

AccessOne

Zutrittskontrollsystem



Systembeschreibung und Anleitung

 Deutsch

Version VF1

BRO2262

Inhalt

1	Über diese Anleitung	6
1.1	Hersteller und Service	7
1.2	Zielgruppen dieser Anleitung	7
2	Zu Ihrer Sicherheit	8
2.1	Sicherheitshinweise	8
2.2	Rechtliche Hinweise	8
2.3	Systemvoraussetzungen	8
2.4	Datenschutz in der AccessOne	8
3	Über AccessOne	10
3.1	Funktions-Erweiterungen	11
3.2	Empfohlene Vorgehensweise zur Ersteinrichtung der AccessOne	12
4	Allgemeine Dialoghandhabung	14
4.1	Sichtmodus – Änderungsmodus	15
4.2	Werkzengleiste	15
5	Anmeldung	18
6	Konfiguration der AccessOne	19
6.1	System-Konfiguration	19
6.1.1	Parameter	19
6.1.2	Bereiche	21
6.1.3	Parkgruppen	21
6.1.4	Arbeitsstationen	22
6.1.5	Leserformate	22
6.1.6	Kartenanalyse	23
6.1.7	Lizenzen	24
6.1.8	Kartenformate	25
6.2	Benutzerdaten	29
6.2.1	Benutzergruppen	29
6.2.2	Benutzerstammdaten	30
6.2.3	Benutzer ACL (Mandantenfähigkeit)	31
6.2.4	Zuweisen der Datensätze zu den Zugriffslisten – ACL	32
6.2.5	Web-Benutzergruppen	33
6.3	Standortdaten	34
6.3.1	Standort anlegen	34
7	Konfiguration der Geräte	35
7.1	Gerätedaten Online-Geräte	36
7.1.1	Geräteübersicht anzeigen	36
7.1.2	Mastercontroller (MAC) anlegen	37
7.1.3	Türsteuerung (LAC) anlegen	39

7.1.4	Eine Tür anlegen	42
7.1.5	Gerätestatus anzeigen	56
7.2	Gerätedaten Offline-Geräte (OSS-SO)	57
7.2.1	Facilitydaten	57
7.2.2	Zylinder (und Beschläge)	58
7.2.3	Offline Geräte programmieren	59
7.2.4	Berechtigungen	60
7.2.5	Datenimport	61
7.2.6	Zeitmodelle	62
8	Konfiguration der Berechtigungen	63
8.1	Berechtigungen	63
8.1.1	Berechtigungen in der Übersicht	63
8.1.2	Generelles zu Zeit- und Tagesmodellen	64
8.1.3	Tagesmodelle	64
8.1.4	Sonder- und Feiertage	65
8.1.5	Zeitmodelle	68
8.1.6	Zutrittsmasken	70
8.2	Berechtigungsprofile	71
8.2.1	Online-Berechtigungen in der Übersicht	71
8.2.2	Offline-Berechtigungen in der Übersicht	72
9	Anlegen von Personendaten	73
9.1	Personendaten	73
9.1.1	Personendaten in der Übersicht	73
9.1.2	Stammdaten	75
9.1.3	Weitere Stammdaten	77
9.1.4	Ausweise (Zutritts-Medien)	78
9.1.5	Berechtigungen	80
9.1.6	Bild aufnehmen	82
9.1.7	Sperren	83
9.1.8	OSS-SO	84
9.1.9	Belehrungen	85
9.2	Gruppenänderungen	86
9.2.1	Personendaten	86
9.2.2	Personensperren hinzufügen oder löschen	86
9.2.3	Personenberechtigungen anpassen	87
10	Anlagendokumentation	88
10.1	Berichte	88
10.2	Logbuch	89
10.2.1	Meldungen	89
10.2.2	Filter	89
11	Fehlerbehebung	91

1 Über diese Anleitung

Diese Anleitung enthält grundlegende Informationen zur Einrichtung und Administration einer Zutrittssteuerungsanlage mit dem Zutrittskontroll-System AccessOne.

Die Anleitung ist als Teil des Produkts zu betrachten und während der gesamten Lebens- und Einsatzdauer des Produkts aufzubewahren. Geben Sie die Anleitung an jeden nachfolgenden Anwender des Produkts weiter.

Mitgelieferte Dokumente

Lizenzaktivierung >	BRO2307_DE_Infoblatt_Lizenzmodul AccessOne aktivieren
Installation >	BRO2313_DE_Kurzanleitung_Installation AccessOne

Gestaltungsmerkmale



Verweist auf weitere Informationsdokumente.



Markiert zusätzliche Informationen und Tipps.



Markiert Warnhinweise in Schrittanleitungen und besonders wichtige Informationen.

Schreibkonventionen

In diesem Dokument werden Bedienelemente der Dialogoberfläche, wie z.B. Schaltflächen, in fetter Schrift ausgezeichnet (Beispiel: Klicken Sie auf **Benutzer anlegen**). Buttons aus der Werkzeugleiste werden zusätzlich in Grossbuchstaben gesetzt (Beispiel: Klicken Sie auf ABBRECHEN). Namen von Datenobjekten, Auswahl- und Freitextfelder und Checkboxen werden in Anführungszeichen dargestellt (Beispiel: Im Feld „Bemerkungen“ tragen Sie zusätzliche Informationen ein).

Abbildungen

Die in der Anleitung abgebildeten Dialoge enthalten nicht alle Optionen, über die das System verfügt. Abhängig von der Lizenz und den aktivierten Optionen können Screenshots und Beschreibung abweichen.

Hinweise zum Markenschutz

MIFARE, MIFARE Classic und MIFARE DESFire sind eingetragene Marken von NXP B.V. und werden unter Lizenz verwendet.

Die in diesen Unterlagen enthaltenen Angaben und Daten können ohne vorherige Ankündigung geändert bzw. technisch weiterentwickelt werden. Ohne ausdrückliche schriftliche Erlaubnis der C.Ed. Schulte GmbH Zylinderschlossfabrik darf kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden.

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

BRO2316-1 Version: VA1



Benutzen Sie immer die aktuellste Version dieser Anleitung. Aktualisierte Versionen erhalten Sie kostenlos unter www.ces.eu.

1.1 Hersteller und Service

Die Urheberrechte der AccessOne liegen bei der ACcesstronic GmbH. Service und Support übernimmt die C.Ed. Schulte GmbH mit Sitz in Velbert. Für Unterstützung im Servicefall setzen Sie sich bitte mit dem CES-Service in Verbindung. Sie erreichen den CES-Service unter +49(0)2051 204 222 oder per E-Mail: hotline@ces.eu

Hersteller

ACcesstronic GmbH
Gartenstr. 38
D-52249 Eschweiler

Service und Support

C.Ed. Schulte GmbH
Zylinderschlossfabrik
Friedrichstr. 243
D-42551 Velbert

Tel: +49 (0) 2051-204-0
Fax: +49 (0) 2051-204-229
www.ces.eu
info@ces.eu

1.2 Zielgruppen dieser Anleitung

Die Einrichtung der AccessOne wird durch den Betreiber der Anlage beauftragt und von eigenen Fachkräften oder Dienstleistern aus dem Bereich IT/Administration ausgeführt. Die Bedienung der Zutrittssteuerungsanlage darf nur durch produktgeschultes Personal erfolgen. Die Informationen in dieser Anleitung richten sich daher an unterschiedliche Zielgruppen. Die Zielgruppen sind zu Beginn jedes Hauptkapitels ausgewiesen. Beachten Sie unsere Empfehlungen zur Vorgehensweise bei Installation, Einrichtung und Bedienung der AccessOne.

Zielgruppe	Kompetenzen
Fachkräfte IT/Administration	besitzen langjährige Berufserfahrung im Bereich IT-Strukturen, Administration und Netzwerke. Besondere Eigenschaften der Zielgruppe: Kenntnis von IT-Fachbegriffen Kenntnis von Aufbau und Pflege von Netzwerken, insbesondere Kenntnis des Netzwerks, das von Ihnen betreut wird
Anlagenbetreiber	besitzen Erfahrung in der Verwaltung von Schließanlagen. Dies können sowohl mehrere Anlagen als auch die tiefe Kenntnis einer einzelnen Schließanlage sein. Besondere Eigenschaften der Zielgruppe: Kenntnis von Fachbegriffen rund um Schließanlagen Kenntnis im Umgang mit einem PC und Software
Produktgeschultes Personal	wurde von CES oder einem CES-Fachpartner am Produkt geschult. Dabei wurde das Personal gezielt und intensiv auf die jeweilige Aufgabe vorbereitet. Besondere Eigenschaften der Zielgruppe: Kenntnis des CESTronics Produkts und Erfahrung im Umgang mit diesen Produkten (Montage, Bedienung usw.)

2 Zu Ihrer Sicherheit

2.1 Sicherheitshinweise

Das in diesem Handbuch beschriebene Zutrittskontroll-System AccessOne darf nur von Personen betrieben werden, welche für diese Aufgabenstellungen befähigt und qualifiziert sind. Qualifiziertes Personal verfügt über langjährige Berufserfahrung im Bereich IT-Strukturen, Administration und Netzwerken und kann aufgrund seiner Erfahrung in der Verwaltung von Schließanlagen bzw. durch die tiefe Kenntnis einer einzelnen Schließanlage Risiken erkennen und mögliche Gefährdungen vermeiden.



Verspernte Tür verhindert Hilfe oder führt zu Sachschäden

Fehlerhaft programmierte Komponenten können zu einem ungewollt versperrten Zugang führen. Wenn in der Folge einer versperrten Tür der Zugang zu hilfsbedürftigen Personen nicht möglich ist oder zu Sachschäden oder anderen Schäden führt, haftet die C.Ed. Schulte Zylinderschlossfabrik GmbH dafür nicht!

2.2 Rechtliche Hinweise

Der Käufer wird hiermit ausdrücklich darauf hingewiesen, dass der Einsatz des Zutrittskontroll-Systems AccessOne gesetzlichen, und hier im Besonderen datenschutzrechtlichen Genehmigungspflichten und Mitbestimmungsrechten der Belegschaft unterliegen kann. Käufer und Endnutzer sind verantwortlich für den rechtskonformen Einsatz des Produkts.

2.3 Systemvoraussetzungen

Die Mindest-Systemvoraussetzungen für die AccessOne lehnen sich an die empfohlenen Systemvoraussetzungen für den Microsoft SQL-Server an.

- Betriebssystem (Server): ab Windows Server 2016
- Betriebssystem (PC): ab Windows 10 Professional
- Arbeitsspeicher: mind. 8GB
- SQL-Server: ab MS SQL Server 2016, Expressvariante nutzbar
- Festplatte: mind. 1x 500GB, 2x 500GB empfohlen
- Netzwerkkarte

2.4 Datenschutz in der AccessOne

Einhaltung der Löschfristen

Die AccessOne verfügt über einen parametrierbaren Löschprozess, der täglich kurz nach Mitternacht startet und Daten, deren Aufbewahrungszeit abgelaufen ist, aus dem System entfernt. Dies beinhaltet insbesondere die Bewegungsdaten. Die Parameter sind vom Nutzer des Systems einstellbar.



Zur Erfüllung der DSGVO kann die Löschung personenbezogener Logbuch-Meldungen konfiguriert werden. Mit dem Parameter ‚LogbookRewriteOffset‘ wird die Anzahl der Tage eingestellt, nach der dies erfolgen soll.

Parameter	Beschreibung	Standardeinstellung
DateDeletedOffset	Verzögerung, nach der Personen-Datensätze mit eingetragenem ‚dateDeleted‘ - Datum endgültig aus der Datenbank gelöscht werden.	3 Tage
VistorDeleteOffset	Verzögerung nach der Besucher gelöscht werden.	183 Tage
EventDeleteOffset	Verzögerung nach der behandelte Events entfernt werden.	183 Tage
AppointmentDelOffset	Anzahl Tage nach der Besuchstermine und alle abhängigen Daten gelöscht werden.	365 Tage
LogbookRewriteOffset	Anzahl Tage nach der personenbezogene Logbuch-Meldungen aus Logbüchern gelöscht werden.	0 (keine Löschung)
LogbookDelMessages	Die Nummern der personenbezogenen Logbuch-Meldungen die gelöscht werden sollen. Es können einzelne Nummern und Nummernbereiche angegeben werden.	alle Begehungsmeldungen
LogbookLastRunTime	Datum an dem die letzte erfolgreiche Ausführung des Löschmodus erfolgte.	Datum der letzten Ausführung

Datenminimierung

Welche Daten für den Betrieb und die Aufgaben notwendig sind, legt der Nutzer fest. Für den täglichen Einsatz der AccessOne sind pro Person nur der Nachname und eine Personalkennung (Eigen/Fremd/Besucher) notwendig. Der Nachname muss nicht der tatsächliche Name des Ausweisträgers sein. Es kann auch ein pseudonymisierter Name (z.B.: „MA_001“) verwendet werden. In der Regel ist die Verwendung des Namens, bezogen auf die DSGVO, als unkritisch zu bewerten.

Eingabekontrolle

Die AccessOne protokolliert jede Datenänderung mit Arbeitsstation, Benutzer und Zeitstempel sowie altem und neuem Wert des entsprechenden Datenfelds.

