via a separate numeric keypad.



9.1.3 Further master data

Nachname: test Firma: Firma 2: Abteilung: Geboren am: Personalausweis / Reisepass Ausweisnr: Art: Cutrit Tatigkeitsbeginn: Datum auswählen Tatigkeitsbeginn: Datum auswählen Erlaubt von: Datum auswählen Erlaubt von: Datum auswählen Datum auswählen Datum auswählen Erlaubt von: Datum auswählen Datum auswählen Denstgang unterdrücken Importsperre Teilnahme Zeiterfassung Aufzuf Vorzugsetage: Dienstgang unterdrücken Aufzuf Vorzugsetage: Dienstgang unterdrücken Aufzuf Vorzugsetage: Dienstgang unterdrücken Einwanderung Datum auswählen Datum: Outm auswählen Seburtsland: Geburtsstadt: Parkgruppe:
Nachname: test Vorname: Firma: Firma 2: Abstellung: Geboren am: Personalausweis / Reisepass Ausweisnr: Art: Cutritt Tatigkeitsbeginn: Datum auswählen is Erlaubt von: Guitig bis: Importspere: Eilaubt von: Datum auswählen is Erlaubt von: Datum auswählen is Erlaubt von: Datum auswählen is Erlaubt von: Datum auswählen is Euler Zeitsaldo: Datum auswählen is Erlaubt von: Datum auswählen is Euler Zeitsaldo: Datum auswählen is Erlaubt von: Datum auswählen is Euler Zeitsaldo: Datum auswählen is </td
Firma: Firma 2: Abteilung: Geboren am: Personalausweis / Reisepass Ausweisnr: Art Ausweisnr: Art Art Gültig bis: Datum auswählen is Tatigkeitsbeginn: Erlaubh is bis: Datum auswählen is Erlaubh von: Datum auswählen is Erlaubh is bis: Datum auswählen is Importspere Telinahme Zeiterfassung aktueller Zeitsaldo: 0000 Dienstgang unterdrücken Erstes Kommen/Letztes Gehen unterdrücken Aufenthaltserlaubhis Gültig bis: Datum: Datum auswählen is Einwanderung Datum auswählen is Datum: Datum auswählen is Geburtsland: Geburtstadt:
Abtellung: Geboren am: Personalausweis / Reisepass Ausweisnr: Art: Curiti Tatigkeitsbeginn: Datum auswählen II Tatigkeitsende: Datum auswählen II Erlaubt von: Datum auswählen III Erlaubt von: Datum auswählen III Erlaubt von: Datum auswählen III Erlaubt von: Datum auswählen IIII Erlaubt von: Dienstgang unterdrücken Erstes Kommen/Letztes Gehen unterdrücken Aufenthaltserlaubnis Gultig bis: Datum auswählen IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
Personalausweis / Reisepass Ausweisnr: Art: Curiti Tatigkeitsbeginn: Datum auswählen Importsperre Tellnahme Zeiterfassung aktueller Zeitsaldo: Ording Aufenthaltserlaubnis Gültig bis: Datum auswählen Importsperre Tellnahme Zeiterfassung aktueller Zeitsaldo: Ordin Aufenthaltserlaubnis Gültig bis: Datum auswählen Importsperre Tellnahme Zeiterfassung aktueller Zeitsaldo: Ordin Aufenthaltserlaubnis Gültig bis: Datum auswählen Importsperre Tellnahme Zeiterfassung aktueller Zeitsaldo: Ordin Aufenthaltserlaubnis Gültig bis: Datum auswählen Importsperre Tellnahme Zeiterfassung Batum auswählen Importsperre Detum auswählen Importsperre Tellnahme Zeiterfassung Batum auswählen Importsperre Datum auswählen Importsperre Batum
Ausweisnr: Art: Gültig bis: Datum auswählen is Zuritt Tatigkeitsbeginn: Datum auswählen is Tatigkeitsende: Erlaubt von: Datum auswählen is Erlaubnis bis: Datum auswählen is Erlaubnis bis: Datum auswählen is Importsperre Tellnahme Zeiterfassung aktueller Zeitsaldo: Outzugsetage: Dienstgang unterdrücken Aufenthaltserlaubnis Gültig bis: Datum auswählen is Permanent Arbeitserlaubnis Gültig bis: Datum auswählen is Permanent
Zutritt Tatigkeitsbeginn: Datum auswählen is Erlaubt von: Datum auswählen is Importsperre Teilnahme Zeiterfassung aktueller Zeitsaldo: 00:00 Aufzug Sonderfahrt Aufzug Vorzugsetage: Importsperre Dienstgang unterdrücken Testes Kommen/Letztes Gehen unterdrücken Aufenthaltserlaubnis Gültig bis: Datum auswählen is Aufenthaltserlaubnis Gültig bis: Datum auswählen is Parkgruppe: Seburtsland: © Geburtsstadt:
