

AccessOne

Logiciel de contrôle d'accès



Description du système et instructions

Français Version VA1 BRO2262

Inhalt

1	À propos	de ces instructions	4
	1.1 Fabric	ant et service après-vente	5
	1.2 Group	es cibles de ces instructions	5
2	A propos	de votre sécurité	6
	2.1 Consig	gnes de sécurité	6
	2.2 Rema	rques légales	6
	2.3 Config	guration système requise	6
	2.4 Protec	tion des données dans l'AccessOne	6
3	À propos	de l'AccessOne	8
	3.1 Exten	sions des fonctions	9
	3.2 Procé	dure recommandée pour la première mise en place de l'AccessOne	10
4	Gestion g	énérale des boîtes de dialogue	12
'	4.1 Mode	affichage – Mode modification	13
	4.2 Barre	d'outils	13
	4.2 Durie		
5	Connexio	n	16
6	Configura	tion de l'AccessOne	17
0	6 1 Confid	auration du système	17
	6 1 1	Daramètres	17 17
	612	70nos	10
	612	Croupes do parking	19 10
	614	Stations de travail	
	615	Formats do loctour	20
	616	Applyco dos badgos	20
	0.1.0	Allaryse des Dauges	⊥∠
	0.1.7	Licences	ZZ
	0.1.0 6 2 Donn	Formats de Dauge	22
	0.2 DUIIII	Croupes d'utilisateurs	
	6.2.1 6.2.2	Données de base des utilisateurs	/ ∠
	0.2.2	Donnees de Dase des dunisaleurs	20
	0.2.5	Attribution des jour de données aux listes d'assès - ACL	29
	6.2.4	Althoution des jeux de données aux listes d'acces – Act	
	0.2.5	Groupes a utilisateurs onnine	
	6.3 Donne	ces a emplacement	
	6.3.L	Creer un emplacement	
7	Configura	tion des appareils	
	7.1 Donne	ées des appareils online	35
	7.1.1	Afficher l'aperçu des appareils	35
	7.1.2	Créer un MasterController (MAC)	
	7.1.3	Créer une commande de porte (LAC)	
	7.1.4	Créer une porte	41
	7.1.5	Afficher le statut de l'appareil	54



7.2 Do	onnées des appareils offline (OSS-SO)	
7.2.1	Données d'équipements	
7.2.2	Cylindres électroniques (et garnitures)	
7.2.3	Programmer les appareils offline	
7.2.4	Autorisations	
7.2.5	Import de données	
7.2.6	Modèles de temps	60
8 Configura	ation des autorisations	61
8.1 Autor	isations	61
8.1.1	Aperçu des autorisations	61
8.1.2	Généralités sur les modèles de temps et de jour	
8.1.3	Modèles de jour	
8.1.4	Jours spéciaux et fériés	
8.1.5	Modèles de temps	
8.1.6	Masques d'accès	
8.2 Profil	s d'autorisation	
8.2.1	Aperçu des autorisations online	
8.2.2	Aperçu des autorisations offline	70
9 Création	de données personnelles	71
9.1 Donn	ées personnelles	71
9.1.1	Aperçu des données personnelles	71
9.1.2	Données de base	73
9.1.3	Autres données de base	75
9.1.4	Badges (médias d'accès)	
9.1.5	Autorisations	
9.1.6	Prendre une photo	
9.1.7	Blocages	
9.1.8	OSS-SO	
9.1.9	Instructions	
9.2 Chan	gements de groupe	
9.2.1	Données personnelles	
9.2.2	Ajouter ou supprimer des blocages de personne	
9.2.3	Adapter les autorisations de personnes	
10 Docu	mentation de l'installation	
10.1 Rap	ports	
10.2 Logi	pook	
10.2.1	Messages	
10.2.2	Filtres	
11 De	épannage	

1 À propos de ces instructions

Ces instructions contiennent des informations de base sur la mise en place et l'administration d'une installation de contrôle d'accès avec le système de contrôle d'accès AccessOne.

Les instructions font partie du produit et doivent être conservées pendant toute la durée de vie et d'utilisation du produit. Transférez les instructions à chaque utilisateur ultérieur du produit.

Documents applicables

 Activation de licence >
 BRO2307_FR_Fiche d'informations_Activation-module-de-licence-AccessOne

 Installation >
 BRO2313_FR_Instructions_Installation-AccessOne

Caractéristiques de conception



Fait référence à d'autres documents d'information.



Indique d'autres informations et conseils.

Indique les avertissements dans les instructions étape par étape et les informations particulièrement importantes.

Conventions d'écriture

Dans ce document, les éléments de commande de l'interface de dialogue, par ex. les touches, sont indiqués en gras (exemple : Cliquez sur **Créer un utilisateur**). Les boutons de la barre d'outils sont en outre indiqués en majuscules (exemple : Cliquez sur ANNULER). Les noms des objets de données, des champs de sélection et de texte libre, ainsi que des cases à cocher sont indiqués entre guillemets (exemple : saisissez des informations supplémentaires dans le champ « Remarques »).

Illustrations

Les boîtes de dialogue illustrées dans les instructions ne contiennent pas toutes les options proposées par le système. En fonction de la licence et des options activées, les captures d'écran et la description peuvent varier.

Remarques sur la protection des marques

MIFARE, MIFARE Classic et MIFARE DESFire sont des marques déposées de NXP B.V. et sont utilisées sous licence.

Les indications et données comprises dans ces documents ne peuvent pas être modifiées ou développées techniquement sans indication préalable. Aucune partie de ces documents ne peut être reproduite ni transmise dans un but quelconque sans autorisation écrite expresse de C.Ed. Schulte GmbH Zylinderschlossfabrik. © 2021 C.Ed. Schulte GmbH Zylinderschlossfabrik, Velbert/Germany BRO2316-1 Version : VA1

Veuillez toujours utiliser la version la plus récente de ces instructions. Les versions mises à jour sont disponibles sur www.ces.eu.



1.1 Fabricant et service après-vente

Les droits d'auteur de l'AccessOne sont la propriété de ACcesstronic GmbH. Le service après-vente et l'assistance sont pris en charge par C.Ed. Schulte GmbH, sise à Velbert. Pour une assistance en cas de service après-vente, veuillez contacter le service après-vente CES. Vous pouvez contacter le service après-vente CES au +49(0)2051 204 222 ou par e-mail : hotline@ces.eu

Fabricant	Service après-vente et			
	assistance			
ACcesstronic GmbH	C.Ed. Schulte GmbH	Tél. : +49 (0) 2051-204-0		
Gartenstr. 38	Zylinderschlossfabrik	Fax : +49 (0) 2051-204-229		
D-52249 Eschweiler	Friedrichstr. 243	www.ces.eu		
	D-42551 Velbert	info@ces.eu		

1.2 Groupes cibles de ces instructions

La mise en place de l'AccessOne est mandatée par l'exploitant de l'installation et effectuée par le propre personnel spécialisé ou les fournisseurs de services du domaine informatique/administration. L'utilisation de l'installation de contrôle d'accès peut uniquement être effectuée par du personnel formé aux produits. Les informations de ces instructions sont donc destinées à différents groupes cibles. Les groupes cibles sont indiqués au début de chaque chapitre principal. Veuillez respecter nos recommandations pour la procédure d'installation, de mise en place et d'utilisation de l'AccessOne.

Groupe cible	Compétences
Personnel spécialisé	Expérience professionnelle de longue date dans le secteur des structures informati-
Informatique/admi-	ques, de l'administration et des réseaux.
nistration	Propriétés spécifiques du groupe cible :
	Connaissance des termes informatiques techniques
	Connaissance de la structure et de l'entretien de réseaux, en particulier connaissan-
	ce du réseau dont vous vous occupez
Exploitants d'instal-	Expérience dans la gestion de systèmes de fermeture. Il peut s'agir de plusieurs in-
lation	stallations ou d'une connaissance approfondie d'un système de fermeture unique.
	Propriétés spécifiques du groupe cible :
	Connaissance des termes techniques liés aux systèmes de fermeture
	Connaissance de l'utilisation d'un ordinateur et de logiciels
Personnel	Formé au produit par CES ou par un partenaire spécialisé CES. Le personnel a été
formé au produit	préparé de manière ciblée et approfondie à la tâche correspondante.
	Propriétés spécifiques du groupe cible :
	Connaissance du produit CEStronics et expérience dans l'utilisation de ces produits
	(assemblage, utilisation, etc.)

2 À propos de votre sécurité

2.1 Consignes de sécurité

Le système de contrôle d'accès AccessOne décrit dans ce manuel peut uniquement être utilisé par des personnes aptes et qualifiées à ces missions. Le personnel qualifié dispose d'une expérience professionnelle de longue durée dans le secteur des structures informatiques, de l'administration et des réseaux, et peut, en raison de son expérience en gestion de systèmes de fermeture ou de ses connaissances approfondies d'un système de fermeture, reconnaître les risques et éviter les éventuels dommages.



Une porte verrouillée empêche l'aide ou entraîne des dommages matériels

Des composants mal programmés peuvent provoquer un accès involontairement verrouillé. Si une porte verrouillée empêche l'accès à des personnes ayant besoin d'aide ou entraîne des dommages matériels ou d'autres dommages, C.Ed. Schulte Zylinderschlossfabrik GmbH décline toute responsabilité !

2.2 Remarques légales

L'acheteur est ici explicitement informé que l'utilisation du système de contrôle d'accès AccessOne peut être soumise à des exigences d'autorisation et des droits de participation légaux, et ici en particulier relatifs à la protection des données. L'acheteur et l'utilisateur final sont responsables de l'utilisation légale du produit.

2.3 Configuration système requise

La configuration système minimale pour l'AccessOne se base sur la configuration système recommandée pour Microsoft SQL Server.

- Système d'exploitation (serveur) : à partir de Windows Server 2016
- Système d'exploitation (ordinateur) : à partir de Windows 10 Professional
- Mémoire : au moins 8 Go
- SQL Server : à partir de MS SQL Server 2016, version Express utilisable
- Disque dur : au moins 1x 500 Go, 2x 500 Go recommandés
- Carte réseau

2.4 Protection des données dans l'AccessOne

Respect des délais de suppression

L'AccessOne dispose d'un processus de suppression paramétrable, qui démarre chaque jour peu après minuit et qui retire du système les données dont le délai de conservation a expiré. Cela comprend en particulier les données de mouvement. Les paramètres peuvent être réglés par l'utilisateur du système.



Pour répondre au RGPD, la suppression de messages de logbook à caractère personnel peut être configurée. Le paramètre « LogbookRewriteOffset » permet de régler le nombre de jours après lequel cela doit être effectué.



Paramètre	Description	Réglage standard
DateDeletedOffset	Délai après lequel les jeux de données personnelles	3 jours
	avec date saisie « dateDeleted » sont définitivement	
	supprimés de la base de données.	
VistorDeleteOffset	Délai après lequel les visiteurs sont supprimés.	183 jours
EventDeleteOffset	Délai après lequel les événements traités sont suppri-	183 jours
	més.	
AppointmentDelOffset	Nombre de jours après lequel les rendez-vous de visite	365 jours
	et toutes les données liées sont supprimés.	
LogbookRewriteOffset	Nombre de jours après lequel les messages de logbook	0 (pas de suppres-
	à caractère personnel sont supprimés des logbooks.	sion)
LogbookDelMessages	Les numéros des messages de logbook à caractère	Tous les messages de
	personnel qui doivent être supprimés. Il est possible de	visite
	saisir des numéros et plages de numéro individuels.	
LogbookLastRunTime	Date à laquelle le dernier processus de suppression a	Date de la dernière
	été effectué avec succès.	exécution

Réduction des données

L'utilisateur détermine les données nécessaires à l'utilisation et aux tâches. Pour l'utilisation quotidienne de l'AccessOne, un nom et une identification personnelle (interne/externe/visiteur) sont nécessaires par personne. Le nom ne doit pas être le véritable nom du propriétaire du badge. Il est également possible d'utiliser un pseudonyme (par ex. : « MA_001 »). En règle générale, l'utilisation d'un nom, en relation avec le RGPD, n'est pas critique.

Contrôle de saisie

L'AccessOne enregistre chaque modification de données avec la station de travail, l'utilisateur et l'horodatage ainsi que l'ancienne et la nouvelle valeur du champ de données correspondant.

Contrôle d'accès

Selon la norme DIN EN 50133-1, l'accès est l'opération d'entrée ou de sortie d'une zone de sécurité. La commande et la régulation s'effectuent via l'AccessOne. L'accès est également l'utilisation logique de données dans des ordinateurs, c'est-à-dire la lecture, l'écriture, la modification et la suppression. Enfin, l'accès est l'introduction logique de l'utilisation d'un système d'information ou d'un réseau de communication. Le contrôle d'accès est donc la vérification mécanique de l'autorisation d'accès à un système d'information ou à un réseau.

Pour la surveillance et le contrôle, des mesures d'organisation technique correspondantes doivent être effectuées par le client en mettant en place ou à disposition une infrastructure informatique (port USB, directives de mot de passe, LDAP, etc.). L'AccessOne soutient cela en offrant la possibilité d'assigner des droits d'utilisateurs correspondants dans l'interface utilisateur.

3 À propos de l'AccessOne

Le système de contrôle d'accès AccessOne est, dans sa version complète, un logiciel de gestion du contrôle d'accès modulable de manière flexible pour des grandes installations jusqu'à 200 000 utilisateurs, 16 000 lecteurs de badges et jusqu'à 100 000 appareils d'accès offline. Une version pour les petites et moyennes entreprises est disponible avec la licence AccessOne PME.

Le système de contrôle d'accès commande des portes, armoires et autres dispositifs de verrouillage. Le noyau du logiciel est une gestion des utilisateurs et des autorisations, qui enregistre toutes les activités des appareils connectés et surveille les processus en cours. L'AccessOne est conçu comme système ouvert et peut gérer et commander aussi bien des appareils online et offline. La communication est chiffrée de bout en bout AES-128 bits. Des concepts optionnels de redondance d'ASI et de serveur garantissent une sécurité élevée contre les pannes et du système.





3.1 Extensions des fonctions

Pour la licence de base de l'AccessOne, les extensions des fonctions suivantes sont disponibles :

	•				
Création à badges	Cette extension de l'AccessOne permet de concevoir sa propre mise en				
Réf. 348120V	forme de badge avec un éditeur graphique.				
Fonction multi-clients	La fonction multi-clients permet d'attribuer logiquement des composants				
Réf. 348121V	définis du système, tels que des portes et des personnes, à différents clients				
	indépendants. Ces clients peuvent gérer indépendamment les composants				
	du système qui leur sont attribués, mais n'ont aucune influence sur les				
	composants des autres clients. Il est tout de même possible de partager des				
	composants du système, tels que des portes d'entrée.				
Gestion de visiteurs	Étend l'AccessOne pour inclure la possibilité d'inscrire des visiteurs dans le				
Réf. 348122V	système et d'émettre des badges à court terme avec un accès limité. L'in-				
	scription a lieu via un navigateur Internet.				
Gestion de la zone de	Étend l'AccessOne pour inclure la gestion de zones de stationnement. Un				
stationnement	nombre « n » de surfaces louées peut être attribué à certains locataires,				
Réf. 348123V	pendant que toutes les places de stationnement restantes sont comptées				
	et sont disponibles pour tous les utilisateurs autorisés restants. Pour utili-				
	ser cette fonction, un dénombrement via un lecteur d'entrée et de sortie est				
	obligatoire.				
Enregistrement du temps	Étend l'AccessOne pour inclure la gestion d'enregistrements d'arrivée et				
Réf. 348124V	de départ sur des lecteurs d'accès et/ou des lecteurs d'enregistrement du				
	temps séparés ainsi que leur mise à disposition quotidienne au format CSV				
	à un système de gestion du temps de travail de niveau supérieur.				
Redondance de serveur	Étend l'AccessOne avec une fonction « Hot Standby ».				
Réf. 348125V					
Gestion d'entreprises	Étend l'AccessOne avec un module de gestion de données de base de				
externes	collaborateurs d'entreprises externes, sans accéder aux données de base du				
Réf. 348126V	personnel interne. Le module autorise l'envoi d'artisans qui doivent travail-				
	ler dans le bâtiment et qui ont besoin de matériaux et/ou d'un badge. Les				
	permissions spéciales ou les instructions nécessaires peuvent être déposées				
	et examinées avec validités. Le collaborateur de l'entreprise externe confir-				
	me, par une signature sur une tablette électronique, avoir réceptionné les				
	matériaux et avoir pris connaissance des documents.				



3.2 Procédure recommandée pour la première mise en place de l'AccessOne

Pour vous faciliter, en tant qu'utilisateur, la saisie de nombreuses données pour la première mise en place de l'installation de contrôle d'accès AccessOne, nous vous recommandons d'effectuer les différentes étapes dans un ordre précis. Nous faisons ici la différence entre la configuration du système d'AccessOne par l'exploitant de l'installation et/ou du personnel spécialisé mandaté du domaine informatique/administration et la création d'appareils, d'autorisations et de données personnelles par du personnel formé aux produits.

L'exécution des premières étapes se fait par l'exploitant de l'installation et/ou du personnel spécialisé mandaté du domaine informatique/administration.

Étape	N°	Action
Configuration de l'AccessOne		Démarrez l'application et connectez-vous en tant qu'utilisateur
	(1)	(voir « 5 Connexion » page 16).
		Avant de commencer la mise en place de votre installation Acces-
	(2)	sOne, vous devez activer la licence dans les paramètres système
		(voir « 6.1 Configuration du système » page 17).
		Après la configuration du système, créez les différents utilisa-
	(3)	teurs, afin qu'ensuite chaque utilisateur AccessOne puisse para-
		métrer le système avec ses droits d'attribution individuels (voir
		« 6.2 Données d'utilisateur » page 27).
		Définissez les données d'emplacement de votre installation
	(4)	AccessOne. Les données d'emplacement peuvent alors être di-
		rectement attribuées lors de la mise en place des appareils (voir
		« 6.3 Données d'emplacement » page 32).



Étape	N°	Action
Créer les appareils		Créez tout d'abord vos appareils online tels que les commandes
		de portes et les lecteurs. Chaque lecteur peut également être
		utilisé comme appareil de mise à jour pour les médias d'accès.
		Ceci est une condition pour la mise en place des appareils offline
		(voir « 7.1 Données des appareils online » page 35).
	\bigcirc	Une fois les appareils online mis en place, créez les appareils
	(2)	offline. Cette étape est une condition pour pouvoir définir par
		la suite les autorisations avec tous les appareils créés (voir « 7.2
		Données des appareils offline (OSS-SO) » page 55).
Créer des groupes et profils		Mettez d'abord en place les groupes d'autorisation pour les appa-
d'autorisation	3	reils online et offline (voir « 9.1.5 Autorisations » page 78).
	4	Les groupes d'autorisation sont rassemblés dans des profils
		d'autorisation. Ainsi, toutes les étapes nécessaires pour votre
		concept d'autorisation sont effectuées (voir « 8.2 Profils d'autor-
		isation » page 69).
Créer des données personn-	F	Les autorisations déjà configurées des appareils online/offline
elles	(5)	peuvent être désormais directement assignées à des personnes
		(voir « 9.2.1 Données personnelles » page 84).
		Pour l'impression de badges, utilisez le concepteur de badges.
	6	Les mises en forme de badges sont alors attribuées à la personne
		(Cette extension de l'AccessOne permet de concevoir sa propre
		mise en forme de badge avec un éditeur graphique.).
		Vous pouvez également attribuer une entreprise à la personne
	()	(La fonction multi-clients permet d'attribuer logiquement des
		composants définis du système, tels que des portes et des per-
		sonnes, à différents clients indépendants.).
Adaptations ultérieures	>	En cas de modifications nécessaires, toutes les données créées
		peuvent être adaptées simplement ultérieurement (voir « 9.2
		Changements de groupe » page 84).

Les étapes suivantes peuvent être effectuées par du personnel formé aux produits :

Œ

4 Gestion générale des boîtes de dialogue

Groupe cible de ce chapitre :

- Personnel formé aux produits
- Personnel spécialisé en informatique/administration
- Exploitants d'installation

L'utilisation de l'AccessOne s'effectue à l'aide d'une interface de dialogue dotée d'un concept de commande cohérent. Toutes les boîtes de dialogue se basent sur le même schéma, un nouvel utilisateur s'y retrouve rapidement dans le système.

L'interface utilisateur est conçue de manière analogue aux produits Microsoft Office connus. En bas à gauche se trouvent les touches de sélection des dialogues (1). Au-dessus se trouve, en fonction du dialogue sélectionné, une liste des objets de données disponibles dans la sélection d'objets (2). En sélectionnant une entrée de la sélection des dialogues (1), les détails de cet élément s'affichent sur un onglet dans une ou plusieurs sections (5) de la fenêtre de dialogue (4). Selon leur étendue, les données d'un objet de données (par ex. personnes ou appareils) sont résumées sur plusieurs onglets. Les boutons de la barre d'outils (3) offrent des fonctions de base pour l'onglet actuel.



Pour chaque dialogue, il est possible de déterminer si un utilisateur a accès et avec quelle autorisation (Lire – Écrire – Supprimer). Si un utilisateur n'a pas d'autorisation pour un dialogue, la touche correspondante n'est pas visible dans l'interface. Cela vaut également pour les onglets dans la fenêtre de dialogue.

AccessOne - Dannées utilisateur	2 harre (d'outils			- n ×
Changer Nouveau Copier Sup	primer Actualiser Assignation	a outilis	~		
2) sélection d'o	bjets) base des utilisateurs	Batour ACL Workflow	(4) fenêtre	de dialogue	
tdmin lart	Nom d'utilisateur		Nom drubitateur Windows		
Asik AsikEN	La pencine Wilde de	- i	Niveau de sécurités	(5) sectio	
faikFR faikNL Veb	Utilisateur du Wet	(manual III)		est bioquit	
	Login LDAP:			Poinciple des 4 year pour l'évail le togbool	_
(1) dialogues	Not de passe		Continuation		
Undialogues	Valdet Loss		Changer d	e mat de patse tom de la prothame conne	
Rapports	Membre de groupes d'utilisateurs				-
Données de l'appareil	Groupe d'utilisateurs		Groupe d'utilisateurs		
OSS		<<		(5) sectio	n)
Liste noire de l'OSS				~	
Données utilisateur		>>			
Concepteur des badges					
	Utilisateuri admin Augun kesteur de	Station de tra	wit INV-11537 Loc. 0 Mar. office	Événements: 0	Timeout: non activé





Les champs obligatoires vides sont marqués en rouge lors de l'enregistrement. Les conseils d'outils donnent des informations complémentaires sur l'élément correspondant, lorsque le curseur est placé dessus.

Données de base de	s utilisateurs	Utilisate	UT ACL	Workflow	Groupes d'utilisateurs	Groupes d'utilisateurs du Web
Données utilisateur						
Nom d'utilisateur:					Nom d'utilisateur Windows:	
La personne:				-	Niveau de sécurité:	*
Valide de:	Select a da	à:	Select	a da 15	Langue:	
Utilisateur du Web						est bloqué
Lonin LDAP						peut activer des autorisations

4.1 Mode affichage – Mode modification

L'AccessOne fait la différence entre le mode affichage et le mode modification. En mode affichage, il est uniquement possible de visionner des données, mais pas de les modifier. Les données sont grisées. En mode modification, les touches et champs de saisie sont activés dans la fenêtre de dialogue. En mode modification, le jeu de données sélectionné est bloqué en interne pour tous les autres utilisateurs de dialogue.

4.2 Barre d'outils

Rechercher

Au-dessus de la sélection d'objets à gauche se trouve le champ de saisie pour la recherche dans la barre d'outils.



Le bouton RECHERCHER de la barre de menu est uniquement actif lorsque le dialogue « Données personnelles » est sélectionné.

En cliquant sur le bouton RECHERCHER, l'onglet « Recherche de personnes » s'ouvre dans la fenêtre de dialogue. Ici, d'autres critères de recherche sont disponibles (par ex. nom, prénom, entreprise, numéro de matricule, autorisation, profil d'autorisation, numéro de badge). La liste de sélection du champ de saisie se met à jour avec chaque caractère saisi.



AccessOne - Données personnelles						-		x
Accuel								-6
\$	Recherche de personne	95						
Nom de fa Prénom N° personn	Données du personnel							
Spind-Mast	Nom		Prénom:	-				
	Entreprise.		Entreprise 2:		(Description)			
	Nº de personnels	-	Plaque d'immatricul:					
	Nº du badge:	1	Version		(seulement avec le n° de badge)			
	Commentaire	[
Données personnelles	tres							
A Autorisations	Autorisation		Autorisation OSS:					
d' Autorisations	Masque d'accès:							
Profils d'autorisation	Profil d'autorisation:							
🚡 Données d'entreprise	Utilisateur: admin	Àusun lecteur sie dialingue ()	Station de travail: INV-TI	537 Has, C Han, prilling	Évenements: 0	Timeout no	on activé	

Pour l'onglet « Recherche de personnes », seules les touches VIDER, EXÉCUTER et ANNULER de la recherche sont à disposition.

En cliquant sur EXÉCUTER, la liste de sélection filtrée se met à jour. Les jeux de données peuvent être sélectionnés et édités individuellement. Les termes de recherche restent actifs jusqu'à ce que vous cliquiez sur ANNULER. Si vous avez donc par ex. sélectionné une entreprise dans le dialogue de recherche, seules les personnes de cette entreprise sont affichées dans la liste de sélection, peu importe quelles saisies supplémentaires vous effectuez dans le champ de recherche au-dessus de la liste de sélection. Ce n'est qu'en sélectionnant à nouveau le dialogue de recherche et en annulant ensuite la recherche que ce critère de recherche est à nouveau supprimé. VIDER supprime le contenu du dialogue de recherche et vous pouvez saisir de nouveaux critères de recherche.



L'exemple ici contient exactement 2 jeux de données dont la première lettre est un « T ». Si l'on n'indique pas de critère de recherche, l'affichage est limité à 150 entrées maximum. Cette valeur peut être réglée via les paramètres système de l'AccessOne. Via la petite touche en bas à droite de la fenêtre de recherche, vous pouvez désactiver brièvement la limitation. Tous les jeux de données adaptés au critère de recherche sont alors chargés dans la liste de sélection. Si vous ne saisissez pas de terme de recherche, tous les jeux de données présents dans la base de données sont chargés.

Modifier

En cliquant sur MODIFIER ou en faisant un double clic sur le jeu de données de la liste de sélection, les champs de saisie et les touches de la fenêtre de dialogue à droite s'activent. Le jeu de données sélectionné est bloqué en interne pour tous les autres utilisateurs de dialogue.



Nouveau

Crée un nouveau jeu de données vide.

Copier

Duplique un jeu de données existant. Les champs qui doivent être uniques pour chaque jeu de données sont automatiquement vidés.

Sauvegarder

Sauvegarde et met à jour le jeu de données dans la base de données. Ensuite, le jeu de données est à nouveau activé pour des modifications par d'autres utilisateurs de dialogue.



Le dialogue actuel est automatiquement sauvegardé lorsque vous quittez la page de dialogue.

Supprimer

Supprime le jeu de données sélectionné (marqué en bleu). L'action est effectuée une fois que vous avez répondu à une question de sécurité.

Actualiser

Charge les données actuelles de la base de données et actualise l'affichage.

Assignation

Assigne le jeu de données actuel à un client. Uniquement actif lorsque la disponibilité des clients est activée.

5 Connexion

Une fois le logiciel installé avec succès, connectez-vous en tant qu'utilisateur. Démarrez le programme en faisant un double-clic sur le symbole qui crée automatiquement l'installation sur votre bureau.

		🔲 🖬 🚾
	c	4
Ð	Benutzername: Kennwort:	
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

Pour la première connexion après l'installation, les données de connexion suivantes sont préinstallées :

Nom d'utilisateur : admin

<u>Mot de passe</u> : admin

Modifiez le mot de passe directement après la saisie pour des raisons de sécurité. Pour cela, allez dans le dialogue « Données utilisateur ».