Zutrittskontrolle – Zugriffskontrolle – Zugangskontrolle

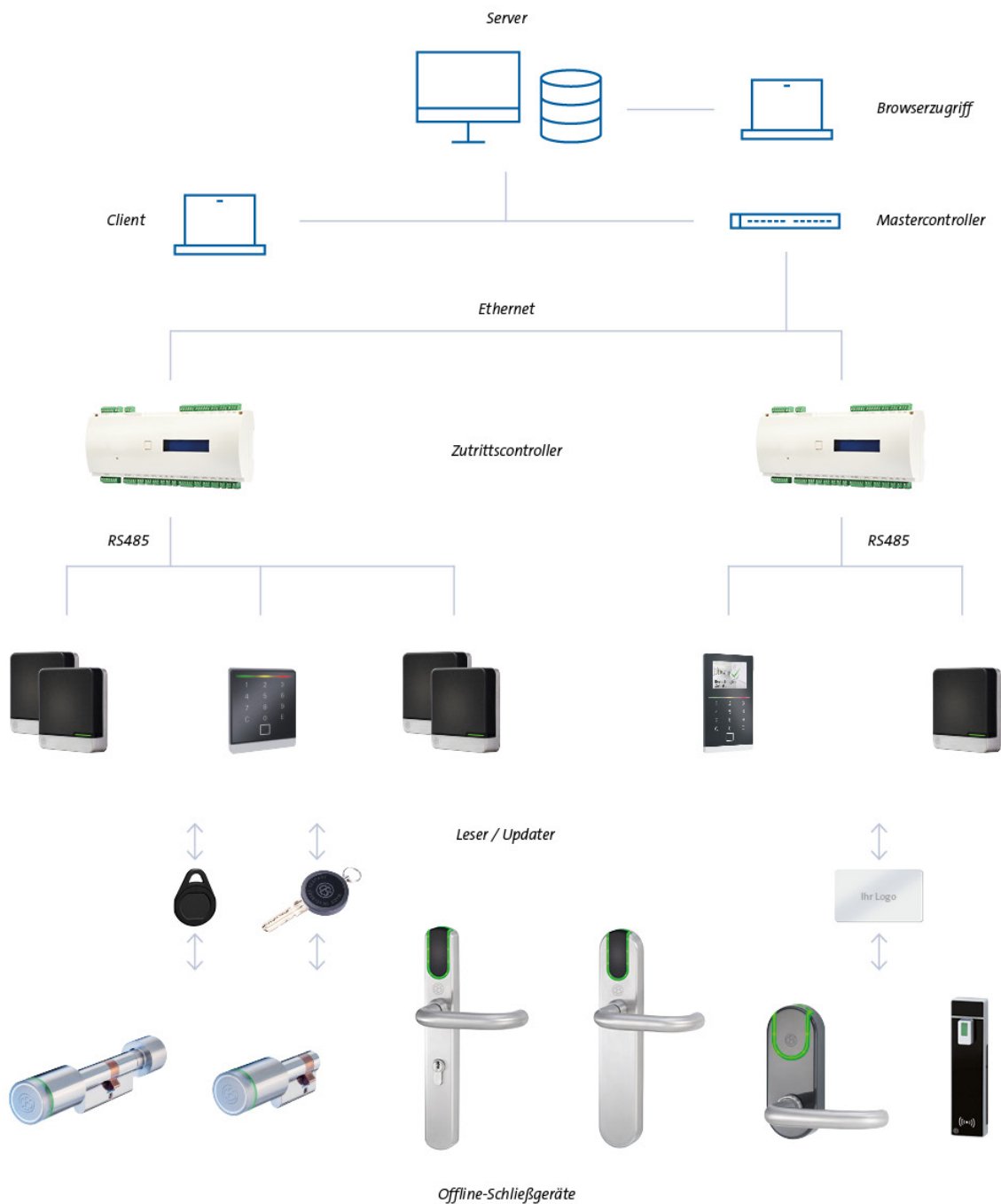
Als Zutritt gilt nach DIN EN 50133-1 der Vorgang des Betretens oder Verlassens eines Sicherheitsbereiches. Die Steuerung und Regelung erfolgt durch die AccessOne. Der Zugriff bezeichnet die logische Benutzung von Daten in Rechnern im Sinne von Lesen, Schreiben, Ändern und Löschen. Der Zugang ist die logische Einleitung der Nutzung eines Informationssystems oder Kommunikationsnetzes. Die Zugangskontrolle ist dementsprechend die maschinelle Prüfung der Zugangsberechtigung zu einem Informationssystem oder Netz.

Für die Überwachung und Kontrolle sind entsprechende technisch-organisatorische Maßnahmen vom Auftraggeber durch die Einrichtung bzw. Vorhaltung der IT-Infrastruktur zu erfüllen (USB-Port, Passwort-Richtlinien, LDAP etc.). Die AccessOne unterstützt dies durch die Möglichkeit entsprechender Zuordnungen von Benutzerrechten in der Bedienoberfläche.

3 Über AccessOne

Das Zutrittskontrollsystem AccessOne ist in der Vollversion eine flexibel skalierbare Zutrittskontroll-Management-Software für große Anlagen mit bis zu 200.000 Nutzern, 16.000 Ausweislesern und bis zu 100.000 Offline Schließgeräten. Eine Version für kleine und mittelständische Unternehmen steht mit der Lizenz AccessOne KMU zur Verfügung.

Das Zutrittskontrollsystem steuert Türen, Schranken und andere Sperrvorrichtungen. Kern der Software ist eine Benutzer- und Berechtigungsverwaltung, die alle Aktivitäten an den angeschlossenen Geräten protokolliert und laufende Prozesse überwacht. Die AccessOne ist als offenes System konzipiert und kann sowohl Online als auch Offline Geräte verwalten und steuern. Die Kommunikation ist mit 128 Bit AES Ende zu Ende verschlüsselt. Optionale USV- und Server-Redundanz-Konzepte stehen für eine hohe Ausfall- und Systemsicherheit.



3.1 Funktions-Erweiterungen

Für die AccessOne in der Basis-Lizenz sind folgende Funktions-Erweiterungen erhältlich:

Ausweiserstellung Art.-Nr. 348120V	Erweiterung der AccessOne um die Möglichkeit ein eigenes Kartenlayout mit einem grafischen Editor zu gestalten.
Mandantenfunktion Art.-Nr. 348121V	Die Mandantenfunktion erlaubt die logische Zuordnung von definierten Teilen des Systems wie Türen und Personen, zu verschiedenen, unabhängigen Mandanten. Diese Mandanten können die ihnen zugeordneten Systemteile eigenständig verwalten, haben aber keinen Einfluss auf die Systemteile eines anderen Mandanten. Es besteht aber die Möglichkeit, dass Systemteile, wie z.B. Eingangstüren, gemeinsam genutzt werden.
Besucherverwaltung Art.-Nr. 348122V	Erweitert die AccessOne um die Möglichkeit Besucher im System anzumelden sowie die Ausgabe von Tagesausweisen mit eingeschränkten Zutrittsmöglichkeiten. Die Anmeldung erfolgt über einen Web-Browser.
Parkbereichsverwaltung Art.-Nr. 348123V	Erweitert die AccessOne um die Möglichkeit Parkbereiche zu verwalten. Bestimmten Mietern können eine Anzahl „n“ Mietflächen gewiesen werden, während die restlichen Stellplätze gezählt aber für alle anderen, berechtigten Nutzer zur Verfügung stehen. Für die Nutzung dieser Funktion ist eine Zählung über Ein- und Ausfahrtsleser zwingend notwendig.
Zeiterfassung Art.-Nr. 348124V	Erweitert die AccessOne um die Möglichkeit an Zutrittslesern und / oder separaten Zeiterfassungs-Lesern Kommen-und Gehen-Buchungen zu erzeugen und diese täglich im CSV Format einem übergeordneten Arbeitszeitmanagementsystem bereit zu stellen.
Serverredundanz Art.-Nr. 348125V	Erweitert die AccessOne um eine Hot-Standby-Funktion.
Fremdfirmenverwaltung Art.-Nr. 348126V	Erweitert die AccessOne um ein Modul, zur Verwaltung von Stammdaten von Mitarbeitern von Fremdfirmen, ohne auf die Stammdaten von Eigenpersonal zuzugreifen. Das Modul gestattet die Abfertigung von Handwerkern, die im Gebäude arbeiten sollen und dafür Materialien und/oder einen Ausweis benötigen. Spezielle Genehmigungen oder notwendige Unterweisungen können mit Gültigkeiten hinterlegt und geprüft werden. Der Fremdfirmen-Mitarbeiter bestätigt den Erhalt von Materialien und die Kenntnisnahme von ausgehändigten Dokumenten mit einer Unterschrift auf einem elektronischen Unterschriften Pad.

3.2 Empfohlene Vorgehensweise zur Ersteinrichtung der AccessOne

Um Ihnen als Benutzer die Eingabe von umfangreichen Daten zur erstmaligen Einrichtung der Zutrittskontroll-Anlage AccessOne zu erleichtern, empfehlen wir, die einzelnen Schritte in einer bestimmten Reihenfolge auszuführen. Dabei unterscheiden wir zwischen der System-Konfiguration der AccessOne durch den Anlagenbetreiber und/oder eine beauftragte Fachkraft aus dem Bereich IT/Administration und dem Anlegen von Geräten, Berechtigungen und Personendaten durch produktgeschultes Personal.

Die Ausführung der ersten Schritte erfolgt durch den Anlagenbetreiber und/oder eine beauftragte Fachkraft aus dem Bereich IT/Administration:

Schritt	Nr.	Tätigkeit
Konfiguration der AccessOne		Starten Sie die Anwendung und melden Sie sich als Benutzer an (siehe „5 Anmeldung“ auf Seite 16).
		Bevor Sie mit der Einrichtung Ihrer AccessOne Anlage beginnen, müssen Sie Ihre Lizenz in den System-Einstellungen aktivieren (siehe „6.1 System-Konfiguration“ auf Seite 17).
		Legen Sie nach der System-Konfiguration die verschiedenen Benutzer an, damit im Anschluss jeder AccessOne Nutzer mit seinen individuellen Vergabe-Rechten das System einrichten kann (siehe „6.2 Benutzerdaten“ auf Seite 27).
		Definieren Sie die Standortdaten Ihrer AccessOne Anlage. Dann können bei der Einrichtung der Geräte die Standortdaten direkt zugeordnet werden (siehe „6.3 Standortdaten“ auf Seite 32).

Die folgenden Schritte können von produktgeschultem Personal ausgeführt werden:

Schritt	Nr.	Tätigkeit
Geräte anlegen	1	Legen Sie zuerst ihre Online-Geräte wie Türsteuerungen und Leser an. Jeder Leser kann auch als Updater für Zutritts-Medien eingesetzt werden. Dies ist Voraussetzung für die Einrichtung der Offline-Gerät (siehe „7.1 Gerätedaten Online-Geräte“ auf Seite 34).
	2	Nachdem die Online Geräte eingerichtet sind, legen Sie die Offline Geräte an. Dieser Schritt ist die Voraussetzung dafür, dass Sie im weiteren Verlauf die Berechtigungen mit allen angelegten Geräten definieren können (siehe „Gerätedaten Offline-Geräte (OSS-SO)“ auf Seite 57).
Berechtigungsgruppen und -profile anlegen	3	Richten Sie zuerst die Berechtigungsgruppen für die Online und Offline Geräte ein (siehe „8.1 Berechtigungen“ auf Seite 61).
	4	Die Berechtigungsgruppen werden zu Berechtigungsprofilen zusammengefasst. Damit sind alle notwendigen Schritte für Ihr Berechtigungskonzept durchgeführt (siehe „8.2 Berechtigungsprofile“ auf Seite 69).
Personendaten anlegen	5	Die bereits konfigurierten Berechtigungen der Online/Offline Geräte können Sie nun den Personen direkt zuordnen (siehe „9.1 Personendaten“ auf Seite 71).
	6	Für den Druck von Ausweisen nutzen Sie den Kartendesigner. Die Kartenlayouts werden dann der Person zugeordnet (Erweiterung der AccessOne um die Möglichkeit, ein eigenes Kartenlayout mit einem grafischen Editor zu gestalten.).
	7	Sie können der Person zusätzlich eine Firma zuweisen (Erweitert die AccessOne um ein Modul, zur Verwaltung von Stammdaten von Mitarbeitern von Fremdfirmen, ohne auf die Stammdaten von Eigenpersonal zuzugreifen).
Nachträgliche Anpassungen	>	Alle angelegten Daten können bei notwendigen Änderungen auch nachträglich einfach angepasst werden (siehe „9.2 Gruppenänderungen“ auf Seite 84).

4 Allgemeine Dialoghandhabung

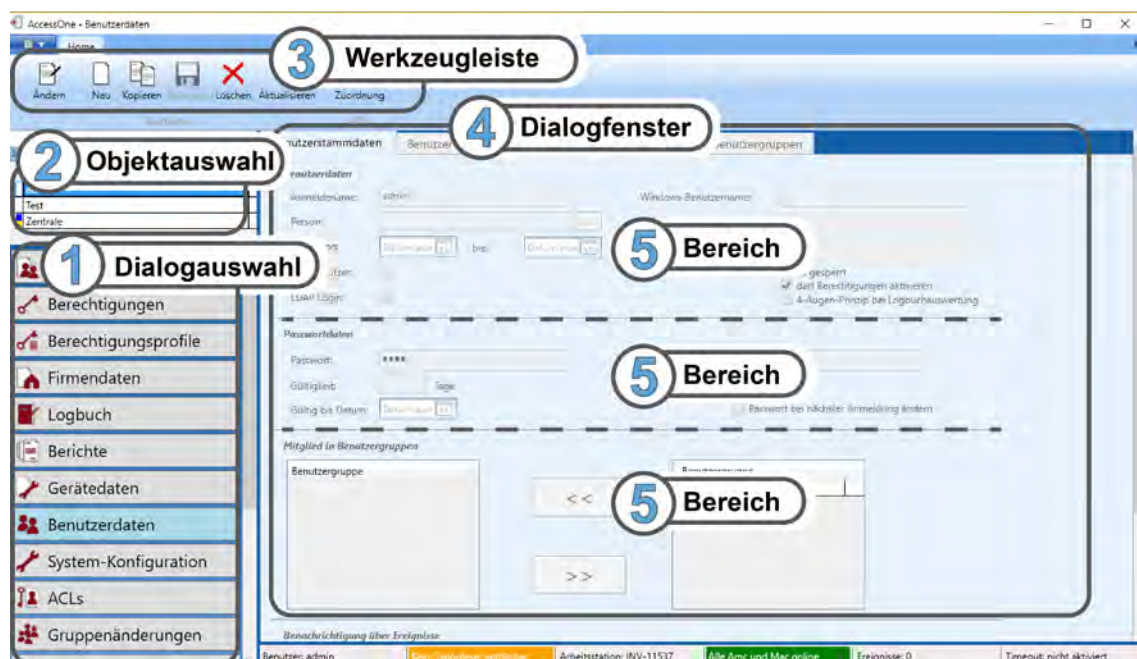
Zielgruppe dieses Kapitels:

- produktgeschultes Personal
- Fachkräfte IT/Administration
- Anlagenbetreiber

Die Bedienung der AccessOne erfolgt über eine Dialogoberfläche mit einem durchgängigen Bedienkonzept. Alle Dialoge sind nach dem gleichen Schema aufgebaut, ein neuer Benutzer findet sich schnell im System zurecht.