Tätigkeitsbeginn: Datum auswählen Tätigkeitsende: Erlaubt von: Datum auswählen Erlaubnis bis: Datum auswählen Erlaubnis bis: Datum auswählen Freendsystemdaten Importsperre Importsperre Teinahme Zeiterfassung akufzug Sonderfahrt Aufzug Vorzugsetage: Dienstgang unterdrücken Erstes Kommen/Letztes Gehen unterdrücken Aufenthaltserlaubnis Gültig bis: Datum auswählen Estes Kommen/Letztes Gehen unterdrücken Aufenthaltserlaubnis Gültig bis: Datum auswählen Estes Kommen/Letztes Gehen unterdrücken Aufenthaltserlaubnis Gültig bis: Datum auswählen Estes Kommen/Letztes Gehen unterdrücken Aufenthaltserlaubnis Gültig bis: Datum auswählen Estes Kommen/Letztes Gehen unterdrücken Parkgnubris: Gültig bis: Datum auswählen Estes Permanent Arbeitserlaubnis: Gültig bis: Datum auswählen Estes Permanent Parkgnubris: Geburtsland: Parkgruppe:
Erlaubt von: Datum auswählen is Erlaubnis bis: Datum auswählen is Verlängerte Türöffnungszeiten Fremdsystemdaten Importsperre Teilnahme Zeiterfassung aktueller Zeitsaldo: 00:00 Aufzug Sonderfahrt Aufzug Vorzugsetage: Importsperre Importsperre Erlaubnis Erlaubnis Erstes Kommen/Letztes Gehen unterdrücken Aufenthaltserlaubnis Gültig bis: Datum auswählen is Permanent Arbeitserlaubnis: Gültig bis: Datum auswählen is Permanent Einwanderung Datum auswählen is Geburtsstadt: Permanent Parkglutz Parkgruppe: V Geburtsstadt: Permanent
Fremdsystemdaten Importsperre Teilnahme Zeiterfassung aktueller Zeitsaldo: 00:00 Aufzug Sonderfahrt Aufzug Vorzugsetage: Dienstgang unterdrücken Erstes Kommen/Letztes Gehen unterdrücken Aufenthalts- und Arbeitserlaubnis Gültig bis: Datum auswählen Aufenthaltserlaubnis: Gültig bis: Datum auswählen Importspere Arbeitserlaubnis: Gültig bis: Datum auswählen Importspere Datum: Datum auswählen Importspere Importspere Parkgruppe: Importspere Importspere Importsperee
Importsperre Teilnahme Zeiterfassung Aufzug Sonderfahrt Aufzug Vorzugsetage: Dienstgang unterdrücken Erstes Kommen/Letztes Gehen unterdrücken Aufenthalts- und Arbeitserlaubnis Gültig bis: Datum auswählen 5 Parkgnuppe: Parkgruppe:
Aufzug Sonderfaht Aufzug Vorzugsetage: Dienstgang unterdrücken Erstes Kommen/Letztes Gehen unterdrücken Aufenthalts- und Arbeitserlaubnis Gültig bis: Aufenthaltserlaubnis Gültig bis: Datum auswählen 5 Permanent Einwanderung Datum: Datum auswählen Seburtsland: Geburtsstadt: Parkplatz Parkgruppe:
Dienstgang unterdrücken Aufenthalts- und Arbeitserlaubnis Gültig bis: Datum auswählen is Parkgnuppe: Dienstgang unterdrücken Dienstgang unterdrücken Dienstgang unterdrücken Batum auswählen is Parkgruppe:
Aufenthalts- und Arbeitserlaubnis Gültig bis: Datum auswählen is Permanent Arbeitserlaubnis: Gültig bis: Datum auswählen is Permanent Einwanderung Geburtsland: Geburtsstadt: Datum: Datum auswählen is Geburtsstadt: Parkplatz V Geburtsstadt:
Aufenthaltserlaubnis Gültig bis: Datum auswählen is Permanent Arbeitserlaubnis: Gültig bis: Datum auswählen is Permanent Einwanderung Datum auswählen is Geburtsland: Geburtsstadt: Datum: Datum auswählen is Geburtsstadt: Geburtsstadt: Parkgnappe: V Geburtsstadt: Geburtsstadt:
Arbeitserlaubnis: Gültig bis: Datum auswählen IS Permanent Einwanderung Datum: Datum auswählen IS Geburtsstadt: Datur: Datum auswählen IS Geburtsstadt: Parkplatz Parkgruppe: Y
Einwanderung Datum: Datum auswählen Isi Geburtsland: Yarkgruppe: Yarkgruppe:
Datum: Datum auswählen Image: Separtsland: Geburtsstadt: Parkglatz Parkgruppe: ✓
Parkplatz Parkgruppe:
Parkgruppe:
Parkbereich: Parkplatz-Nr.: freie Nummer: Suchen
Nummembereich:
Berechtigt bis: Datum auswählen 15 00:00 Preiskategorie:
Sonstiges
Verkaufskategorie: Statusbericht: Erstellen

Enter all of the data that you wish to store for the person.