CAccessOne - Données utilisateur			- 🗆 X
Accuel			-6
Arvaler	0 4		
ter E	Données de base des utilisateurs Utilisateur ACa V	Vontion Groupes d'utilisateurs Groupes d'utilisateurs du Web	
(demo	Dannees utilisateur Martin	Non of all other Westman	
Main Control	La cersonce	Nieses de sécurité	
NextR	Valide de Select a dar 15 at Select a d	artist Langue 11 to the	
Witta	Utilicateur du Wet:	est bloque	
	Login LDAP:	peut activer des autorisations Principe des 4 yeux pour l'évail le logbook	
	a contraction of the second		
	Données du mot de passe	and the second s	
	Mot de passe	Confirmation:	
	Valore Jours		
	Varide Tradit an Delection on USU	The state of the second s	
	Membre de groupes d'utilisateurs		
	Groupe d'utilisateurs	Groupe d'utilisateurs	
	Na - Employe	< Administrator	
d was			
Liste noire de l'OSS			
🎎 Données utilisateur		~~	
Concepteur des badges	Natification pour d'événements		
J& ACLs	Type d'événement	Type d'événement	
🗽 Visiteurs / Dates		< Apparel Nutoritation	
2 Entreprises externes		Autorisation office Système	

Dans la sélection d'objets, sélectionnez le nom de connexion « admin » et cliquez ensuite dans la barre d'outils en haut à gauche de la fenêtre sur le bouton MODIFIER. Saisissez votre propre mot de passe. Un mot de passe aussi long que possible, composé de lettres et chiffres, est particulièrement sûr. La longueur du mot de passe est libre. Pour comparer, répétez le mot de passe dans le champ « Confirmation ».

Si vous souhaitez attribuer un mot de passe à validité limitée, vous en avez la possibilité ici. Confirmez votre modification avec le bouton SAUVEGARDER.

La création d'autres utilisateurs est décrite en détail plus loin dans ce manuel (voir « 6.2 Données d'utilisateur » page 27).

6 Configuration de l'AccessOne

Groupe cible de ce chapitre :

- Personnel spécialisé en informatique/administration
- Exploitants d'installation

Pour réussir les conditions pour la mise en place de l'installation de contrôle d'accès, vous devez adapter certains paramètres du système. Vous déterminez des zones et mettez en place des stations de travail. En outre, vous définissez les formats de lecteurs et de badges utilisés. En saisissant les données d'utilisateur et d'emplacement, vous créez les conditions pour la configuration des appareils et des autorisations.

6.1 Configuration du système

6.1.1 Paramètres

Affiche les paramètres de votre système.

AccessOne - Configuration du système									- 🗆 X
Elsen Accuel									6
Changer Rouveau Coper Su	opumer Actualizer								
A un El	Paramètres	Zanes	Groupes de parking	Stations de travail	Formites des lecteur	Analyse des badges	Licences.	Formata de carte	Classes de personne
Nom Cadepore EventBioter Hose AdMaterCon MasCharSignerTimesper AdMaterCon MasCharSignerTimesper AdMaterCon CharDataSignerTimesper AdMaterCon Distributive Television Con Distributive Television Con Distributive Distributive MasCharDester Distributive Delevision Con Distributive Distributive Delevision Con Distributive Distributive Delevision Distributive Delevision Con Distributive Delevision Con Distributive Delevision Con Distributive Delevision Con Distributive Delevision Con Distributive Delevision Con Distributive Delevision Con Distributive Delevision Con Distributive Distributi	Parameters Romi Describe Valear Page de la Velear								
* Workflow									
Herein Changements de groupe	-		-		-			-	
& cart and a second	Utilisateur admin		Anicel InCost the Girls	Station de tra	veit INV-11537	O Macation	Evénements: 0	Tan	eout: non active

Explications des paramètres

Nom	Traduction	Explication
EventBufferFileSize	Taille de la mé-	Taille de la mémoire tampon (Mo), pour sauvegarder des
	moire tampon	événements pour un seul MAC.
MacDataExpireTimespan	Durée d'expira-	Durée en minutes sans connexion au MAC, après laquelle
	tion des données	les données tampon d'événement deviennent invalides.
MacEncryptionAlgorithm	Algorithme de	Algorithme de cryptage pour la communication entre
	cryptage	AccessOne et les MAC (préréglage : aucun).
DateDeletedOffset	Supprimer les	Durée en jours après laquelle les jeux de données personn-
	jeux de données	elles sont définitivement supprimés de la base de données
		après la suppression dans le dialogue.
EventDeleteOffset	Supprimer les	Nombre de jours après lequel les événements sont suppri-
	événements	més de la base de données.
VisitorDeleteOffset	Supprimer les	Nombre de jours après lequel les visiteurs supprimés sont
	visiteurs	supprimés de la base de données.
LastRunTime	Dernière exécut-	Date de la dernière exécution du processus
(LastAccessProcess)	ion du processus	



Nom	Traduction	Explication
LastRunTime	Dernière exécut-	Date de la dernière exécution du processus
(LockProcess)	ion du processus	
CardNoRecyling	Réutiliser les nu-	1 = réutilisation de numéros de badge, en recherchant des
	méros de badge	vides liés à des badges supprimés.
		0 = attribution continue de numéros de badge.
DatabaseNumber	Numéro de base	Identifiant dans la base de données en cas de plusieurs
	de données	bases de données (jusqu'ici 00)
LockingTimeout	Durée de blocage	Durée en secondes pour le blocage de jeux de données en
	du jeu de don-	cours de traitement. Si, pendant cette durée, le blocage
	nées	n'est pas renouvelé par le client, le blocage du processus
		maître est arrêté.
LogonTimeout	Période de renou-	Durée en secondes au cours de laquelle un client doit
	vellement de la	renouveler sa connexion au maître avant d'être automati-
	connexion	quement déconnecté.
NumberLogonFailures	Nombre d'échecs	Nombre max. de tentatives de connexion échouées
	de connexion	
ProcessLogfileAge	Âge des fichiers	Âge max. en jours des fichiers logbook de débogage
	logbook de débo-	
	gage	
ProcessLogfileSize	Taille des fichiers	Taille max. en Mo des fichiers logbook de débogage
	logbook de débo-	
	gage	
XmlDoorDataDir	Répertoire des	Répertoire pour l'échange de données de portes OSS
	données de	
	portes	
CardNoZeroes	Numéros de	Remplissage de numéros de badges imprimés avec des
	badges	zéros jusqu'à la longueur totale indiquée.
CardToCodeAlgorithm	Algorithme de	Algorithme de détermination des numéros de badges
	code	depuis les données du code. Standard : 0 = le numéro de
		badge correspond aux données du code.
DialogTimeout	Dépassement	Dépassement standard en secondes pour la non-utilisa-
	de la période de	tion d'un dialogue. En cas de dépassement de cette durée,
	dialogue	l'utilisateur est automatiquement déconnecté.
EntitiesToTake	Entités	Nombre de jeux de données affichés dans la liste de sélec-
		tion.
MaxPinLength	Longueur de PIN	Longueur max. des PIN (PIN, EMA1, EMA2)
	maximale	
MaxPinValidity	Validité de PIN	Validité max. des PIN en jours
	maximale	
OfflineValidityTime	Durée de validité	Validité standard d'un badge offline en heures, minutes
	offline	(standard : 24,0).



6.1.2 Zones

AccessOne - Configuration du système					- 0 >
Accueil					
Changer Nouveau Copier	komer Actualizer				
ue 14	Par mètres Zones Strout a de partiong	Stationi de travail Formats des lacteur	Analyse des bedges	Licenses Formats de carri	Elasses de personni
éom	Zinte				
W	Nam.				
1	Dermetion				
2	- Contraction -				
3	Paramètres				
4	Zone parents	Options			
leutral N	-	industrial for some off the			
55.2		A DECKE IN LEDGED THE	COLUMNS OF		
VSS Test	Entrépose	Reference eva-			
1.	Personnes min:	Personnes mas			
ACLs	Max. lemps de rétention (t.)		🔲 Remine à phro du comp	oteur de sone à minuit	
🛓 Visiteurs / Dates		Civim feux de trafic via			
🗽 Entreprises externes		N°de contact:			
• Workflow					
E Changements de groupe					
	Utilisateur, admin Aucun hoteur de qua	Station de travail: INV-1(537	Mix plline	Événements: 0	Timeout: non active

Chaque porte dans AccessOne mène d'une zone source à une zone cible. Ces zones ne doivent pas forcément être différentes. Si votre bâtiment est divisé en plusieurs zones de sécurité, une entrée peut par ex. mener de la zone de sécurité extérieure (ZSE) à la zone de sécurité intérieure (ZSI). Une porte intermédiaire peut cependant aussi mener de ZSI à ZSI.

Avec « Entrée lieu » et « Sortie lieu », vous choisissez la zone source et cible.

Paramètres

Sous « Paramètres », une zone peut être à nouveau divisée. Dans « Zone normale », la saisie d'un nombre de personnes minimal et maximal autorisé au sein de la zone est possible. Pour une « Zone de parking », il est par ex. possible d'indiquer le nombre maximal de places de stationnement disponibles.

6.1.3 Groupes de parking

(Uniquement actif en cas d'utilisation du module supplémentaire Gestion de la zone de stationnement, réf. 348123V)

Offre la possibilité de rassembler des personnes dans un groupe de parking. Elles peuvent ensuite être assignées à une zone de parking spécifique.



6.1.4 Stations de travail

C AccessOne - Configuration du système		– 🗆 X
Accueil		
Chenger Nouveau Copier Supprim	er Actualiser Assignation	
	Paramètres Zones Groupes de parkint Stations de travail o	maits des lecteur Analyse des badges Licence Classes de personnel
Nom	Station de travall	
INV-11537	Nom: (NY-11587	
	Description: Maik's PC	
	Lieu, salie:	
	Configuration	
	Deconnexion autom: 0 [secondes]	
	Lecteur de dialogue: Identitiox (Multi)	
	Interface de lecteur COM11 Taux de baud du lec	thur 115200
1 Aris	Nom d'encodeur imprim	
	Ribte d'encod imprimi	-
Visiteurs / Dates	Interface d'encodeur: Encodeur Java Be b	and -
2 Entreprises externes		
- Workflow	Capt. données biométri	
Here Changements de groupe	Interface UZ RESULT: Interface DS Rin Stor	<i>a</i>
Configuration du système	D	
9 Données d'emplacement		

Dans l'onglet « Stations de travail », les différents clients AccessOne sont créés avec leur nom d'ordinateur Windows exact. Il est déterminé de manière locale pour la station de travail concernée si un lecteur de dialogue (par ex. une IdentBox) ou une imprimante de badges avec station de codage est installé(e). Pour le périphérique, les bons ComPorts doivent être réglés. Vous pouvez lire les ComPorts dans votre gestionnaire d'appareils Windows.

6.1.5 Formats de lecteur

AccessOne - Configuration du système								- 0	1 8
Accueil	1997 - Carlos Carlos (1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997								R
Changer Nouveau Copier Supprimer	C Actustiser			-					
	Paramètres Zones	Groupes de parking	Stations de In	avail Formats	des lecteur	Analyse des budge	Licences	Formats de carte	Classies
Nom	Formal de lecture			-	_				
OSS-Desfire	Nom D55-	Destine			I format act	C			
00000	Descoption OSS-	Destire							
	pour protocole:								
	Configuration.								
	Technologie des badges	Mifare Destine Ev1	Nu	mèro de cliento - I	De 0				
		MAD est utilisé	AJI	de l'ublicateurs	Q#				
	Mifare MAD clé A.		- Mi	are MAD cle B					
	Numleo du secteur Miller								
	Mifare Clin A / Deshre File Read Cle		De	tare Cle B / slive File Write Cle					
JI ACLs	ID application Destine	Ge F75000	De	sfire application the					
Visitours / Dates	N° de cié Desfire:	1	1C ⁴	de fichrer Desfires	Q.				
Visiteurs / Dates		Clé Desfire styptée			Destine dé	diversitié			
Le Entreprises externes	Legic Stamp.		Le	pic Stamp longueur					
- Workflow		🔆 Naméro de série co	nme numéro de ci	ste					
	Début du n° de code:	72	Lo	igueur.	32	Format	Big endlan		
Changements de groupe	Début de version		Lo	ngwewr:		Formab			
Configuration du système	Début de n° de cilent:		Lo	igueur:		Formut			
9 Données d'emplacement	Utilisateun admin	Racun lecteur de auro	gue cercon Statio	n de travail: INV-11	537	Wac offene	Événements: 0	T	imeout con a

Vous pouvez régler ici les formats de lecteur qui doivent être lus par le lecteur de badges du contrôleur de porte.



6.1.6 Analyse des badges

AccessOne - Configuration du système								D	×
Accuei									U
B D F H X	0								
	Hermaniser,				-	_			
(m)	Paramètres Zones	Groupes de parking	Stations de travail	Formars des lecteu	Analyse des badges	Libences Forma	ts de carte	Time	t de p
Nom	Configuration					-			
Lecteur de d'alogue	Carge multimum	Line dates.							
	Carthering	Supporter		_					
	Analyse	Indiana							
	Description	164	-						
	Description	vare							
X Concepteur des badges									
ACLs									
Visiteurs / Dates									
🗽 Entreprises externes									
- Workflow									
Here Changements de groupe	gemplacement des badges	5							
Configuration du système) de badge der	à.			Cri	and a			
Données d'emplacement	Utilisateur, admin	Augminteentergeg	Station de tra	vail: INV-11537	sc 0 Mazielfine	Événements: 0	Tim	eout non	activé

Dans l'onglet « Analyse des badges », des badges maîtres (par ex. badges LEGIC, IAM), qui sont importants pour l'utilisation de la fonction d'écriture de votre lecteur de dialogue (IdentBox), peuvent être lus ou supprimés.

Le bouton Analyser permet de lire en détail les badges d'un format de badge créé au préalable via le lecteur de dialogue raccordé.

La section « Remplacement des badges » permet de créer une quantité définie de badges de remplacement dans la plage de numéros de badges correspondante de la base de données.



6.1.7 Licences

AcceisOne - Configuration du système										- 0 ×
Accuell										
BUDEX	Actualiser						_		_	
	Panimitras	Terries Group	en de privleng	Stations of horas	Emmans this kertara	dualpiede	n to per	Licences	For lats da ca	rie – Clamen da 1
Nom	Activation						-		_	
Licences	Arthouse .									
	Veulliez ro	witacter votre pistribute	ur. Vous avez besoi	n des noms des licences	à activer et de la signature d'o	rdinateur				
		Signati	ure d'ordinateur:	E4F9 6E94 0461 1C70	E386 711D 13C5 3678					
	Les clés re activées a	ques peuvent être saise vec le bouton împorter	es individuellement	dans le champ Clé d'acti	ation ou peuvent être lues in	tégralement à	partië d'un Ri	chieriet		
		Cles d	activation							
				1				4	meaniter.	
					1					
				-	Actives					
		Cles du	a système Milare:	Importer						
	Id No	m du paquet	Description	du paquet		Disponible	Activé	Date d'expira	ation	
	1 Bas	è Intioni Der hedret	1000 Badge	s, 50 lecteurs, 50 apparei	s de ferméture offline, 2 statio	tean	1			
	3 Exte	insion: Lecteurs	25 autres le	cteurs (max. 16000)		637	1			
	4 Exte	ension: Offline	25 autres ap	pareils de fermeture offi	ne (max. 100000)	3798	200			
Concentrus des hadres	5 Exte	ension: Des stations de l	travail 1 autre stati	on de travail (max. 100)		97	3			
Concepteur des bauges	6 Exte	ension: Mises à jour des	logici Mises à jour	du logiciel pendant 1 an	née supplémentaire (max: 100	0 100	0	-		
1. ACLE	7 Exte	ension: Mise en page du	a badg Creation de	la mise en page du bado	é	0	1			
ACD .	0 Exte	ension : Visiteurs	Dialogues d	e visiteur		0	1			
Visitours / Datas	10 Exte	mision: Zone de parking	Gestion de l	a zone du parking		0	1			
Visitedis/ Dates	11 Exte	ension: Enregistrement	du ten Gérer les do	nnées de temps d'entrée	et de sortie	0	1			
Entrapricas avternas	12 Exte	ension : Workflow	Dialogues si	ar les workflows d'autoris	ation	0	3			
Chilephises externes	13 Exte	ension: Redondance des	s serve Hot Standby	avec 26me serveur		0	1	-		
-O+ Workflow	14 Exte	ension: Importation de j	persor Importation	de données relatives au	personnel à partir d'un fichier	cito	10		-	
Changements de groupe	Limites	1 Visiteurs personnes	ges, 75 Lecteur, 50 , 1 Zone de parking	T Enregistrement du fer	omine, 3 Stations de travail 1ps, 1 Workflow, 1 Redondans	e du serveur, l	I Importation	de		
Configuration du système	Nº de cher	nti 9999		Misses à jour de	s logiciels à 16.06.2022					
Ponnées d'emplacement	Utilisateur, admin	0	or kost in Se	Station d	travale INV-11517	ac theory	-	Evéne	ments: 0	Timeoutin

L'onglet « Licences » montre une liste des différentes licences de programme et de leurs contenus.

Pour l'activation de la licence, la signature de votre ordinateur de serveur AccessOne est nécessaire. Sans activation de licence, votre installation AccessOne est uniquement utilisable comme licence de démonstration avec des restrictions.

Il existe trois types de licences :

- Une licence de test avec étendue de système minimale, qui est directement activée après l'installation du logiciel AccessOne.
- Une licence de démonstration qui est limitée dans le temps et qui est créée selon les besoins du client. Ce type de licence peut être renouvelé deux fois. Une fois cette période écoulée, la licence de démonstration devient automatiquement une « licence de test ».
- La licence d'achat offre toutes les fonctions standard.

6.1.8 Formats de badge

L'onglet « Formats de badge » permet de définir les formats nécessaires à la description d'un badge sur un lecteur de dialogue, une station de codage éventuelle de l'imprimante de badges ou un terminal mural de badge (appareil de mise à jour pour médias d'accès).

Pour chaque technologie de badge (Mifare, LEGIC, etc.), seul un format de badge doit être actif. Plusieurs formats de badge inactifs de la même technologie de badge peuvent cependant être créés.

La définition d'un format de badge suppose que l'utilisateur AccessOne est familier des réglages possibles de chaque technologie de badge. Comme Mifare-DESFire laisse en particulier beaucoup de libertés pour la définition de droits d'accès, de nombreux badges peuvent être créés, qui ne sont plus utilisables quand les réglages sont contradictoires. Le texte suivant donne des indications sur quels paramètres ont un impact sur quelles caractéristiques du badge. Il ne remplace cependant pas la lecture de la documentation NXP et LEGIC correspondante.

Accuel			
P UM H X	OA		
Changer Nouveau Copier Supprim	er Actualiser Assignation		
the second second second			
Coller			-
27	Paramètres Zones	Groupes de parking. Stations de travail Formats des lecteur. Analyse des badges. Lisence Formats de cart	e C sses de personn
n	and the last		
FS. Mastar Sattarial antis	rannur du bunge		
S. Martar BattaniDarfuel	Norric -D	S Decline acognes à la clesse du personnel	
PS-Master Spind (Legic)	Description: 02	S-Format Milane Detire	
ES-Master Spind/Detfire)			
ES-RF-Master (Desfine)	Configuration		
ES-RF-Mester (Legic)			
ES-RF-Master Zeit (Desfire)	recimiciogie der cooge	s Middle Dedre ball Criteria Counte Homitine des approximents	
ES-RF-Muster Zeit (Legic)	Mifare MAD dif Ac	Mitare MAD de E Picc Master de	
OSS-Blacklist-Desfine		many a set of the second set of the second set of the	
SS-Blacklist-Legic		Clé Uestrie cryptile Destrie de diversité Statile Destrie Contra pression de r	
\$\$-Desire	Applications;	N* Nom Description	
SS-Desfire - Intervention		1 OSS-Applicati OSS-Application (Demo Keys)	
SS-Destire Test Markus	1	Manual approximation	
SS-Legic			
&Z-Batterieviechsel		X Support application	
8/2-Battenewechsel (Legic)	and the second se		
6/2+Demontage	reambres	Namy Description	
&Z-Demontage (Legic)	Farametres class T	Da Denne trict 2 Da Application 10: Da	
	-	INVest and when when any finder	
ACLS	CIEO / A	CIETUS: CIEZ: CIEZ:	
	Oe4	- DV 9 - CM 6 - CM //	
Visitaurs / Datas	714 F	many and many and and and and and	
Visitedis/ Dates	and an		
Entransland automas	0612	Ce 13	
Entreprises externes	Second	Nº Nom Description	
	segment.	No. of the second	
 Workflow 		Accession and and	
Changements de groupe		X Secular senses	
Configuration du système	Nombre:	Non Description	
	Louisia	(bottow)	
P Données d'emplacement	Unisateur admin	Anna Jacob Martin Station de travail (NV-11537 11 an D Mar alling)	Timeout non activit
and the second se			and the second s

Les paramètres sont créés dans différents niveaux de structure :

- Paramètres au niveau du badge
- Paramètres au niveau de l'application
- Paramètres au niveau du fichier

6.1.8.1 Paramètres au niveau du badge

Lors de la création d'un nouveau badge, la clé PICC Master est d'abord réalisée de la valeur standard à la valeur définie ici. Ensuite, les propriétés qui se rapportent à l'utilisation de cette clé PICC Master sont définies. Les réglages sont enregistrés dans la valeur de « Desfire Config Byte ».

La valeur est codée par bits et s'interprète de la manière suivante :

Les bits 4 à 7 doivent être de 0.

Le bit 3 détermine si cette configuration peut à nouveau être modifiée ou non (même via un formatage du badge).

- 0 : la configuration ne doit plus être modifiée.
- 1 : la configuration peut être modifiée, si une authentification avec la clé PICC Master a été effectuée



auparavant.

Le bit 2 détermine si la clé PICC Master est nécessaire ou non pour créer ou supprimer une application.

- 0 : la création et la suppression d'une application fonctionne uniquement avec la clé PICC Master.
- 1 : la création d'une application fonctionne sans clé PICC Master ou clé Application Master, suppression d'une application avec clé PICC Master ou clé Application Master.

Le bit 1 détermine si la clé PICC Master est nécessaire ou non pour consulter le contenu du badge.

- 0 : la consultation fonctionne uniquement avec la clé PICC Master.
- 1 : la consultation ne nécessite pas de clé PICC Master.

La clé PICC Master ne doit pas être transmise. Si vous souhaitez autoriser des tiers à créer leurs propres applications, 0x0f serait par ex. un réglage pertinent pour « Desfire Config Byte ». Avec cette définition, vous n'avez pas besoin de transmettre la clé PICC Master.

6.1.8.2 Paramètres au niveau de l'application

Selon le standard DESFire, la clé 0 est toujours la clé Application Master (APMK). Toutes les autres clés peuvent être définies, mais cela n'est pas obligatoire. Il est recommandé de définir au moins une clé supplémentaire, pour éventuellement donner l'accès à des tiers sans devoir transmettre l'APMK.

« Paramètres clés 1 » détermine ce qui est contrôlé via la clé Application Master. 0xE1 serait par ex. une valeur pertinente.

Réglages de l'application de l'APMK :

		1	1	I	I.	I.	I
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	BitO
Modificati	ification des droits d'accès aux clés			Configuration modifiable	Création/sup- pression libre	Accès libre aux listes de	Autoriser la modification
Bit3	Bit2	Bit1	BitO			APMK	

Au niveau de l'application, le codage est interprété comme suit (l'AID sélectionné n'est pas 0x00) :

Bit 7 – Bit 4 Déterminez les droits d'accès pour la modification des clés d'application (commande ChangeKey).

> 0x0 : l'authentification de l'APMK est nécessaire pour modifier n'importe quelle clé (standard).

0x1...0xD : l'authentification avec la clé indiquée est nécessaire pour modifier n'importe quelle clé. Une clé de modification et une clé PICC Master peuvent uniquement être modifiées avec l'APMK après l'authentification. Pour d'autres clés, une authentification avec la même clé est nécessaire.

0xE : l'authentification avec la clé à modifier (même numéro de clé) est nécessaire pour modifier une clé.

0xF : toutes les clés (sauf l'APMK, voir bit 0) au sein de cette application sont gelées.

Indique si une modification des réglages de l'APMK est autorisée :

0 : la configuration n'est plus modifiable (gelée).

1 : cette configuration peut être modifiée, en cas d'authentification avec l'APMK (réglage standard).

Bit 3



Bit 2	Indique si l'authentification de l'APMK avant CreateFile/DeleteFile est nécessaire.
	0 : CreateFile/DeleteFile est uniquement autorisé avec l'authentification de l'APMK.
	1 : CreateFile/DeleteFile est également autorisé sans l'authentification de l'APMK.
Bit 1	Indique si l'authentification par clé Master est nécessaire pour l'accès au répertoire de
	fichier :
	0 : pour l'exécution des commandes GetFileIDs, GetFileSettings et GetKeySettings, une aut-
	hentification réussie par clé Master est nécessaire.
	1 : les commandes GetFileIDs, GetISOFileIDs, GetFileSettings et GetKeySettings sont possib-
	les indépendamment d'une authentification par clé Master précédente (réglage standard).
Bit 0	Indique si l'APMK est modifiable :
	0 : l'APMK n'est plus modifiable (gelée).
	1 : l'APMK est modifiable (l'authentification avec l'APMK actuelle est nécessaire (réglage
	standard)).

« Paramètres clés 2 » définit le nombre de clés valables pour cette application, et le type de cryptage pour l'accès à cette application.

Le paramètre « Paramètres clés 2 » définit plusieurs réglages :

Bit 0 à 3	Nombre de clés qui peuvent être sauvegardées au sein de l'application à des fins crypto-
	graphiques. Un maximum de 14 clés peuvent être sauvegardées dans une application de
	MIFARE DESFire EV1. Il est également possible de créer une application sans clé !
Bit 4	La RFU doit être réglée sur 0.
Bit 5	Indique l'utilisation de numéros de fichier à deux octets ISO/CEI 7816-4 pour les fichiers au
	sein de l'application :
	0 : aucun numéro de fichier à deux octets n'est pris en charge au sein de l'application.
	1 : des numéros de fichier à deux octets sont pris en charge au sein de l'application.
Bit 6 à 7	Indique la méthode de cryptage de l'application :
	00 : indique des opérations DES et 2K3DES pour toute l'application.
	01 : indique des opérations 3K3DES pour toute l'application.
	10 : indique des opérations AES pour toute l'application.
	Une valeur valide est par ex. 0x82, lorsque deux clés ont été saisies pour l'application. La
	norme ISO/CEI 7816-4 n'est pas prise en charge. Les bits 4 et 5 doivent donc être 0. En règle
	générale, AES est utilisé pour le cryptage.

CEStronics

6.1.8.3 Paramètres au niveau du fichier

Pour les réglages de communication et de fichier, il existe des cases de sélection pratiques préparées en conséquence. Pour les droits d'accès, il faut régler pour le fichier quelle clé d'application a un droit de lecture ou d'écriture et quelle clé peut éventuellement modifier ce réglage (de droit d'accès) précis (voir tableau).

Si vous souhaitez par ex. pouvoir lire et écrire avec la clé 1 mais uniquement modifier ces réglages avec la clé 0 (APMK), la valeur pour ces droits serait alors la suivante : 0x1110.

Si vous réglez une valeur sur 0xe, cela a pour conséquence que la communication passe de « cryptée » à « non cryptée ». Cela se heurte alors éventuellement aux réglages de l'application.