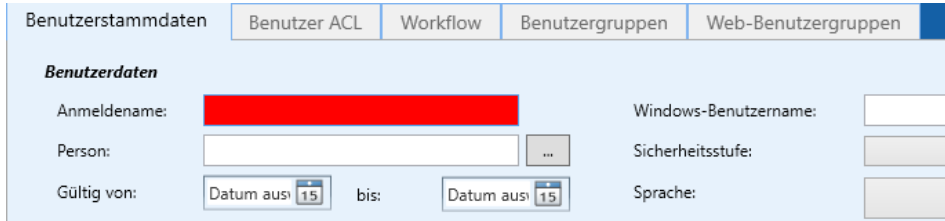
Die Bedienoberfläche ist analog zu bekannten Microsoft Office Produkten aufgebaut. Links unten sind die Schaltflächen zur Anwahl der Dialoge (1). Darüber befindet sich, abhängig vom jeweilig angewählten Dialog, eine Liste der verfügbaren Datenobjekte in der Objektauswahl (2). Wählt man einen Eintrag aus der Dialogauswahl (1), werden im Dialogfenster (4) die Details zu diesem Element auf einer Registerkarte (Tab) in einem oder mehreren Bereichen (5) angezeigt. Die Daten zu einem Datenobjekt (z. B. Personen oder Geräte) werden je nach Umfang auf mehreren Tabs zusammengefasst. Buttons in der Werkzeugleiste (3) bieten grundlegende Funktionen zum jeweils aktuellen Tab.

 Für jeden Dialog kann festgelegt werden, ob ein Nutzer Zugriff hat und mit welcher Berechtigung (Lesen – Schreiben – Löschen). Hat ein Nutzer für einen Dialog keine Berechtigung, ist die entsprechende Schaltfläche in der Oberfläche nicht sichtbar. Gleiches gilt auch für die Tab-Seiten im Dialogfenster.





Leere Pflichtfelder werden beim Speichern rot hinterlegt. Werkzeugtipps geben ergänzende Informationen zu dem zugehörigen Element, wenn die Maus darüber bewegt wird.



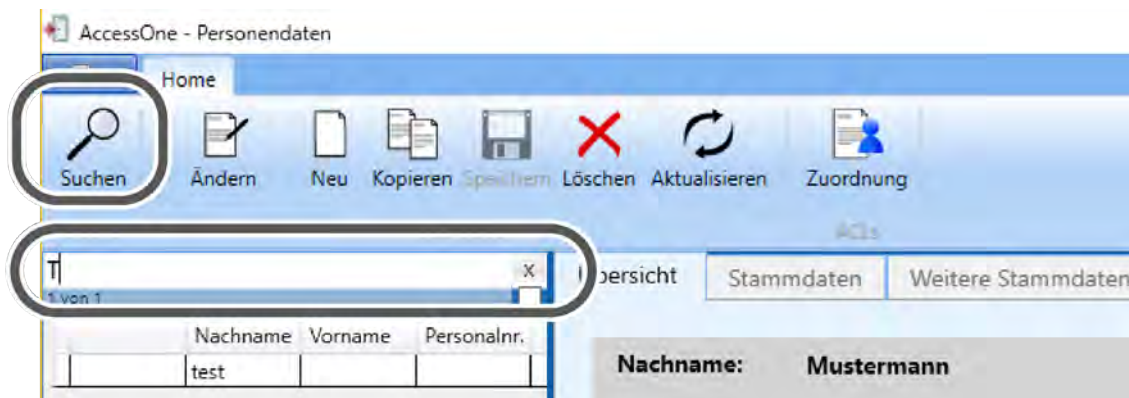
4.1 Sichtmodus – Änderungsmodus

Die AccessOne unterscheidet zwischen Sichtmodus und Änderungsmodus. Im Sichtmodus können Daten nur angesehen, aber nicht verändert werden. Die Daten sind ausgegraut. Im Änderungsmodus werden die Schaltflächen und Eingabefelder im Dialogfenster aktiviert. Im Änderungsmodus wird der ausgewählte Datensatz intern für alle anderen Dialogbenutzer gesperrt.

4.2 Werkzeugleiste

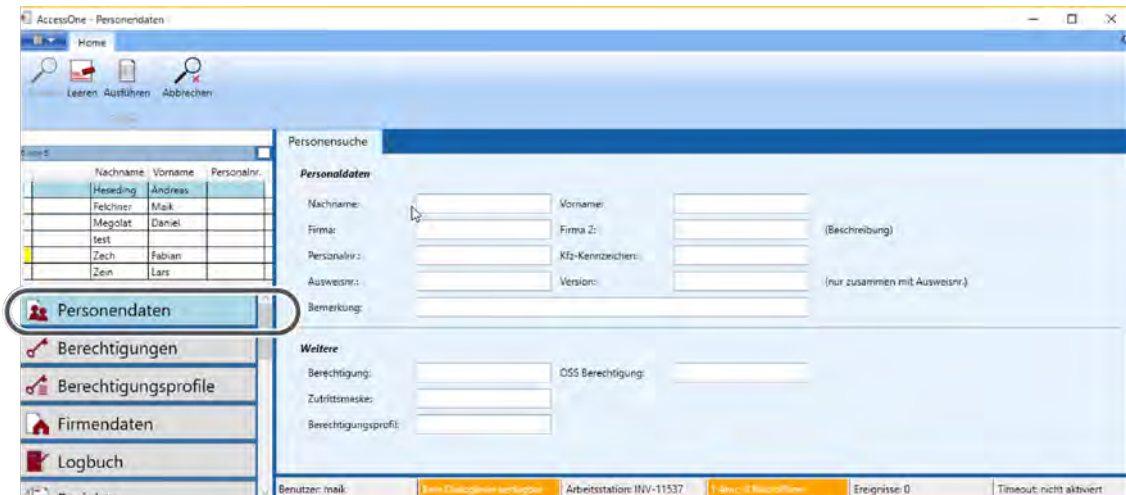
Suchen

Über der Objektauswahl auf der linken Seite befindet sich in der Werkzeugleiste das Eingabefeld für die Suche.



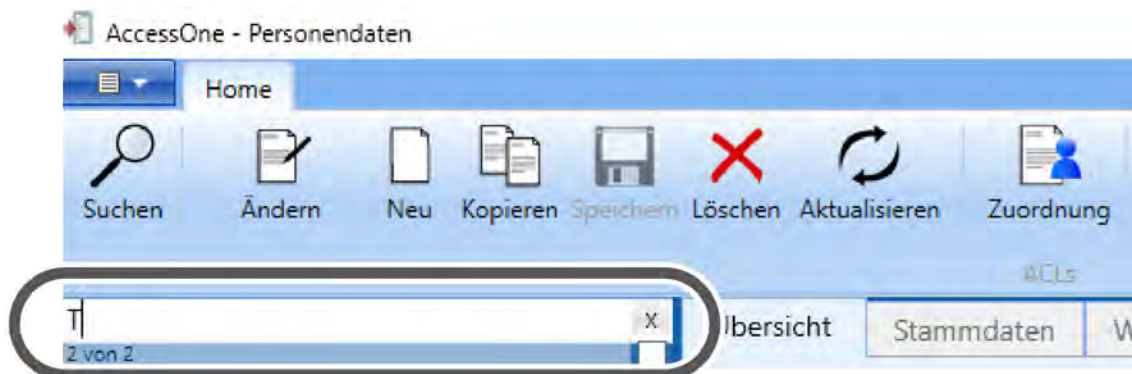
Der Button SUCHEN in der Menüleiste ist nur aktiv, wenn der Dialog „Personendaten“ gewählt wird.

Klicken auf den Button SUCHEN öffnet im Dialogfenster den Tab „Personensuche“. Hier stehen weitere Suchkriterien zur Verfügung (z.B. Name, Vorname, Firma, Personalnummer, Berechtigung, Berechtigungsprofil, Ausweisnummer). Die Auswahlliste im Eingabefeld aktualisiert sich mit jedem eingegebenen Zeichen.



Für den Tab „Personensuche“ stehen nur die Schaltflächen LEEREN, AUSFÜHREN und ABBRECHEN der Suche zur Verfügung.

Ein Klick auf AUSFÜHREN aktualisiert die gefilterte Auswahlliste. Datensätze können einzeln angewählt und bearbeitet werden. Die Suchbegriffe bleiben aktiv bis ABBRECHEN angeklickt wird. Haben Sie also z. B. im Suchen-Dialog eine Firma vorgewählt, werden in der Auswahlliste nur Personen dieser Firma angezeigt, unabhängig davon, welche zusätzlichen Eingaben Sie im Suchfeld über der Auswahlliste vornehmen. Erst durch erneutes Anwählen des Suchen-Dialogs und anschließendes Abbrechen der Suche wird dieses Suchkriterium wieder gelöscht. LEEREN löscht den Inhalt des Suchen-Dialogs und Sie können neue Suchkriterien eingeben.



Im Beispiel hier gibt es genau 2 Datensätze, deren Anfangsbuchstabe mit „T“ beginnt. Gibt man z. B. kein Suchkriterium an, so ist die Anzeige auf maximal 150 Einträge begrenzt. Dieser Wert ist über die Systemparameter der AccessOne einstellbar. Sie können über die kleine Schaltfläche in der rechten unteren Ecke des Suchfensters die Einschränkung kurzfristig ausschalten. Dann werden alle zum Suchkriterium passenden Datensätze in die Auswahlliste geladen. Wenn Sie keinen Suchbegriff eingeben, werden alle in der Datenbank vorhandenen Datensätze geladen.

Ändern

Klicken auf ÄNDERN oder Doppelklick auf den Datensatz in der Auswahlliste aktiviert die Eingabefelder und Schaltflächen im Dialogfenster auf der rechten Seite. Der ausgewählte Datensatz wird intern für alle anderen Dialogbenutzer gesperrt.

Neu

Legt einen neuen, leeren Datensatz an.

Kopieren

Dupliziert einen vorhandenen Datensatz. Felder, die pro Datensatz eindeutig sein müssen, werden automatisch geleert.

Speichern

Speichert und aktualisiert den Datensatz in der Datenbank. Anschließend ist der Datensatz wieder für Änderungen durch andere Dialogbenutzer freigegeben.



Der aktuelle Dialog wird automatisch gespeichert, sobald Sie die Dialogseite verlassen.

Löschen

Löscht angewählten Datensatz (blau hinterlegt). Nach Bestätigung einer Sicherheitsabfrage wird die Aktion ausgeführt.

Aktualisieren

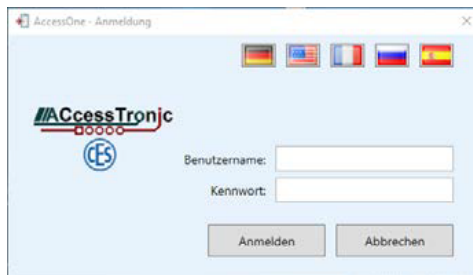
Lädt aktuelle Daten aus der Datenbank und aktualisiert die Ansicht.

Zuordnung

Weist den aktuellen Datensatz einem Mandanten zu. Nur aktiv, wenn Mandantenfähigkeit aktiviert ist.

5 Anmeldung

Nachdem die Software erfolgreich installiert wurde, melden Sie sich als Benutzer an. Mit einem Doppelklick auf das Symbol, welches die Installation automatisch auf Ihrem Desktop anlegt, starten Sie das Programm.

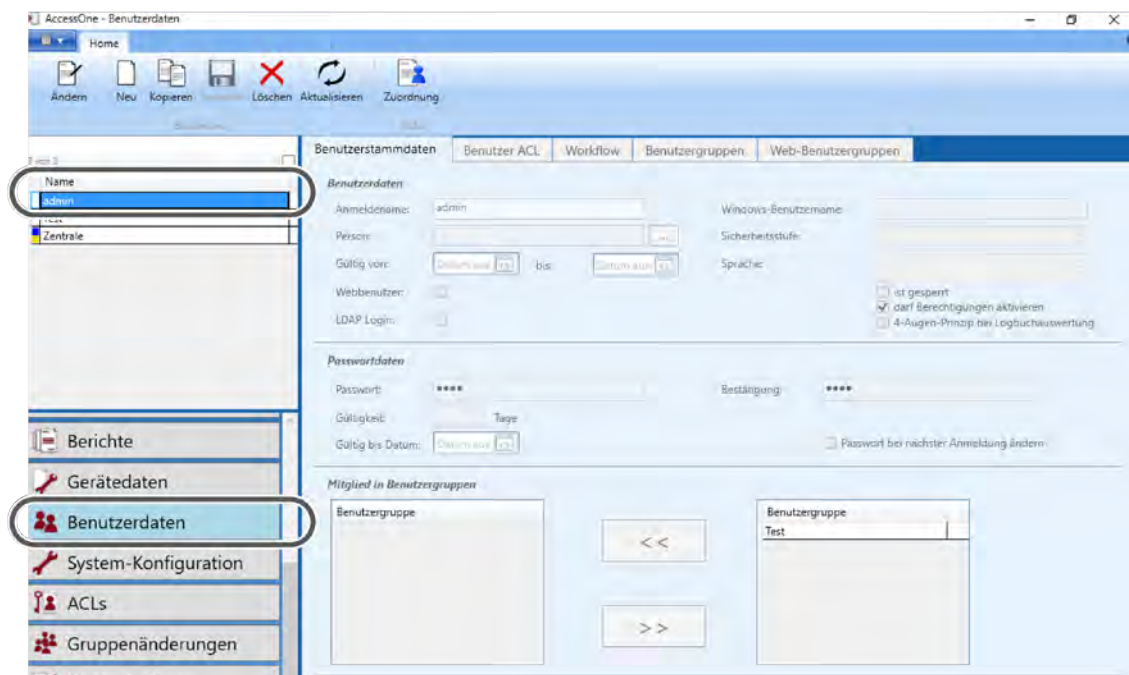


Für die erste Anmeldung nach der Installation, sind folgende Login-Daten voreingestellt:

Benutzername: admin

Kennwort: admin

Ändern Sie das Passwort aus Sicherheitsgründen direkt nach der Eingabe. Gehen Sie dafür in den Dialog „Benutzerdaten“.