ID card/passport

Here you can enter the number of the person's ID card or passport together with its duration and validity. This data is stored for documentation purposes only.

Access

Start and finish dates (e.g. for limited contracts) are entered here so that appropriate lockouts can be set automatically. For staff, this data is, for example, used to specify the start date of new employees or the leaving date for employees who have given notice. An appropriate lockout is set before the start date or once the finish date is reached. Persons can thus be entered into the system before their first day of work. An element of this occurs automatically through the interface for the personnel data management system of the personnel department. When the leaving date is reached, the ID card is automatically locked.

External system data

Here you can select an import lock, preventing the system from synchronising data with external SAP sources on a daily basis, for example. When data is changed in AccessOne, it should not be possible to overwrite it again.

Instruction

If there is an obligation in the company for binding training to be given to new employees, you can enter the date of the first and second training sessions here. You can also enter the date on which the next training session must take place.

Residence and work permit

A valid residence and work permit is a statutory prerequisite for employment. For persons with limited residence and/or work permits, the system monitors compliance, provided that the relevant data is entered here. Entry of this data is in the interest of the employer, who is liable to prosecution if persons work on his system without this permit.

Immigration



This entry is for documentation purposes only and is optional.

Miscellaneous

The 'Vending category' is used to enable the use of an ID card at vending machines. A prerequisite is that the cards are coded by AccessOne.

9.1.4 ID cards (access media)

C AccessOme - Person data					- 🗆 X
Home Home					08
	XO	4			
-	-	F			
apt.	Cverview Magaet	dila Fuither master i da	Cards Authona Capture picture Locko	uts Access manks (QSS)	
Lettiname Firstiname Personne	Last name:	Spind-Master	First name:		
	Company:		Company 2:		
	Department:		Date of birth:		
	Charles and				
	Number Version	Valid from Valid until Status Rep Active	Vie Create-reas Return Layout back Layout front Unknown CES Systemicartie	Info text Last print	
					1
					Mew card
					X Delete card
	First card assignment	ton: 07.12.2020 Last car	d assignment on; 07.12.2020 Cards produced:	2	
	Selected card				_
	Number:	100 new	Version: 0 Code date: 100	Change card	
	Valid from:	Select a date 15 00:00	Valid until: Select a date 11 0000	Assign card	
	Stature	Active -	Count using per day: 0	Accume code data	
12	Layout Back:	CES Systemikarte -	front:	a montane	
Person data	Remarks:	Spind-Master,		Coding	
Authorizations	Infà text:			Coos Uni Uni	
	Last print:	Never printed	Count printed 0 Format CES-Master	Spind(Ded Card format:	
de Authorization profiles	Special type:	Guard		CES-Maiter Betterie(Legic)	-
Company data	Création reasons	Unknown -	Date returned: Select a diste	Print / code card	
- Lozhook	1			The Descor call	
- colocos				in the second seco	
Reports	Liser admin	And and a second second	Workstation: WV-11537	Events 0	Timeout not active

On this tab you can create, change, assign or print ID cards. In the table view you can see all the ID cards defined for this person.



A person can have more than one card. This is particularly necessary where different ID card technologies are in use.

To create a new ID card, select a person, then click CHANGE in the upper menu bar and click 'New card'.

To delete an ID card, select it in the list and then click 'Delete card'.

CAUTION: No security prompt is given before final deletion. If this button is pressed inadvertently, click the CANCEL button in the toolbar. Changes made in the current tab are then discarded.

Selected card

All of the data related to the ID card can be entered or updated here. The ID card number serves only as a classification criterion. Generally this has nothing to do with the code number in the ID card, although it can be identical to it.

The version number is a single digit ranging from 0 to 9 or A to Z. If an ID card is faulty, an identical ID card with the same card and code number can be produced again, but with the version number increased by one and stored together with the number coded in the ID card. Only the ID card with the current version number is thus valid. This number is checked at the door. If the number does not match, an appropriate message is

CEStronics

generated and access is denied.

Valid from/until

Cards may only be valid for a limited amount of time. This validity period is monitored by the system. The card is rejected outside the validity period. If no value is set, this means that the validity is unlimited.

Status

Only active ID cards are loaded on to the door controllers. Accordingly, an inactive ID card will not work. The system will then report: 'Card unknown'. Select 'Active' here if the ID card should also be valid.

Layout back/front

The 'Card designer' dialogue explains how to print cards. There you can also choose between various predefined layouts. If you are creating a new ID card, specify here which layout you wish to use. Layouts can be defined separately for each ID card.

A default layout can be determined based on the personnel class of the person, where the relevant layouts for each personnel class are created by the administrator (see 'Master data' on page 72).

Code data exist

When the ID card is created, the associated information stored in the card must also be saved. In cases where pre-coded ID cards are used, this is done using the **Assign card** button. A prompt asks you to hold up an ID card to the dialogue reader, so that the card information can be read and stored in the dataset. The display turns green and shows 'Code data exist'.