MSBit												LSBit
b15		b12	b11		b8	b7			b4	b3		Ь0
	R			Ŵ			R	&W			ċ	_
	\sim			\leq				, · · ·			\sim	
					-	1						
				H	ex	K	еу]				
				0	x0	0)					
				0	x1	1						
				0	x2	2)					
				0	x3	3	;					
				0	x4	4	ļ]				
				0	x5	5	;					
				0	x6	6	;					
				0	x7	7	·					
				0	x8	8	}					
				0	x9	9)					
				0	xa	10	0					
				0	xb	1	1					
				0	хс	12	2]				
				0	xd	1.	3					
				0	xe	"fre	e"	←	1			
				0	xf	ne	/er	←	2			

¹ pas d'authentification possible

² pas d'accès



6.2 Données d'utilisateur

Dans une première étape, créez si besoin différents groupes d'utilisateurs avec des autorisations de dialogue individuelles. Ensuite, les groupes d'utilisateurs crées sont attribués à différents utilisateurs dans l'onglet « Données de base des utilisateurs ».

6.2.1 Groupes d'utilisateurs

L'onglet « Groupes d'utilisateurs » permet de créer et de rassembler des droits de dialogue dans des groupes. Les droits de dialogue dans les colonnes Lire – Modifier – Sauvegarder – ACL (en option) peuvent simplement être activés/désactivés par un clic.



Pour faciliter le travail, vous pouvez sélectionner et cliquer sur plusieurs cases en même temps en maintenant la touche de la souris appuyée. Les différentes saisies des cases sont alors changées (Oui>Non et Non>Oui).

Attribuez un nom pertinent et une description du groupe.

En cliquant sur le bouton MODIFIER, la fonction correspondante est sélectionnée et marquée en vert. En cliquant sur le bouton SAUVEGARDER, les autorisations indiquées sont sauvegardées dans le système. Dans l'exemple suivant, le groupe d'utilisateurs « Employés réception » est créé et les droits d'un employé à la réception du bâtiment principal sont limités à la création et la modification de données personnelles. L'employé peut par ex. modifier des données personnelles de base et utiliser les fonctions de badge et de blocage dans le dialogue d'aperçu.

cessOne - Données ublisateur									- 0
Accueil									
Biller Savegarder X	0 1		_						
	Données de base des stillisate	an Utilitation ACL Workflow	Groupes	d'ublisateurs	Gitteres	d'ul abre	I da Web		
		1			1				
	Données du groupe		-	_					
PATALO P	Nom Personnel	de la réception							
We will be	-								
Institute	Description: Personnel	de la réception							
	Droits de dialogue								
	Fonction de dialogue	Page de dialogue	Line .	Changer	Supprimer	4CL			
	ACLs	ACL Stammdates	0	De l	Non	Non.	1		
	ACIS	ACI, Entráce	1 and	10m	Non	Non	-	20	
	Benutzerdaten	Benutterstaminidaten	(Dec	1.00	Nan	Non			
	Benutzerdeten	Benutzer ACL		100	Nan	Nan		-11	
	Benutzendizzen	Worldow	1	100	Non	Non		-11	
	Benutzerdaten	Benutzeraruppen	-	(Dave	Non	Nee		- 11	
	Benutzenfaten	Web-Benutzeronuncen	1	No.	Non	Non		-11	
	Barachtinuscien	Barachtouonan	Cal	Non	Non	Nee		- 1	
	Barachtinumen	Zeitmodelle	-	Non	Non	Nee		- 1	
	Berechtigungen	Tanensodelle		Non	Non	Non			
20	Berechtigungen	Sonder, und Feiertage	1	Non	Nau	Non		- 1	
	Berechtinumen	ZutoHemackan	1	Blog.	bian	New		- 1	
ste noure de l'OSS	Riese Information	Chilos		Non	Non	New		- 1	
ste noire de noss	Berechtinungsuinfile	055	1	Non	New	Non		- 1	
and the state of t	Berechtigungsbergfile	Zutrittimasken	1	Dec.	Non	Non		-	
onnees utilisateur	Benciste	Recipite	1	E.u.	Non	Non			
	Benchte	Gerateliste	a	The second	Non	Non			
oncepteur des badges	Berichte	Garatectatics I solvuchausurertung	00	1 mar	Non	Nee			
	Berichte	Leter Batteriettatut	-	100	Non	Nee		- 1	
Cls	Resident	Rephticupen	1	Con.	Non	Non		-	
999 C	Benichte	Reachtournen pro Person	1	1	Non	Non		- 1	
Colores A Baller	Registe	Dook of		10	New	Mag	-	-	
isiteurs / Dates	Registe	Fertopen	12	100	Nicer	Nor		-	
	Workering .	Liter advised i			1 90011	1.4.4.4			

Il ne faut ici pas donner d'accès à l'ACL aux membres du groupe « Employés réception », afin d'éviter qu'ils n'ajoutent des personnes à d'autres listes d'accès. Les membres de ce groupe ont seulement un droit de lecture à toutes les données de base, pour éventuellement pouvoir répondre à des questions sur le badge et les autorisations.



Les employés de la direction et/ou de l'administration doivent être autorisés d'accéder aux données personnelles des employés qui ont le droit de pénétrer dans le bâtiment.



6.2.2 Données de base des utilisateurs

AccessOne - Données utilisateur				- O, P
Accueil				
Armeler	0 18			
101	Données de base des utilisateurs	Pur ACL Workflow	Groupes d'utilisateurs	Groupes d'utilisatieurs du Web
Nom	Données utilisateur			
admin	Nom d'utilisateur: MaikFR		Nom d'utilisateur Windows:	
Maik:	La marterina		Nineau de sécurité	~
MintPi			lassa	
MaikNL	Valide de: Select a da' (15) a:	Select a da' [15]	Langue	1.1 fr-FR *
web	Login LDAP:			est bloqué peut activer des autonsations Principe des 4 yeux pour l'éval. le logboc
	Données du mat de passe			
	Mot de passe: ••••		Confirmation: ••••	
	Validité: Jours			
	Valide jusqu'au Select a da' 15		Cha	nger de mot de passe lors de la prochaine conn
	Membre de groupes d'utilisateurs			
	Groupe d'utilisateurs		Groupe d'utilisateu	rs
	KG - Employé	<<	Personnel de la réce	eption
g 035		1 2 2		
Liste noire de l'OSS		1 Alto		
Données utilisateur		>>		
📝 Concepteur des badges	Notification pour d'événements		-	
1 ACLs	Type d'événement	1.00	Type d'événement Personne	
🗽 Visiteurs / Dates		<<	Appareil Autorisation	
Entreprises externes		_	Autorisation offline Système	
- Workflow		>>		
He Changements de groupe				

Créez maintenant des utilisateurs qui ont le droit de se connecter à l'AccessOne.

Données d'utilisateur

Attribuez un nom pour la connexion. Si le nom d'utilisateur Windows est indiqué, le logiciel AccessOne l'utilise pour la connexion automatique (Single Sign-on). La personne peut être sélectionnée dans une liste. Si le profil d'utilisateur doit uniquement être valide pour une durée limitée, une date de/à peut être indiquée. Lorsque cette validité expire, l'utilisateur est automatiquement bloqué. Un utilisateur peut aussi être bloqué à tout moment de manière manuelle (pour cela, cochez la case).

Dans le masque, l'utilisateur peut en outre recevoir l'attribut « Principe des 4 yeux pour les éval. du logbook », c.-à-d. que l'affichage d'informations détaillées du logbook présuppose la connexion d'un autre utilisateur avec cette autorisation.

En outre, le droit « Activer des autorisations » peut être attribué à l'utilisateur. Ce droit est nécessaire pour certaines autorisations qui nécessitent une propre activation.

Données de mot de passe

Attribuez un mot de passe pour l'utilisateur. Vous pouvez indiquer une validité limitée pour une période précise ou uniquement avec « Valide jusqu'au ».

Activez « Changer de mot de passe lors de la prochaine connexion ». Une fois que l'utilisateur a saisi pour la première fois son nom de connexion et le mot de passe attribué dans le masque de saisie, il lui est demandé de saisir un nouveau mot de passe et de le confirmer. Lors de la saisie du mot de passe, vous pouvez choisir autant de caractères que vous souhaitez. La longueur de mot de passe maximale est réglable dans le système. Membre de groupes d'utilisateurs

Attribuez à l'utilisateur AccessOne les pages de dialogue et les fonctions qu'il a le droit de voir ou d'éditer

CEStronics

après sa connexion. Ces droits de dialogue sont définis au préalable pour les groupes d'utilisateurs. Vous trouverez d'autres informations sous « 6.2 Données utilisateur » à la page 28.

Autorisations d'événements

Attribuez à l'utilisateur AccessOne les événements qu'il a le droit de voir ou d'éditer après sa connexion.

6.2.3 Utilisateur ACL (disponibilité des clients)

(Uniquement disponible en cas de séparation des données.)

Ici, des Access Control Lists (ACL) peuvent être attribuées aux utilisateurs de dialogue. Les ACL peuvent être réglées et modifiées. Condition : la fonction ACL est activée par l'administrateur.

C AccessOne - Données utilisateur	- 🗆 X
Accueil	6
Annuler	0 1
(m) (Données de base des utilisateurs Utilisateur ACL Vorkflow Groupes d'utilisateurs Groupes d'utilisateurs du Web
Nom	
admin	Nom d'utilisateur: MaikFR
Mark	
Master	La personne:
Maikhi	
Web	ACLs assignés
	ACL
	Velber: << Koln
o - 000	Valide de Select a dar 15 A: Select a dar 15 Le droit de line
Liste noire de l'OSS	Le droit d'écrire
Bonnées utilisateur	Les nouveaux enregistrements sont outomatiquement ajoutés à cette ACL
📝 Concepteur des badges	
14 ACLs	>>
Visiteurs / Dates	
Entreprises externes	Utilisateur: admin Jusun lector sé diarque () Station de travais INV-11537 Lac DTMuc office Événements: 0 Timeout: non activ

La disponibilité des clients est recommandée lorsqu'une installation/base de données AccessOne est utilisée par plusieurs clients et que chaque client peut uniquement voir et éditer ses propres données. Les jeux de données qui ne sont attribués à aucune clientèle sont disponibles pour les utilisateurs de toutes les clientèles. Le traitement de tels paramètres incombe à une personne supérieure (administrateur système). La direction et l'administrateur système doivent toujours obtenir des droits maîtres ou supplémentaires. Pour les employés, par ex. les personnes à la réception, des systèmes partiels propres de l'installation de contrôle d'accès doivent être mis en place, pour pouvoir visualiser, éditer et supprimer les données de base. Les utilisateurs d'un système partiel, par ex. le groupe « Employés réception », ne doivent par ex. pas avoir accès à l'ACL, car ils peuvent sinon ajouter des personnes dans d'autres listes d'accès. L'autorisation de lecture de données de base est suffisante pour les utilisateurs de ce système partiel.





Lorsqu'une seule liste d'accès (ACL) est attribuée à un utilisateur AccessOne, il peut uniquement attribuer les autorisations qui sont comprises dans la même ACL. Ainsi, l'utilisateur AccessOne peut uniquement attribuer des autorisations pour les portes activées pour la zone de réception du bâtiment aux membres du groupes « Employés réception ». D'autres portes ne sont pas affichées dans la liste de sélection.

Les membres du groupes « Employés réception » peuvent visualiser, modifier et supprimer les autorisations, mais pas les ajouter à nouveau. Cela ne s'effectue que via l'administrateur du système ou une personne disposant du droit d'accès ou d'attribution correspondant. La répartition des données selon ses exigences (de sécurité) de manière sensée reste à la discrétion et la responsabilité de l'utilisateur.

Workflow

L'onglet Workflow permet de créer des processus de travail pour certaines actions à effectuer, par ex. lorsque la permission d'un supérieur hiérarchique est nécessaire.

6.2.4 Attribution des jeux de données aux listes d'accès – ACL

Si des données ont déjà été saisies dans le système, dont l'accès doit être limité ultérieurement, ces données doivent être attribuées via le bouton ASSIGNATION d'une ACL.

Important : les données qui ne sont pas assignées à une ACL, sont visibles par tous !

Andern Neu Kopieren Laschen Actualidere Andern Neu Kopieren Laschen Actualidere DMS Fisuptgebäude I. Essge Hauptgebäude Zentrale Basier entrance Reader entrance Reader entrance Reader entrance Reader entrance Beseir e	en Zuordnung ammdaten 10-Module ne: Hauptjoblaude ahrebung: Tim 3 koffer ndort, Raim: C. Mac Referenz: ellangen ⊋l Athy.	ACL Zuordnung zugeordnete ACLs Name Beschreibung	-
Andem New Kopieren Läschen Aktualidere Ander New Kopieren Läschen Aktualidere DMS Hauptgebäude 1. Etage Hauptgebäude Zentrale Resder entrance Resder entr	en Zuordnung ammdaten 10-Module me: Hauplgebillude zhrebung: Tim 3 koffer ndort, Raim: C. Mac Referenz: ellangen V. Aktry	ACL Zuordnung zugeordnete ACLs Name Beschreibung	-
Andem New Kopieren Läschen Astualiders DMS	en Zuordnung tammdaten 10-Module me: Haupfgebäude zhrebung: Tim 3 koffer ndort, Raum: C. Mac Referenz: ellangen ⊋l Attiv	ACL Zuordnung zugeordnete ACLs Name Beschreibung	-
DMS	ne: Haupfgebäude zhreibung: Tim i koffer ndort, Raum: C. Mac Referenz: eflangen ⊋l Attry	ACL Zuordnung zugeordnete ACLs Name Beschreibung	-
And Antipation An	mei Hauptgebäude chreibung: Tim i Koffer ndorf, Raum: C. Mac Referen: ellangen V Aktry	I. Prese ALL Zuordnung zugeordnete ACLs Name Beschreibung	- C X nicht zugeordnete ACLs Name Beschreibung Velbert Kain
Hauptgebaude Zentrale Parkplatz Einfahrt Reader entrance Reader exit Nebengebaude Zentrale Eingang Gerätedaten Gerätedaten System-Konfiguration Lac	me: Hauptgebäude chreibung: Tim s Koffer ndort, Raim: C. Mac Referenc: ellangen ⊋! Aktry	ACL Zuordnung zugeordnete ACLs Name Beschreibung	- C × nicht zugeordnete ACLs Name Beschreibung Velbert Koln
Parkplatz Enfahrt Resder entrance Resder entrance Resder entrance Benutzerdaten System-Konfiguration	chrebung: Tim 1 Koffer ndort, Raum: C. Mac Referenz: eflanger eflanger V Aktiv	ACL Zuordnung zugeordnete ACLs Name Beschreibung	- × nicht zugeordnete ACLs Name Beschreibung Velbert Koln Koln
Resder entrance Resder exit Nebengebäude Zentrale Eingang Gerätedaten Senutzerdaten System-Konfiguration	ndort, Raum: C. Mac Referenz: ellangen V. Aktiv.	zugeordnete ACLs Name Beschreibung	nicht zugeordnete ACLs Name Beschreibung Velbert Koln
Area and a second and a se	K. Mac Referenz: ⊯llanger √ Aktiv	zugeordnete ACLs Name Beschreibung	nicht zugeordnete ACLs Name Beschreibung Velbert Kain
Eingang Edit Gerätedaten Einste Benutzerdaten LaC System-Konfiguration Dev	Referenz: vilangen V Aktiv	Name Beschreibung	Name Beschreibung Velbert Köln
Gerätedaten	rilangen √ Aktiv		Kölm
Benutzerdaten LAC System-Konfiguration Dev	Aktiv		_
System-Konfiguration	Type TSS Compact		
System-Konfiguration	Adresse: 192,168,100,10		
	oug-Lever 0		
ACLS	nware: TSGV1854.BIN		**
Gruppenänderungen	c-Adresse		10 0.4
Kartendesigner	iennummer: 26279955		nderungen verwerfen Ånderungen speichern
Bus		C	
1.1	Protokell, Datasec	Baucrate Schlösel:	
Besucher / Termine 2.8	Protokoli: Datasec	Eaudrate Schlossel	
Fremdfirmen-MA	Protokoli. Detisec	- Eautrate Schlussel	
A.	Protokoll: Dataser	Baudrate Schlüssel:	

Procédure et ordre recommandés

Commencez par les portes du dialogue « Données d'appareil ». Cliquez pour cela sur le bouton ASSIGNATION de la barre d'outils.

Sélectionnez une porte dans la liste de sélection sur le côté gauche et assignez-la à l'ACL correspondante. Ensuite, cliquez sur la touche SAUVEGARDER LES MODIFICATIONS. L'objet sélectionné est alors marqué par une barre de couleur correspondante.



Procédez exactement de la même manière pour les dialogues « Données personnelles » et « Autorisations ».

6.2.5 Groupes d'utilisateurs online

(Uniquement disponible en relation avec le module de licence Gestion de visiteurs, réf. 348122V.)

	Donnees de mase	Autres données de base	Badges	Autorisations	Prendre une photo-	Blocages	Masques d a
Spind-Mast	Nom:	P	Prénom:			_	
	Entreprise: Départment:	Assignation ACL					×
Descriére province aller	Leu actue: Inconnu Demière visite: 29.06.2021 13:56 Zone de parlöng: Inconnu Badges Date d'identification pendant de 1, déli 10 0 0	Nom Descrip	otion	8	Nom Des Velbert Star Köln	cription dort Velbert	±
Autorisations	Blocages				Sauvegarder	Алли	iler
Profils d'autorisation	Blocage d'accès Raison					_	
Données d'entreprise							
Logbook					× Suppr	imer	
	lashask und a sel	Augusta 1					Client

Les pages web pour la connexion des utilisateurs online et la gestion des employés d'entreprises externes dans les groupes d'utilisateurs online sont regroupées ici.

En outre, le Lightweight Directory Access Protocol (LDAP) permet de mettre à dispositions des informations sur les utilisateurs et leur appartenance à un groupe et de les ajouter au système. Le LDAP permet de consulter les informations d'un répertoire LDAP.



6.3 Données d'emplacement

Les données d'emplacement vous permettent de représenter toutes les structures d'objet pertinentes pour l'installation de contrôle d'accès. La représentation s'effectue de manière claire sous la forme d'une arborescence.

1

Indiquez de manière aussi complète et détaillée que possible les données de l'emplacement, car elles seront ensuite utilisées lors de la création de composants matériels.

Si plusieurs emplacements sont créés, l'onglet « Recherche d'emplacement » est utile. Un clic sur « Emplacements » dans l'arborescence affiche tous les emplacements créés, triés par type. Un double-clic sur un emplacement de la liste ouvre l'emplacement dans l'arborescence à gauche.

6.3.1 Créer un emplacement

AccessOne - Données d'emplacement			- D ×
Accueil			6
Changer Nouveau Copier Supp	nmer Actualiser		
Emplacements Velbert Service Main-Building Area 1	Recherche d'emplacement		
E123	Nom	Description	Type
	Velbert	Velbert	Objet
	Service	Service	Zone
9	Main-Building	Main-Euliding	Bâtiment
ACLS	Area T	Area 1	Étage
A CONTRACT OF A CONTRACT.	E123	E123	Salle
2 Visiteurs / Dates	<u>F173</u>	E123	Porte
intreprises externes			
🔹 Workflow			
# Changements de groupe	Ublication admin	Station de travail INV-11537	Evénements 0 Timeout non artivé

Sélectionnez « Données d'emplacement » dans la sélection de dialogue. L'onglet « Recherche d'emplacement » s'ouvre et les données des objets, zones, bâtiments, étages, pièces et portes s'affichent de manière hiérarchique dans l'arborescence à gauche.

En cliquant sur le niveau correspondant, une saisie peut être effectuée ou adaptée à l'aide des boutons NOU-VEAU et MODIFIER.

Objet

Attribuez un nom d'objet à l'emplacement dans lequel se trouvent les zones, bâtiments, portes, cylindres électroniques, lecteurs et appareils offline. Plusieurs emplacements peuvent être créés au niveau de l'objet.

Zone

Attribuez des noms aux zones qui se trouvent dans l'objet (par ex. « Production », « Développement », « Comptabilité », etc.).

Bâtiment

Attribuez un nom au bâtiment dans lequel se trouvent toutes les zones de l'objet (par ex. « Maison 3.1. ») et créez pour cela les données d'adresse et de contact.

Étage

Saisissez le nom de l'étage et le numéro de l'étage dans lequel les portes, les cylindres électroniques, les lecteurs et les appareils offline du bâtiment général de votre objet se trouvent, par ex. « Rez-de-chaussée ».



Pièce

Attribuez ici des noms aux pièces du même étage, par ex. « 0.12 », et configurez les pièces selon Personnes responsables, Type d'utilisation et Étages.

Porte

Saisissez le nom de la porte de la pièce, par ex. « Porte 0.12 extérieur ».

7 Configuration des appareils

Groupe cible de ce chapitre :

• Personnel formé aux produits

La mise en place des appareils commence par les contrôleurs maîtres de niveau 2. Ensuite, les contrôleurs de porte de niveau 3 sont configurés et les modules IO sont créés. Enfin, mettez en place les appareils online et offline de niveau 4 connectés.





D'un point de vue matériel, l'AccessOne se base sur un concept à quatre niveaux pour une évolutivité quasiment sans limites. Les processus de serveur Application et Base de données fonctionnent sur des systèmes d'exploitation Windows Server ainsi qu'un SQL Server installé. Le logiciel du serveur fonctionne dans la plupart des cas dans un environnement virtuel (niveau 1). Le MasterController répartit les données aux commandes de portes (Door Control Unit) et met toutes les fonctions regroupant les commandes de portes à disposition (niveau 2). Le MasterController ne doit pas être disponible comme composant physique autonome, il peut également être rendu virtuel comme le logiciel du serveur. Le MasterController est relié localement aux commandes de portes par réseau (niveau 3). Chacune des commandes de portes raccordées est autonome et dispose, lorsque les données ont été chargées une fois, de toutes les données d'autorisation d'une personne, y compris les données offline. Toutes les décisions d'accès sont ainsi effectuées de manière locale (niveau 3). Les lecteurs sont raccordés via une interface RS485 (niveau 4). Chaque lecteur peut également être utilisé comme appareil de mise à jour pour les appareils offline.

7.1 Données des appareils online

7.1.1 Afficher l'aperçu des appareils

AccessOne - Données de l'appareil								-	D X
Accueil									
Changer Nouveau Copier Suppri MeuMac Mac Mac Mac	mer Actualiser	-							
CES Terminal	1		Tous						
PHG Terminal	Appareil	Type	Statut	Programme	Power	Sabotage	Mode	Statut	Système
PM	Mac	MAC	Online	Inconnu	1	1	1	1	1
SDC	- Aufzug 1	LAC	Inconnu	Inconnu	Inconnu	Inconnu	-	-	-
	- IO Modul: 6	Module IO	Incomu		Inconnu	1	1		
	Entrée principale	LAC	Office	Inconnu	Inconnu	Inconnu	-		-
	- CES Terminal	Porte	Lane .				Inconnu	Inconnu	Inconnu
	- CES Leser 1	Lecteur	Inconnu		Inconnu	Inconnu			
	- PHG Terminal	Porte	Incomm		1		Inconnu	Inconnu	Inconnu
Logbook	- Infoterminal	Lecteur	Inconiu		Inconnu	inconnu	-	1	
and the second se	- PM	Porte	Line		-		Inconnu	Inconna	Inconnu
Rapports	- Entrance-Terminal	Lecteur	Incontu		Inconnu	inconisu	-		
(- CES Leser Modul	Module IO	Incomu		Inconnu	-			
Données de l'appareil	- IO Moduli T	Module IO	Incomu		Inconnu	-			
bennees ac rupparen	- CES URC	Access-Point	Inconsu		Inconnu				
1055	-SDC	LAC	Inconnu	Inconnu	Incionnu	Inconsu		1	
g 055	- test1	Porte	Inconnu				Inconnu	Inconnu	Inconnu
	- Test CES	Lecteur	Incornel		Inconnu	Inconsu		1	-
Liste noire de l'OSS	- IO Modul: 5	Module IC	Inconsu		Inconnu			1	
	ICAL AND	1.65	1100						_

Pour créer et paramétrer des appareils, l'AccessOne met à disposition l'éditeur de données d'appareil. Celui-ci affiche les appareils dans une arborescence dans la sélection d'objets à gauche. L'entrée supérieure est le Data Management System (DMS) sous lequel sont disposés les appareils. Toutes les modifications de données et tous les messages du contrôleur de porte (TSG1, TSG8, AMC ou LAC*) s'effectuent ici. Les messages de statut y sont donc également interprétés, collectés dans la mémoire et affichés.

Cliquez sur l'entrée « DMS » lorsque vous souhaitez voir l'aperçu du statut de tous les appareils. Vous ne pouvez pas supprimer l'entrée DMS, ni en créer une deuxième.

Le statut d'un appareil individuel (online ou offline) est également visible dans la vue détaillée de l'appareil.

Dans la fenêtre de dialogue, le statut de tous les appareils disponibles est affiché sous forme de liste. Cet affichage n'est pas automatiquement mis à jour. Pour une mise à jour, veuillez cliquer sur le bouton ACTUALI-SER. Une fenêtre de recherche se trouve à gauche, au-dessus de la sélection d'objets. Si des lettres sont saisies ici, la liste en-dessous filtre tous les appareils qui contiennent ces lettres, ils ne doivent pas commencer par ces lettres. La casse est également ignorée pour faciliter la recherche. Les noms des appareils sont affichés en bleu, ce qui signifie généralement dans l'AccessOne qu'un double clic sur le nom permet une navigation directe vers l'onglet de cette entrée. Au centre se trouve une possibilité de filtrage supplémentaire par statut d'appareil. Si l'on souhaite par ex. voir uniquement les appareils qui sont actuellement online, il faut sélectionner l'entrée « Online » dans le menu déroulant. Un clic droit sur le nom d'une porte affiche les ordres de commande possibles qui sont autorisés pour une porte.

* TSG = appareil de commande de porte, AMC = Access Modular Controller, LAC = Local Access Controller

CEStronics

CEStronics

7.1.2 Créer un MasterController (MAC)

Pour créer un nouveau MasterController (MAC), sélectionnez l'entrée « DMS » dans l'arborescence et cliquez sur le bouton NOUVEAU.

AccessOne - Données de l'appareil							-		×
Accueil									- 0
Annuler Sauvegarder	0								
	Données de base du	MAC							
	мас								
	Nom:								
	Description:	E123 - E123							
	Référence exti				1000				
	Paramètres								
Logbook	1	Actif	_	Statut:	16100				
Rannorts	Adresse IP: Adr.IP, Proch. MAC	r	_	Port, Proch. MAC	16110				
La napporta	Niveau de debug:	2 +		Crypten					
Données de l'appareil	Firmware	MACV0011.ZIP	-	Système offline:	OSS -				
S OSS	Adresse Mac N° d'inventaire:								
🧩 Liste noire de l'OSS	Date d'installation	Select a date							
22 Données utilisateur	Nomèro de sene:			Options:					
Concepteur des badges									
1: ACIS	Ublisateur: admin	Alacan Instear de dialógue dia	Station de travail: INV-115	87 1 Jac II Mac off	Événements	0	Timeout no	on activé	-

7.1.2.1 Données de base MAC

Sur le côté droit, un onglet non rempli relatif au MAC s'affiche alors, et vous pouvez y saisir les données. Chaque MAC nécessite un nom qui doit être choisi de manière à décrire la zone de responsabilité de cet appareil. En règle générale, un MAC suffit pour une petite installation. Pour des installations plus grandes, un MAC est souvent présent pour chaque complexe de bâtiments. Il est donc pertinent de nommer le MasterController d'après ce complexe. Un seul MAC peut gérer jusqu'à 32 Access Modular Controller (AMC).

Vous avez la possibilité d'indiquer également une « description », par ex. l'emplacement exact. La boîte de sélection « Emplacement » fournit la liste des emplacements configurés au préalable. En cas de nouveau système, seul l'emplacement « inconnu » est disponible. Vous pouvez remplir cette liste avec des emplacements supplémentaires via le dialogue « Configuration du système > Emplacements » (voir « 6.1 Configuration du système » page 17). Pour les applications où l'installation de contrôle d'accès se répartit sur plusieurs emplacements, nous recommandons de créer ces emplacements au préalable et de les sélectionner uniquement dans la liste au niveau de l'installation des appareils. Les données d'emplacement contiennent, selon leur type, d'autres informations, par ex. l'adresse d'un interlocuteur avec numéro de téléphone, et sont donc utiles en cas de panne.