Wählen Sie in der Objektauswahl den Anmeldennamen „admin“ und klicken Sie danach in der Werkzeugleiste oben links im Fenster auf den Button ÄNDERN. Vergeben Sie ein eigenes Passwort. Besonders sicher ist ein möglichst langes, aus Buchstaben und Ziffern bestehendes Passwort. Die Länge des Passworts ist frei wählbar. Wiederholen Sie zum Abgleich das Passwort nochmals im Feld „Bestätigung“.

Möchten Sie ein Passwort mit begrenzter Gültigkeit vergeben, haben Sie an dieser Stelle die Möglichkeit dazu. Bestätigen Sie Ihre Änderung mit dem Button SPEICHERN.

An späterer Stelle im Handbuch wird das Anlegen weiterer Nutzer ausführlich beschrieben (siehe „6.2 Benutzerdaten“ auf Seite 27).

6 Konfiguration der AccessOne

Zielgruppe dieses Kapitels:

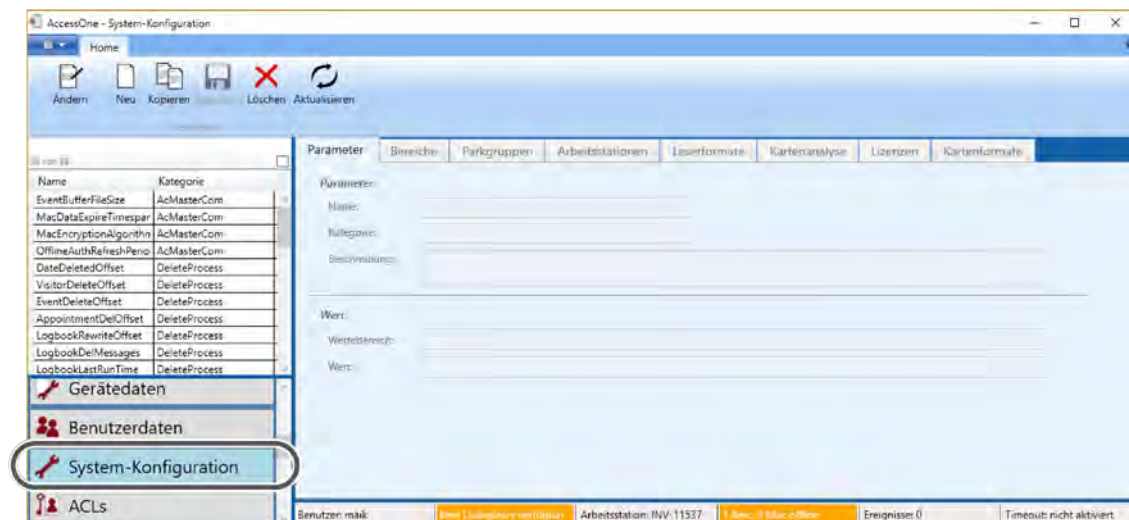
- Fachkräfte IT/Administration
- Anlagenbetreiber

Um die Voraussetzungen für die Einrichtung der Zutrittskontroll-Anlage zu schaffen, müssen Sie einige Systemparameter anpassen. Sie legen Bereiche fest und richten Arbeitsstationen ein. Darüber hinaus definieren Sie verwendete Leser- und Kartenformate. Mit der Eingabe der Benutzer- und Standortdaten schaffen Sie die Voraussetzungen für die Konfiguration der Geräte und Berechtigungen.

6.1 System-Konfiguration

6.1.1 Parameter

Zeigt die Systemparameter für Ihr System an.

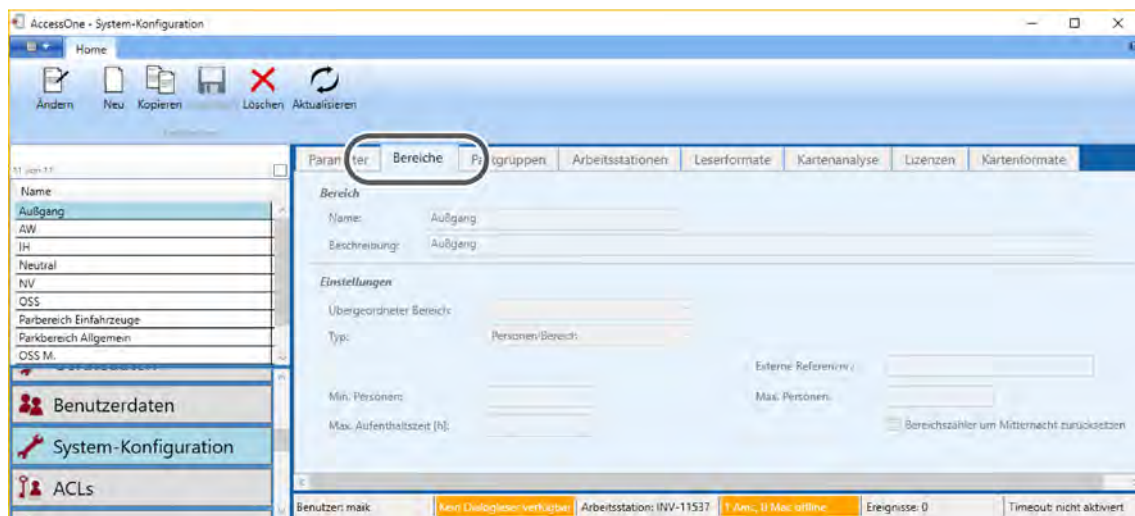


Erläuterungen der Parameter

Name	Übersetzung	Erläuterung
EventBufferFileSize	Dateipuffergröße	Dateipuffergröße (MB), um Ereignisse für einen einzelnen MAC zu speichern.
MacDataExpireTimespan	Datenablaufzeit	Zeit in Minuten ohne Verbindung zum MAC, nach dem die Event-Buffer-Daten ungültig werden.
MacEncryptionAlgorithm	Verschlüsselungsalgorithmus	Verschlüsselungsalgorithmus für die Kommunikation zwischen AccessOne und MACs (Voreinstellung: Keine).
DateDeletedOffset	Datensätze löschen	Zeit in Tagen nach der Personen-Datensätze nach einer Löschung im Dialog endgültig aus der Datenbank gelöscht werden.
EventDeleteOffset	Ereignisse löschen	Anzahl der Tage nach der Ereignisse aus der Datenbank gelöscht werden.
VisitorDeleteOffset	Besucher löschen	Anzahl der Tage nach der gelöschte Besucher aus der Datenbank gelöscht werden.
LastRunTime (LastAccessProcess)	Letzte Prozessausführung	Zeitpunkt der letzten Prozessausführung

Name	Übersetzung	Erläuterung
LastRunTime (LockProcess)	Letzte Prozessausführung	Zeitpunkt der letzten Prozessausführung
CardNoRecycling	Kartennummern wiederverwenden	1= Wiederverwenden von Kartennummern, indem nach Lücken durch gelöschte Karten gesucht wird. 0 = Kartennummern fortlaufend vergeben.
DatabaseNumber	Datenbanknummer	Kennung im Datensatz beim Vorhandensein mehrerer Datenbanken (bisher 00)
LockingTimeout	Datensatzsperrzeit	Zeit in Sekunden für die Sperrung von Datensätzen in Bearbeitung. Falls innerhalb dieser Zeit die Sperre durch den Client nicht erneuert wird, wird die Sperrung vom Masterprozess aufgehoben.
LogonTimeout	Zeitspanne Anmeldeerneuerung	Zeit in Sekunden innerhalb der ein Client seinen Log-On beim Master erneuern muss, bevor er automatisch angemeldet wird.
NumberLogonFailures	Anzahl Fehlanmeldungen	Max. Anzahl der Anmeldefehlversuche
ProcessLogfileAge	Alter der Debug-Logfiles	Max. Alter in Tagen der Debug-Logfiles
ProcessLogfileSize	Größe der Debug-Logfiles	Max. Größe in MB der Debug-Logfiles
XmlDoorDataDir	Türdaten-Verzeichnis	Verzeichnis für den OSS-Türdatenaustausch
CardNoZeroes	Kartennummern	Auffüllen gedruckter Kartennummern mit Nullen bis zur angegebenen Gesamtlänge.
CardToCodeAlgorithm	Code-Algorithmus	Algorithmus zur Bestimmung von Kartennummern aus den Codedaten. Standard: 0 = Kartennummer entspricht Codedaten.
DialogTimeout	Dialogzeitüberschreitung	Standard-Timeout in Sekunden für die Nicht-Verwendung eines Dialogs. Bei Überschreitung dieser Zeit wird der Benutzer automatisch abgemeldet.
EntitiesToTake	Entitäten	Anzahl der in der Auswahlliste angezeigten Datensätze.
MaxPinLength	Maximale PIN-Länge	Max. Länge der Pins (PIN, EMA1, EMA2)
MaxPinValidity	Maximale PIN-Gültigkeit	Max. Gültigkeit der Pins in Tagen
OfflineValidityTime	Offline-Gültigkeitszeit	Standardgültigkeit eines Offlineausweises in Stunden, Minuten (Standard: 24,0).

6.1.2 Bereiche



Jede Tür in der AccessOne führt von einem Quell-Bereich in einen Ziel-Bereich. Diese Bereiche müssen nicht zwingend unterschiedlich sein. Wenn Ihr Gebäude in mehrere Sicherungsbereiche aufgeteilt ist, könnte z. B. ein Eingang vom äußeren Sicherungsbereich (ASB) in den inneren Sicherungsbereich (ISB) führen. Eine Zwischentür kann aber auch von ISB nach ISB führen.

Mit „Ort Eingang“ und „Ort Ausgang“, wählen Sie den Quell- und Zielbereich aus.

Einstellungen

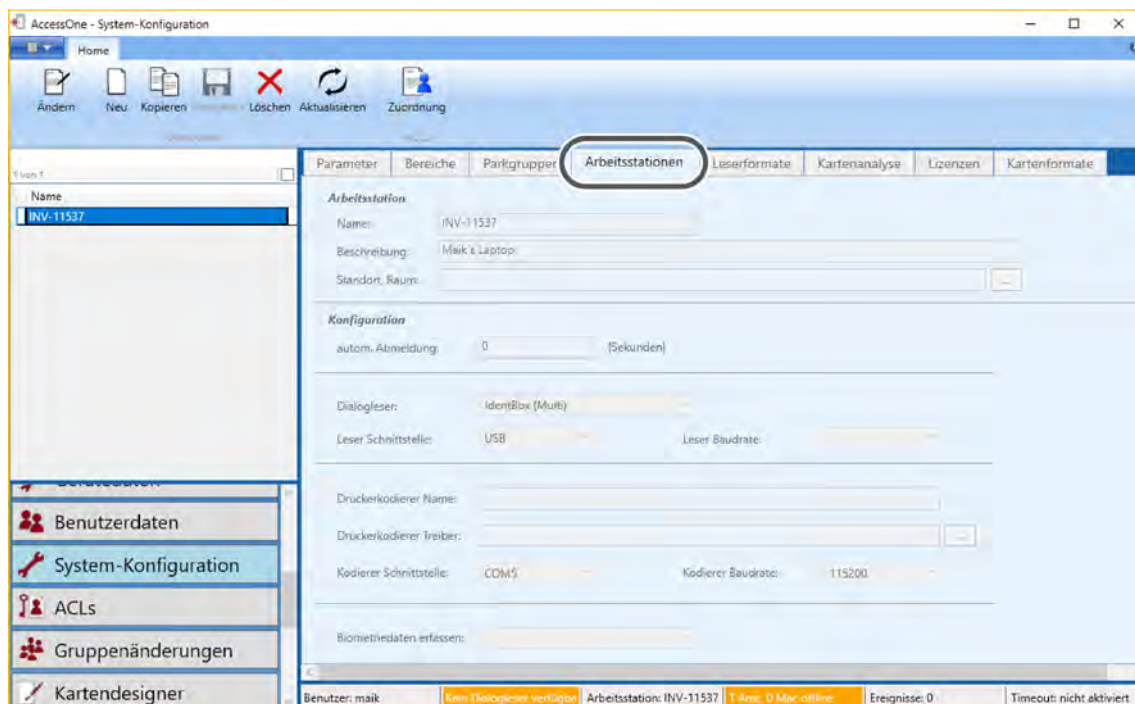
Unter „Einstellungen“ kann ein Bereich weiter unterteilt werden. Bei „Normaler Bereich“ ist die Vorgabe einer minimal und maximal erlaubten Personenzahl innerhalb des Bereiches möglich. Für einen „Parkbereich“ kann z. B. die Anzahl der maximalen verfügbaren Stellplätze angegeben werden.