If the cards are coded by AccessOne, the **Assign code data** button is active instead. In this case, AccessOne applies a rule that corresponds to the customer's card format and determines a unique free code number. This number is assigned to the ID card. The **Code UHF card** button is used to code the ID card via the dialogue reader. Alternatively, the card can be coded and printed in a single step by pressing the **Print / code card** button. For this, a coding unit must be installed in the printer.

Print / code card

Shows a print preview of the ID card and its prepared layout. Once confirmed, the ID card is printed. If the printer is capable, the ID card is coded at the same time.

- 'Last print' shows the date and time when this card was last printed.
- 'Count printed' shows the number of cards printed for the selected person.
- 'Creation reason' allows you to select a reason for (re)issuing the card.
- 'Date returned' specifies the date on which the card was handed back. After this date the card is locked.



9.1.5 Authorisations

AccessOne - Person data			- 🗆 X
Home Home	and the second		te.
	× o J		
Sp. 1911	X Overseev Machin data Further macher data	Cards Authorizations appliane picture Lockputs Access market 055	
Dparent Albarr	Last name: Spind-Master	First name:	
	Company:	Company 2:	
	Department	Date of birth:	
	Default: Temporary:	- Vald from: Select a date 12 until Select a date 12	
	Overview		
	Profile Description	Valid from Valid until Active	
			D and
			V
			Deiste
	Authorization Description	Valid from Valid until Time model Active	
			Add
Person data	8		X Delete
Authorizations	Reader auth Description Entrance-Terminal Instruce-Terminal	Valid from Valid unt/ Time model Active	And
🖌 Authorization profiles			X Deletz
Company data	Selected reader		
Y Logbook	Entzance-Terminal from	Eleipti a date 🛐 until: Select a cate 🛐 Time model 👘 Active: 1	Apply changes
Reports	User admin	Workstation: INV-11537 The ONVersion Events 0	Timeout not active

In this menu, defined time models are allocated to the person. These must have first been created in the 'Authorisations' dialogue (see 'Authorisations' on page 60).

All of the information relevant to the access authorisations is included here:

Time models

A standard time model can be specified for each person. This then applies if there is no specific time model assigned to the authorisation. You can thus, for example, specify that a person normally has access from 09:00 to 17:00 but can continue to access the underground parking area after that time. Alternatively, access to particular areas can be restricted more tightly.

If no time model is specified, access is not time-restricted.

Additionally, you can specify a temporary time model that overwrites the standard time model for a particular period. Such a time model could allow a shorter time window (e.g. in cases of short-time working) or a longer window (e.g. for weekend working).

Beneath this are the two lists containing the selected profiles and authorisations for the person.

Profiles

A profile consists of a group of authorisations. Multiple authorisations can be combined under one profile. Profiles allow authorisations to be set up according to the person's function. One profile can thus be created for cleaning staff and another for technicians, for example. This method simplifies the choice of authorisations that each employee requires to perform their work.

Example: the building entrances are linked under one authorisation, and a profile for building entrances then contains the authorisations for each building.

Changes to the authorisations contained in the profiles will have immediate effect on the profiles. AccessOne transfers the profiles directly to the door controllers, so that a change to an authorisation or a profile immediately affects all persons who have been assigned this profile, without the need for additional datasets to be transferred.

CEStronics

A limited validity and a time model can be specified for each profile. If no time model is specified, the time model stored for the person applies. The profile is valid without limit if no validity restriction is entered. If a start date is given but no end date, the profile has unlimited validity from the start date. If an end date is entered it limits the validity.

To remove a profile from the list, select it and click the Delete button beside the selection list. To create a new profile, press the 'Add' button. A selection box opens, from which the required profile can be selected. You can make multiple selections by holding down the CTRL key while clicking.

Authorisations

Authorisations combine readers into a related group. See also the 'Authorisations' dialogue (see 'Authorisations' on page 60). The same rules apply for authorisations as for profiles.

Selected authorisation

If one or more authorisation or profile is selected by clicking, the details are shown in these fields and can be edited here. Click the

Apply changes button to then enter the changed fields into the authorisation or profile.



To adopt the changes, the **Apply changes** button must be pressed, otherwise the changes are not saved.

Up to 64 authorisations and/or profiles can be allocated to one person (e.g. 10 profiles plus 22 authorisations). If the same authorisations are always specified for a large number of persons, we recommend that these authorisations are combined in their own authorisation profile.



If a person is assigned an authorisation that is already contained in an authorisation profile allocated to that person, this redundant authorisation is deleted during the automated midnight maintenance process.