Pour chaque MAC, une adresse IP et un numéro de port doivent être indiqués. L'adresse IP des MAC est indiquée dans la configuration du réseau sur le MAC. Sur le MasterController, vous pouvez également ouvrir une fenêtre de commande (cmd.exe) et saisir l'ordre « ipconfig ». L'adresse IP4 affichée pour l'adaptateur LAN est l'adresse IP du MAC. En cas de question, veuillez contacter l'administrateur système de votre réseau.

Sur les MasterController nouvellement installés, l'adresse du port est réglée sur 50100. Cette adresse peut être modifiée au choix, mais doit cependant correspondre dans la configuration du MAC (Datasec\Mac\config\MacConfig.ini) et dans les données d'appareil, sinon aucune communication ne peut être établie. Le champ « Niveau de débogage » est un outil d'aide pour le fabricant, lui permettant de créer des protocoles d'erreurs détaillés en cas de panne. Plus le niveau de débogage est grand, plus les enregistrements que le


MasterController écrit pour toutes les actions sont importants. Veillez à ce que la valeur ne soit pas supérieure à 1, car cela peut avoir des effets sur la performance de l'appareil.

La case à cocher « Crypter » vous permet de régler si la communication entre DMS et MAC AES doit être cryptée. Le cryptage de données ralentit la vitesse lors de l'établissement de la connexion et a ensuite un léger impact sur le débit lors de l'échange de données.

Le champ « Firmware » sert à saisir ici la nouvelle version du logiciel lors d'une mise à niveau. Celle-ci est automatiquement répartie et activée sur tous les MasterController. Important : chaque MAC dispose de son propre firmware.



Modifiez uniquement la valeur préréglée si vous avez obtenu une mise à jour correspondante de CES ! Si votre MAC commande des lecteurs de badges avec fonction de mise à jour pour les systèmes offline, vous devez le régler lors de la création du MAC. Dans ce cas, la sélection du/des firmware(s) à utiliser pour le MAC change. Une modification **ultérieure** de cette fonction MAC est **impossible**. Dans ce cas, un nouveau MAC doit être créé dans le DMS et les LAC déjà attribués doivent être portés vers le nouveau MAC.

En option, vous pouvez également saisir pour l'appareil l'adresse MAC, un numéro d'inventaire et la date d'installation. Important : l'adresse MAC peut être importante lorsque votre réseau utilise uniquement des adresses MAC configurées, afin d'éviter que des personnes non autorisées se connectent à votre réseau.



Il existe une case à cocher pour chaque appareil et chaque porte qui active l'appareil. Ce n'est que lorsque cette case est cochée que les données sont chargées sur l'appareil et qu'il est démarré. Les appareils peuvent ainsi être déjà configurés, et activés seulement après l'installation. Avantage : les appareils non activés ne sont pas surveillés par le système. Les appareils préconfigurés mais non activés ne sont ainsi pas indiqués comme appareils défaillants. Au total, jusqu'à 32 commandes de portes locales peuvent être raccordées par MAC.



7.1.3 Créer une commande de porte (LAC)

7.1.3.1 Données de base LAC

AccessOne - Données de l'appareil						- 🗆 X
Accuel						
Changer Nouveau Copier Suppri	mer Actualiser Assignat	ion				
Mar Mac	Données de base L/	AC Modules IO	Lecteur Access-Poe	a (
Em Entrée principale	LAC					
The source	Nom:	Autrug T				
	Description					
	Lieu, sale	Mar				
	Référence est	1938				
	Descendence					
	Parametres	Actif		Batul:		
	Type de ILAC	TSG B/Ascenseur		Definition de l'atc		
	Adhesse (P)	19216810057		Port: 10001		
Logbook	Nirreinu de debugi.	0		Crypten		
Rapports	Firmwords	TSGV1910.BIN		Système officie		
C	Adresse Mac			Zone offline:	and a second	
Données de l'appareil	N° di riventtane.			Oute d'installation: Statistics		
OSS	Numitio de Mirie			Optons		
Me in the lease	Sas	1.0.5	and the set	74 A		
a Liste noire de l'OSS	2. protocole	D-Des	Tata de peut	Cie de rodane		
🎎 Données utilisateur	3. protocole		Taux de baud	Clé de sodage		
Concepteur des badges	4. protocole-		Tion de brud	Clé de codage		
IL ACLS	Conturts			Di de contrare		
	Sabotage Lanuc			10" de postart		
Visiteurs / Dates	Foretion speciale			(4" de comaco		
Entranrises externer	- Contrast Montane					

Les commandes de portes locales, Local Access Controller (LAC), sont créées sous le MAC auxquelles elles sont raccordées. Sélectionnez à l'aide de la souris le MasterController souhaité et cliquez sur

Nouveau.

L'onglet pour une commande de porte s'affiche alors dans la fenêtre de dialogue.

Chaque LAC nécessite un nom et une description. Procédez ici de la même manière que pour le MasterController MAC. Ici aussi, il est pertinent de choisir un nom qui indique la zone de responsabilité. La description vous offre en outre la possibilité d'indiquer l'emplacement d'assemblage exact.

	Actif	Statut:	Offline
ype de l'LAC:	TSG 8/Compact *		
dresse IP:	TSG 8/Compact	Port:	10001
Viveau de debu	TSG 8/Ascenseur TSG 1/SDC	Crypter:	
irmware:	AMC2_4R4 (Bosch)	Système offline:	1
dresse Mac:	AMC2_WIE (Bosch)	Zone offline:	1 - OSS Test *
l" d'inventaire:		Date d'installation:	03.12.2020
uméro de série:	26280029	Options	1

L'AccessOne prend en charge des commandes de portes de différents fabricants. Sous Type de LAC, sélectionnez le type de matériel que vous utilisez. Les commandes peuvent être combinées dans une installation.

- Contrôleur d'accès TSG 8/Compact (réf. 348007V) pour jusqu'à 8 portes avec jusqu'à 16 lecteurs
- Contrôleur d'accès TSG 1/SDC (réf. 348008V) pour 1 porte avec jusqu'à 2 lecteurs
- AMC2_4R4 avec 4 connecteurs RS485 pour jusqu'à 8 portes
- AMC2_WIE avec 4 interfaces Wiegand pour jusqu'à 8 portes

Saisissez une adresse IP pour la LAC qui est accessible depuis le MAC. L'adresse de port est préréglée sur

10001 et ne doit pas être modifiée. Pour régler l'adresse IP sur la commande de porte, sélectionnez la configuration adaptée à la commande de porte.

En option, vous pouvez également saisir pour l'appareil l'adresse MAC, un numéro d'inventaire et la date d'installation.

La case à cocher « Crypter » vous permet de régler si la communication AES doit être cryptée. Le cryptage de données ralentit la vitesse lors de l'établissement de la connexion et a ensuite un léger impact sur le débit lors de l'échange de données.

La case à cocher « Système offline » signifie que l'AMC reconnaît lorsque les systèmes offline sont commandés et un appareil de mise à jour est disponible.

Selon le matériel et l'interface, les protocoles correspondants peuvent être saisis ici.

Bus					
1. Protokoll:	CES-FastCrypt *	Baudrate:	Ŷ	Schlüssel:	
2. Protokoll:	CES-FastCrypt *	Baudrate:	۲	Schlüssel:	
3. Protokoll:	CES-FastCrypt *	Baudrate:	÷	Schlüssel:	
4. Protokoll:	Datasec v	Baudrate:		Schlüssel:	
Kontakte	DE-Bus				
Sabotage:	L-Bus	*	1	Kontaktnummer:	
Störung:	V-Bus			Kontaktnummer:	
Conderfueltion	Aperio			Kontaktnummer	
Sondentinktion	PHG Crypt				
Legic OS Firmware	CES-FastCrypt	4			
1.5	Datasec				6
1. Firmware:	Nedap	2. Firmware:		3. Firmware:	
	Wiegand				
	reig				

Il existe une case à cocher pour chaque appareil et chaque porte qui active l'appareil. Ce n'est que lorsque cette case est cochée que les données sont chargées sur l'appareil et qu'il est démarré. Les appareils peuvent ainsi être déjà configurés, et activés seulement après l'installation. Avantage : les appareils non activés ne sont pas surveillés par le système. Les appareils préconfigurés mais non activés ne sont ainsi pas indiqués comme appareils défaillants. Au total, jusqu'à 32 commandes de portes locales peuvent être raccordées par MAC.

Dans la sélection de dialogue « Rapports », il existe une liste d'appareils qui indique toutes les données pertinentes relatives à la documentation de matériel pour tous les appareils. Si toutes les données sont indiquées, le système peut fournir à tout moment une documentation d'installation complète.

7.1.3.2 Modules IO

Dans les caractéristiques de la commande de porte, il existe un onglet supplémentaire pour les modules IO. Chaque commande de porte locale nécessite des composants matériels pour la surveillance des signaux d'entrée (par ex. signaux de l'état de porte) et pour l'émission d'ordres de commande. Il s'agit des modules IO (modules Input-Output) de la LAC. Un module IO dispose de plusieurs circuits de commutation d'entrée pour vérifier si un contact externe est ouvert ou fermé.



Dans l'AccessOne, les modules IO sont généralement traités de manière séparée, même si le matériel correspondant est compris dans la commande de porte ou dans le lecteur de badges. Cela permet une assignation libre de signaux sur tous les modules IO disponibles.

CEStronics

CEStronics

L'AccessOne fait la différence entre les modules IO à bord de la LAC et les modules IO séparés à distance. Le module IO embarqué est créé par défaut en même temps que la LAC. Les modules IO à distance doivent être ajoutés manuellement avec leur adresse bus correspondante. La programmation des signaux des modules IO est effectuée ultérieurement de manière individuelle dans la configuration de chaque porte.

Passez à l'onglet « Modules IO » pour configurer le matériel pour les entrées et sorties de la commande de porte.

	XOD				
nger Nouveau Copier Sup	oprimer Actualiser Assigna	dion			
	Données de base L	Modules IO Li teur Access	Pennt		
Aufzug T					
Entrée principale	LAC	Entrée principale			
PHG Terminal	and a second sec	and a function of the			
D PM	Nom	Description		Adresse	
Side entrance	IO Modul: 1	Onboard Kontakte		0	
	CES LESER MODUL	Les Leser Modul		13	
					Crem un multiple (1
					X Sec.
	Madule 10				
	Nom.	DD Modul: 1	Statut:	1000	
	Description:	Enboard Kontakte		-	
	Lieu, saile:				
	Recorders				
	Parametres	0/	24/84	0	
	Monesse du modure:	10000	Uko y Dvoc		
Autorisations	Nouchus diamate	\$	Mixed outputs	5	
Profils d'autorisation	Numbre de state		Contra	-	
	Billionan and		Ciypier:		
Données d'entreprise	NENGRACE INC.		Fulloware		

Si vous avez sélectionné une commande de porte, qui dispose déjà d'entrées et de sorties contenues dans l'appareil, ce module IO est automatiquement créé lors du passage à cette page.

Pour créer un nouveau module IO, cliquez sur la touche Nouveau module IO et remplissez les champs de saisie correspondants. Pour les contacts internes, l'adresse de module est 0.

Comme type, sélectionnez « AMC-IO », si vous avez sélectionné une AMC comme commande de porte. Si vous utilisez un contrôleur d'accès TSG, choisissez « TS2 » comme type pour un module de commande de porte avec 4 entrées et sorties et 2 interfaces de lecture ou « IO8 » pour une carte relais avec 8 entrées et sorties. Pour les modules de commande de porte à distance, qui sont raccordés au bus de lecture, saisissez l'adresse de bus réglée et choisissez « TSM » comme type. Les modules de commande de porte TSM ont deux entrées et deux sorties (remarque : cela varie selon la version/le type). Indiquez ici uniquement le nombre effectivement disponible, sans quoi des ordres de commande pour des relais non disponibles pourraient entraîner des messages d'erreur.

Jusqu'à 64 signaux d'entrée et 64 signaux de sortie peuvent être commandés par commande de porte. La répartition sur les modules IO n'est pas pertinente, tant que la plage d'adresse du bus de lecture ne dépasse pas un maximum de 16 participants.



7.1.4 Créer une porte

7.1.4.1 Données de base de porte

Pour créer une porte sur une commande de porte (LAC), choisissez la commande de porte correspondante dans la liste de sélection à gauche et cliquez sur le bouton NOUVEAU. La page de propriétés pour une commande de porte s'affiche alors à droite dans la fenêtre.

AccessOne - Données de l'appareil		- 🗆 ×
Accueil		
BDDH	X O 🗟	
Changer Nouveau Copier - Su	pprimer Actualiser Assignation	
Les.		
A MICE Mac	Données de base de la porte Lecteur Paramètres P Paramètres I Paramètres O	
	Porte	
CES Termina	Nom: CIS Terminal	
ET PM	Description: CES Terminal	
EE SDC	Lieu salle: E123 - E123	
Side entrance	LAC: Entrite principale	
	Référence est	
	Paramètres et la cré	
	Type: Porte/tournauet avec lecteur d'entrée. Une eule cirection	
	Numbro He pome: 3	
	Temps d'activation de l'auvre-parte: 40 (0.1 s) Temps d'auverture min: 10 (0.1	0
	Temps de refrond de la porte: (0,1 %) Code P/N de la porte. Nou	v.
	Mode upfiniture: Fonctionnement normal	
	Nivaau de debugi 0.	
	Alame	
Autorisations	Max. temps d'ouverture porte avait 200 [0,1:5] Pre-alume 100 [0,1:5]	1
Profils d'autorisation	Sup Parte overte tool londemos	
	and the second s	
A Données d'entreprise	Modèles de temps	
Logbook	Modele temps sam code Pric. Modelet en permanence	
Deserved.	Mod. temps code PIN pointe active:	
Rapports		

Dans cet onglet, les propriétés générales d'une porte sont déterminées. Outre un nom pertinent, cela implique également l'indication de l'emplacement ainsi que le type de porte souhaité. Le type détermine le déroulement de la visite et quels signaux d'entrée et de sortie sont utilisés. L'AccessOne met à disposition des modèles de portes préconfigurés, qui couvrent toutes les tâches courantes d'une porte. Sur demande, d'autres modèles de portes spéciaux répondant aux exigences spécifiques au client peuvent être ajoutés. Choisissez le type adapté à votre application. L'exemple suivant montre une porte d'entrée simple avec une seule direction.

CEStronics



Une fois le type de porte choisi, les paramètres de base de cet accès peuvent être réglés via les champs de saisie.

Section « Paramètres »

Il existe une case à cocher « Actif » pour chaque appareil, qui permet d'activer l'appareil. Ce n'est que lorsque cette case est cochée que les données sont chargées sur l'appareil et qu'il est démarré. Les appareils peuvent ainsi être déjà configurés, et activés seulement après l'installation. Avantage : les appareils non activés ne sont pas surveillés par le système. Les appareils préconfigurés mais non activés ne sont ainsi pas indiqués comme appareils défaillants.

Avec « Entrée lieu » et « Sortie lieu », vous choisissez la zone source et cible. Chaque porte dans AccessOne mène d'une zone source à une zone cible. Ces zones peuvent être différentes, mais cela n'est pas obligatoire. Exemple : si votre bâtiment est divisé en plusieurs zones de sécurité, une entrée peut par ex. mener de la zone de sécurité extérieure (ZSE) à la zone de sécurité intérieure (ZSI). Une porte intermédiaire peut cependant aussi mener de ZSI à ZSI.

Les zones sont créées dans la sélection de dialogue « Configuration du système » dans l'onglet « Zones ». Pour une zone dans un bâtiment, le système peut calculer combien de personnes s'y trouvent actuellement et par ex. vérifier si le nombre maximal de personnes est atteint. Dans ce cas, aucun autre accès ne serait autorisé. La condition pour cela est qu'une personne sans badge ne puisse pas accéder à la zone correspondante et que les entrées et sorties soient dotées d'installations d'accès individuel, par ex. des tourniquets, afin qu'il ne soit pas possible pour plusieurs personnes avec une autorisation d'accès d'entrer dans la zone en même temps.

Chaque porte nécessite un numéro de porte clair au niveau de la commande de porte. Il doit se situer entre 1 et 8, car un maximum de 8 personnes peuvent être prises en charge par commande de porte.

La valeur du champ « Temps d'activation de l'ouvre-porte » détermine la durée maximale d'activation de l'ouvre-porte en cas de média d'accès autorisé. L'indication est en dixièmes de secondes. La saisie 40 signifie donc par exemple 40 x 0,1 s = 4 secondes. Si la porte dispose d'un contact de porte, la commande de porte peut déterminer que la porte a été ouverte. Dans ce cas, l'activation est annulée dès que la porte a été détectée comme ouverte. La valeur du champ « Temps d'ouverture min. » permet de s'assurer dans ce cas que l'ouvreporte est actionné suffisamment longtemps pour garantir une ouverture sûre.

Il existe des contacts d'ouverture de porte qui sont intégrés au verrou ou au dispositif de blocage magnétique, et qui indiquent que la porte est ouverte lorsqu'elle a seulement été déplacée de quelques millimètres. Dans ce cas, sans une indication de durée d'ouverture minimale, la porte serait à nouveau directement verrouillée et un accès serait alors éventuellement impossible.

La valeur du champ de saisie « Temps de rebond de l'ouvre-porte » indique la durée d'attente de l'AMC après une visite et la détection qu'une porte a été refermée, avant qu'il active à nouveau la surveillance d'intrusion de la porte. Sur les portes lourdes, il peut arriver qu'un battant de porte amortisse légèrement lors de l'arrivée dans le cadre, de sorte que la porte soit brièvement détectée comme fermée par la commande de porte, puis à nouveau ouverte pendant une fraction de seconde, et enfin fermée de manière permanente. Sans ce temps de rebond, il pourrait éventuellement encore y avoir après une visite le message d'une ouverture de porte.

En mode opératoire, il est possible de choisir parmi les alternatives suivantes :

Туре:	Porte/tournig	1					
Numéro de porte:	3						
Temps d'activation de l'ouvre-porte:	40	[0,1 s]	Temps d'ouverture min:	10	[0,1 s]		
Temps de rebond de la porte:		[0,1 s]	Code PIN de la porte:		Nouv.		
Mode opératoire:	Fonctionnement normal						
Niveau de debug:	Fonctionnement normal						
	Fonctionnement normal interieur le modèle de temps, bloqué à l'extérieur Ouverture permanente, entrée						
larme	Ouvert en per	manence, sortie		Contractor Strends To			
Max, temps d'ouverture porte ava	Ouvert en per	manence dans le r	nodèle de temps, fonctionneme	ent normal à l'extérieur			
T	Blorage perm	Ouverture permanente intérieure le modèle de temps, fonctionnement normal à l'extérieur après le premier accès autorisé					
temps de suppression de l'alarme	Blocage permanent, entree						
Sun 'Porte ouverte tron longtemo	Blocage permanent, sortie						

« Fonctionnement normal » (standard) : dans ce mode, la porte peut uniquement être utilisée avec l'autorisation correspondante et un badge valide.

« Ouvert en permanence » : l'ouvre-porte est toujours actif, la LED verte du lecteur de badges est allumée en permanence et chaque personne peut ouvrir cette porte sans badge.

« Ouverture permanente dans le modèle de temps, fonctionnement normal à l'extérieur » : la porte peut être ouverte sans badge lors des horaires de bureau normaux, mais après cette période à définir librement, seules les personnes autorisées peuvent avoir un accès.

« Ouverture permanente dans le modèle de temps, fonctionnement normal à l'extérieur après le premier accès autorisé » : Après la première ouverture autorisée, la porte reste ouverte. La porte passe à l'état « ouvert en permanence » dans le modèle de temps choisi. Cela permet de garantir qu'au moins un employé autorisé est présent.

« Fonctionnement normal dans le modèle de temps, bloqué à l'extérieur » : En-dehors du modèle de temps attribué, cette porte ne peut pas être utilisée, même avec un badge autorisé. Dans le modèle de temps, un badge valide et l'autorisation correspondante sont nécessaires pour l'ouverture.

CEStronics



Alarme

La section « Alarme » détermine les paramètres pour l'alarme de porte.

Alarme					
Max. temps d'ouverture porte avant	200	[0,1 s]	Pré-alarme:	100	[0,1 s]
Temps de suppression de l'alarme:	0	[0,1 s]			
Sup. 'Porte ouverte trop longtemps'			Supprimer 'Forcer porte':		

« Temps d'ouverture porte max. avant alarme » : temps d'attente du système jusqu'à ce que la porte soit refermée, avant qu'une alarme soit générée. Cette valeur est indiquée en dixièmes de secondes. Lorsque le temps saisi est dépassé, le système génère un message de logbook avec le texte « Porte ouverte trop long-temps ».

« **Pré-alarme** » : la valeur du champ doit être inférieure à la valeur du champ précédent. Elle indique quand un signal d'avertissement doit être généré sur le lecteur. Ainsi, la personne peut encore fermer la porte avant un message d'alarme. Si la porte est ouverte plus longtemps que cette valeur, le lecteur de badges monté sur la porte génère un bip répété jusqu'à ce que la porte soit à nouveau fermée ou que le message d'alarme soit généré.

« Temps de suppression de l'alarme » : l'indication est obligatoire pour les portes qui sont surveillées en permanence par un système de détection d'intrusion supplémentaire. Ici, il peut être nécessaire d'indiquer à ce système via un signal de sortie que la porte est ouverte de manière autorisée. Ce signal est annulé après que la porte est à nouveau fermée, mais au plus tard après le temps correspondant à la valeur dans ce champ.

« Sup. 'Porte ouverte trop longtemps' » : vous commandez ici si le système doit générer un message d'intrusion ou

non lorsque la porte a été ouverte sans badge.

« Supprimer 'Forcer porte' » : avec cette case à cocher, vous commandez le signal d'alarme sur place.

Le système ne génère pas de messages d'état de porte séparés. L'information si la porte a été ouverte ou non se trouve dans le message de logbook correspondant relatif à l'accès. Entrées de logbook :

- « Autorisé, accès » : la porte a été ouverte après un accès autorisé.
- « Autorisé, pas d'accès » : la porte n'a pas été ouverte, alors qu'elle a été débloquée.

Modèles de temps

Dans cette section, les modèles de temps éventuellement souhaités pour le comportement général peuvent être sélectionnés :

Zeitmodelle		
Zeitmodell ohne Motorschloss:	Zeitmodell permanent offen:	
Zeitmodell ohne PIN:	Zeitmodell keine Türalarme:	

Au total, quatre modèles de temps sont disponibles :

« **Mod. temps sans serrure à moteur »** : si la porte dispose d'une serrure à moteur, alors la sollicitation mécanique est réduite en activant la serrure à moteur uniquement avant et après le modèle de temps saisi.

« Mod. temps sans code PIN » : la saisie d'un code PIN sur le lecteur de badges est réduite aux temps en-dehors du modèle de temps saisi.

« Ouverture permanente » : l'ouvre-porte est toujours actif et la porte peut être franchie sans badge (ce réglage correspond au modèle de temps « Ouvert en permanence »).

« Mod. temps pas d'alarme porte » : les alarmes de porte n'ont lieu qu'en-dehors du modèle de temps saisi.



7.1.4.2 Lecteurs

AccessOne - Données de l'appareil						
Accuel	Assignatio	10				
DMS	Données de base LAC	Modules Lecteur	veso Point			
PM.	Nom	Description		Position Adresse		
E Side entrance	Infoterminal	Entrance-Terminal Infoterminal		Entrée 1 2		
	Funko-7 CES Leser 1	Fanka-1 CES Leser	_	Entrée 1 3	Noineexlactour	
					X Supprent & Includ	
	Lecteur					
	Name	Entranta-Terminal	Sa	Natr	100 C	
	Description	Entral-sce-Terminal				
	Lies, porte	01 5-1				
	Workflow	. G1, 1017		antiver par appropatieur		
	Paramétres					
	Adresse du medules	1		Compiteur d'usage		
	Numèro de siñie:	17496478		Mode turnet:		
Lenheek	Advenne	T Gid / Det	Bernalis	Crypter:		
LOGDOOK	Lieu d'entrèe:	Unbekannt:	Lieu de soitie	Unbekannt		
Rapports	Date of installation	anune [17]	Rélérence est			
Données de l'appareil	Groupe and parasiaste		Options.	ą.		
OSS	Claviny disposible:		Le lecteur soit deres-	Oui		
A state water de linner	Allichage disponible		Contole du retrait	Farantities -		
Liste noire de l'OSS	État de la bâttene:	1000	Date of etat battene	Line Alater (17)		
La Données utilisateur	Changement de la batt	TT		Dwnger les données batt	tene	

Dans l'onglet « Lecteur », les lecteurs de badges appartenant à la porte sont définis.

Pour créer un nouveau lecteur, cliquez sur la touche Nouveau lecteur. Le système ajoute alors une nouvelle ligne dans la liste d'aperçu et vous donne la possibilité de saisir les paramètres appartenant au lecteur dans les champs en-dessous.

Section « Lecteur »

Dans la section « Lecteur », vous indiquez le nom, la description, l'emplacement, le niveau de sécurité et le workflow.

Lecteur			
Nom:	Entrance-Terminal	Statut:	Online
Description:	Entrance-Terminal		
Lieu, porte:			4
Niveau de sécurité:		activer par a	pprobateur
Workflow:			

Niveau de sécurité

Pour le niveau de sécurité, il est possible de choisir parmi cinq niveaux différents, allant de « très faible » à « très élevé ». Ce lecteur peut uniquement être saisi dans une autorisation ou pour une personne si l'utilisateur dispose d'un niveau de sécurité égal ou supérieur au niveau de la station de dialogue. Les niveaux de sécurité vous permettent de faire en sorte que tous les utilisateurs AccessOne ne puissent pas autoriser l'accès à des zones sensibles.

La case à cocher « Permis par le concédant » implique une activation supplémentaire par un utilisateur avec l'autorisation correspondante.

Workflow

Vous pouvez ici créer des étapes de travail définies, qui doivent être autorisées par un supérieur, par ex. l'attri-



bution d'autorisations pour une zone précise.

Section « Paramètres »

Dans la section « Paramètres », vous saisissez les propriétés techniques du lecteur de badges.

Paramètres					
Adresse du module:	1			Compteur d'usage:	
Numéro de série:	17498478			Mode tunnel:	
Adresse:	1	Gid / Did:		Crypter:	
Firmware:	MRS_0292.BIN		Protocole:	Datasec	
Lieu d'entrée:	Unbekannt	-	Lieu de sortie:	Unbekannt.	1
Date d'installation:	103.12.2020	5	Référence ext:		
Groupe anti-passback:			Options:	Q	
Clavier disponible:		*	Le lecteur sait écrire:	Oui	
Affichage disponible:		~			
Avec retrait:		-	Contôle du retrait:	Paramètres	
État de la batterie:	Inconnu		Date d'état batterie:	Select a date	
Changement de la batt:	Select a state	5-1		Changer les données bat	tterie

Adresse du module

Le premier champ est un simple champ d'affichage et indique l'index de lecteur interne attribué par le système. Celui-ci est utilisé pour la compilation des autorisations et ne peut pas être modifié.

Numéro de série du lecteur de badges

Le numéro de série du lecteur est nécessaire afin d'effectuer l'adressage interne du bus du lecteur. Sur ces lecteurs, l'adresse du bus ne peut pas être réglée par commutateur DIP, mais est commandée via un logiciel de configuration. L'AccessOne assigne automatiquement l'adresse lorsque le numéro de série du lecteur a été saisi. Par ex., si un lecteur configuré sur l'adresse 3 ne se signale pas, la commande de porte essaie d'identifier ce lecteur à l'aide du numéro de série. En cas d'identification réussie, l'adresse correspondante lui est attribuée, ici : 3.