6.1.3 Parkgruppen

(Nur aktiv bei Verwendung des Zusatzmoduls Parkbereichsverwaltung, Art.-Nr. 348123V)

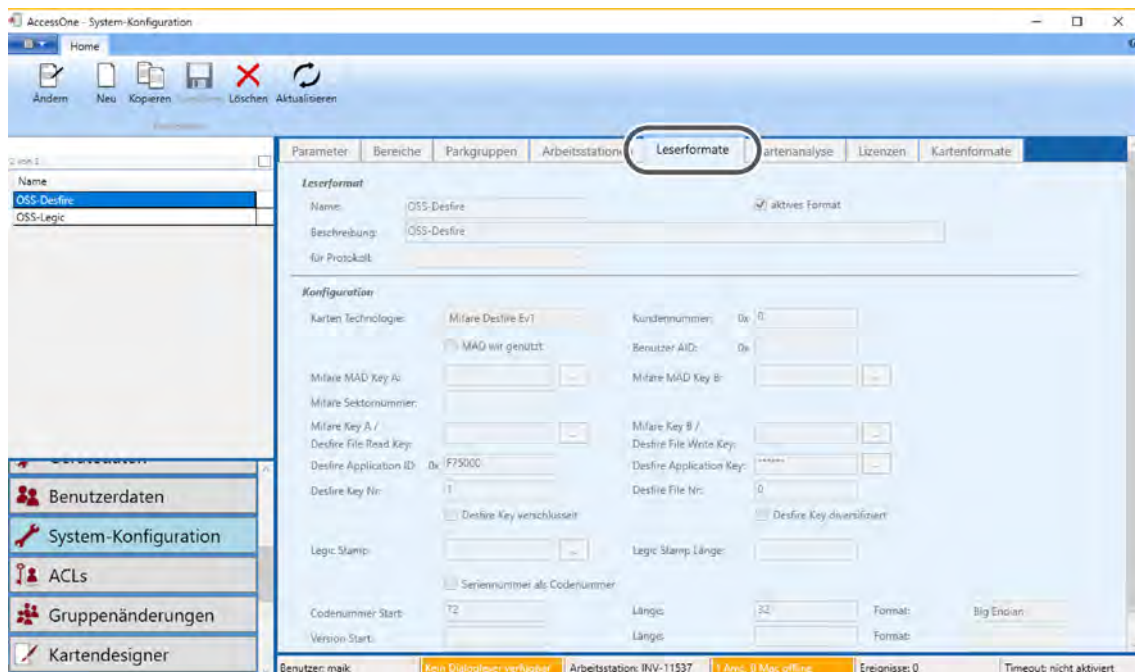
Bietet die Möglichkeit, Personen zu einer Parkgruppe zusammenzufassen. Diese können dann einem bestimmten Parkbereich zugeordnet werden.

6.1.4 Arbeitsstationen



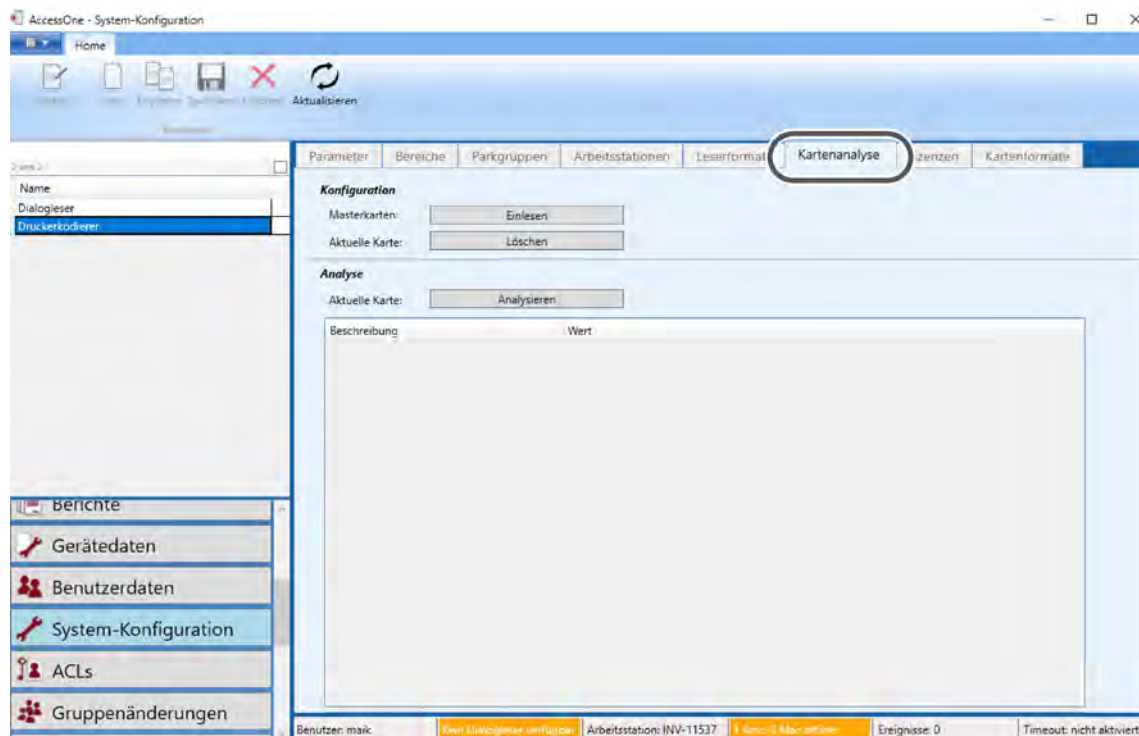
Im Tab „Arbeitsstationen“ werden die jeweiligen AccessOne Clients mit ihren exakten Windows-Computernamen angelegt. Hier wird lokal für die jeweilige Arbeitsstation festgelegt, ob ein Dialogleser (z. B. eine Identbox) oder ein Kartendrucker mit Codierstation installiert ist. Für das Endgerät müssen die jeweils richtigen ComPorts eingestellt werden. Die ComPorts können Sie in Ihrem Windows Gerätemanager ablesen.

6.1.5 Leserformate



Hier stellen Sie die Leserformate ein, die vom Kartenleser des Türcontrollers gelesen werden sollen.

6.1.6 Kartenanalyse

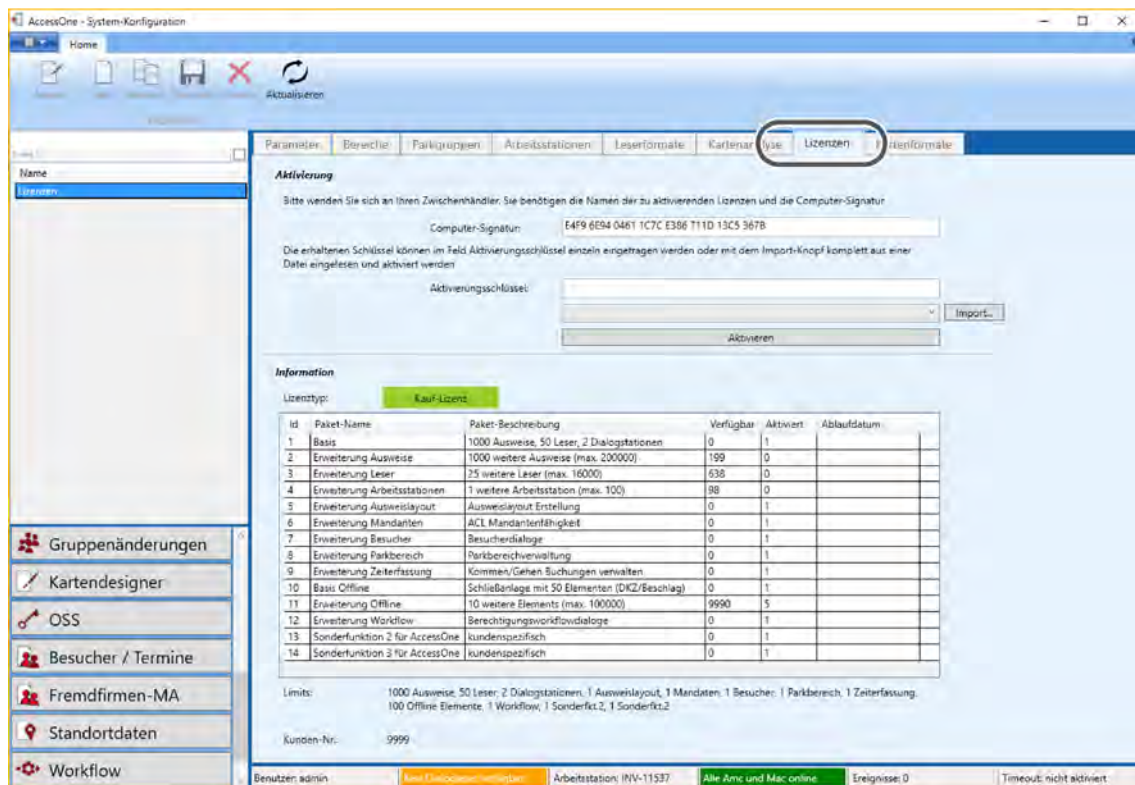


Im Tab „Kartenanalyse“ können Masterkarten (z.B. LEGIC, IAM Karten), die für die Nutzung der Schreibfunktion Ihres Dialoglesers (Identbox) wichtig sind, eingelesen oder gelöscht werden.

Über die Schaltfläche Analysieren werden über den angeschlossenen Dialogleser Transponderkarten eines zuvor angelegten Kartenformats im Detail ausgelesen.

Im Bereich „Ersatzausweise“ kann eine definierte Menge von Ersatzausweisen im entsprechenden Kartennummernbereich in der Datenbank angelegt werden.

6.1.7 Lizenzen



Der Tab „Lizenzen“ zeigt eine Auflistung der jeweiligen Programmlizenzen und deren Inhalte an.



Für die Lizenzfreischaltung wird die Computer-Signatur Ihres AccessOne Server PCs benötigt. Ohne Lizenzfreischaltung ist Ihre AccessOne Installation nur als Demo Lizenz mit Einschränkungen zu verwenden.

Es gibt drei Lizenztypen:

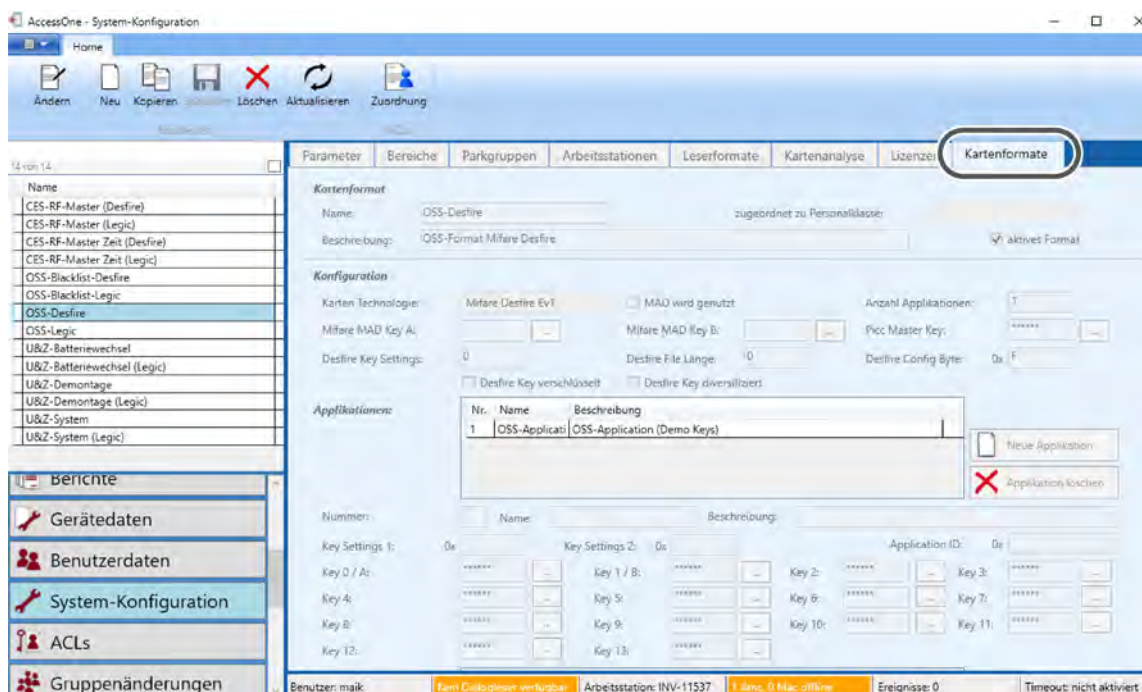
- Eine Test-Lizenz mit minimalem Systemumfang, die direkt nach der Installation der AccessOne Software aktiv ist.
- Eine Demo-Lizenz, die zeitlich befristet ist und nach Kundenwünschen erstellt wird. Dieser Lizenztyp kann zweimal erneuert werden. Nach Ablauf dieses Zeitraums wird aus der Demo-Lizenz automatisch eine „Test-Lizenz“.
- Die Kauf-Lizenz bietet alle Standardfunktionen.

6.1.8 Kartenformate

Im Tab „Kartenformate“ werden die Formate definiert, die zum Beschreiben einer Karte an einem Dialogleser, Kodierstation ggf. im Kartendrucker oder eines ZK-Wandlers (Updater für Zutritts-Medien) benötigt werden. Es darf je Kartentechnologie (Mifare, LEGIC etc.) nur ein Kartenformat aktiv sein. Es können aber durchaus mehrere inaktive Kartenformate der selben Kartentechnologie angelegt sein.



Die Definition eines Kartenformates setzt voraus, dass der AccessOne Nutzer mit den möglichen Einstellungen der jeweiligen Kartentechnologie vertraut ist. Da speziell Mifare-DESFire dem Nutzer sehr viele Freiheiten in der Definition von Zugriffsrechten lässt, können dadurch auch Karten erzeugt werden, die nicht mehr brauchbar sind, wenn die Einstellungen widersprüchlich sind. Der folgende Text gibt Hinweise, welche Parameter auf welche Eigenschaften der Karte Einfluss haben. Er ersetzt jedoch nicht die Lektüre der entsprechenden NXP und LEGIC Dokumentation.



Die Parameter werden auf verschiedenen Strukturebenen angelegt:

- Parameter auf Kartenebene
- Parameter auf Applikationsebene
- Parameter auf File-Ebene

6.1.8.1 Parameter auf Kartenebene

Beim Anlegen einer neuen Karte wird zuerst der PICC-Masterkey vom Standardwert auf den hier definierten Wert durchgeführt. Danach werden die Eigenschaften, die sich auf die Verwendung dieses PICC-Masterkeys beziehen, eingestellt. Die Einstellungen werden im Wert von „Desfire Config Byte“ hinterlegt.