9.1.6 Capture picture

AccessOne - Person data					~ ¤ ×
	×Q	<u>-</u>	_	_	
Int Last name First name Personnel (Last name: Company: Departmen	forther matter date Spind-Master t:	Canda Authonizationer Caedium piet (v Lo First name: Company 2: Date of birth:	ckeuts A) es imats -065	
	Lockeut	Reson	Pran Unil	Mes Jobair	
	Selected lockos Lockout: Ressor:	er Freie Eingabe Tistgleietende Tärsgleietende	Providence PR	Deter lodout	
Person data	Remark:	Abwesenheitszeit Ausweis nicht zurücksegeben	a until Select a date [18]		
Authorizations		Mehirlach falscher Pincode			
Authorization profiles					
Company data					
Logbook					
Paparte	User: admin	Na dalog meant cometer	Workstation: INV-11537	Events 0	Tenhout: not active

In the 'Capture picture' tab you can allocate an image to a person by importing it, or alternatively taking a photograph.

If you wish to import an image for the person, select the person in the selection control on the left and click CHANGE in the toolbar above. Now press the **Import picture** button.

You can select files in the *.bmp, *.png or *.jpg formats. To take a photo, a camera must be connected to your PC/laptop.

In the 'Camera' dropdown box, select the relevant device. You can select a different resolution and other camera settings to suit the type of device connected.

Press the **Start camera** button to take the photograph.

After choosing the preferred image section (green frame), press the Save

picture button and the image will be displayed in the preview in the top right-hand area.



If you move to another tab without saving, the image is not retained for further editing.



9.1.7 Lockouts

C AccessOne - Personendaten						- 🗆 X
Home Home						0
Abarecher Speichern	×O	B			2	
Ne s Tamit La Nacharen Vornana Penopalar te:	Ubecsicht Stam Nachname: Firma: Abteilung:	ntasken Weitere Stammdaten test	Ausweise Berechtigungen Vorname: Firma 2: Geboren am:	Bild auffrehn Sperren	7 rittemasken X55 Sp	ndo Bulémungen
	Sparre	food	Van:	Be	New Spane	
	Gewählte Sperre Sperre:		-			
2 Personendaten	Grund: Gültig von:	Tötigkeitsende Tötigkeitsende	Datum ausw	shien 15		
🖌 Berechtigungen	Bemerkung:	Abwesenheitszert Ausweis nicht zurückgegeben Mehrfach falschar Bincode				
🗲 Berechtigungsprofile	1	Instruction and the second				
Firmendaten						
📕 Logbuch	Benutter, admin	ben Delageter verfustas	Arbeitsstation: INV+11537	Alle Amc und Mac online	Ereignisse D	Timeout nicht aktiviert

In this tab you can lock people out, e.g. if an employee has lost their ID card.

To do so, double-click the person in the selection control on the left whom you wish to block. This takes you into editing mode. The **New lockout** button is now active and you can assign a lockout to the person. You implement additional settings in the 'Selected lockout' section.

If the lockout is time-limited (e.g. prior to a start of work date), select the 'Valid from' and 'Valid until' dates accordingly.

Enter any comments about the lockout in the 'Remark' input field. Save the lockout by clicking the SAVE button in the toolbar. You can delete a lockout by selecting it in the list and pressing the **Delete lockout** button. AccessOne distinguishes between automatic and manual lockouts. Additional lockouts can also be predefined in the system if required.

Example: lockouts before the start of work and after the end of work.

This lockout can also be set manually and is effective immediately. It should be noted in this case that during the night, the system updates the lockout based on the data entered for the person. If a person is, for example, locked out after the end of work, but has to return to the office the next day, the lockout can be manually deleted, but will automatically be set again after midnight.



9.1.8 OSS-SO

Thanks to the OSS Standard Offline, electronic cylinders and handle sets from different manufacturers can read the same authorisations from the card and can interpret them in the same way.

C AccessOne - Person data		- 🗆 ×
	XOB	
Spa 1971 Last norm: First name Personnel Bener2Maw	Last name: Spind-Master First same: Company: Company 2: Department: Date of birth: Offlice date	\supset
	Nmm Card Card Default velocity: Ø 0 h.m. valid sole 2806.0411500 Default backer reservation: Ø 0 b.m. valid sole 2806.0411500 Default backer reservation: Ø 0 b.m. valid sole 2806.0411500	
	Oversive Authorization Description Veild Irom Veild und Time modelt Active Toggie Auth Irvet	
		Add
Person data	Cylinder Auth Description Valid from Valid until Time model Active Toggle Auth Invest Schwark 1 Schwark 1	Leter
Authorizations		X Delete
Authorization profiles	Selected authorizations	tert some
Company data	nom peed a sate (b) unit: Seed a sate (b) inne moder.	Appay cranges
Logbook	Emoure Offine search -000 lists	and transmit
Reports	User admin No. microsom Workstation INV-11537 1140 Mar Byerts 0	Timeouti not active

The setup and management of electronic cylinders and handle sets that are compatible with the OSS standard is fully integrated into AccessOne. To set up an electronic cylinder, you also need the configuration tool supplied by the respective manufacturer so that the configuration data can be programmed in.