Adresse (saisie manuelle)

Chaque lecteur doit avoir une adresse de bus comprise entre 1 et 8.

En fonction du protocole du lecteur, une valeur chiffrée fixe est ajoutée à l'adresse de bus, comme dans certains protocoles de lecteurs, les adresses de A à H sont attribuées. Cela s'effectue automatiquement, car les conventions des différents protocoles de lecteur sont enregistrées dans la commande de porte.

Firmware

Champ de sélection pour la version du firmware. La version actuelle correspondante est affichée. **GID/DID**

Si des lecteurs avec un ancien protocole V ou 9 sont raccordés à la commande de porte, outre l'adresse de bus logique, un ID de groupe (GID) et un ID d'appareil (DID) doivent être indiqués. Le GID est le chiffre des dizaines et le DID le chiffre des unités. Les deux valeurs doivent être comprises entre 1 et 8. Exemple : la valeur « 12 » décrit une adresse de lecteur avec GID 1 et DID 2.

Compteur d'utilisation

Le lecteur vérifie si le badge a atteint l'utilisation maximale pour cette journée.

Mode tunnel

Uniquement pertinent pour les lecteurs LEGIC avec bus DE. Les lecteurs de badges Deister peuvent, comme la plupart des autres lecteurs, uniquement évaluer un Stamp pour les badges LEGIC. Si le badge dispose de plus d'un segment et si tous les segments doivent être évalués, l'intelligence du lecteur doit alors être désactivée et le mode tunnel utilisé. Les commandes données à la puce LEGIC pour la recherche et la lecture d'un

segment sont transmises du lecteur au MasterController. Le firmware de l'AMC peut alors lire à la suite les segments

qui sont activés dans les formats de lecteur de l'AccessOne.

Pour le bus DE et le bus Datasec, la communication vers le lecteur de badges peut également disposer d'un cryptage AES.

Crypter

La connexion entre le MAC et le contrôleur est cryptée de manière supplémentaire.

Date d'installation

Est automatiquement réglée avec le jour actuel lors de la création du lecteur, mais peut être modifiée au choix. La date d'installation sert à la documentation de l'installation.

Numéro de référence externe

Pour la désignation interne au client.

Options

Pour la désignation interne au client.

Groupe anti-passback (relatif au temps)

Empêche qu'un média d'accès soit cédé à une autre personne après l'accès et que cette personne entre également avec le même média d'accès. Pour traiter de la même manière des portes se situant l'une à côté de l'autre, celles-ci peuvent être réunies dans un groupe. Les lecteurs avec le même groupe anti-passback sont traités comme s'ils étaient montés l'un à côté de l'autre et commandent le même accès. Un média d'accès qui a été utilisé sur un lecteur de ce groupe est bloqué au niveau de tous les autres lecteurs du même groupe pour une durée définie (la période est réglable dans les paramètres de porte). La valeur saisie est un nombre entre 1 et 99. Jusqu'à 99 groupes de portes peuvent être formés.

Position du lecteur

Dans l'AccessOne, une porte peut être équipée de max. quatre lecteurs : deux pour l'entrée et deux pour la sortie. Exemple : pour les entrées de véhicules, il peut être pertinent de monter au-dessus du lecteur pour voitures également un lecteur positionné plus haut pour les camions.

Le lecteur sait écrire

Le lecteur peut écrire des badges. Exemple : mise à jour de droits d'accès sur les appareils d'accès offline. Sur certains lecteurs, le logiciel peut le reconnaître automatiquement, sur d'autres il faut l'indiquer de manière explicite. Si aucune valeur n'est saisie, la fonction d'écriture éventuellement disponible du lecteur n'est pas utilisée.

Clavier disponible

Pour certains accès, la saisie d'un code PIN pour activer le système de détection d'intrusion (EMA) ou comme caractéristique biométrique supplémentaire est nécessaire. Comme sur certains lecteurs, le clavier doit être activé via un ordre de la commande de porte, il est ici possible de l'indiquer de manière explicite. Dans la plupart des cas, la commande de porte reconnaît automatiquement la présence d'un clavier.

Affichage disponible

Un affichage du lecteur est uniquement commandé lorsque la saisie correspondante est effectuée ici.

Avec retrait

Il est possible de saisir ici si le lecteur doit être équipé d'un retrait motorisé.

Avec retrait:	. v.	Contôle du retrait:	Paramètres	
État de la batterie:	Non Oui (avec LEDs)	Date d'état batterie:	Select a date 15	
Changement de la batt:	Oui (sans LED)		Changer les données batterie	
tilisateur: admin	Automatique	disponible Station de travail: IN	V-11537 Tous Lac et Mac online	

Si la fente de retrait motorisé est équipée de LED, celles-ci doivent être commandées à la place des LED du lecteur. Dans ce cas, sélectionnez « Oui (avec LEDs) ». Lors de la sélection « Oui (avec LEDs) », les diodes lumineuses du lecteur sont commandées.

CEStronics



Contrôle du retrait

En cas de retrait motorisé, il est déterminé ici si le badge doit être à nouveau rendu après la lecture ou dans quelles conditions il doit être retiré.

	1			🐔 Retrait du badge 🛛 🗡
Adresse du module:				
Numéro de série:	17498478			Retirer le badge si
Adresse:	1	Gid / Did:		🗌 toujours
irmware:	MRS_0292.BIN	v	Protocole:	Badge inconnu
iau d'antréa	Unbekannt	~	Lieu de cortie:	Badge expiré
en d'ennee.	SUPERBUILT		Lieu de sorde;	bloqué manuellement
ate d'installation:	03.12.2020 15]	Référence ext:	bloqué en raison d'un code PIN invalide
roupe anti-passback:			Options:	Badge visiteur
		1		 aucune autorisation d'accès
lavier disponible:		<u> </u>	Le lecteur sait éc	Accès refusé en dehors du modèle temps d'utilisation
fichage disponible:		1		Mauvaise version de badge
wec retrait:	Oui (avec LEDs)		Contôle du retra	
tat de la batterie:	Inconnu		Date d'état batte	Sauvegarder Annuler
hangement de la batt:	Select a date	1		Changer les données batterie



7.1.4.3 Paramètres P

nnées de base de la porte Le	cteur +	'arametres P	Paramètres I	Paramètres O	
Désignation de la porte: C	ES Termin	al			
aramētres généraux					
Paramètres	Direction	Valeur			
Options	Entrée	0			
Séparation	Entrée	Non			1
Taux de randomisation	Entrée	0			
Temps de l'anti passback	Entrée	0			
Vérification de la zone	Entrée	0			
Accompagnateur requis	Entrée	Non			
Visite de groupe	Entrée				
Compteur d'utilisation	Entrée	Non			
Ignorer les erreurs de codage offline	Entrée	Non			
Toujours mettre à jour les données o	Entrée	Oui			
Code PIN requis	Entrée	Non			
Temps d'impulsion Armement	Entrée	0			
Armement automatique	Entrée	0			
Créer un message d'enregistrement	Entrée	0			
Temps pout l'alarme de menace	Entrée	0			
Batthew water Dalawais also wasanas	Entrée	0			

Cet onglet contient les paramètres qui concernent la commande d'expiration de la porte. En fonction de la complexité du type de porte sélectionné, plus ou moins de paramètres sont affichés sur cette page. Par la suite, nous prenons comme exemple la porte standard avec un sens de passage. Pour les portes, qui doivent être franchies dans les deux sens, les paramètres sont disponibles pour le sens d'entrée et de sortie.

Options	Des options sont utilisées pour permettre des traitements spécifiques au client.
	Pour chaque type de porte, la valeur 1 implique que le modèle de temps pour
	l'autorisation peut être ignoré sur cette porte. Une application pertinente pour
	cela est par ex. le lecteur de sortie.
	Exemple : une personne ne doit plus pouvoir entrer dans le bâtiment après 17 h
	mais encore pouvoir le quitter. Après 17 h, le lecteur d'entrée refuse la personne
	avec le message « Non autorisé, en dehors du modèle de temps ».
	Le lecteur de sortie vérifie avec l'option 1 activée uniquement s'il existe une
	autorisation pour ce lecteur et ignore le modèle de temps.
	Il est déterminé ici, si la commande exige de refermer les portes après chaque
Séparation	accès autorisé avant d'accepter le prochain badge.
	Lorsqu'un contrôle de sac doit être effectué de manière aléatoire, une valeur
Taux de randomisation	comprise entre 0 et 100 % peut être réglée ici. Le logiciel utilise un générateur
en %	aléatoire.
	Exemple : une valeur de 50 signifie qu'en cas de 100 passages, exactement
	50 personnes sont refusées avec le message « Contrôle autorisé ». Un blocage
	est alors effectué pour cette personne, et est à nouveau supprimé après le
	contrôle par le personnel de sécurité. Le blocage implique qu'un accès est égale-
	ment refusé à d'autres endroits.



Temps de l'anti-passback	Indication du temps pendant lequel un badge est bloqué après une utilisation
· · · · · · · · · · · · · · · · · · ·	réussie sur des lecteurs du même groupe d'anti-passback (temps en secondes).
Contrôle des zones	Le lieu (=zone) d'une personne est enregistré par l'AccessOne lors de chaque uti-
	lisation du badge sur un lecteur. Ainsi, la commande de porte peut également
	vérifier si la personne qui présente actuellement son badge contre le lecteur
	est inscrite dans la même zone que celle où est positionné le lecteur. Si ce n'est
	nas le cas la personne est passée par une porte ouverte sans utiliser le badge
	sur un lecteur ou le badge a été volé. Si le contrôle des zones est activé, il est
	uniquement possible de franchir une porte lorsque le lieu correspond au lieu
	du lactour de badges. La condition nour cela est une sénaration slaire des zones
	d'a se en la condition pour cela est une separation cialle des zones
	d'acces et un controle d'entrée et de sortie permanent du système de controle
	d'acces.
A	Les visiteurs ne peuvent pas rentrer dans certaines zones sans être accompag-
Accompagnateur requis	nés. La commande de porte fonctionne ainsi : après la détection d'un badge
	visiteur, elle attend pendant 10 secondes maximum un deuxième badge qui
	doit être un badge de personnel interne. Lorsque cela a lieu et que la personne
	accompagnatrice dispose de l'autorisation nécessaire à cette porte, la porte est
	débloquée. Pendant temps d'attente, la LED verte du lecteur clignote pour sig-
	naliser qu'une autorisation est présente, mais qu'un autre badge est attendu.
	Lorsque plusieurs personnes sont nécessaires pour pouvoir entrer dans une
Visite de groupe	zone, cela peut être réglé via ce paramètre. Si par ex. la valeur 3 est saisie, il faut
	présenter au moins trois badges de personnes autorisées différentes à la suite
	sur le lecteur avant que la porte ne soit débloquée.
	Dans l'AccessOne, il est possible de créer un badge avec une utilisation maxi-
Compteur d'utilisation	male. Si la valeur du badge est réglée sur 1, celui-ci est comparable à un badge
	d'entrée à usage unique. Chaque lecteur qui a réglé ce paramètre vérifie si l'uti-
	lisation maximale du badge est supérieure à 0. Si oui, et si la personne dispose
	de l'autorisation nécessaire, la porte est débloquée et décompte l'utilisation.
	Lorsque le compteur est arrivé à 0, plus aucune porte sur laquelle ce paramètre
	est également réglé ne s'ouvre. Si ce paramètre est réglé sur le lecteur de l'ent-
	rée du bâtiment, cela implique que le visiteur peut entrer une seule fois dans le
	bâtiment. À l'intérieur du bâtiment, le compteur n'est pas vérifié et le visiteur
	n'v est nas limité
	Ce paramètre est uniquement pertinent sur un système de fermeture offline et
Ignorer les erreurs de	définit si un accès doit également être autorisé lorsque le codage de l'autor-
codage	isation d'assès pour les portes offline a pulêtre effectué sans erreur. En temps
offline	narmal la parte c'euvre alers uniquement lers que le prepriétaire du badge a
	normal, la porte s'ouvre alors uniquement lorsque le proprietaire du bauge a
	presente son badge devant le lecteur, de manière à ce qu'il puisse être code
— · · · · ·	avec succes.
loujours mettre à jour les	Pour eviter trop de procedures d'écriture, la commande de porte met uni-
aonnees offline	quement à jour le badge lorsqu'au moins la moitie de la durée de validité est
	écoulée. Cette mise à jour a cependant uniquement lieu sur les systèmes de
	fermeture offline.
	Cette valeur détermine si un code PIN doit être saisi pour l'accès. Cela implique
Code PIN requis	que le lecteur dispose d'un clavier.



7.1.4.4 Paramètres I

Sur cette page, les signaux d'entrée (Inputs) sont définis, c.-à-d. avec quelle entrée du circuit IO correspondant les contacts de retour du périphérique raccordé sont connectés.

nnees de base de la porte Le	cteur	Parametres P	Farametres i	Parametres O	
Désignation de la porte: C	ES Termi	nal			
Paramètres d'input					
Paramètres	Direction	Valeur		Lac	_
Module IO de contact de porte	Entrée			I	
N° du contact du contact de la porte	Entrée				
Module IO, interrupteur de porte	Entrée	IO Modul: 1	-		
N° de contact du bouton de porte	Entrée	2			1
Contact de verrouillage loModul	Entrée				
Nº de contact, contact de verrou	Entrée	22 1			
Entrée d'inhibition loModul	Entrée	- 7			
N° de contact, blocage de l'entrée	Entrée				
Module IO de contact de sabotage	Entrée	-20.			
N° de contact, contact de sabotage	Entrée	- P () *			
Module IO, activation du lecteur	Entrée				
N° de contact pour l'activation du les	Entrée				
Module IO, EMA est prête pour l'arm	Entrée			1 I.	
N° de contact, L'EMA est prête à s'ar	Entrée	and the second			
Module IO I'EMA sharp	Entrée	IO Modul: 1			
N° de contact, EMA armé	Entrée	3			
Interrupteur à clé Alarm IoModul	Entrée				
N° de contact d'interrupteur à clé ala	Entrée				
Cardinal de Carles a dade	cui-			1	1

Voici la signification des différents signaux d'entrée, en fonction du type de porte :

Module IO de contact de	Module IO auquel le contact de porte est connecté (Input).
porte	
N° du contact du contact de	Numéro du contact sur ce module.
la porte	
Module IO d'interrupteur de	Module IO auquel le contact de demande de sortie (libération manuelle) est
porte	connecté (Input).
Module IO de contact de	Un signal supplémentaire qui indique si la porte est fermée, mais aussi si le
verrouillage	verrou de fermeture est sorti.
Module IO d'entrée d'inhi-	Module IO auquel le contact de blocage du passage est connecté.
bition	
Module IO de contact de	Si ce signal est détecté, un message de sabotage est généré et le relais de
sabotage	sabotage activé.
Visite de groupe	Lorsque plusieurs personnes sont nécessaires pour pouvoir entrer dans une
	zone, cela peut être réglé via ce paramètre. Si par ex. la valeur 3 est saisie, il
	faut présenter au moins trois badges de personnes autorisées différentes à
	la suite sur le lecteur avant que la porte ne soit débloquée.
Module IO d'activation du	Module IO auquel le contact de boucle/la barrière lumineuse est connec-
lecteur	té(e).



Module IO EMA est prête	Module IO auquel le contact « Système d'alarme prêt » est connecté.
pour l'armement	
Module IO armer l'EMA	Module IO auquel le contact « Système d'alarme armé » est connecté.
Module IO interrupteur à clé	Module IO auquel le contact (de clé) « Veuillez armer le système d'alarme »
alarme	est connecté.
Module IO de contact de	Se déclenche lorsque la poignée de porte d'une porte qui ne dispose pas de
poignée de porte	lecteur de badges est activée de l'intérieur. Cela évite un message d'intru-
	sion lors de l'ouverture à l'aide de la poignée.
Module IO de contact de clé	Comme pour le contact de poignée de porte, un signal activé signifie que la
	porte a été ouverte à l'aide d'une clé



7.1.4.5 Paramètres O

Sur cette page, les signaux de sortie (Outputs) sont définis, c.-à-d. avec quelle sortie de relais du circuit IO correspondant les actionneurs du périphérique raccordé sont connectés.

or master data	Reader	Parameter P	Parameter I	Parameter O
Door name:		CES Termina	1	
Output parameter				
Parameter		Direction	Value	Lac
Door opener loMa	dule	Entrance	IO Modul: 1	1
Door opener relay	no	Entrance	1	
Alarm suppression	oModule	Entrance	10	
Alarm suppression	relay no	Entrance		
Motor lock loMod	ule	Entrance	12	
Motor lock relay n	ø	Entrance		
Door alarm loMoo	lule	Entrance	IO Modul: 1	
Door alarm relay r	10	Entrance	7	
Pre alarm loModu	le	Entrance	-	
Pre alarm relay no	KC	Entrance	i in an ann	
EMA arming loMo	dule	Entrance	IO Modul: 1	
EMA arm relay no	1.000	Entrance	3	
Additional relay 1	loModule	Entrance		
Additional relay 1	relay no	Entrance		
Additional relay 2	IoModule	Entrance		
Additional relay 2	relay no	Entrance	1	
Light IoModule		Entrance	5	
Light relay no		Entrance	1	
	Interior da	F-1-		

Voici la signification des différents signaux de sortie :

Module IO d'ouverture de porte	Module IO auquel le relais d'ouverture de porte est connecté (Output).
Module IO de suppression	Module IO auquel le relais de suppression d'alarme est connecté (Out-
d'alarme	put).
Module IO de verrouillage du	Sur les portes auto-verrouillantes, outre l'ouvre-porte, le verrouillage du
moteur	moteur doit également être commandé pour faire rentrer le pêne. Ce
	signal de sortie peut être combiné à un modèle de temps. Si la porte est
	à l'état « Ouvert en permanence », ce signal est activé en permanence.
Module IO d'alarme de porte	Signal de sortie pour l'EMA. Il est toujours activé lorsqu'une porte a été
	ouverte sans autorisation ou qu'elle est ouverte trop longtemps. L'activa-
	tion de ce signal peut être supprimée dans les paramètres.
Module IO de pré-alarme	Si un temps de pré-alarme est saisi pour une porte, ce signal est activé
	après l'ouverture de porte et une fois le temps écoulé.
Module IO d'armement de l'EMA	Module IO auquel le relais d'activation du système d'alarme est connec-
	té (Output).
Module IO du relais supplémen-	Module IO auquel le relais de fonction spéciale 1 est connecté (Output).
taire 1	
Module IO du relais supplémen-	Module IO auquel le relais de fonction spéciale 2 est connecté (Output).
taire 2	



7.1.5 Afficher le statut de l'appareil

AccessOne - Donnees de l'appareil										- U	
Accueil	and the second										
PDBD	XC										
hanner flourer Coner	innormet definitiver										
nenger Houses capies as	Winner Hetmanach										
	-		_	_	_	_		_		_	
45	Statut de l'appareil										
Inca Marc											
Autzug 1	Statut de l'apparell										
Entrée principale			-								
E CES Terminal			lous -								
PHG Terminal	Apparei	Type	Statut	Programine	Power	Sabotage	Mode	Statut	Système d'alz		
EJ PM	Mec	MAC	Online	Inconnu							
Em SDC	- Aufzug 1	LAC	Incons	Inconnu	Inconnu	Inconnu					
Side entrance	- 10: Modul: 6	Module O	Incomu		Inconnu		1 M	-			
	 Entrée principale 	LAC	Online	Initialiser	Alarme de bal	Sabotage	1				
	- CES Terminal	Porte	Online				Fonctionneme	Inconnu	Inconnu		
	- CES Leser 1	Lecteur	Online		Inconnu	Inconnu					
	- PHG Terminal	Porte	ысоны				Inconnu	Inconnu	Inconnu		
	- Infoterminal	Lecteur	21	-	Inconnu	Inconnu	1		_		1
	PM.	Porte	Online	1		1	Fonctionneme	Inconnu	Inconnu		
	- Entrance-Terminal	Lecteur	Online		inconnu	inconnu					
	+ CES Laser Modul	Module 10	Online	1.000	Inconnu		1.				
	- 10 Modult 1	Module IO	Online		Inconnu		1				
Loghook	- CES URC	Access-Point	Online	1	Inconnu		1				
			A DESCRIPTION OF TAXABLE PARTY.								_

Faites un clic gauche sur l'entrée « DMS » de l'arborescence lorsque vous souhaitez voir l'aperçu du statut de tous les appareils. Le statut d'un appareil individuel (online ou offline) est visible dans la vue détaillée de l'appareil. Vous ne pouvez pas supprimer cette entrée, ni en créer une deuxième.

Un clic droit sur « DMS » génère une autre possibilité de sélection. Ici, un nouveau MAC, un nouvel EMC ou une nouvelle PS-Online (armoire à clé) peut être créé(e).



7.2 Données des appareils offline (OSS-SO)

Pour chaque installation d'OSS Standard Offline, des données d'équipements doivent être créées. Ici, les données de base pour les appareils offline tels que les cylindres électroniques et garnitures sont saisies. Ces données permettent entre autres de déterminer quelle est la taille de la mémoire pour les données offline sur le média d'accès et combien de place doit être réservée pour les événements et les saisies dans la liste de blocage. Pour Mifare, les données d'équipements obtiennent la clé d'accès sur les segments offline du badge et sur l'ID d'application, pour LEGIC, le Stamp est enregistré ici.

7.2.1 Données d'équipements

En règle générale, les données d'équipements sont pré-installées par CES, elles peuvent cependant également être saisies ou modifiées par l'utilisateur. Il existe un jeu de données par système. Pour créer une nouvelle saisie, cliquez sur Nouveau dans la barre d'outils.

AccessOne - OSS					- ¤ ×
Changer Nouveau Copies Supp	Srimer Actualiser				
in i	Cylindre Autorisations	Modèles de temp	Données sur la facilité mport	de données	
Nom					and the second
Facility_Legic	Nomi	Facility-Desfine			of active
Facility-Destire	Type de données:	Mifare Desfire			
	Version principale.	1	Version mineure:	1	
	Max événements par bade	3	Max entrées à liste noire par hadge	3	
	Configuration événementa:	 Faible charge batterie Erreur d'ouverfure Accès refuse 	Batterie remplacée Cylindre Teritative manipulation Badge d	bloqué Evénement de e la liste noire Liste noire est	u système 🔲 Erreur interne t pleine 📝 Accès permis
	Legic Advant Stamp: Longueur en lecture seule		Longueur du Stamp:	Long, du seg	ment
Logbook	Mitare Class/Dest. clé	-	ID application Destine Or	P75000 Début bloc d	Sinto n'a 🗇
Rapports	Long, höhler données	512			
🌽 Données de l'appareil					
St OSS					
Liste noire de l'OSS					
La Données utilisateur	Utilisateur: admin A	urun lecteur de disloque dis	Station de travail: INV-11537 Tous Lac	et Mac online Événemer	nts: 0 Timeout

Attribuez un nom et choisissez le type de données. Saisissez la version principale et secondaire (par ex. les chiffres 1 et 0 pour la version 1.0). Le numéro de version est une caractéristique de différenciation obligatoire. La section « Configuration événements » permet de régler quels événements doivent être réécrits du cylindre électronique au badge. Ces réglages valent pour tout le système, ils sont donc écrits de la même façon pour tous les médias d'accès sur l'appareil de mise à jour.

Pour un système LEGIC advant, saisissez le Stamp et la longueur du Stamp. Pour la saisie du Stamp, cliquez sur la touche derrière le champ de saisie. Le Stamp ainsi que la clé sont habituellement indiqués au format hexadécimal, c.-à-d. que les chiffres de 0 à 9 et les lettres de A à F sont autorisés. Au total, la valeur de clé pour Mifare DESFire doit être de 32 caractères (Mifare Classic 12 caractères).



Les clés d'accès sont enregistrées de manière cryptée dans la base de données. Une fois saisie, cette valeur n'est plus jamais (!) affichée en texte clair pour des raisons de sécurité, seule une nouvelle valeur peut être indiquée.



Si vous modifiez la clé, cette modification est directement active. Cela peut signifier que plus aucun média d'accès ne pourra être mis à jour à partir de ce moment.

Cliquez sur SAUVEGARDER dans la barre d'outils lorsque les saisies sont complètes.

7.2.2 Cylindres électroniques (et garnitures)

Les composants offline sont créés dans cet onglet. Dans la barre d'outils, cliquez sur NOUVEAU et saisissez les données pour le cylindre électronique.

Dans le champ « Description », indiquez l'emplacement d'installation exact. Les systèmes offline sont alimentés par batterie et capables, en tant que composants Standard Offline, de réécrire l'état de la batterie sur le média d'accès, lorsque la batterie passe sous une valeur de tension définie. Pour le remplacement d'une batterie faible, l'emplacement d'installation doit être connu.

			yindre Autors	ations Modèles de temps	Données sur la facilité	import de donnes	25	
lom E	Description St.	atut						
as type PM	6.A.	odili M	Nome	Cas type PM	Inde	tr.	1	Membre en autorisations: 1
est de l'outil	Market Market	odifie	Descaphore					
M124 P M125 S	nind PM	aarte	Line i menter					
M126	M	odifie	men ponte:					
rmoire 1	M	odiifie	Niveau de sécurité:		activer par l'approbates	ar 🗍		
est	Ex	porté	Workflow:					
VT-II Test V	WT-II Test	austin -	Propriétés					
			Type de cylindre:	Cylindre CES	Temps d'ouve	ture (s)		Temps di ouverture prolonge [s]: 70
			Zone offline	1 - DSS Test	Modèle temp			Intervalles 1 (1.) Intervalles 2 (1.)
			Paramétres	Logging (Traceback) Beeps Mode Mailbox	Basculer le Béeps Aco	mode és refusé		Feedback sur Tevénement
		2	Relais de lecleun		Autovisiation d	Youverture - Badge : Cylini	dre	
Donné	es de l'appare	eil	Longueur ext. Imm		Longueur (nt.	(mm):		Ovinore de panique

Les cylindres électroniques et garnitures sont clairement différenciés via leur numéro. L'AccessOne attribue automatiquement le numéro lors de la création et de la sauvegarde d'un nouveau cylindre électronique (affichage dans le champ « Index »).

Section « Propriétés »

Indiquez des informations supplémentaires sur l'appareil monté.

Type de cylindre

Sélection entre cylindre électronique, garniture et terminal mural. Les appareils peuvent nécessiter différentes batteries.

Temps d'ouverture

Indique combien de temps un cylindre électronique reste enclenché en cas d'accès autorisé. Une valeur de 5-10 secondes est généralement suffisante (réglage standard : 5).

Temps d'ouverture prolongé

Pour des groupes de personnes spécifiques, le temps d'ouverture standard peut être prolongé.

Zone offline

Le numéro de zone offline (ID d'emplacement) doit toujours être indiqué avec Standard Offline. Un 0 n'est pas autorisé ici. Via le numéro de zone, une installation peut être divisée en plusieurs zones. Dans ce cas, le cylindre électronique avec le numéro 1 existe plusieurs fois, soit une fois pour chaque zone. Cela signifie que le numéro de cylindre électronique est uniquement univoque en association avec le numéro de zone. Lors du passage d'une zone à une autre, l'appareil de mise à jour supprime les données de la zone précédente et les remplace par celles de la zone actuelle. Grâce à la répartition en plusieurs zones, le nombre d'appareils d'accès offline d'une installation peut, en théorie, être aussi grand que possible.



Modèle de temps

Possibilités de sélection pour le modèle de temps. La fonction dépend du type d'appareil et du fabricant.

Intervalles 1 et 2

La fonction dépend du type d'appareil et du fabricant.

Paramètres

Les possibilités de réglage dépendent du type d'appareil et du fabricant.

Relais de lecteur

La fonction dépend du type d'appareil et du fabricant.

Cylindre de panique

Indication sur le type d'appareil.

Longueur

Indication sur la longueur intérieure et extérieure.

Numéro de série

Indication du numéro de série.