Der Wert ist Bit-codiert und ist wie folgt zu interpretieren:

Bit 4 bis 7 müssen 0 sein.

Bit 3 legt fest, ob diese Konfiguration jemals wieder geändert werden darf (auch nicht durch Formatieren der Karte).

- 0: die Konfiguration darf nie mehr geändert werden,
- 1: die Konfiguration darf geändert werden, wenn man sich vorher mit dem PICC Masterkey authentifiziert hat.

Bit 2 legt fest, ob zum Anlegen oder Löschen einer Applikation der PICC-Masterkey erforderlich ist oder nicht.

- 0: Anlegen und Löschen einer App funktioniert nur mit PICC-Masterkey,
- 1: Anlegen geht ohne, Löschen einer App geht mit PICC-Masterkey oder Application Master Key.

Bit 1 legt fest, ob zum Abfragen des Inhaltsverzeichnisses der Karte der PICC-Masterkey erforderlich ist oder nicht.

- 0: Abfragen funktioniert nur mit PICC-Masterkey,
- 1: Abfragen benötigt keinen PICC-Masterkey.



Der PICC-Masterkey sollte nicht weitergegeben werden. Wenn Sie Dritten erlauben wollen, eigene Applikationen anzulegen, wäre für das „Desfire Config Byte“ z. B. 0x0f eine sinnvolle Einstellung. Mit dieser Definition müssen Sie den PICC-Masterkey nicht weitergeben.

6.1.8.2 Parameter auf Applikationsebene

Nach DESFire Standard ist der Key 0 immer der Application Masterkey (APMK). Alle weiteren Keys können, müssen aber nicht definiert werden. Es empfiehlt sich, mindestens einen zusätzlichen Key zu definieren, um evtl. Dritten Zugriff zu geben, ohne den APMK weitergeben zu müssen.

Key settings 1 legt fest, was über den Application Masterkey kontrolliert wird. 0xE1 wäre z. B. ein sinnvoller Wert.

Einstellungen der Anwendung des APMK:

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Ändern der Schlüsselzugriffsrechte				Konfiguration veränderbar	freies Erstellen/ Löschen ohne APMK	freier Zugriff auf Verzeichnisse ohne APMK	Änderung des APMK zulassen
Bit3	Bit2	Bit1	Bit0				

Auf Anwendungsebene wird die Kodierung interpretiert als (die ausgewählte AID ist nicht 0x00):

Bit 7 – Bit 4 Bestimmen Sie die Zugriffsrechte für das Ändern von Applikationsschlüsseln (Befehl ChangeKey).

0x0: Die Authentifizierung des APMK ist erforderlich, um jeden beliebigen Schlüssel zu ändern (Standard).

0x1...0xD: Die Authentifizierung mit dem angegebenen Schlüssel ist notwendig, um jeden beliebigen Schlüssel zu ändern. Ein Änderungsschlüssel und ein PICC-Master Key können nur nach Authentifizierung mit dem APMK geändert werden. Für andere Schlüssel wird eine Authentifizierung mit demselben Schlüssel benötigt.

0xE: Die Authentifizierung mit dem zu ändernden Schlüssel (gleiche KeyNo) ist notwendig, um einen Schlüssel zu ändern.

0xF: Alle Schlüssel (außer APMK, siehe Bit 0) innerhalb dieser Anwendung sind eingefroren.

Bit 3 Gibt an, ob eine Änderung der Einstellungen des APMK zulässig ist:

0: Konfiguration ist nicht mehr änderbar (eingefroren)

1: Diese Konfiguration kann geändert werden, wenn mit dem APMK authentifiziert wird (Standardeinstellung).

- Bit 2** Gibt an, ob die Authentifizierung des APMK vor CreateFile/DeleteFile erforderlich ist.
 0: CreateFile / DeleteFile ist nur mit der Authentifizierung des APMK erlaubt.
 1: CreateFile / DeleteFile ist auch ohne Authentifizierung des APMK erlaubt.
- Bit 1** Gibt an, ob für den Zugriff auf das Dateiverzeichnis die Masterschlüsselaauthentifizierung erforderlich ist:
 0: Für die Ausführung der Befehle GetFileIDs, GetFileSettings und GetKeySettings ist eine erfolgreiche Masterschlüsselaauthentifizierung erforderlich.
 1: Die Befehle GetFileIDs, GetISOFileIDs, GetFileSettings und GetKeySettings sind unabhängig von einer vorhergehende Masterschlüsselaauthentifizierung (Standardeinstellung) erfolgreich.
- Bit 0** Gibt an, ob der APMK änderbar ist:
 0: Der APMK ist nicht mehr änderbar (eingefroren).
 1: Der APMK ist änderbar (Authentifizierung mit dem aktuellen APMK ist erforderlich (Standardeinstellung)).

Über „Key settings 2“ wird die Anzahl, der für diese Applikation gültigen Keys, und die Art der Verschlüsselung für den Zugriff auf diese Applikation definiert.

Der Parameter „Key settings 2“ definiert mehrere Einstellungen:

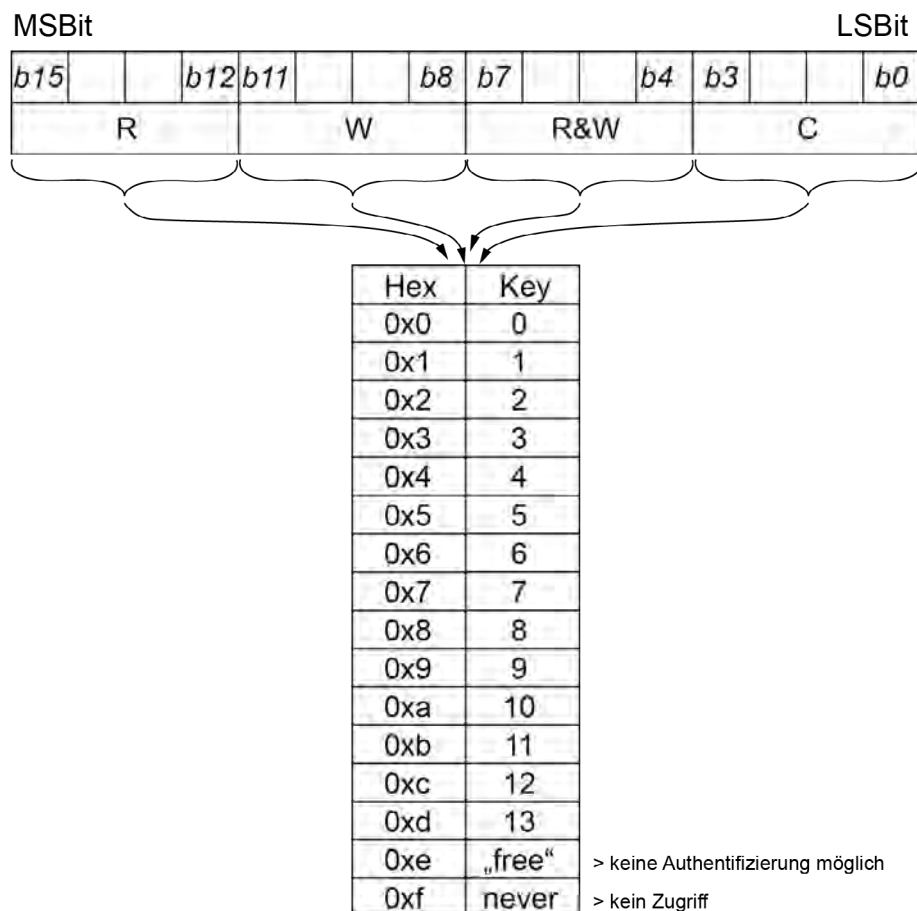
- Bit 0...3** Anzahl der Schlüssel, die innerhalb der Anwendung für kryptografische Zwecke gespeichert werden können. Es können maximal 14 Schlüssel innerhalb einer Anwendung von MIFARE DESFire EV1 gespeichert werden. Man kann auch eine Anwendung ohne Schlüssel erstellen!
- Bit 4** RFU muss auf 0 gesetzt sein.
- Bit 5** Gibt die Verwendung von 2 Byte ISO / IEC 7816-4 Dateinummern für Dateien innerhalb der Anwendung an:
 0: Es werden keine 2 Byte Dateinummern innerhalb der Anwendung unterstützt.
 1: Es werden 2 Byte Dateinummern innerhalb der Anwendung unterstützt.
- Bit 6...7** Gibt die Krypto-Methode der Anwendung an:
 00: gibt DES und 2K3DES Operationen für die gesamte Anwendung an.
 01: gibt 3K3DES Operationen für die gesamte Anwendung an.
 10: gibt AES Operationen für die gesamte Anwendung an.
 Ein gültiger Wert ist z. B. 0x82, wenn zwei Keys für die Applikation eingetragen wurden.
 ISO/IEC 7816-4 wird nicht unterstützt. Bit 4 und 5 müssen daher 0 sein. Generell wird AES für die Verschlüsselung verwendet.

6.1.8.3 Parameter auf File-Ebene

Für die Comm- und File-settings gibt es entsprechend vorbereitete komfortable Auswahlboxen. Bei den Access Rights muss für den File jeweils eingestellt werden, welcher der Applikationsschlüssel lesenden oder schreibenden Zugriff hat und welcher Key ggf. genau diese (Zugriffsrecht-) Einstellung ändern darf (siehe Tabelle).

Wenn man z. B. möchte, dass man mit Key 1 Lesen und Schreiben kann, aber nur mit Key 0 (APMK) diese Einstellungen ändern kann, dann sähe der Wert für die Rechte so aus: 0x1110.

Wenn Sie einen Wert auf 0xe setzen, hat das zur Folge, dass die Kommunikation von „verschlüsselt“ auf „unverschlüsselt“ wechselt. Das wiederum kollidiert ggf. mit den Einstellungen der Applikation.



¹ keine Authentifizierung möglich

² kein Zugriff

6.2 Benutzerdaten

In einem ersten Schritt legen Sie je nach Bedarf unterschiedliche Benutzergruppen mit individuellen Dialogberechtigungen an. Die angelegten Benutzergruppen werden danach auf dem Tab „Benutzerstammdaten“ einzelnen Benutzern zugeordnet.

6.2.1 Benutzergruppen

Auf dem Tab „Benutzergruppen“ werden Dialogrechte in Gruppen erstellt und zusammengefasst. Die Dialogrechte in den Spalten Lesen – Ändern – Speichern – ACL (optional) können einfach per Klick aktiviert/deaktiviert werden.

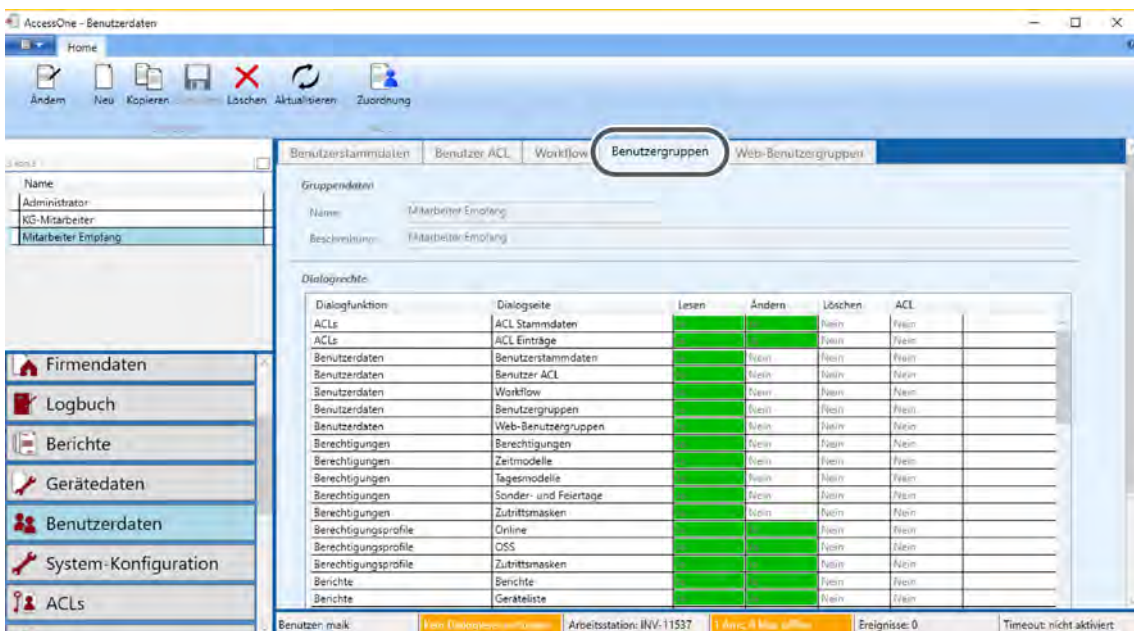


Zur Arbeitserleichterung können Sie mehrere Zellen gleichzeitig mit gedrückter Maustaste auswählen und anklicken. Die jeweiligen Einträge in den einzelnen Zellen werden dann umgeschaltet (Ja>Nein und Nein>Ja).

Vergeben Sie einen aussagekräftigen Namen und eine Beschreibung der Gruppe.

Durch Klicken auf den Button ÄNDERN wird die jeweilige Funktion ausgewählt und grün markiert. Klicken auf den Button SPEICHERN speichert die angegebenen Berechtigungen im System.

Im folgenden Beispiel ist die Benutzergruppe „Mitarbeiter Empfang“ angelegt und die Rechte eines Mitarbeiters am Empfang des Hauptgebäudes auf das Anlegen und Ändern von Personendaten beschränkt. Der Mitarbeiter kann z.B. Personenstammdaten ändern und die Ausweis- und Sperren-Funktionen im Übersichtsdialog nutzen.