All of the configuration data is stored in AccessOne. You can then generate an .xml file from the user interface that is read in by the relevant configuration tool. This file contains all the data for initialising the electronic cylinder.

After the requisite licence has been installed, the function selection includes an OSS button. This enables you to open dialogues in which to maintain the data for offline components. Here you specify the validity of the cards for each person and add profiles, authorisations and electronic cylinder authorisations. Finally, you code the ID card.



9.1.9 Instructions

Nachname Vomame Personale	Obersicht Staromdaten Nachname: Sest	Weitere stammoaten	Auswerse Derocht	igungen Bitd a	ufnenimen Sperren	Zutritismasken	OSS Spinde	Belehnungen
Jan 1 J	Firma:		Firma 2:					
	Ableitung:		Geboren a	KYT:		_		
	Belehrung	Beschräibung		Datum	Nächster Termin			
						10 tors		
						Xinter		
	5 - 00 - 0 - 0 - 0					- 92		
	ACMINIC PERCHANNEL	Danse	Dimension	Ter Sharman Ten	_			
		- Lawrence		TO Presente and				
ersonendaten	F							
Versonendaten Nerechtigungen	n							
Personendaten Berechtigungen Berechtigungsprofile								
Personendaten Berechtigungen Berechtigungsprofile								
Personendaten Berechtigungen Berechtigungsprofile Firmendaten Logbuch								

Instructions that must be given within a specific timeframe (e.g. for accident prevention regulations (UVV), data protection (GDPR), etc.) can be stored here. Click the 'Add' button to select these and enter them with a date.



9.2 Group changes

In the 'Group changes' dialogue, changes to person data, person lockouts and authorisations can be applied to entire groups by means of a data import.

9.2.1 Person data

AccessOne - Gruppinsänderungen							- 0
Home C							
eeren Ausführen							
Sougest-in-derungen Prozontikerschägungen Prozontikerschägungen Prozontigerren	Personendiatem Dotern Organisation: Tasgietesiendie Himenietenang Filma Eurosat Zechnodati Standardi Tempode	Indem Isichem	arth-		TTTT DB: 11-00-0-00000000 [12]		
					(impatrieren		
System-Konfiguration							
ACLS							
Gruppenänderungen							
Kartendesigner							
* OSS							
	Benutzen admin	New Parling root and a	Arbeitsstation	INV-11537	Alle Anic und Macionline	Eleignisse 0	Timeout nicht ektivert

In the 'Person data' tab, previously created data for person groups that have been imported by clicking the **Import** button can be changed or deleted.

The data to be imported must be available in *.csv file format. This file can be generated by means of the dialogue page 'Reports > Persons > Person group export'. Various filters for configuring person groups are available on this dialogue page. When a report is created, the created person group can be stored on the hard drive as a MS Excel file and continue to be edited.

The *.csv file saved from this program serves as an import file for all group change dialogues.

9.2.2 Adding or deleting person lockouts

4 AccessOne - Group changes							-	×
Home								0
Clear Elecute								
Group changes Person data	Person lockouts	1						
Person lockauds	Lockouts	🔾 defete 🔿 add						
	Lockout	2	-					
J& ACLs	Reason	Freie Eingabe Täbigkeitsende						
Le Visitor / Appointments	Valid from:	Tätigkeitsbeginn Abwesenheitsteit	and i	Select a date	223			
k External employee	Remark	Ausweis nicht zurückgegeben Mehrfach falscher Pincode						
A 10. 10						lane .		

In the 'Person lockouts' tab, lockout data for a specific person group can be added by importing a file or deleted.



The 'Lockout' input field offers various reasons for the lockout; that can be selected with a validity period.

9.2.3 Modifying person authorisations

Home					- 0
ren Austühren					
		-			
Puntoonsberrentigungen	Personenberechtigungen	1			
Personendaten Personensperren	Berechtigungen				
	🔾 káso	chen 🔾 hinzuflügen			
	Frofil	Gultig von Gultig bis	Status Aktiv		
				Hinzufügen	
				X Läschen	
	Ta and	(Pality and Pality and	a desire da		
	Berechtigung	Guitag van Guitag bis	Zertmodeli Status Aktiv	T water	
				- Minzurugen	
				X Löschen	
	Gewählte Berechtigungen				
		von: Datum auswah	bis: Datum ausmät 15 Zeitmodelt	* Aktivi 🗀	
			Status:	-	
				Anderungen übernehmen	
	-				
				Importieren	
System-Konfiguration					
ACLs					
Gruppenänderungen					
Kartendesigner					
the rest of the second s					
OSS					
Besucher / Termine	Benutzen admin	for Selative Helight	Arbeitistation: NV-11537	Alle Amc und Mac online Ereignisse: 0	
		- 0 ×	Profile		
Berechtigungen					
Gerechtigungen			Ĺ		□ ;
Berechtigungen			ĺ.		
Berechtigungen Nøme	Beschreibung		Name	Beschreibung	
Berechtigungen Name Demoboard Blau	Beschreibung Demoboard Blau		Name Aufzüge zu den Besprechun	Beschreibung Igsräume Aufzüge zu den Besprechungs	I)
Serechtigungen Name Demoboard Blau Finance and controlling	Beschreibung Demoboard Blau		Name Aufzüge zu den Besprechun Besprechungsräume	Beschreibung Igsräume Aufzüge zu den Besprechungs	I :
Berechtigungen Name Demoboard Blau Finance and controlling Musterkoffer DM	Beschreibung Demoboard Blau Musterkoffer		Name Aufzüge zu den Besprechun Besprechungsräume	Beschreibung ngsräume Aufzüge zu den Besprechungs	I :
Berechtigungen Name Demoboard Blau Finance and controlling Musterkoffer PM Production	Beschreibung Demoboard Blau Musterkoffer		Name Aufzüge zu den Besprechun Besprechungsräume	Beschreibung Igsräume Aufzüge zu den Besprechungs	I)