État de la batterie

Le champ « État de la batterie » affiche si un appareil offline a indiqué une batterie faible. Le champ Date de l'état batterie indique quand ce message a été généré. Lorsque la batterie est remplacée, l'appareil offline indique un message « Changement de batterie » lors du prochain enregistrement, qui revient dans le système via le badge, et les données sont mises à jour en conséquence. Le rapport « État de la batterie du lecteur » permet de générer à tout moment une liste des appareils dont la batterie est faible.

Ensuite, transférez les données via la touche Transmettre.

7.2.3 Programmer les appareils offline

La programmation des données sur les appareils offline s'effectue directement depuis l'onglet. Pour cela, vous avez besoin des

éléments suivants :

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

Procédure :

- 1. Insérez le RF-Stick dans l'ordinateur.
- 2. Cliquez sur TRANSMETTRE.
- 3. Lancez la licence A dans l'AccessOne (procédure unique sur le premier appareil programmé).
- 4. Maintenez le RF-Stick-Master devant l'appareil.



7.2.4 Autorisations

Rassemblez plusieurs portes dans un groupe de portes.



Lorsque vous attribuez une nouvelle autorisation à un cylindre électronique, vous devez également transférer ces données à l'appareil offline.



Les autorisations doivent être effectuées de manière à ce qu'elles rassemblent uniquement des pièces de même niveau de sécurité. Lorsqu'une pièce ou un couloir dispose de plusieurs accès, les cylindres électroniques correspondants doivent être rassemblés dans une autorisation. Via les profils d'autorisation, vous rassemblez alors les groupes de portes selon le profil d'utilisateur.

henger Nouveeu Copier Supp	rimer Actualiser As	signation					
	Cyune Auton	sations oddles de	temps Danotes tur la t	with Import de c	ionnéns		
m Description							
upe de service	Plane:	annica de service			Ingen		
	Descriptore.	1.000.000	In a horas			eco-et bei wooktoostere.	
	Zone-offinite.	1 1722 1942	Niveau de seconte		Workstone		
	Cylindres assignis	e					
	Nom	Description	Niv, de sécuri		-		
	Castype PM		Sans		Nom	Description	Niv. de sécuri
	WT-II Test	WT-II Test	Sans		PM124	Porte d'entrée PM	Sans
					PM 125	Spind PM	Sans
					Test		Sans
					Test de l'outil OSS		Sans-
				~~			
Données de l'appareil							
OSS				>>			
Liste noire de l'OSS							
Données utilisateur							
Concepteur des badges							



7.2.5 Import de données

Accessione - CSS Accuel Accuel	K O	- ¤ ×
0 op z	Eylindre Autonsations Modèles de temps Dannées sur la facilité Import de données Zone effine 1 - 055 Teat - - - -	-
	Cylindre	
	Nom Description Type de cylindre. Niu de sécuri Temps d'ouverti. Longueur esté Longueur in: Prolong du temps d'Sta	Lire dans
	1	Importer
Données de l'appareil		
S* OSS		
😻 Liste noire de l'OSS		
🎎 Données utilisateur		
Concepteur des badges		-
Pa	Ublisateur, admin Autor Leibor phinosoppe allens, Station de travaik INV-11537 Tous luc et Mac online Événements: 0	Timeout non ec

Permet l'import d'une liste de portes *.csv. Sélectionnez la zone offline et cliquez sur **Lire dans**. Sélectionnez la liste de portes correspondante du répertoire.

En règle générale, la liste de portes est créée par CES lors de la mise en place de l'installation. La liste peut également être éditée par le client.

Nom	Description	Type de cylindre	Niv. de sécuri	Temps d'ouverti	Longueur exté	Longueur in:	Prolong, du temps d'	Statut
PM125	Porte d entree PM	Cylindre CES	Sans	5	42	42	10	
PM126	Coffre-fort PM	Ecusson CES	Sans	5	42	42	10	
PM127	Entree laterale PM	Serrure de méuble CES	Sans	5	42	42	10	

AccessOne - OSS										- D
Accuel								-		
B D D D D >	K O Actualiser									
	Cylindre Aut	atriations Modèlles	de temps - Donness	sur la testiti	Import de c	ionnées				
om	Zone offline:	1-OSS Test								_
	Nom PM125	Description Porte dientree PM	Type de cylindre Cylindre CES	Niv. de sécuri Sans	Temps d'ouvertu	Longueur exté	Longueur in 42	Prolong, du temps d	Statut	1 Editors
	PM126 PM127	Coffre-fort PM Entres laterale PM	Ecuision CES Semure de meuble CES	Sans Sans	5	42	42	10		oorter.
Données personnelles		1	14.0.04.040100	Trans	1.		-	12		9
 Autorisations 										
Profils d'autorisation	A									
A Données d'entreprise	3 des 3 en/ogist	trémients de données lues p	our Timportation							
Logbook										
Rapports										
* Depender de l'appareil	Utilisateur: admin	land in the	a ful president lactore Sto	tion de travait	NV-11537	Line D Manufacture	-	Evenements: 0		Timeout: non activit

Le fichier lu peut désormais être vérifié à nouveau dans l'affichage de liste dans le champ « Cylindre ». Appuyez sur la touche Importer pour importer la liste dans la base de données. La configuration s'effectue dans le champ de texte sous le champ.

7.2.6 Modèles de temps

OSS Standard Offline utilise un autre format pour les modèles de temps et n'est pas aussi flexible que l'AccessOne pour les composants online. Pour cette raison, les modèles de temps online ne peuvent pas être utilisés en continu et il existe un onglet propre pour les modèles de temps OSS Standard Offline.

Un modèle de temps dans OSS Standard Offline se compose de max. quatre intervalles. Pour chaque groupe d'intervalles, il est possible de sélectionner les jours auquel il est valide. Si aucun modèle de temps n'est saisi pour l'autorisation d'une personne, celle-ci est valide toute la journée.

and a second	1.4	Madalar	de temps)	L THE L			_			
Cyandre	Autonsatio	ons modeles	de temps	Jonneys sur u	r faculite 1r	libert de denn	100				
om mpt de traval	Te	mgs. die travisio			Indes						
Description	Te	mps de travail									
Intervalles	de temps										
Intervalle	t der	07.00		20.00	veige	V. Lundi	W March	Meruredi	No. Inidi	W Vendra	
	de		1			Sameth	Dimanche	Jour fene			
	de		1.6								
	der										
Intervalier	7 dér	07.00	18.	14:00	valide	Lords	Marci	Mercrildi	in Jesel	Vendres	
	déy		181			Sames	Dimanche	🗇 Jour tene			
	de		1								
	ditr		14								
intervalle	i dé		÷			Lund	Marci	Mercredi	1. Jead	L_ Vendres	
Rapports	de		14			Samete	_ Dimanche	🖾 sour leve			
Brandan de Brannen B	dey										
Donnees de l'appareil	de		4					_			
OSS	il de		4		valide	Lunifi	March	() Alisondi	Agosdi	1 Wend/mil	
Liste noire de l'OSS	der		18.			Samedi	Dimenche	inst web			
	de		141								
Liste noire de l'OSS	de:		181								

Dans l'exemple, l'accès est autorisé du lundi au vendredi de 7h00 à 20h00 et le samedi de 7h00 à 14h00. Le dimanche et les jours fériés, l'accès est impossible.

8 Configuration des autorisations

Groupe cible de ce chapitre :

• Personnel formé aux produits

8.1 Autorisations

Mettez d'abord en place des groupes d'autorisation pour les appareils online et offline. Déterminez ensuite via Modèles de jour et de temps d'autres restrictions ou fonctions de portes (par ex. fonctions d'ouverture à des périodes précises de la journée) en prenant en compte les jours spéciaux et fériés.

8.1.1 Aperçu des autorisations

10	Cyune Autorisations	odèles de temps	Donotes tur la faci	té import de d	conéns .			
n Description	Name Groups	e de vervice			linger.			
	Descriptions.					ATTENT DIS ACONDOSTION		
	Zone offline. 1 175	5 Jast New	eau de sécurité		Warkfilm			
	Cylindres assignes							
	Nom Des Armoire 1	scription	Niv. de sécuri Sans		4.6.7	No. of Concession, Name	LANCE CLOSE	
	Cas type PM		Sans		PM124	Porte d'entrée PM	Sans:	
	W)-It test (W)-	-Il Test	bans		PM125	Spind PM	Sans	
					PM 120 Test		Sans-	
					Test de l'outil OSS		Sans	
	-							
Données de l'appareil				>>				
iste noire de l'OSS								
Données utilisateur								
Concepteur des badges								

La sélection de dialogue « Autorisations » ouvre plusieurs onglets dans la fenêtre de dialogue.

Dans l'onglet « Autorisations », plusieurs lecteurs peuvent être rassemblés dans un groupe. Les lecteurs sont sélectionnés dans la liste des lecteurs non assignés (liste de droite) et assignés au groupe actuel via la touche « << ».

Les groupes d'autorisation se composent d'autorisations rassemblées. Les autorisations créées dans le côté droit de la fenêtre (non assignées) peuvent être des autorisations uniques ou des autorisations de groupe.



8.1.2 Généralités sur les modèles de temps et de jour

Les modèles de temps sont utilisés à différents endroits de l'AccessOne.

- Pour restreindre l'accès : ici, un modèle de temps peut être enregistré de manière individuelle, comme modèle de temps pour un employé. Si aucun modèle de temps propre n'est indiqué pour une autorisation, le modèle de temps individuel s'applique toujours.
- Les modèles de temps sont utilisés sur les portes, par ex. pour déterminer une fonction d'ouverture permanente à des périodes précises de la journée.

Dans l'AccessOne, un modèle de temps peut correspondre à un plan hebdomadaire et se compose de modèles de jour individuels pour chaque jour de la semaine ou de modèles de jour supplémentaires pour les jours spéciaux ou fériés.



Chaque modèle de jour peut contenir trois intervalles et détermine les horaires d'accès pour un jour précis.

Lors de la définition des plans, nous recommandons la procédure suivante :

- 1. Créer des modèles de jour.
- 2. Rassembler les jours spéciaux et fériés dans des groupes.
- 3. Créer des modèles de temps pour les portes.

8.1.3 Modèles de jour

AccessOne - Autorisations					
Accueil					
Changer Nouveau Copier Suppri	mer Actualiser	Assignation			
i de l	Autorisations	Modèles de temp	Modèles de jour	ours spéciaux et fériés	Masques d'accès
Nom					
07-22	Nom:	07-22			
13-14	Dessinhing	07-22			
Ignorer les jours spéciaux	Description.	P			
	Intervalles de l	emps			
	de:	07:00	è.	22:00	
	de		te .		
	de:		4		

Dans la barre d'outils, cliquez sur NOUVEAU. Attribuez un nom à votre modèle de jour, en option vous pouvez y ajouter une description.

Pour les « intervalles de temps », indiquez au moins 1. Vous devez les définir avec un temps « de »/« à ». Ensuite, cliquez sur SAUVEGARDER.

CONSEIL Créez également le modèle de temps « Pas d'accès ». Le modèle de temps est par ex. adapté aux employés qui sont uniquement autorisés certains jours et pas d'autres. Cela permet également de prendre en compte facilement les jours fériés.



8.1.4 Jours spéciaux et fériés

Cliquez sur NOUVEAU et saisissez une « désignation » pour votre jour spécial. Les catégories servent à rassembler les jours spéciaux dans des groupes et ainsi à déterminer un modèle de jour pour un tel groupe. **CONSEIL** Rassemblez les jours fériés nationaux dans une catégorie. Pour ces jours, le modèle de jour « Pas d'accès » s'applique alors (alternative : pas d'entrée dans cette catégorie correspond à un modèle de jour avec un intervalle de 0h00 à 0h00). En répartissant les jours fériés dans les catégories correspondantes, il est possible de prendre en compte pour les modèles de temps les jours fériés de la région concernée et d'ignorer les autres.

AccessOne - Autorisations					
Accueil					
Annuler Sauve	garder Q	ADA			
	Autorisations	Modèles de temps	Modèles de joir	Jours spéciaux et fériés	N sques d'accès
Description					
Easter Sunday	Description:	Easter Sunday			
	Catégorie:	1 *			
	Valide pour off	line:			
	Méthode de calo	ul			
	Type:	dépendant de Pâque	5	19	
	Date	0			
	Priorité:	1 - écrase le jour de	travail	*	
	Valida de	1 - écrase le jour de	travail		
	Torone des	2 - écrase samedi 3 - écrase dimanche			

Vous pouvez sélectionner plus bas la procédure de calcul :

La plupart des jours de commémoration et fériés de l'année liturgique dépendent de la date du dimanche de Pâques :

- Mercredi des Cendres = 46 jours avant Pâques
- Dimanche des Rameaux = 7 jours avant Pâques
- Jeudi saint = 3 jours avant Pâques
- Vendredi saint = 2 jours avant Pâques
- Lundi de Pâques = 1 jour après Pâques
- Ascension = 39 jours après Pâques (le 40^e jour)
- Pentecôte = 49 jours après Pâques (le 50^e jour)
- Dans l'Église catholique, les jours suivants s'appliquent également :
- Fête-Dieu = 60 jour après Pâques
- Fête du Sacré-Cœur = 68 jours après Pâques

La commande de porte calcule automatiquement la date du dimanche de Pâques et peut donc déterminer les jours fériés dépendant de Pâques lorsqu'ils sont créés dans le système. Pour les jours qui sont calculés en fonction de Pâques, le nombre de jours qui doivent être ajoutés à la date calculée est saisi dans le champ de date.



AccessOne - Autorisations					
Accueil					
	1 4 0	EX.			
	A Q				
Annuler Sauveg	arder Supporter Tellemen	Comparison of Contract of Cont			
Idate		ML			
44.1	Autorisations	Modèles de temps	Modèles de jour	Jours spéciaux et fériés	Masques d'accès
Description		_	-		
Dimanche de Páques	Description:	Dimanche de Pâque			
	Catégorie:				
	Valide pour of	fline: 🛄			
	Méthode de ca	lcul			
	Туре:	dépendant de Páqu	25		
	Date:	Date fixe	_		
	Driorités	répéter annuelleme	nt		
	Phonte:	dependant de Paqu	es		
	Valide de:	Seject a date [15]	di Select a dat	e [15]	

Dans l'exemple, le lundi de Pâques (= 1 jour après Pâques) est défini comme suit :

Si le jour férié se situe avant Pâques, une valeur négative peut aussi être indiquée. Exemple : pour le Vendredi saint (2 jours avant Pâques), la saisie est « -2 ».

• Date fixe

Les jours spéciaux, qui doivent être créés à nouveau chaque année, ou les événements ponctuels tels que les fêtes d'entreprises sont créés avec une date fixe. Ils sont alors valides une seule fois.

Répéter annuellement

Il existe des dates qui se répètent annuellement comme jour spécial ou férié : par ex. le 1^{er} mai ou le 24 décembre. Pour cela, choisissez une date du calendrier. L'année est ignorée lors de la vérification.

Priorité/Catégorie

La priorité d'un jour spécial détermine sa pertinence. Un jour férié normal a la priorité 1, c.-à-d. que s'il tombe sur un jour ouvré, ce n'est pas le modèle de jour de ce jour ouvré qui s'applique mais le modèle de jour du jour spécial.

Exemple 1 : le réveillon de Noël est assigné à la catégorie 8 et pour tous les jours spéciaux de la catégorie 8, un modèle de demi-jour de travail (7h00 - 12h00) est saisi dans votre modèle de temps. Lorsque le réveillon de Noël tombe sur un lundi, il est possible d'entrer dans les zones sécurisées de 7h00 à 12h00. Si le réveillon de Noël tombe sur un samedi ou un dimanche, aucun accès ne doit être autorisé. Dans ce cas, la priorité pour le réveillon de Noël doit être placée sur 1, car le samedi et le dimanche ont une priorité plus élevée.

Exemple 2 : pour l'inventaire du week-end, l'accès doit être autorisé à certains employés. Pour ce jour spécial, une priorité 2 ou 3 doit être définie, afin que le modèle de jour normal du samedi ou du dimanche soit écrasé.



Jour férié	Champ d'application
Nouvel An	National
Épiphanie	Bade-Wurtemberg, Bavière, Saxe-Anhalt
Vendredi saint	National
Dimanche de Pâques	National
Lundi de Pâques	National
Fête du travail/1 ^{er} mai	National
Ascension	National
Dimanche de Pentecôte	National
Lundi de Pentecôte	National
Fête-Dieu	Bade-Wurtemberg, Bavière, Hesse, Rhénanie du Nord-West-
	phalie, Rhénanie-Palatinat, Sarre
Assomption	Bavière (dans les zones catholiques), Sarre
Jour de l'Unité allemande	National
Fête de la Réformation	Brandebourg, Mecklembourg-Poméranie-Occidentale, Saxe,
	Saxe-Anhalt, Thuringe
Toussaint	Bade-Wurtemberg, Bavière, Rhénanie du Nord-Westphalie,
	Rhénanie-Palatinat, Sarre
Jour de pénitence et de prières	Saxe
1 ^{er} jour de Noël	National
2º jour de Noël	National

Le tableau suivant offre un aperçu des jours fériés en Allemagne :

Il est recommandé de sélectionner les catégories de jours spéciaux de manière à ce que les jours fériés qui sont valides

dans la même région soient aussi dans la même catégorie.

dans la meme region solent aussi dan	is la meme categorie.
Jours fériés nationaux	Catégorie 1
Épiphanie	Catégorie 2
Fête-Dieu	Catégorie 3
Assomption	Catégorie 4
Fête de la Réformation	Catégorie 5
Toussaint	Catégorie 6
Jour de pénitence et de prières	Catégorie 7
Autres jours spéciaux catégorie 8	Catégorie 8

CEStronics

8.1.5 Modèles de temps

	Autorisations	Modèles de temps	dèles d	te jour Jours	spéciaux et fériés	Masques d'accès
Nom MacEr 7-32	Nom:	Mo-Fr 7-22		Ind	ev:	1
and the repair	Description:					
	Modèle de jour, j	ours de la semaine				
	Lundi:	07-22	v.	Samedi:	07-22	-
	Mardi:	07-22	*	Dimanche:	07-22	~
	Mercredi:	07-22	ų			
	Jeudi	07-22	*			
	Vendredi:	07-22	*			
	Modèle de jour, j	ours spéciaux et jours fériés				
	Catégorie 1:	Ignorer les jours spéciaux	U.	Catégorie 5:		~
	Catégorie 2:	Ignorer les jours spéciaux		Catégorie 6:		-
Données personnelles	Catégorie 3:			Catégorie 7:		-
Autorisations	Catégorie 4:			Catégorie 8:		- 1

Si aucun jour spécial n'est enregistré dans le système, aucun accès n'est autorisé à cette date. Cliquez sur NOUVEAU et effectuez les saisies correspondantes. Sauvegardez le modèle de temps. Changez de page sans sauvegarder, dans ce cas, l'AccessOne le fait automatiquement.

Le champ de saisie « Description » sert à l'assignation interne à l'entreprise.

L'indication dans le champ « Index » décrit un numéro de contrôle continu, qui indique l'ordre de création des modèles de temps.



AccessOne - Autorisations										
Accueil										
Annuler	0									
141	Autorisations	Modèles de temps	Modèles d	de jour	Jours spéciaur e	t fériés	Masques d'accès			
Nom										
Mo-Fr. 7-22	Nom:	Mo-Fr. 7-22			Index		1			
	Description:									
	Modèle de jour, jours de la semaine									
	Lundi:	07-22		Samedi:	07-22		-			
	Mardi:	07-22		Dimanche	07-22					
	Mercredit	07-22								
	Jeudi:	07-22	14							
	Vendredi:	07-22	**							
	Modèle de jour	, jours spéciaux et jours fe	rlés							
	Catégorie 1:	Ignorer les jours spe	ciaux -	Catégorie	5:		-			
-	Catégorie 2:	07-22		Catégorie	6:		÷.			
2 Données personnelles	Lategone st	-		Catégorie	7:					
Autorisations	Catégorie 4:		<i>w</i> .	Catégorie	8:		<i>6</i>			
Profils d'autorisation										

Dans cet exemple, le même modèle de jour s'applique du lundi au vendredi. Les jours fériés de catégorie 1 sont ignorés dans ce modèle de temps, c.-à-d. que le modèle du jour de la semaine sur lequel tombe ce jour férié s'applique. Il existe un modèle de jour correspondant pour les jours spéciaux de catégorie 2. Pour tous les autres jours spéciaux de catégorie 3 à 8, aucun modèle de jour n'est saisi et l'accès est donc interdit.

AccessOne - Autorisations					
Accueil					
Changer Nouveau Copier Sup	primer Actualiser	Assignation		4	
i de i	Autorisations	Modèles de tem s	Modèles de jour	lours spéciaux et fériés	Masques d'accès
Nom 07-22 13-14 Ignorer les jours spéciaux	Nom: Description:	Ignorer les jours spi	éciaux		
	Intervalles de	temps			
	des	00:00	á:	24:00	
	de	00:00	à:	24:00	
	de:	00:00	ā:	24:00	

Pour pouvoir ignorer un jour spécial, c'est-à-dire appliquer le modèle de jour normal du jour ouvré correspondant, un modèle de jour spécial doit être créé, s'il n'est pas créé automatiquement lors de l'installation (par ex. « Ignorer les jours spéciaux »).



8.1.6 Masques d'accès

C AccessOne - Autorisations							- 0 ×
Accueil							
Changer Nouveeu Copier Sup	Actualizer Assignation						
kine.							
	Autorsations Modèles de temps	Medèles da	Hour Jours spec	oux at lands	Masques d'accès		
Nom Description	1						
Test elevator 1 Test elevator 1	Nom Test elevator 1				Index		
	Description Test elevater 1						
	Gemane d'actorname (C				manager (A)		
	Town for many and internation				Automa of		
	Alter an internal and a strength and				And and a second		
					Thinniu de beconte		
	Workflows				activer par l'approbabilier		
	Élogei aisignés						
	Nom de l'étage	Étage	Depart & Fav Arrive	a l'av Départ l	Tar Annuer & Far		
	2. Etage	Z		Man	Nan		
	1.Etage	1		Man	Tean		
	1 Listamarcheor	0	Nen Nen	Mas	Non		
	2. Untergeschoss	2	Non Non	Non	Nan		
		10					
2 Données personnelles	i la						
Autorisations							
🚰 Profils d'autorisation							
à Données d'entreprise							
💕 Logbook							
Rapports							
Données de l'appareil							
	Ublisheur stimen		Station	le travail INV-T	537 Tous Lac et Mac onine	Evenements: 0	Timeput non active

Le dialogue « Masques d'accès » permet de créer des autorisations d'accès sur un groupe d'ascenseurs créé au préalable. Pour cela, créez un masque d'accès vide à l'aide de NOUVEAU. Saisissez le nom et la description et choisissez un groupe d'ascenseurs pour afficher les étages de ce groupe. Ensuite, définissez le type de masque (« Utilisateur » ou « Urgence »). Pour autoriser les accès aux étages, passez ou glissez les portes « Début » et « Cible » de « Non » à « Oui ». Sauvegardez les saisies.

CEStronics

8.2 Profils d'autorisation

Dans le dialogue « Profils d'autorisation », l'utilisateur a la possibilité de créer un profil d'autorisation depuis plusieurs groupes d'autorisation. Il existe ici la possibilité de relier des autorisations pour les appareils online et offline et de les rassembler dans un profil.

C AccessOne - Profils d'autorisation							- 8 *
Accuel							
Changer Nosvenu Cepier Sup	primer Actualizer Assign	ation					
	Online Ciss. M	esques d'accès					
Nom Description							
Salles de conférence	None S	ense des employes			1000		
Service des employés PM	Descoptions					anter per aproxime.	
Profile 1	Towned day willighter 1	Sport Roesild	e secure i the place	white	Restored.		
Viniteurs	Autorisations assigner						
	L Norr	Description	Modèle temps	Niv. de sécur			
	Groupe de service	Dispositifs en Opre en sérvice	1	Sans.		Nam Description fillivite secul Contrôle d'accès et temps Contrôle d'accès et temps Bans	T
					<<		
Données personnelles							
Autorisations					>>		
A Profils d'autorisation							
Données d'entreprise							
Logbook							
E Rapports							
🧨 Données de l'appareil							
	Utilisateur admin		Station	de travali INV-11537	Tous lac et M.	Prenements 0 Timeout n	on active

8.2.1 Aperçu des autorisations online

Dans l'onglet « Online », des groupes d'autorisation peuvent être rassemblés dans un profil d'autorisation. Les groupes sont sélectionnés dans la liste des groupes non assignés (liste à droite) et assignés au profil actuel (liste à gauche) via la touche « << ».



	1 0									
ger Nouvawu Copier Supp	errer Actualiser Ass	utpration (
					_			_		
	Onlin OSS	asques d'accès								
Convertee		-								
de confissees	Man	Santon dar antelevent			-					
des envelvairs	Them.	Service and Entrongine			1000					
	Description						editer.			
1	Dunio de validité	1 Jam	Niese de Sourie	-	Worktow					
rs										
	Autorisations / cyl	Indens unsignety								
	E Alexan	Pasininfian	Links terror	Norda Main Midahana P						
	Smille Meterylite	Participation of the second se	Concert of the	Sans 11		-				
		-				Nom	Desception	Nin, de sécur	Nº de pore c	
					<<					
Données personnelles										
Données personnelles										
Données personnelles										
Données personnelles Autorisations					>>					
Données personnelles Autorisations					>>					
Données personnelles Autorisations Profils d'autorisation	-				>>		Deroter	Min davies	Manus	
Données personnelles Autorisations Profils d'autorisation					>>	Non	Description	Niv, de sécu	n Millezones	
Données personnelles Autorisations Profils d'autorisation Données d'entreprise					>>	Nom Armorie 1 Cata bole PM	Description	Nin, de sécu Sans Sans	r N' dezonez.	
Données personnelles Autorisations Profils d'autorisation Données d'entreprise					>>	Non Amoin 1 Casiya M Partiza	Description Porte dentree PM	Nin, de sécu Sans Sans Sans Sans	r N' lie zone z 1 1 3	
Données personnelles Autorisations Profils d'autorisation Données d'entreprise Logbook	-				>>	Non Amole 1 Castype PM FM125 PM125	Description Porte derstree PM Zeind PM	Nin, Besécu Sans Sans Sans Sans Sans	r N ² Site Zone z 1 1 1 2	
Données personnelles Autorisations Profils d'autorisation Données d'entreprise Logbook					>>	Non Amoirs 1 Cas type PM PM124 PM125 PM125	Description Rone deriver PM Spind RM	Nin, sle sécu Sans Sans Sans Sans Sans Sans	r. Nº dezones. 1. 1. 1. 1. 1. 1.	
Données personnelles Autorisations Profils d'autorisation Données d'entreprise Logbook Rapports					>>	Non Amoint 1 Catilyo PM PM124 PM125 PM125 Test Test	Description Ports denyce PM Solid RM	Nin, de sécul Sans Sans Sans Sans Sans Sans Sans	r. Nº dezonez. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	

8.2.2 Aperçu des autorisations offline

L'onglet « OSS » permet également de rassembler les appareils offline dans le profil sélectionné. Dans la liste du côté droit (groupes et appareils non assignés), vous avez la possibilité d'assigner aussi bien un groupe d'autorisation qu'un appareil offline individuel au profil actuel via la touche « << ».

La condition pour l'intégration des appareils offline est la mise en place des appareils offline (voir « 7.2 Données des appareils offline (OSS-SO) » page 55).

9 Création de données personnelles

Groupe cible de ce chapitre :

• Personnel formé aux produits

Le dialogue « Données personnelles » vous offre la possibilité d'attribuer des autorisations et d'enregistrer toutes les données nécessaires relatives à une personne. Assignez directement les autorisations des appareils online et offline configurées au préalable aux personnes.