Dialogfunktion	Dialogseite	Lesen	Ändern	Löschen	ACL
ACLs	ACL Stammdaten	Nein	Nein	Nein	Nein
ACLs	ACL Einträge	Nein	Nein	Nein	Nein
Benutzerdaten	Benutzerstammdaten	Nein	Nein	Nein	Nein
Benutzerdaten	Benutzer ACL	Nein	Nein	Nein	Nein
Benutzerdaten	Workflow	Nein	Nein	Nein	Nein
Benutzerdaten	Benutzergruppen	Nein	Nein	Nein	Nein
Benutzerdaten	Web-Benutzergruppen	Nein	Nein	Nein	Nein
Berechtigungen	Berechtigungen	Nein	Nein	Nein	Nein
Berechtigungen	Zeitmodelle	Nein	Nein	Nein	Nein
Berechtigungen	Tagesmodelle	Nein	Nein	Nein	Nein
Berechtigungen	Sonder- und Feiertage	Nein	Nein	Nein	Nein
Berechtigungen	Zutrittsmasken	Nein	Nein	Nein	Nein
Berechtigungsprofile	Online	Nein	Nein	Nein	Nein
Berechtigungsprofile	OS	Nein	Nein	Nein	Nein
Berechtigungsprofile	Zutrittsmasken	Nein	Nein	Nein	Nein
Berichte	Berichte	Nein	Nein	Nein	Nein
Berichte	Geräteleiste	Nein	Nein	Nein	Nein

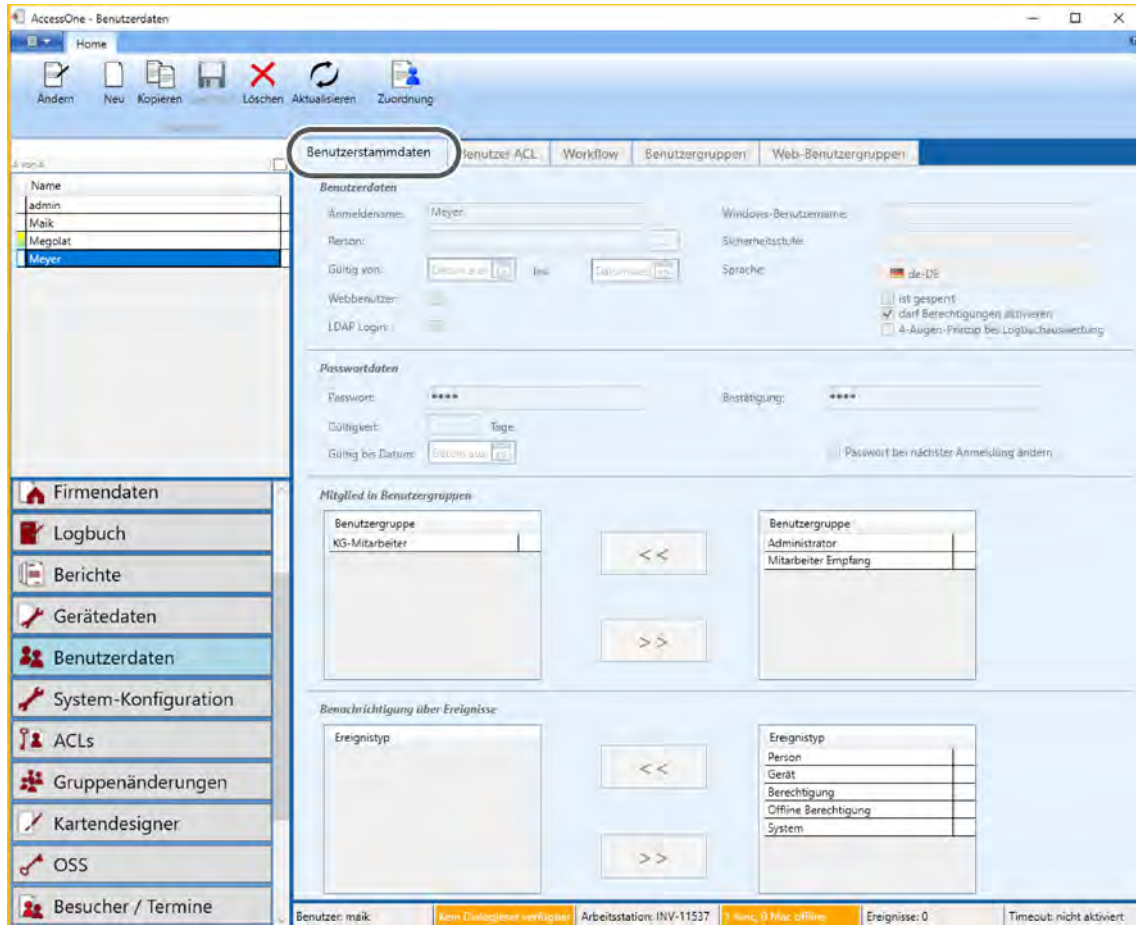
Den Mitgliedern der Gruppe „Mitarbeiter Empfang“ soll hier kein Zugriff auf die ACL eingeräumt werden, um zu verhindern, dass sie Personen in andere Zugriffslisten einfügen können. Die Mitglieder dieser Gruppe haben nur lesenden Zugriff auf alle Stammdaten, um gegebenenfalls Fragen zum Ausweis und Berechtigungen beantworten zu können.



Mitarbeiter der Geschäftsleitung und/oder der Administration sollten berechtigt werden, die Personaldaten der Mitarbeiter, die das Gebäude betreten dürfen, in den Zugriff zu geben.

6.2.2 Benutzerstammdaten

Legen Sie jetzt Benutzer an, die sich in der AccessOne anmelden dürfen.



Benutzerdaten

Vergeben Sie einen Namen zur Anmeldung. Wird der Windows Benutzername angegeben, verwendet die AccessOne Software diesen zur automatischen Anmeldung (Single Sign-on). Die Person kann aus einer Liste ausgewählt werden. Soll das Benutzerprofil nur begrenzt gültig sein, kann ein von/bis-Datum angegeben werden. Läuft diese Gültigkeit ab, wird der Benutzer automatisch gesperrt. Ein Benutzer kann jederzeit auch sofort manuell gesperrt werden (dazu Checkbox aktivieren).

In der Maske kann dem Benutzer zusätzlich das Attribut „4-Augen-Prinzip bei Logbuchauswertungen“ zugewiesen werden, d.h. die Anzeige detaillierter Informationen aus dem Logbuch setzt das Log-In eines weiteren Benutzers mit dieser Berechtigung voraus.

Ebenso kann dem Benutzer das Recht „Berechtigungen aktivieren“ zugewiesen werden. Dieses Recht wird bei bestimmten Berechtigungen, die eine eigene Aktivierung erfordern, benötigt.

Passwortdaten

Vergeben Sie ein Passwort für den Benutzer. Eine begrenzte Gültigkeit können Sie für einen bestimmten Zeitraum festlegen oder nur mit einem „Gültig bis Datum“ angeben.

Aktivieren Sie „Passwort bei nächster Anmelden ändern“: Nachdem der Nutzer in der Eingabemaske seinen Anmeldenamen und das zugewiesene Passwort erstmalig eingegeben hat, wird er aufgefordert ein neues Passwort einzugeben und dieses zu bestätigen. Bei der Eingabe des Passwortes können Sie beliebig viele Zeichen wählen. Die maximale Passwortlänge ist im System einstellbar.

Mitglied in Benutzergruppen

Weisen Sie dem AccessOne-Nutzer die Dialogseiten und Funktionen zu, die er nach seinem Log-In sehen oder

bearbeiten darf. Diese Dialogrechte werden vorher für sogenannte Benutzergruppen definiert. Weitere Informationen finden Sie unter „6.2 Benutzerdaten“ auf Seite 28 .

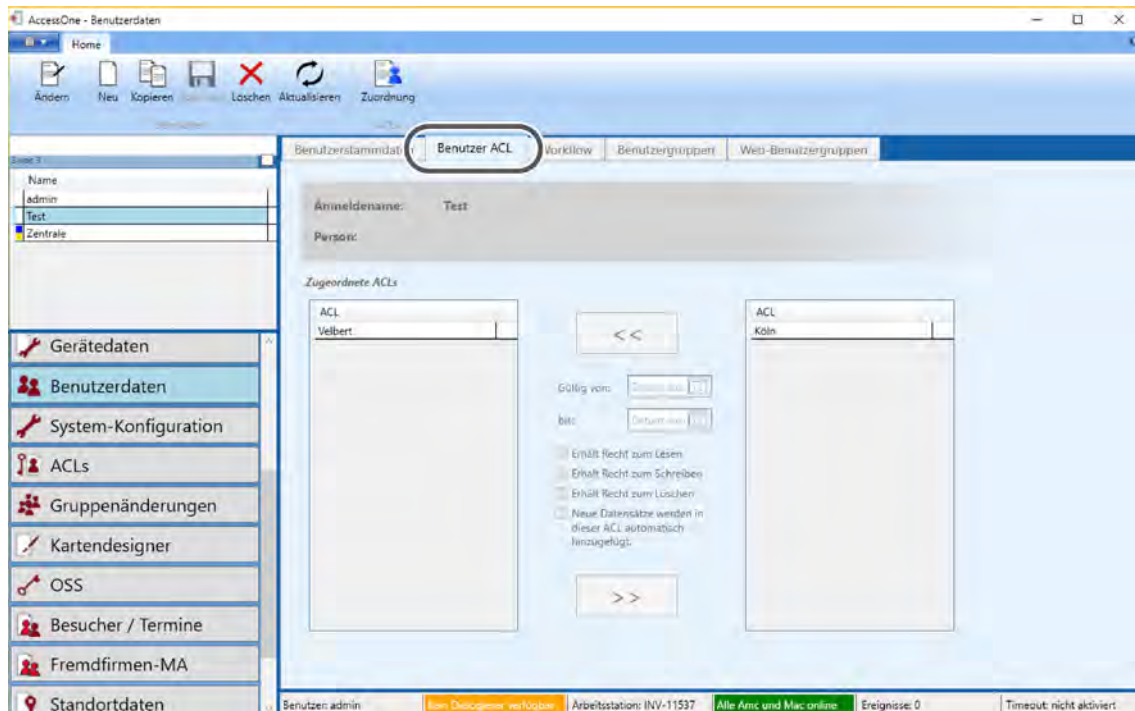
Berechtigungen über Ereignisse

Weisen Sie dem AccessOne-Nutzer die Ereignisse zu, die er nach seinem Log-In sehen oder bearbeiten darf.

6.2.3 Benutzer ACL (Mandantenfähigkeit)

(Nur bei Datentrennung vorhanden.)

Hier können Dialogbenutzern Access Control Lists (ACL) zugewiesen werden. Die ACLs können eingestellt und verändert werden. Voraussetzung: Die ACL-Funktion ist durch den Administrator freigeschaltet.



Die Mandantenfähigkeit ist dann empfehlenswert, wenn eine AccessOne Installation/Datenbank mehrere Kunden (Mandanten) bedient und dabei jeder Kunde nur seine eigenen Daten sehen und bearbeiten kann. Datensätze, die keiner Mandantenschaft zugewiesen sind, stehen Benutzern aller Mandantenschaften zur Verfügung. Die Bearbeitung solcher Parameter obliegt einer übergeordneten Person (Systemadministrator). Geschäftsleitung und Systemadministrator sollten immer Master- oder Zusatzrechte erhalten. Für Mitarbeiter, wie z. B. Personen am Empfang, sollten eigene Teilsysteme der Zutrittskontroll-Anlage eingerichtet werden, um Stammdaten einzusehen, bearbeiten und löschen zu können. Benutzer eines Teilsystems, wie z. B. die Gruppe „Mitarbeiter Empfang“, sollten z. B. keinen Zugriff auf ACL haben, da sie sonst Personen auch in andere Zugriffslisten einfügen können. Die Berechtigung zum Auslesen von Stammdaten ist für Benutzer dieses Teilsystems ausreichend.



Wenn einem AccessOne Benutzer nur eine Zugriffsliste (ACL) zugeordnet ist, kann er nur diejenigen Berechtigungen zuweisen, die in der gleichen ACL enthalten sind. Somit kann der AccessOne Benutzer Mitgliedern der Gruppe „Mitarbeiter Empfang“ nur Berechtigungen für die für den Gebäudebereich Empfang freigegebenen Türen vergeben. Andere Türen werden in der Auswahlliste nicht angezeigt.

Die Mitglieder der Gruppe „Mitarbeiter Empfang“ können die Berechtigungen einsehen, ändern und löschen, allerdings nicht wieder hinzufügen. Dieses geschieht nur über den Systemadministrator oder einer Person mit dem jeweiligen Zugriffs- bzw. Vergaberecht. Es liegt im Ermessen und der Verantwortung des Anwenders, die Daten sinnvoll und nach seinen (Sicherheits-)Anforderungen aufzuteilen.