In the 'Person authorisations' tab, authorisations for a given person group can be added or deleted by means of a file import or by entering profile and authorisation information. Always confirm changes by pressing **Apply changes**.



10 System documentation

To document the system at a specific point in time, reports can be created and logbook entries viewed and exported.

10.1 Reports

The 'Reports' dialogue selection allows all of the previous entries to be viewed and exported. AccessOne can export a complete system documentation at any time.

AccessOne - Reports				- <u> </u>
Home Home				
Cear Execute				
* Reports	Authorizations			
Devices Device status by logbook	Search			
Reader battery state	Profile.	Description		
Authorizations Authorizations Authorizations per person Authorizations in authorization profiles. Offine authorizations per person Authorizations per person Authorizations per person			- Add	
Authorization history per device			X Defete	
List of authorizations Vericus Logiscolk Blacklisted cards in cylindien Persons Persons	Authorization	Description		
Person authorizations Persons in areas 4 Visitor / Appointments				
Apparatments			X Delete	
	Reader	Description		
Authorization profiles				
A Company data				
Logbook			Add	
Reports			Delete	
P Device data	viow			
	User; admin	Section realization	Warkstation INV 11537	Events: 0 Timoout not active



10.2 Logbook

The 'Logbook' dialogue lets you retrieve all current messages of the day and create individual filters.

10.2.1 Messages

Home										
S D B B X	0									
	A Real Property lines			_		_	_	-	_	
	Messages Iter			_						
Name Rescription	Date LAC/WS	Reader / Login	Area / Program	No.	Message	Card	Last name	First name	Company	
ktsell Alle Tagesmeldungen	28.10.2021 07:25:32 INV-11537		MasterProcess	807	Master starting AccessOne syst	-	-		-	-
stteriewamung	26.10.2021 07:25:34 INV-11537	-	LogWriter	800	Process starting	-	-			
ES Leser	28.10.2021 07:26:34 HVV-11537		LogWriter	801	Process started	-				
atasec Leser	28.10.2021 07:26:36 INV 11537		Nobfier	800	Process starting	-	-			
AC	28.10.2021.07/25:36 INV-11537		Notifier	801	Process started	-	1		1	
ffine Gerät	28.10.2021 07/25:38 INV-11537		LogReader	800	Frocuse Starting					
	28.10.2021 07:26:45 INV-11537		LogReader	801	Process started		÷			
	26.10.2021 07:26×17 INV-11537		LicenseProcess	800	Process starting					
	28-10-2021 07/26:47 INV-11537		LicenseProcess	801	Process started					
	28 10 2021 07:26:49 INV 11537		AcMasterCom	829	Connection to Mac Mac estate					
	28.10.2021 07:26:49 INV-11537	-	AcMasterCom	800	Process starting	-	1			
	28:10:2021 07:26:49 INV-11537		AcMasterCont	801	Frokess staded		1		1.000	
	28.10.2021 07:26:50 INV-11537	Mac	1.000	420	Software info: MACV0011:		-			_
	28.10.2021 07/26/51 INV-11537		PersonImport	1800	Process statting					
	28.10.2021 07:26:53 INV-11537		PersonImport	801	Process started					_
	25 10 2021 02/26-55 16/0-11532		MahFathanna	BOIL	Process Hartion	_				-
	28 10 2011 07/25/55 UNV-11537		WahEschange	801	Fromes started					-
	20 10 2011 07 20 07 180 1927		Web Anna	000	Protoco starting					-
	20 10 2021 07 20 37 100V-11307		WebAlleo	000	Process starting					_
	25.10.2021 07:26:57 INV-11:537		WebAccess	1001	Process started	-				-
	28.10.2021 07/2037 11/04 11937		MasterProcess	000	Waster started Accessione syste	_				-
	28:10:2021 07:27:08 Mac	Haupteingang		401	Device not running			-		_
	28.10.2021 13:01:49 INV+11537		MasterProcess	807	Matter starting Accessiona syst	_				
Authorization profiles	28.10,2021 13:01:51 INV-11537		LogWriter	008	Process starting					_
Authorization promes	26.10.2021 13:01:51 INV-11537		LogWriter	801	Process started	_	-			_
	28.10.2021 13:01:53 INV-11537		Natifier	600	Process starting		-			_
Company data	28.10.2021 13:01:53 INV-11537		Natifier	801	Process started	-				
	0.2021 13:01:56 INV-11537		LogReader	300.	Process starting	-				-
Logbook	28, 12021 13:02:02 INV-11537		LogReader	801	Process started		1		-	
1	0.2021 13:02:04 INV-11537		LicenseProcess	800	Process starting	-				
Reports	28.10.2021 13:02:04 HVV-11537		LicemieFront	801	Process started					
	28.10.2021 13:02:06 INV-11537		AcMasterCom	829	Connection to Mac 'Mac' estab-					
Device data	Total months of females				in second			-		
					L_ Activate up	screates.		14	16.5	