9.1 Données personnelles

9.1.1 Aperçu des données personnelles

Dans le premier onglet, toutes les données essentielles relatives à la personne sont affichées et il existe la possibilité de supprimer un blocage ou, pour les personnes qui ont oublié leur badge, d'attribuer un nouveau badge (touche Changer de badge). Le badge actif jusqu'ici est alors désactivé.

Cet aperçu est adapté à l'enregistrement rapide de propriétés assignées à une personne (par ex. pour la protection de l'objet).

AccessOne - Données personnelles				- o x
Accueil	the second second			4
Rechercher Ohanger Nouveau Coper	Supplement Actualizer Assignation			
1981	Vue d'ensemble Données de base Autres donnée	es de base Bildges Autorijations	Prendre une photo Blocages Masques d'accès	oss
Nom de fan Prénom N° person Internetion	Nom: Intervention Medium	Prénom:		
	Entreprise:	Entreprise 2:		
	Départment	Né le:		
	Lieu Lieu actuel incomru	depuis: -	Changer de lieu	
	Dernière visite Aucune entrée			
	Zone de parking: Inconnu	depuis: -	Changer sone parking	
	Badges			
	Date d'identification pendant de 1 délivrance hadige:	Schüsselausgabetun	nube */	
	19 6 Valide de Vali	de jusqu'au Statut Badge de rempla		
			Imprimer le formulisire	
			Changer de badge	
Données personnelles	ages		_	
buinces personnenes	B cage d'accès Raison	De A		
Autorisations				
Profils d'autorisation			Хзорртите	
A Données d'entreprise	Logbook Jours 2 Actualises		Client	1
💕 Logbook	Date LAC / Sd7 Lecteur / Login Lieu	/ Programm N*. Message	Badge Chent	
E Rapports				
🧨 Données de l'appareil				
1 nss	URisateun admin	Station de travail INV-11537	for las et Mac onine Extremente 0	Timeout non active

Section « Lieu »

La section « Lieu » affiche « Lieu actuel », « Dernière visite » et « Zone de parking ».

Lieu actuel

Lorsqu'une personne avec badge autorisé franchit une porte sécurisée par AccessOne, le lieu est enregistré. Les zones limitrophes de chaque porte sont définies. La zone pénétrée au moment de l'enregistrement s'affiche ici.

Dernière visite

Chaque jour à minuit, le logbook du jour actuel est lu et la dernière visite est saisie dans le jeu de données de la personne. Cette information est affichée sous « Dernière visite ». Il peut arriver qu'une visite date de plusieurs semaines. Dans ce cas, le lieu actuel est inconnu. La date de la dernière visite enregistrée pour la personne

CEStronics

reste cependant maintenue.



Cette date peut également être utilisée dans l'AccessOne pour bloquer automatiquement des personnes qui étaient absentes pendant une période réglable. Ceci s'effectue via le type de blocage « Période d'absence » (voir « 9.1.7 Blocages » page 81).

Badges

La liste est un aperçu des médias d'accès qui sont assignés à une personne. Le statut correspondant et la validité sont sauvegardés. La touche « Changer de badge » vous permet de changer le média d'accès appartenant à la personne. Si la personne a perdu son badge, un badge de rechange doit être activé.

Blocages

Affiche si un blocage est saisi pour cette personne. Les blocages peuvent s'appliquer à l'avenir et sont actifs uniquement à un moment ultérieur. Les blocages actifs actuellement sont marqués en orange. Les blocages peuvent également être marqués et supprimés dans ce dialogue. Si un badge perdu est retrouvé, le blocage correspondant peut être supprimé ici. Pour cela, sélectionnez simplement le blocage actif et cliquez sur la touche Supprimer.

Logbook

Cliquez sur la touche Actualiser pour afficher les messages du logbook des deux derniers jours relatifs à la personne. Vous pouvez régler la valeur entre 2 et 7 jours.

Exemple : une personne n'a plus accès et elle informe la sécurité du bâtiment. Le service de sécurité peut alors regarder à quelle porte la personne a été refusée et si des modifications des données relatives à la personne ont été effectuées, par ex. si une autorisation a été retirée ou si un modèle de temps a été modifié.


9.1.2 Données de base

C AccessDne - Données personnelles		- 🗆 X
Accuel		0
P B D B Sau		
	Vue d'emembre Données de base Judres données de base Eadrase Autorisations Frendre une mois Elecarges Masques d'acols (05)	
Nor 7 Norm do face Dalacente Def statement		
[interestion]	Nome Prénom: Autres	
	Titre Nom naissance	
	Date naissance: Seliett a state 📅 Lieu de naissance: Rays naissance -	
	Genre: 🗍 léminin 🔿 masculin Etat civil - Nationalite:	
	Entreprise: • Profession:	
	Entreprise 2. Départment 2. Activités	
	N° de personnel: Classe de persons E - Egenpersonal Référence externe:	
	Organisation: Hiérarchie: Plaque d'immatricul:	
	Commentaire	
	Adresse / coordonnées	
	Pays: -	
	Code portal Lieu Rue	
	Téléphone: FAX:	
Données personnalles	Tel.mobile: E-mail:	
Connees personnenes	Coordonnées internes	
d Autorisations	Téléphone: Bureou: Bâtiment:	
A Profils d'autorisation	Supervision	
Designed	Nom superviseur: Dépt.	
Données d'entreprise	Approuver les visites:	
Logbook	Pin	
(C)	Pilk:	
Rapports	Amer (EMA: désamer –	
🖌 Données de l'appareil		
A nes	Utilisateur: admin daan vedens de temper de noeder Station de temais 190/-11537 Tain Lac et Mar colleur fereiements D	Timeout non activit

Pour créer des nouvelles données personnelles, cliquez sur le bouton NOUVEAU. L'onglet « Données de base » s'ouvre automatiquement. Si vous souhaitez quitter cet onglet, vous devez remplir les deux champs obligatoires marqués en rouge « Nom » et « Classe de personnel ».

Données personnelles

Dans cette section, il existe des champs obligatoires qui doivent être remplis pour chaque personne (« Nom » et « Classe de personnel »). L'AccessOne distingue principalement entre Personnel propre, Personnel extérieur et Visiteurs. D'autres classes de personnel peuvent être créées dans la base de données par l'administrateur, mais doivent cependant être assignées aux trois classes de base prédéfinies (Personnel propre, Personnel extérieur, Visiteurs). L'utilisateur peut diviser le personnel extérieur par ex. en « Entreprises extérieures avec mission intérimaire » ou « Entreprises extérieures ». Certains blocages sont activés en fonction de la classe de personnel. Il est ainsi possible de définir qu'un blocage pour trop longue absence soit activé seulement après six semaines pour le personnel propre et après deux semaines pour le personnel extérieur. La classe de personnel est également évaluée aux points d'accès.

Exemple : pour les contrôles de sac, le réglage peut s'effectuer de manière à ce que les visiteurs soient toujours contrôlés alors que le personnel propre n'est contrôlé que de manière aléatoire réglable.

Le numéro de matricule est un critère d'ordre externe, qui provient habituellement d'un système de gestion du personnel externe (par ex. SAP). Il sert à l'assignation des personnes depuis le système de contrôle d'accès avec les données des ressources humaines. Le numéro de matricule est également autorisé comme critère de recherche.

Le dialogue « Données d'entreprise » vous permet de définir l'entreprise et le département. Pour les entreprises, il est défini s'il s'agit d'une entreprise propre ou d'une entreprise extérieure. Dans le champ de saisie « Entreprise », seules les entreprises propres peuvent être sélectionnées. Dans le champ « Entreprise 2 », seules les entreprises extérieures peuvent être sélectionnées. Les départements sont d'abord définis dans les données d'entreprise et peuvent uniquement être sélectionnés ici. Dans l'ordre de saisie, il faut donc créer d'abord les entreprises, puis les personnes.

Adresse

Saisissez ici toutes les données d'adresse pertinentes pour la personne.

Données de contact

CEStronics

Saisissez ici toutes les données de contact pertinentes pour la personne.

Superviseur

Pour les employés d'entreprises extérieures, un superviseur peut être indiqué. Il faut absolument que ce soit une personne du personnel propre. Le superviseur est l'interlocuteur responsable des personnes qu'il supervise.

Codes PIN

Trois codes PIN sont gérés dans l'AccessOne. Un PIN est le code numérique personnel pour le contrôle d'accès. Il existe des portes qui peuvent uniquement être franchies après saisie du code PIN. La longueur minimale du PIN est réglable via un paramètre de système (standard 4 chiffres, maximum 6 chiffres).

Le PIN peut présenter une validité limitée et également être bloqué. Lorsque le mauvais code PIN a été saisi trois fois, ce code PIN est automatiquement bloqué et doit être modifié dans le système.

Pour l'activation et la désactivation du système de détection d'intrusion (EMA), deux autres codes PIN sont gérés dans le système. Le PIN peut être identique pour l'activation et la désactivation, il doit cependant être différent du PIN pour le contrôle d'accès.

Il s'agit d'une exigence de la norme VDS*1 d'avoir deux codes PIN différents. Ces codes PIN n'ont pas de validité temporelle limitée. Pour une porte, il peut être choisi dans l'autorisation de la personne, si celle-ci peut activer, désactiver ou les deux. Une saisie du code PIN est uniquement possible si cette autorisation existe.

Pincode:		
Pincode bestäti	gen:	
vincode zurück	setzen:	

Tous les codes PIN doivent être saisis de manière cachée. Le code PIN de quatre à six chiffres doit être saisi deux fois et se composer d'au moins trois chiffres différents. La saisie est effectuée par le propriétaire du badge correspondant via un clavier numérique séparé.



9.1.3 Autres données de base

AccessOne - Données personnelles		- 🗆 x
Accuel		1
PPDB		
Rechercher Changer Nouveau Copier	Supprimer Actualiser Ausgration	
North In		
l de T	Vue d'ensemble. Donnien de base Autres données de base Badges Autoritations Prindre line photo Blocages. Maisques d'accès 005	
Nom de fan Prénom N° person	nr Intervention Madium Prénom:	
	Entreprise: Entreprise 2	
	Départment: Né le:	
	Carte d'identité/passeport	
	N° au todge: Type: We jodga at 1000 1 au	
	Acces Distant of Cartonic Series To Ended actions To	
	Autorité par	
	Duanter du système enterne	
	Witteu d'Amport III Panicipation à l'envegidirement d'alence du temps actues (0000	
	Autombour - voylege spéciel - voylege prioritaine:	
	Permir de visue et le trunal	
	Termendeskjour Viel jungs it inner a tana 📅 Termenent.	
2 Données personnelles	Permin de forvail Visi jouquisi. Some f subare 🔛 🗇 Permanent	
Autorisations	Immigration	
A Beefle discharization	Date Protection In Payshounce Webnicken:	
of Profils d autorisation	Company de Carlos	
h Données d'entreprise	Zine de parting N° du anting. Nonjo like Redmitter	
Logbook	Plage tie n/onthins:	
Rapports	Adoral Juspice: Dest scient II (300) Despine to bra	
Données de l'appareil	Divers Categorie de vierde Rapport statue	
A ore		
	Utilisaseur admin Loom Tochus na Sungue di spunder Station de travail: INV-11537 Tocs Lac et Mac colline Événements: 0 Tin	neout: non activé

Saisissez toutes les données que vous souhaitez enregistrer sur la personne.

Carte d'identité/passeport

À cet endroit, vous avez la possibilité de saisir le numéro de la carte d'identité ou du passeport et sa durée de validité. Cette saisie n'a lieu qu'à des fins de documentation.

Accès

Le début et la fin de l'activité (par ex. pour des contrats à durée limitée) sont saisis ici, pour configurer des blocages automatiques correspondants. Ces données sont par ex. utilisées pour le personnel propre, pour déterminer la date de début pour les nouveaux ou la date de fin en cas de résiliation. Avant le début de l'activité et lorsque la date de fin est atteinte, un blocage correspondant est activé. Il est ainsi possible de créer des personnes dans le système avant qu'elles ne commencent leur premier jour de travail. Cela s'effectue en partie de manière automatique via l'interface du système de gestion des données personnelles du département des ressources humaines. Lorsque la date de résiliation est atteinte, le badge est automatiquement bloqué.

Données de système externe

Il est possible de sélectionner ici un blocage d'importation, c.-à-d. que le système ne récupère pas des comparaisons de données quotidiennes de sources SAP externes. Lorsque des données ont été modifiées dans l'AccessOne, elles ne doivent pas pouvoir être écrasées à nouveau.

Instruction

Lorsqu'il existe dans l'entreprise une obligation d'instructions contraignantes pour les nouveaux employés, vous pouvez saisir à cet endroit la date de la première et de la deuxième instruction, ainsi que la date de la prochaine instruction.

Permis de séjour et de travail

Un permis de séjour et de travail valide est une condition légale pour l'emploi. Pour les personnes disposant d'un permis de séjour et/ou de travail limité, le système vérifie le respect de ce point, lorsque les données correspondantes ont été saisies ici. La saisie est dans l'intérêt du client, qui peut être sanctionné si des personnes travaillent sur son installation sans ce permis.



Immigration

Cette saisie sert uniquement à des fins de documentation et est optionnelle.

Divers

La « Catégorie de vente » est utilisée pour activer un badge pour l'utilisation à des distributeurs de vente. La condition est que les badges soient codés avec l'AccessOne.

9.1.4 Badges (médias d'accès)

AccessOne - Données personnelles							- 🗆 x
Accuel		- <u>_</u>					
P B D B F	XO						
Rechercher Change' Nouveau Copier	Supprimer Actualise	r Assignation					
	Mus d'annamble De	sinder the base. Autres does	Annale Land	An Alexandres	Discontra luna chana	Blancium Mannue d'arrie 105	
an I	YDE A ENGENIDE DO	need as but hunes but	ers de clie ton	- Horisadora	L'IENNO E ROME PORTO	unitages manuars traves 00	
Intervention	Nom: In	tervention Medium	Prénor	n:			
	Entreprise:		Latrep	rise Z:			
	Départment:		Né le:				
	Numero Version 1	alide de Valide jusc Statut Rem	p. Raison de cré. Retor	ar Moe en page arr	Mise en page de- Texte info	Imprimé demi	
	ם ער	Adu	home	CES Systemicarte			
						No.	
						X	
	Première acconstant d	hadro- 28/01.2021 Demilee	arcignation de badme	26.01.7021 Bar	danes al-Mr 0	100	
	Rodar selectionse	and the second second	and concernance				
	Nambre	10	Vesion á	M ^a de cuite-		Thursey de beder	
	Valide de	International International	Valide Muqu'a	74.8		Annual Academ	
🗽 Données personnelles	Statute	Adul	Utilisation per jour	0.			
Autorisations	Mise on page avidee	CES.Systemkane	wwet			Carlo and a second on the	
A. D. D. L. L. C.	Remarquist	Interention Medium,				Codage	
Profils d autorisation	Texte info					Charge do coender DHF	
🔥 Données d'entreprise	Demière impletaion.	Jamaes imprime	Nombre Imprimé	d Format	055 Disting Interview	i comat du badge	
V Logbook	Type: special:	Garde de sécurite	1 (Mergention)			Ces-Master Baltimo(Degic)	
	Raidon de la création.	Incanal	Oste de retouc			manner / coore a casp:	
📔 Rapports						Em Foder III badge	
 Rapports Données de l'appareil 						Foder III badge	

Cet onglet vous permet de créer, remplacer, assigner ou imprimer des badges. Dans l'aperçu sous forme de tableau, vous voyez tous les badges définis pour cette personne.



Une personne peut avoir plusieurs badges. Ceci est notamment nécessaire lors de l'utilisation de plusieurs technologies de badge.

Pour créer un nouveau badge, sélectionnez une personne, cliquez sur le bouton MODIFIER dans la barre de menu supérieure et cliquez sur la touche Nouveau badge.

Un badge est supprimé en le sélectionnant dans la liste puis en cliquant sur Supprimer le badge.



ATTENTION : il n'existe pas de question de sécurité avant la suppression définitive ! Si la touche a été pressée par erreur, cliquer sur le bouton ANNULER dans la barre d'outils. Les modifications de l'onglet actuel sont alors rejetées.

Badge sélectionné

lci, toutes les données relatives au badge peuvent être saisies ou modifiées. Le numéro de badge sert uniquement de critère de classement. En temps normal, il n'a rien à voir avec le numéro codé dans le badge, mais peut cependant être identique au numéro codé dans le badge.

L'indication de la version contient un caractère et va de 0 à 9 ou A à Z. Si un badge est défectueux, un badge identique avec le même numéro de badge et de code peut à nouveau être produit, mais le numéro de version est alors augmenté d'un caractère et sauvegardé avec le numéro codé dans le badge. Ainsi, seul le badge avec le numéro de version actuel est valide. Ce numéro est vérifié à la porte. S'il ne correspond pas, un message est généré et l'accès est refusé.

Valide de/à

Les badges peuvent avoir une validité limitée. Cette période de validité est vérifiée par le système. En dehors de cette validité, le badge est refusé. Si aucune valeur n'est réglée, cela implique une validité illimitée.

Statut

Seuls les badges actifs sont chargés aux commandes de portes. Un badge inactif ne fonctionnerait donc pas. Le système indique alors : « Badge inconnu ». Pour un badge qui doit aussi être valide, sélectionnez ici l'entrée « Actif ».

Mise en page arrière/avant

Le dialogue « Concepteur de badges » décrit la méthode d'impression des badges. Vous y avez la possibilité de sélectionner différentes mises en page, qui ont été définies au préalable. Lorsque vous créez un nouveau badge, vous définissez ici quelle mise en page doit être utilisée. Les mises en page peuvent être déterminées séparément pour chaque badge.



Un pré-réglage de la mise en page peut avoir lieu via la classe de personnel de la personne, lorsque l'administrateur enregistre les mises en page correspondantes dans la classe de personnel (voir « 9.1.2 Données de base » page 73).

Données de code disponibles

Lorsque le badge a été créé, les informations correspondantes du badge doivent être enregistrées. Au cas où des badges précodés sont utilisés, l'enregistrement s'effectue via la touche **Assigner le badge**. Il est alors demandé de présenter un badge sur le lecteur de dialogue, ce qui permet de consulter les informations du badge et de les enregistrer en tant que jeu de données. L'affichage passe en vert « Données de code disponibles ».

Lorsque les badges sont codés par l'AccessOne, la touche **Assigner le numéro de code** est active. Dans ce cas, une disposition correspondant au format de badge du client est utilisée et un numéro de code libre unique est déterminé. Celui-ci est attribué au badge. La touche **Codage du badge UHF** permet de programmer le badge via le lecteur de dialogue. Il est également possible de coder et d'imprimer en une seule étape de travail via la touche **Imprimer/coder le badge**. La condition pour cela est qu'une unité de codage soit installée dans l'imprimante.

Imprimer le badge des deux côtés

Affiche le badge avec la mise en page préparée dans un aperçu d'impression. Après la confirmation, le badge est imprimé, et, selon la capacité de l'imprimante, il est également codé lors de la même étape de travail.

- « Dernière impression » indique la date et l'heure de la dernière impression de ce badge.
- « Nombre imprimé » indique le nombre de badges imprimés de la personne sélectionnée.
- « Raison de la création » offre la possibilité de sélectionner une raison pour la (nouvelle) création.

• « Date de retour » détermine le jour où le badge doit être rendu. Une fois cette date écoulée, le badge est bloqué.

CEStronics



9.1.5 Autorisations

C AccessOne - Données personnelles		- a x
Armuler D Ba Saw		u
t an T Som de fair Prison N ⁴ procee I Intervention	Ver d'ensemble Donnes de taxe Autres données de taxe Bady Autonisations Tendre Lee photo Blocages Masques d'acc Nom: Intervention Medium Prénom: Entreprise : Entreprise 2: Départment: Né le:	4 035
	Standardt Temponains Validar der Seters a date 🗊 à Seters a date 🗊	
	Profile Description Valide de Valide jungvisui Actif	Ajouter
	Autorisation Description Valide de Valide jurgs/ks Modele temps Actif Exercisé access at hences Controller & sonie at temps Frequery absolute/control Adapted by types Adapted by types Controller & sonie at temps Controller & sonie at temps	
Données personnelles		Ajoure-
🖌 Autorisations	×	Supprimer
💰 Profils d'autorisation	Autorisation du lecteur Description Velde de Valide jusqu'au Modèle temps Actif	N
Données d'entreprise		Ajouter
📕 Logbook		Supprimer
Rapports.	Autorisonen serectionmen de Select a date 📆 a Shect a date 📆 Mod tomps 7 Acta 🧭 Act	cepter les changements-
Données de l'appareil		
A riss	Utilinateur admin Saue Macael Access de Langue Excesso Station de traveis INV-11537 Tous Lac et Macaeline Évenements 0	Timeout non active

Dans ce menu, des modèles de temps définis sont assignés à la personne. Ceux-ci doivent être créés dans le dialogue « Autorisations » (voir « 9.1.5 Autorisations » page 78).

Toutes les informations pertinentes pour les autorisations d'accès sont résumées ici :

Modèles de temps

Un modèle de temps standard peut être déterminé pour chaque personne. Celui-ci s'applique alors lorsqu'il n'existe pas de modèle de temps propre pour une autorisation. Vous pouvez ainsi par ex. déterminer qu'une personne doit avoir accès de 9h00 à 17h00 chaque jour en temps normal, mais qu'elle peut encore utiliser le parking souterrain une fois cette période écoulée. Il est également possible de limiter davantage l'accès à des zones précises.

Si aucun modèle de temps n'est indiqué, alors l'accès n'est pas limité dans le temps.

En outre, il est possible d'indiquer un modèle de temps temporaire, qui écrase le modèle de temps standard pour une période définie. Le modèle de temps peut présenter une période plus petite (par ex. en cas de chômage partiel) ou plus grande (par ex. en cas de travail le week-end).

En-dessous se trouvent les deux listes avec les profils et autorisations sélectionnés pour la personne. **Profils**

Un profil comprend un groupe d'autorisations. Il est possible de rassembler plusieurs autorisations dans un profil. Les profils permettent de rassembler les autorisations selon la fonction de la personne. Il est ainsi par ex. possible de créer un profil pour le personnel de nettoyage et un pour les techniciens. Cette procédure facilite la sélection des autorisations dont a besoin l'employé correspondant pour effectuer ses tâches. Exemple : les entrées de bâtiments sont rassemblées dans une autorisation et un profil pour les entrées de bâtiment contient alors les autorisations par bâtiment. Les modifications des autorisations qui sont comprises dans les profils s'appliquent alors directement aux profils. L'AccessOne transfère les profils immédiatement aux commandes de porte, de sorte que la modification d'une autorisation ou d'un profil s'applique à toutes les personnes auxquelles ce profil a été attribué, sans devoir transférer des jeux de données supplémentaires.

CEStronics

Une validité limitée et un modèle de temps peuvent être indiqués pour chaque profil. Si aucun modèle de temps n'est indiqué, le modèle de temps enregistré pour la personne s'applique. Si aucune validité n'est saisie, ce profil est valide de manière illimitée. Si une date de début est disponible, mais pas de date de fin, le profil s'applique de manière illimitée à partir de la date de début. Une date de fin saisie arrête la validité.

Pour supprimer un profil de la liste, sélectionnez-le puis appuyez sur la touche Supprimer à côté de la liste de sélection. Pour créer un nouveau profil, ouvrez une case de sélection en cliquant sur la touche Ajouter. Le profil souhaité peut alors y être sélectionné. Une sélection multiple est possible en cliquant avec la touche CTRL appuyée.

Autorisations

Les autorisations rassemblent les lecteurs dans un groupe correspondant. Voir pour cela également le dialogue « Autorisations » (voir « 9.1.5 Autorisations » page 78). Pour les autorisations, les mêmes règles s'appliquent que pour les profils.

Autorisation sélectionnée

Si un(e) ou plusieurs autorisations ou profils sont sélectionné(e)s par clic, les détails sont affichés dans ces champs et peuvent y être modifiés. En cliquant sur la touche

Appliquer les changements, les champs modifiés sont alors appliqués dans l'autorisation ou le profil.



Pour appliquer la modification, il faut appuyer sur la touche **Appliquer les changements**, sans quoi les modifications ne seront pas sauvegardées.

Il est possible d'attribuer jusqu'à 64 autorisations et/ou profils à une personne (par ex. 10 profils et 22 autorisations). Si les mêmes autorisations s'appliquent toujours à de nombreuses personnes, nous recommandons de rassembler ces autorisations dans un propre profil d'autorisation.



Lorsqu'une autorisation est attribuée à une personne et qu'elle est déjà comprise dans un profil d'autorisation attribué à la personne, cette autorisation redondante est supprimée dans le cadre des processus de maintenance automatisés lors du changement de jour.



9.1.6 Prendre une photo

C AccessOne - Personendaten			- 🗆 X
Home Home	and the second se		0
P B D D Speche	×O		
10 2	Ubersicht Stammasten Weitere Stammdaten	Ausweise Ben-Ontigungsn Bild aufnehn in Sperren	Trittimasken IDSS Spinde Beleinungen
Hachterns Vorname Personalor	Nachname: test Firma:	Vorname: Firma 2:	
	Abteilung:	Geboren am:	
	Sperre Grund	Viter Bin	
			New Spene New Spene
	Gewählte Sperre		
	Sperre:		
Personendaten	Gruns: Tätigkeitsende Gültig von: Tätigkeitsende	Datum auswahlen	
🖌 Berechtigungen	Abwesenheitszeit Bemerkung: Ausweis nicht zurückigegeben		
🚰 Berechtigungsprofile	Mehrfach falscher Pincode		
Firmendaten			
📕 Logbuch	Ranutter admin	Arbeitsetation: IN/s11537 Alle Arec und Mac peine	Freinnisse B Timesut nicht altwett

Dans l'onglet « Prendre une photo », vous pouvez attribuer une photo à une personne, en important cette photo ou en prenant directement une photo.

Si vous souhaitez importer une photo pour la personne, sélectionnez la personne dans la fenêtre de sélection à gauche et cliquez sur le bouton MODIFIER dans la barre d'outils en haut. Appuyez alors sur la touche **Im**-

porter une image.

Vous pouvez sélectionner des fichiers au format *.bmp, *.png ou *.jpg. Pour prendre une photo, une caméra doit être raccordée à votre ordinateur fixe/portable.

Dans le menu déroulant « Caméra », sélectionnez l'appareil correspondant. Une autre résolution et d'autres réglages de la caméra peuvent être paramétrés en fonction du type d'appareil raccordé.

Avec la touche **Démarrer la caméra**, prenez une photo de la personne.

Une fois la section d'image adaptée choisie (cadre vert), celle-ci s'affiche via la touche **Sauvegarder** l'image dans l'aperçu en haut à droite.



Lors du passage à un autre onglet sans sauvegarder, le cliché n'est plus disponible pour un traitement ultérieur.



9.1.7 Blocages

C AccessOne - Personendaten						- 🗆 X
Home Home						0
P P Specter Spectrem	XO	à		_	_	
te z	Ubersicht Stammasker	Weitere Stammdaten	Nusweise Benedittigungsn Bill	d aufnehn in Sperren	7 ritemasken X355 Spin	nde Beleinungen
Nachname Vorname Personalior.	Nachname: test Firma: Abteilung:		Vorname: Firma 2: Geboren am:			
	Sperre	Grund	Väm	Bas		
					Neue Sperre	
					Spene Köschen	
	Gewählte Sperre					
	Sperre:		2			
Rersonendaten	Grund: Tätigke Gültig von: Tätigke	ngabe itsende itsende	Datum auswahlen			
🖌 Berechtigungen	Bemerkung: Auswei	nnheitszeit is nicht zurückigegeben				
💣 Berechtigungsprofile	Mehrfa	ch falscher Pincode	_			
Firmendaten						
Logbuch						

Cet onglet vous permet de bloquer des personnes, par ex. lorsqu'un employé a perdu son badge. Pour cela, faites un double clic sur la personne que vous souhaitez bloquer dans la fenêtre de sélection à gauche pour accéder au mode de traitement. La touche **Nouveau blocage** est alors activée et vous pouvez attribuer un blocage à la personne.