10.2.2 Filters

Define individual filters. AccessOne offers a variety of options for adding a filter.

C AccessOne - Logbook							-	D	×
Home									-00
Change New Copy Delete	Reload Assignment	ne							
		ter							
Name Description	Name an enter	0.02							
Aktuell Alle Tagesmeldungen		Etrainum en	Printer and	0					
Bittenewarnung	PUBW /MPIHE	and the sold	canality.	Fuu-					
Datasec Leser	Description								
MAC	Duite								
Offline Gerät	fromte	Lings pig. 7 0000	xorte	for the second	100 0000				
			Time window						
	Person data								
	Laitname		First name:						
	Carrine		Company name:						
		Excession and an			_				
	Device data	Name Description	ŋ.,	lype					
					IF	1.4.20			
						1486			
					×	Does			
	Message dato	Message		Number	1				
Authorization profiles		Battery voltage good (Level: '(0)')	442						
Company data		Battery voltage low	476		1.				
n company data		Battery voltage low or missing (Level:)	0))	441		Alt			
Logbook					×	Deep			
E Reports									
🧨 Device data									
A 055	User: admin	Terr (Baller) entrative Lorenzett	Workstatio	NV-11537	In This other	Events	2		11-



Click the **Add** button to open a window listing all of the devices and message data that can be used for filtering.

AccessOne - Logbook					
Home					
Cancel De Save	<u>.</u>				
Messages	Filter				
e E Managar	1.000				
Name Dewription Name an ca	legory				
Alle Tagesmeldungen Filter name	Batteriewarnung	Category:	Ohne	2	
TS Lear-			-		-
latases Leser			(Lease		
AAC Date			* Messages	- 0	×
ffline Gerät	Entration (2000)		1		
trom:	Select a tiate	until	E		
A second s		Time win	W Message	Number	
Person data			III Definition of logbook message nur	nt 835	
Last name:		First nam	OQIAM read	483	- 10
Contract		Company	(0) single licenses of type '[1]' activate	d 710	
Card Hot		Company	Access denied, antipassback error	259	
Device data	Name Descript	fion	Access mask '(0)' assigned	51	
	1000		Access mask '(0)' changed, Property: '	(1 54	
			Access mask [0]' changed, Property:	(1 728	
			Access mask '(0)' created	726	
			Access mask '[0]' deleted	729	-
			Access mask '[0]' removed	53	-
			Access mask '[0]' removed, valid until	1 55	-
			Access mask (U), Property: [1:R], Val	36 32	
Message data	Message		Access mask (0), Property: (1:R), val	200	
Authorization profiles	Battery changed		- Access permittee	811	
- Contraction of the contract	Battery voltage good (Level: '(0)')		- ACL 101 channed Property 11-S1 of	11 657	-
Company data	Battery voltage low		- ACL '(0)' created	655	
Company data	Battery voltage low or missing (Level	E. (0).)	-		-
Logbook		-		Select. Cance	C
Reports			<u></u>		
🌶 Device data					
A nac	No many search crem	ware Wa	rkstation: INV-11537	Events 0	

11 Troubleshooting

Connection between the	In installation directory	Check the entries in the file ClientConfig.xml in
clients		the installation directory\AccessOne\config.
and AccessOne server		Do the entries for 'MasterHost' and 'Master-
not working		Port' match?
	On the server	- Have the SQL Server and SQL Browser services
		been started and have the TCP/IP and named
		pipes protocols been activated?
		- Check the firewall rules. Are the SQL Server
		port
		(standard: TCP 1433), SQL Browser port (stan-
		dard: UDP 1434) and the configured AccessOne
		ports (e.g. TCP 50000-500xx) accessible?
	Server-client	Is the time synchronised between the client
	interaction	and AccessOne server?
		A time difference of less than 5 minutes is
		allowed.



Teaming up for security



C.Ed. Schulte GmbH

Zylinderschlossfabrik Friedrichstraße 243 42551 Velbert, Germany © +49 2051 204 0 © +49 2051 204 229 © info@ces.eu