Dans la section « Blocage sélectionné », vous pouvez effectuer des réglages supplémentaires.

Si le blocage doit être limité dans le temps, par ex. avant un « début d'activité », sélectionnez une date « Valide de/à ».

Indiquez des informations sur le blocage dans le champ de saisie « Commentaire ». Le bouton SAUVEGARDER de la barre d'outils vous permet de sauvegarder le blocage. Vous pouvez supprimer un blocage en le sélectionnant dans la liste et en appuyant sur la touche **Supprimer le blocage**.

L'AccessOne fait la différence entre blocage automatique et manuel. Sur demande, d'autres blocages peuvent être prédéfinis dans le système.

Exemple : blocage avant le début d'activité et après la fin d'activité

Ce blocage peut également être réglé manuellement et s'applique directement ! Dans ce cas, il faut veiller à ce que le système mette à jour le blocage lors des heures de nuit à l'aide des données saisies pour la personne. Lorsqu'une personne est par ex. bloquée à cause d'une fin d'activité, mais qu'elle doit encore aller au bureau le lendemain, ce blocage peut être supprimé manuellement, mais il sera automatiquement réactivé après minuit.



9.1.8 OSS-SO

Grâce à OSS Standard Offline, les cylindres électroniques et garnitures de différentes marques peuvent lire les mêmes autorisations du badge et les interpréter de la même manière.

			- 0 x
Accueil			
PBDB			
Annuler 5a	kuvegarder		
Loco L			(
	Vue d'ensemble Dannées de trase Autres dannées de	Dase Badges Autonsations Prendre une photo Blocages Masques d'ac	
Nam de tair Prenom N° persol	Nom: Intervention Medium	Prénom:	
	Entreprise:	Entreprise 2:	
	Départment:	Né le:	
	Données offline	X Supprime	
	Badge		
	Validité standard: 😥 💷 👘 Heure : Min	vel. jusqu'e 31.03.2021 14:32	
	Reservation standard casier: 🗹 👘 Heure : Min	and the second second second second	
	Evenements standard: 🕑 -	Entrées de la liste noire standard: 12 3	
	vue a ensemble		1
	Contraction Contraction		
Données personnelles	-		
 Données personnelles Autorisations 			Ajouter
 Données personnelles Autorisations Profils d'autorisation 			Acuter
 Données personnelles Autorisations Profils d'autorisation Données d'entreprise 	Autorisation du cylindre Description	Valide de Valide jusqu'au Modèle temps Actif Toggle Nik de securité	Acuter Suppriment Acuter
Données personnelles Autorisations Profils d'autorisation Données d'entreprise Loobook	Autorisation du cylindre Description	Valide de Valide jusqu'au Modèle temps Actif Toggle Nik de skrunte	Acuter Supprimer Acuter Supprimer
Données personnelles Autorisations Profils d'autorisation Données d'entreprise Logbook	Autorisation du cylindre Description Autorisation stitectionnées	Valide de Valide jusqu'au Modèle temps Actif Toggle Nik de skunte	Acuter Supprimer Acuter Supprimer
 Données personnelles Autorisations Profils d'autorisation Données d'entreprise Logbook Rapports 	Autorisation du cylindre Description Autorisation stitectionnées des Talect a clare is	Valide de Valide jusqu'au Modèle temps Actif Toggle Nix de skrume & Select a date III Mod temps Actif Easculer [Acuter Acuter Acuter Accepter les changements
 Données personnelles Autorisations Profils d'autorisation Données d'entreprise Logbook Rapports Données de l'appareil 	Autorisation du cylindre Description Autorisation stitectionnées ide Stelect a clare is Encodage	Valide de Valide jusqu'au Modèle temps Actif Toggle Nik de skrunte & Select a date IS Mod temps • Actif : Basculer: Zone offline 1-005 test	Accept los chargements

La mise en place et la gestion de cylindres électroniques et de garnitures, qui sont compatibles avec OSS Standard, sont complètement intégrées dans l'AccessOne. Pour la mise en place, vous avez également besoin de l'outil de configuration fourni par le fabricant correspondant, qui permet de programmer les données de configuration dans les cylindres électroniques.

Toutes les données de configuration sont enregistrées dans l'AccessOne. Depuis l'interface utilisateur, vous pouvez alors créer un fichier XML qui sera lu par l'outil de configuration correspondant. Ce fichier contient toutes les données pour l'initialisation du cylindre électronique.

Après l'installation de la licence correspondante, une touche pour OSS est disponible dans la sélection des fonctions. Elle vous permet d'accéder aux dialogues de gestion des données des composants offline. Vous y déterminez la validité des badges des personnes et ajoutez des profils, autorisations et autorisations de cylindre électronique.

Pour terminer, codez le badge.



9.1.9 Instructions

e Nachsame Vorname Personaln	Doersicht Staromidaten Nachname: sest Firma: Abteifung:	Weitere Stamminaten	Ausweise Berechtigur Vormame: Firms 2: Geboren ann	ngen Bild aufnenmen	Sperren	Zuhntsonasken	QSS Spinde	Belehrungen
	Belehrung	Beschräßung		Datum Nachste	ır Termin			
	Gewählte Betehnning	Hauve	Dumanetter 13	Hanna Tore				
Personendaten	6							
A Berechtigungen								
A Berechtigungsprofile								
A Firmendaten								
Logbuch								
ATT N AND A ATT								

Il est possible d'enregistrer ici des instructions qui doivent avoir lieu dans une période définie (par ex. prévention des accidents du travail, RGPD). La touche Ajouter permet de les sélectionner et de les saisir avec une date.

CEStronics

9.2 Changements de groupe

Le dialogue « Changements de groupe » permet d'appliquer des changements de données personnelles, de blocages de personnes et d'autorisations sur des groupes entiers par importation de données.

AccessOne - Group changes					-	D	×
Home Kome Clear Execute							0
Forego changes Praser 1416 Praser 1416 Pra	n data	delete delete v o v v active active active active active active active active active active active active active active active active active active activ	valid from:	united and			
Image: ACLs Image: ACLs Image: ACLs Image: ACLs					Import		

9.2.1 Données personnelles

L'onglet « Données personnelles » permet de modifier ou de supprimer les données créées au préalable, qui ont été chargées en cliquant sur la touche **Importer**.

Les données à importer doivent être présentes sous forme de fichier *.csv. Ce fichier peut être créé à l'aide de la page de dialogue « Rapports > Personnes > Groupes de personnes Exportation ». Sur cette page de dialogue, de nombreux filtres pour configurer les groupes de personnes sont disponibles. Si un rapport est créé, le groupe de personnes créé peut être sauvegardé comme fichier MS Excel sur le disque dur et édité ultérieurement.

Le fichier *.csv sauvegardé depuis ce programme sert de fichier d'importation pour tous les dialogues de changement de groupe.

9.2.2 Ajouter ou supprimer des blocages de personne

AccessOne - Gruppenänderungen Home Home AccessOne - Gruppenänderungen Home Home AccessOne - Gruppenänderungen						- 1	2	×
Gruppenlinderungen Personenberschligungen Personenderen Personenderen	Personensperren Sperren Sperre: Grund:	lischen hinzufügen						
	Gültig von: Bemerkung:	Tätigkeitsende Abwesenheitiszeit Ausweis nicht zurückgegeben Mehrfach falscher Pincode	bis:	Datum auswählen				

L'onglet « Blocage de personne » permet d'ajouter ou de supprimer des données de blocage par importation



de fichier pour le groupe de personnes correspondant.

Le champ de saisie « Blocage » vous propose plusieurs raisons de blocage qui peuvent être saisies avec une validité.

AccessOne - Group changes							~	D	×
B Home									(
Clear Execute									
Group changes Person state	Person data	C change	🖸 delete						
	Organisation: End job: Personnel class Company Company 2 Default time model			active					
	Temporary:			active	valid from:	Import			
Sa ACLs									
🗽 Visitor / Appointments									
🗽 External employee									
- Workflow									
# Group changes	User admin	1	idialog redet correc	wo Wo	rkstation: INV-11537	T Lac; 0 Mac offine	Ever	ts: 0	_

9.2.3 Adapter les autorisations de personnes

Name	Beschreibung	Name	Beschreibung
Demoboard Blau	Demoboard Blay	Aufzüge zu den Besprechungsräume	Aufzüge zu den Besprechungsräume
inance and controlling		Besprechungsräume	
Austerkoffer	Musterkoffer	1	1
M			
roduction			
ervice			

L'onglet « Autorisations de personnes » permet d'ajouter ou de supprimer des autorisations par importation de fichier ou saisie de profil et d'autorisation pour le groupe de personnes correspondant. Confirmez toujours les modifications via **Appliquer les changements**.



10 Documentation de l'installation

Pour la documentation de l'installation à un moment donné, il est possible de créer des rapports et de lire et exporter des saisies de logbook.

10.1 Rapports

La sélection de dialogue « Rapports » permet de lire et d'exporter toutes les saisies effectuées. L'AccessOne peut exporter à tout moment une documentation d'installation complète.

AccessOne - Rapports			
Accueil			
Vider Exécuter			
4 Patrende	In the second second		
- Apparels	Autorisations		
Liste des appareils	Recherche		
État de la batterie du lecteur	1		
Appareils offline	Profile	Description	
Autorisations	Parent .		
Autorisations par personne			
Autorisations dans les profils Autorisations offline			The Alexander of the Al
Autorisations offline par personne			Apouter
Historique des autorisations par personne Historique des autorisations par annareil			X Supprimer
Liste des autonsations			
* Divers	Autorisation	Description	
Badges de liste noire en cylindre			
Personnes			
Autorisations de personnes			
Personnes dans zones 4 Visiteurs / Dates			Apuler
Visiteurs			
Dates de visite			X Supprimer
	Lecteur	Description	
A Données d'entrenrise			
of bonnees dendeprise			
Logbook			
6			Ajouter
Rapports			
			Supprimer
Données de l'appareil	1.00		
2005	Vue		
0 000		Répéter les titres des rolonnes sur	chaque page
Liste noire de l'OSS	-	Instantion and and constitutes 201	all date have



10.2 Logbook

Le dialogue « Logbook » permet de consulter tous les messages journaliers actuels et de créer des filtres individuels.

10.2.1 Messages

AcuessOne - Logoook								-	II X
and the drawn									4
	XO								
	Actuality								
	Lawrence Description								
faet	Messages Filtra								
Nom Description	Date LAC / SdT	Lischeur / Loger	Lieu / Program	e Nº.	Messige	Badge Nom de famil	le Prenom Entrepo	÷	
Alte Tageometdungen	02.11.2021 08:00:57 INV-11537		MasterProcess	807	Master demarrage le système A				_
Alerte isatiesie	02.11.2021 08/01:00 INV-11537	-	LogWriter	800	Démanage du processus	-	-		_
Disposible from Agent	02.11.2021 08:01:00 INV-11557	-	LogWriter	801	Processus est en marche	-			
Let letteurs du 125	02.11.2021 08:01:03 INV-11537		Notifier	800	Démarrage du processus				
MAG	02.11.2021 08/01/03 INV-11537		Notifier	801	Processus est en marche				_
	02.11.2021 DB/01-05 INV-11537		LogReater	800	Démanage no processus				
	02.11,2021 08:01:06 INV-11537		LogReader	801	Processus est en marche				
	02.11.2021 00:01:06 INV-11537		LionseProcess	806	Démarrage du processas				_
	02.11.2021 08:01:09 INV-11537		LicenseProcess	801	Processus est en marche				-
	02.11.2021 08/01:11 WV+11511	-	AcMetterLom	800	Démanage du processus		and the second		_
	02.11.2021 08:01:11 INV-11517		AcMatterCom	801	Processus est eo marche				_
	02.11.2021 08:01:14 INV-11537	-	AdMasterCom	629	Convexion 3 Mac 'Mac établie	P			
	02.11.2021 08:01:13 INV-11537	-	PersonImport	800	Démantage du processus				
	02.11.2021 08:01:16 INV-11537	Mac		420	Informations sur le logiciet: MA				
	02.11.2021 08:01:18 INV-11537	1	Personimport	801	Processus est en marche				-
	02.11.2021 08:01:21 INV-11537		WebExcharige	800	Démanage do processa				
	02.11.2021 09:01:21 INV-11537		WebEkchange	801	Processus est en marche				
	02.11.2021.0801:34 INV-11537		WebAccess	500	Démarrage du processus				
	02.11.2021 08:01:37 INV-11537		WebAccess	801	Processus est en marche				
A Données d'entrennise	03.11.2021 08:01:58 INV-11537	Contraction of the local division of the loc	MasterProcess	808	Master a reusal à démarrager A				
bonnees d'entreprise	2021 08/01:40 Mac.	Entrée principa		401	Appareil n'est pas prét à fonction			5	
Lonbook	02.11. 21 13:43:29 INV-11537	admin	Dialog	817	Utilisateur aumin sur le station				
Eugloook	02.11/ 21 13:43:29 INV-11537	admin	Logon5ervice	820	Utilizateur 'admin' s'est connec				
Rapports	Med 1,2021 3426:33 Mac	Entrée principal		470	Informations sur le logiciei: SW				
IEI wabbore	02.11.2021 14:26:33 Mac	Entrée principa	-	420	Informations sur le logicie: CF-		-		
A Doppior de l'appareil	02.11.2021 15:26:20 Mac	Entrée ponorpa		403	Début du programme				
Donnees de l'apparen	02.11.2021 15:26:20 Entrée princ	IO Modul:1		400	Appareil prêt a fonctionner				_
1 000	03.11.2021 15:26:21 Mac	Entree principal		420	Informations tur le logiciet 'Au				
d 055	02/11/2021 15:26:21 Mac:	Entrée principa		420	Informations sur le logiciel: Ber			1	_
Liste noire de l'OSS	02.11.2021 15:26:21 Mac	Entrée principa		420	Informations sur le logiciel: Pro	1			
	02.11.2021 14:26:33 Mar.	Entrée principa		400	Appareil prét à fonctionner				_
to Describer of Frances	02.11.2021.14:26:34 Mac	Entrée onnoipa		421	Données de l'appareil chargées			1	
Donnees utilisateur	02.11.2021 14:26:34 Mar	Entrée principa		422	L'autorisations ont été chargée			1	
📝 Concepteur des badges	Number Isali at meslager (saves) (11			Atsored in	niers a jour	~		
98 xm	Inclusion of casion 1	_	_	1000		The second second		Printing a	COLUMN T
1 - 1 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -	Utilisateur agrini			Static	n ae travaic in V+11037	Lac et Mariphine	Evenements 0	Timeout	non active

10.2.2 Filtres

Déterminez vos filtres individuels. L'AccessOne offre de nombreuses possibilités de saisie.

Accueil									
		-	EN.						
R T A		9	-						
Changes Nouveau Copier	r Suppor	mer Actualiser Ad	ssignation						
		-	-						
		Missage Filtr	•)	_					
a	0	C							
Nom Desc	cription	Noni et caligaria							
Aktueli Alie Alie	Tøgesmeldungen	Nom du filtre:	Aurre patrene		Catégorie	Ohne			
Dispositifs hors ligne		Descention							
Les lecteurs du CES.		Description.							
MAC		Date							
		de'	inum La clade	00.00	ñ.	1 December 1	0000		
					Tanàn Ing ang ang ang ang ang ang ang ang ang a		Second Second		
		Données personne	effes		tranches noraires				
		News-			- Enderson				
		THEORY -			(Freedom)				
		Nº du bagger			Nom de l'entreprise				
		Don. d'annareil	Nom	Description		Type			
		and a strange		(and a set		044			
								n	
								Stone	
								×	
								-	
		Dan. du message	Message			Numéro			
			Changement de batt	eric		477			
Profils d'autoris	sation		Tension de batterie b	onne (niveau; [0]')		442	_		
			Tension de batterie faible 476				D		
Données d'entr	reprise			n sie mei dipente par	and fell	1-21	-		
								X Summer	
Logbook									
Rapports									
Ponnios de l'a	pagarail								
Donnees de l'a	pparen								



La touche **Ajouter** ouvre une fenêtre qui liste toutes les données d'appareil et de message pouvant être utilisées comme filtres.

Pone Prove Socional Mediangen Primeinen werden werde	AccessOne - Logbuch						
Proben Spicitum Proben Spicitum Proben Mediangen Pitter Name and Ketopric Beschreibung: Beschreibung: Dolam Vori Dolam Vori Vori Betamane: Ausreal Spicitum Vori Betam auswählen Vori Medangen Vori Medangen Ausreaf 25 Solkstel 107 na Bisckist veri Ausreaf 25 Solkstel 107 na Bisckist veri Ausreaf 25 Solkstel 107 na Bisckist veri Ausreaf 107 permanent geldscht Ausreaf 107 permanent geldscht Berechtigungen Betreitigungen Betreitigungen Betreitigungen Betreitigungen offile Firmendaten Lasebracht	Home						
Neckin Spician Berechtigungen Meldungsdeen Meldungsrofile Meldungs referenze generatien (10) auch beter (10) Berechtigungen Beterespennung referig (Offine) Berechtigungen Meldung referenze (10) auch beter (10)	PY D D D V	C. 1	1 I				
Meldungen Filter met met Kategorie Name und Kategorie Beschreibung all Alle Tagennelaungen Beschreibung Betchreibung Datum Datum von: Datum Auswein: Auswein: Auswein: Gerätedaten Name Beschreibung Berechtigungen Keldung Berechtigungen Meldung Berechtigungen Meldung Betreingennung nichtig (Offline) Batteriegennung nichtig (Offline) Betreingennung nichtig oder Hild Lie All Betreingennung nichtig (Offline) Betreingennung nichtig oder Hild Lie All Betreingennung nichtig (Offline) Betreingennung nichtig oder H			à				
Moldungen Filter wei als Tugesmeldungen Moldungen inzerer ingenendungen Beschreibung: Dotum Beschreibung: Dotum Moldungen Vors Datum auswählen Schweistritt Ausweistritt Ausweistritt Ausweistritt Ausweistritt Datumeistritte Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung Beschreibung	bbrechen Speichern						
Meldungen Filter ne Bischreibung Jaser Beschreibung Detum Beschreibung Dotum Voll Voll Detum auswählen Auswein Schlosel (0) aus Bockles gel 177 Auswein Gerötedaten Name Beschreibung Meldungsdnen Gerötedaten Name Beschreibung Meldungsdnen Meldungsdnen Batteriegannung zuft Level: 100/1 425 Ausweist laden geschatel (Offine) Batteriegannung zuft Level: 100/1 Batteriegannung nieding (Offine) Batteriegannung zuft Level: 100/1 Batteriegannung zuft Level: 100/1 445 Batteriegannung zuft		-					
Beckhendungen Berechtigungen Berechtigungen Berechtigungen Firmendaten	-	Maldungan F	ilter				
Mail Alle Taperneldungen Alle Taperneldungen Alle Taperneldungen Alle Taperneldungen Alle Taperneldungen Berechtigungen Filtemanne Berechtigungen Filtemanne Berechtigungen Filtemanne Berechtigungen	S-	meleoniden .					
Alle Tagesmelsburgen Filtemanne Bitteiewarnung Ketegonie Beschreibung Beschreibung Beschreibung Meldungen	ame Beschreibung	Name und Kateg	gorie				
Berechtigungen Meldungsdaten Meldung Berechtigungen Meldung ut der gewechteit (Offine) Berechtigungen Meldung ut der gewechteit (Offine) Berechtigungen Meldung ut der gewechteit (Offine) Berechtigungen Meldung (Offine) Betweitigen Meldung (Offine)	tuell Alle Tagesmeldungen	Damas	Patteriessenture	Kataania			
Lener Beschreibung: Dotim von: Datum auswählen is 0000 Personendaten Nachname: Ausweis / Schlussel (Vin Backsits ver 7) Beter (Sterre gewechselt (Offline) Batteriespannung nieding (Verline)	troowanung	Filtername;	sauenewarnong	Kategorie:		_	
Dotum vori Datum vori Datum Vori Personendaten Nachname: Ausweis / Schlussel (0)? aus Blackist veri / 716 Ausweis / Schlussel (0)? aus Blackist veri / 716 Ausweis / Schlussel (0)? aus Blackist veri / 716 Ausweis / Schlussel (0)? aus Blackist veri / 716 Ausweis / Schlussel (0)? aus Blackist veri / 716 Ausweis / Schlussel (0)? Blackist veri / 716 Ausweis / Schlussel (0)? Nummer Ausweis / Schlussel (0)? Reset / 716 Batteriespannung gut (Level: / 0)? Batteriespannung niedig (Offline)	is taser	Beschreibung:		(1		
Dotum von: Datum auxwählen 15 0000 Personendoten Nachname: Auswein / Schlussel (0)" aus Blackist ver 716 Auswein / Schlussel (0)" aus Blackist ver 717 Batteriegannung gut (Level: (0)) Batteriegannung gut (Level: (0)) Batteriegannung gut (Level: (0)) Batteriegannung niedig (Offline)	lasec Leser	-		Meldungen		- 0	×
work Datum autwählen is 0000 K Personendaten Nachname: Nachname: Auswein // Schlussel (V)ri Batzausser // Auswein // Schlussel (V)ri Batzer // Auswein // Schlussel // V)ri Batzer // Auswein // Schlussel // V)ri Batzer // Auswein // Schlussel // V)ri Batzer // Batzer // Schlussel // V)ri Batzer // Batzer // Batzer // Batzer // V)ri Batzer	IAC .	Datum					-
Berechtigungen Meldung Berechtigungsprofile Meldung Firmendaten Satteriespannung niedrig Offine)		line	Datum auswählen	1			_
Personendaten Nummer Nachname: Ausweir / Schlussel (0) [*] aus Blackitst ver Ausweir / Schlussel (0) [*] gewechselt ta Erstazusser 7-6 Ausweir / Schlussel (0) [*] gewechselt ta Erstazusser 7-6 Ausweir / Schlussel (0) [*] gewechselt ta Erstazusser 7-6 Ausweir / Schlussel (0) [*] gewechselt ta Erstazusser 7-6 Ausweir / Schlussel (0) [*] gewechselt ta Erstazusser 7-7 Ausweir / Schlussel (0) [*] gewechselt ta Erstazusser 7-7 Ausweir eitsden 6 Ausweir eitsden 6 Ausweir eitsden 6 Ausweir i gehandert 6 Ausweir i gehandert 6 Ausweir i gehandert 4 Ausweir i gehandert 4 Ausweir i gehandert 4233 Batterie gewechselt (Offline) 477 Batterie gewechselt (Offline) 476 Batterie gewechselt (Offline) 466 Batterie gewechselt (Offline) 849 Batterie gewechselt (Offline) 846 Batterie gewechselt (Offline) 465 Batterie gewechselt (Offline) 846 Batterie gewechselt (Offline) 846 Batterie gewechselt (Offline) 846 Batterie gewechselt (Offline) 465 Batterie gewechselt (Offline)		Vors.	(11111111111111111111111111111111111111	1 Environment	The second		-
Berechtigungen 1 Berechtigungsprofile 1 Firmendaten 1 Firmendaten 1		Personendatea		2 Meldung	Nummer		1.7
Nachname: Ausweis (2) gewechtert u. Stratusurer 7 Ausweis (2) permanent gelöcht 661 Ausweis (2) permanent gelöcht 61 Ausweis (2) permanent gelöcht 61 Ausweis (2) permanent gelöcht 62 Ausweis (2) permanent gelöcht 63 Ausweis (2) permanent gelöcht 64 Batteriespannung nicht gelöcht 64 Batteriespannung ni		rersonenuoten		Ausweis / Schlussel '[0]' aus Blacklist gi	2 717		+^
Ausweisne: Ausweisne: Gerötedaten Name Berechtigungen Meldung Berechtigungsprofile Filmendaten Filmendaten Ausweisne: Loopburch Ausweisne:		Nachname:		Ausweis / Schlussel (0) in blackist vers	5 / 10		-11
Berechtigungen 1 Berechtigungsprofile 1 Firmendaten 1				Ausweis (0) gewechseit zu Ersatzausw	601		+
Berechtigungen ** Berechtigungsprofile ** Firmendaten **		Ausweishr:		Ausweis entronen	5		+
Berechtigungen ** Berechtigungsprofile ** Firmendaten **		Gerätedaten	Name Reschreihung	Ausweis geändert	6		+
Berechtigungen * Berechtigungsprofile * Firmendaten *		Geroteusten	out of the second secon	Ausweis in Version '(0)' kodiert	25		+
Berechtigungen ** Berechtigungsprofile ** Firmendaten 1 ***				Ausweis zugewiesen	4		
Berechtigungen * Berechtigungsprofile * Firmendaten •				Ausweise laden beendet ('(0)' Karten)	424		+
Meldungsdoten Meldung Berechtigungen Image: Steriespannung niedrig Offline) Berechtigungsprofile Image: Steriespannung niedrig Offline) Firmendaten Image: Steriespannung niedrig oder fehit (Level: '0)				Ausweise laden gestartet	423		1
Berechtigungen ** Berechtigungsprofile ** Firmendaten 1 ***				Batterie gewechselt (Offline)	477		T
Berechtigungen Meldungsdaten Meldung Berechtigungsprofile Batteriespannung nieding Offline) Batteriespannung nieding Offline) Berechtigungsprofile Batteriespannung nieding oder fehlt (Level')0 Firmendaten Image: State in the spannung nieding oder fehlt (Level')0				Batteriespannung gut (Level: '{0}')	442		
Meldungsdaten Meldung Berechtigungen " Berechtigungsprofile " Firmendaten Loopburch				 Batteriespannung niedrig (Offline) 	476		-
Berechtigungen Firmendaten Indexen Berechtigungsprofile Firmendaten Berechtigungsprofile Firmendaten Berechtigungsprofile Firmendaten Berechtigungsprofile Firmendaten Berechtigungsprofile Firmendaten Berechtigungsprofile Firmendaten Firmendaten Berechtigungsprofile Firmendaten Fir		Meldungsdaten	Meldung	Eattenesponnung niedrig oder fehilt (L	2 441		
Berechtigungen " Berechtigungsprofile " Firmendaten Image: State (1) State			Batterie gewechselt (Offline)	Beginn Export '[0]' nach Datei '[1]'	849		+
Berechtigungsprofile Firmendaten Loopbush	and the second se	1	Batteriespannung gut (Level: '(0)')	Beginn Import '(0)' aus Date: '(1)	846		+
Berechtigungsprofile Firmendaten Iogeburgh	Berechtigungen		Batteriespannung niedrig (Offline)	Belehrung (0) geändert, Eigenschaft: 1	(00		10
Berechtigungsprofile Firmendaten I C 7 7	a she daalaa hadaa ahaa ahaa		Batteriespannung niedrig oder fehlt (Level-'(D			-
Firmendaten	Berechtigungsprofile				Auswählen	Abbrecher	n
Laphuch	Firmondaton				1.12.7		
Logbuch	rumendaten						_
	Loobuch						

La connexion du client	Dans le répertoire d'instal-	Contrôlez les saisies dans le fichier ClientCon-
au serveur AccessOne	lation	fig.xml du répertoire d'installation \AccessOne\
ne fonctionne pas		config.
		Les saisies pour « MasterHost » et « Master-
		Port » sont-elles correctes ?
	Sur le serveur	- SQL Server et le service SQL Browser sont-ils
		démarrés et les protocoles TCP/IP et Named
		Pipess sont-ils activés ?
		- Contrôlez les règles du pare-feu. Le port SQL
		Server
		(standard : TCP 1433), le port SQL Browser
		(standard : UDP 1434) et les ports AccessOne
		configurés (par ex. TCP 50000-500xx) sont-ils
		accessibles ?
	Interaction	L'heure chez le client et sur le serveur AccessO-
	serveur-client	ne est-elle synchronisée ?
		Une différence de d'heure inférieure à 5 minu-
		tes est
		autorisée.

11 Dépannage

Teaming up for security since 1840



C.Ed. Schulte GmbH

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

www.ces.eu