Workflow

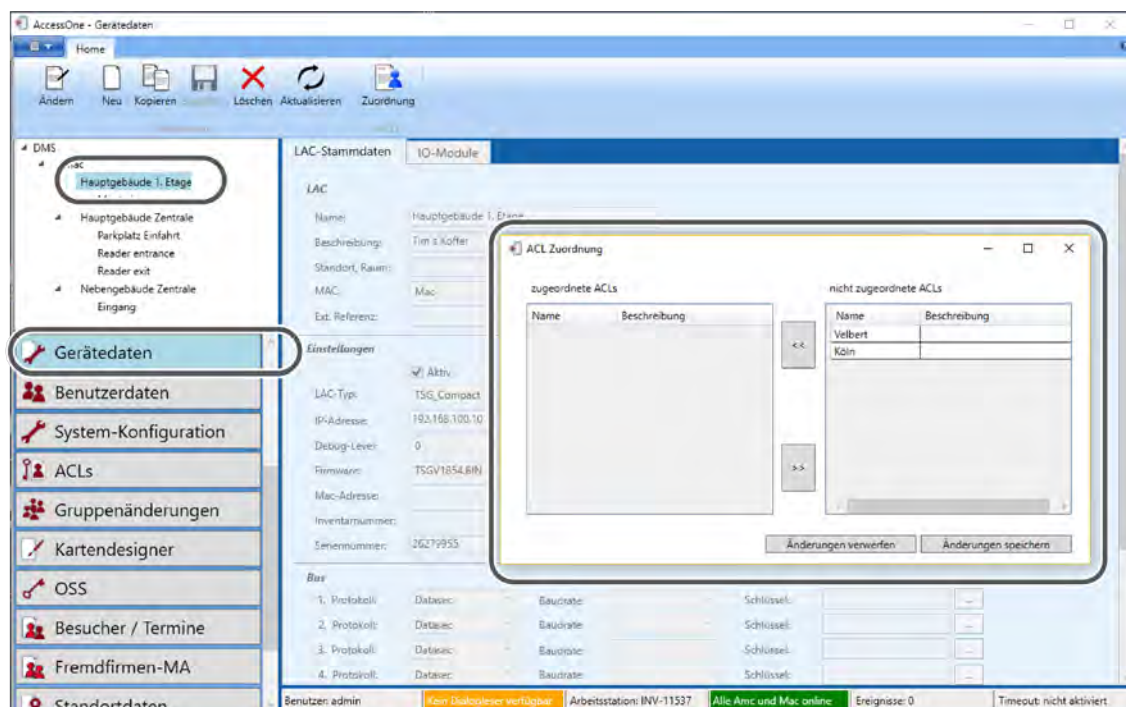
Über den Tab Workflow können für bestimmte auszuführende Aktionen Arbeitsabläufe erstellt werden, z. B. wenn eine Genehmigung durch einen Vorgesetzten erforderlich ist.

6.2.4 Zuweisen der Datensätze zu den Zugriffslisten – ACL

Sind bereits Daten im System eingepflegt worden, deren Zugriff nachträglich eingeschränkt werden sollen, müssen diese Daten über den Button ZUORDNUNG einer ACL zugewiesen werden.



Unbedingt beachten: Daten, die keiner ACL zugeordnet sind, sind für jeden sichtbar!



Empfohlene Vorgehensweise und Reihenfolge

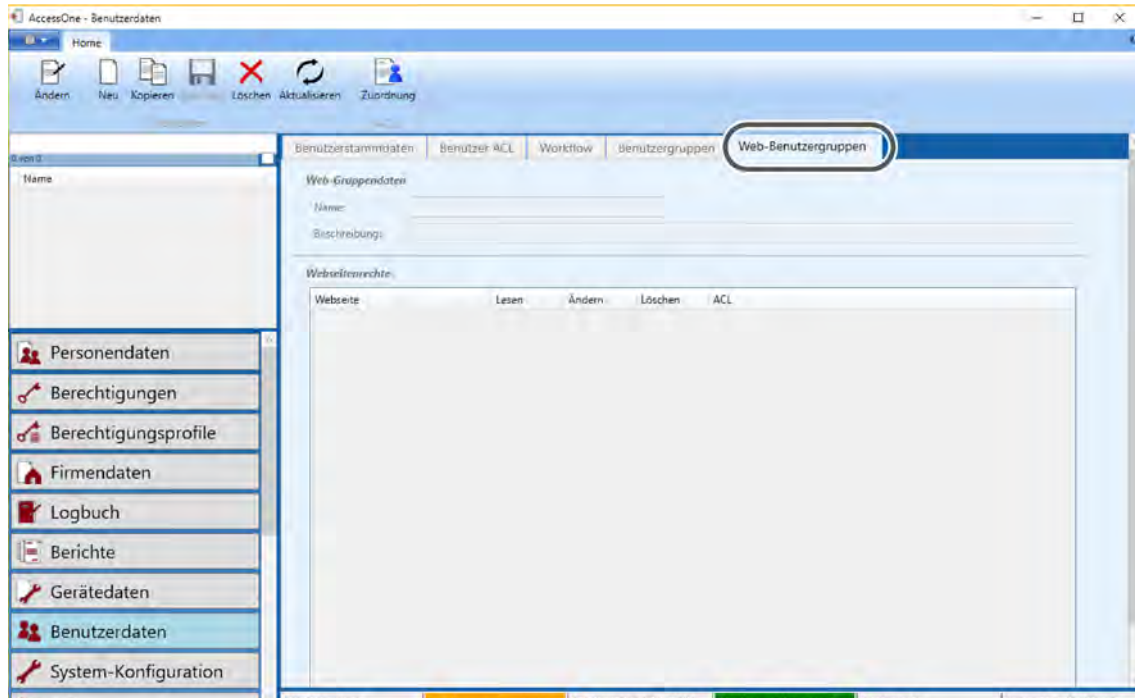
Beginnen Sie mit den Türen im Dialog „Gerätedaten“. Klicken Sie dazu auf den Button ZUORDNUNG in der Werkzeugleiste.

Wählen Sie eine Tür in der Auswahlliste auf der linken Seite aus und ordnen Sie sie der entsprechenden ACL zu. Anschließend klicken Sie auf die Schaltfläche ÄNDERUNGEN SPEICHERN. Das gewählte Objekt wird dann mit einem Farbbalken entsprechend gekennzeichnet.

Für die Dialoge „Personendaten“ und „Berechtigungen“ gehen Sie genauso vor.

6.2.5 Web-Benutzergruppen

(Nur in Zusammenhang mit Lizenzmodul Besucherverwaltung, Art.-Nr. 348122V, verfügbar.)



Hier werden Web-Seiten für die webbasierte Besucheranmeldung und die Verwaltung von Fremdfirmenmitarbeitern zu Web-Benutzergruppen zusammengefasst.

Ebenso können über Lightweight Directory Access Protocol (LDAP) Informationen über Benutzer und deren Gruppenzugehörigkeit bereitgestellt und dem System hinzugefügt werden. LDAP ermöglicht, Informationen eines LDAP-Verzeichnisses abzufragen.

6.3 Standortdaten

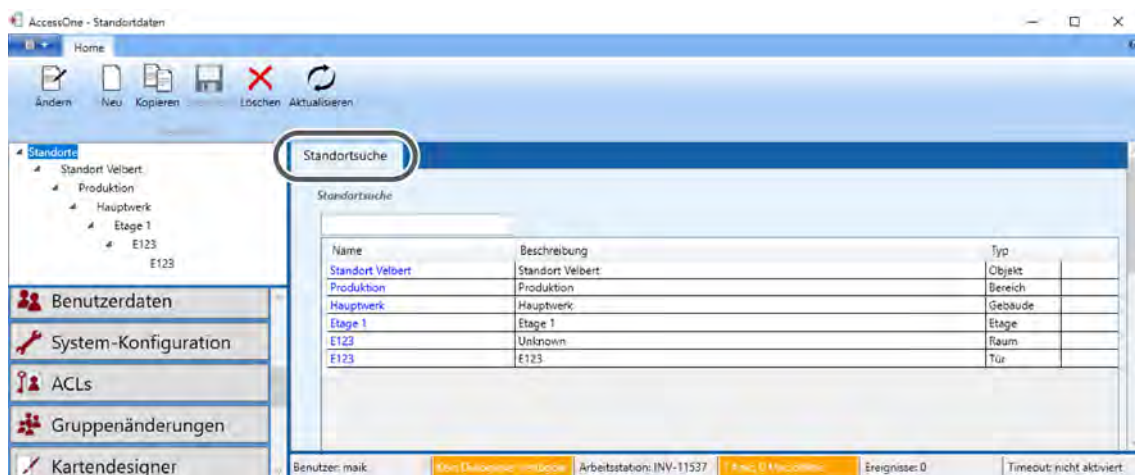
Mit den Standortdaten bilden Sie alle für die Zutrittskontroll-Anlage relevanten Objektstrukturen ab. Die Darstellung erfolgt übersichtlich in Form eines Strukturbaums.



Geben Sie die Standortdaten möglichst komplett und detailliert an, da sie später beim Anlegen von Hardwarekomponenten genutzt werden.

Sind mehrere Standorte angelegt, hilft der Tab „Standortsuche“. Ein Klick auf „Standorte“ im Strukturbaum zeigt alle angelegten Standorte nach Typ sortiert. Doppelklicken auf einen Standort in der Liste öffnet den Standort im linken Strukturbaum.

6.3.1 Standort anlegen



Wählen Sie „Standortdaten“ in der Dialogauswahl. Der Tab „Standortsuche“ öffnet sich und im Strukturbaum links werden die Daten zu Objekten, Bereichen, Gebäuden, Etagen, Räumen und Türen hierarchisch angezeigt. Durch Klicken auf die entsprechende Ebene kann mit den Buttons NEU und ÄNDERN ein Eintrag erfolgen bzw. angepasst werden.

Objekt

Vergeben Sie für den Standort, an dem sich Bereiche, Gebäude, Türen, Zylinder, Leser und Offline-Geräte befinden, einen Objektnamen. Es können auf Objektebene mehrere Standorte angelegt werden.

Bereich

Vergeben Sie Namen für Bereiche, die sich im Objekt befinden (z. B. „Produktion“, „Entwicklung“, „Buchhaltung“ etc.).

Gebäude

Vergeben Sie einen Namen für das Gebäude, in dem sich alle Bereiche des Objekts befinden (z. B. „Haus 3.1.“), und legen Sie dafür Adress- und Kontaktdaten an.

Etage

Geben Sie den Etagennamen und die Etagennummer ein, in dem sich Türen, Zylinder, Leser und Offline-Geräte des übergeordneten Gebäudes Ihres Objektes befinden, z. B. „EG“.

Raum

Vergeben Sie hier Namen für Räume auf der gleichen Etage, z. B. „0.12“, und konfigurieren Sie die Räume nach verantwortlichen Personen, Nutzungsart und Gewerken.

Tür

Geben Sie den Namen der Tür des Raumes ein, z. B. „Tür 0.12 Außen“.

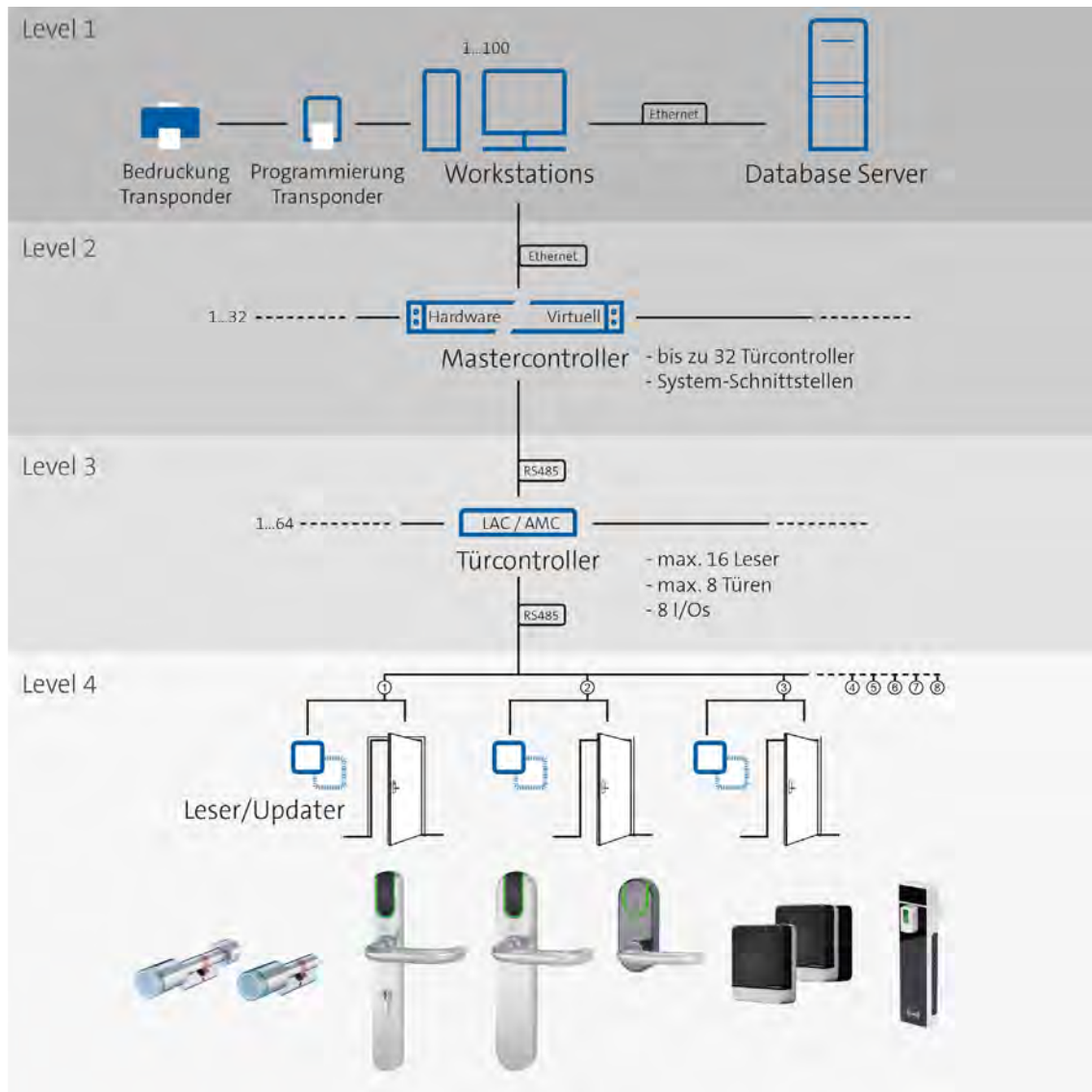
7 Konfiguration der Geräte

Zielgruppe dieses Kapitels:

- produktgeschultes Personal

Die Einrichtung der Geräte beginnt mit den Mastercontrollern auf Level 2. Dann werden die Türcontroller auf Level 3 konfiguriert und die I/O-Module angelegt. Zuletzt richten Sie die angeschlossenen Online- und Offline-Geräte auf Level 4 ein.

AccessOne – Das 4-Ebenen-Konzept

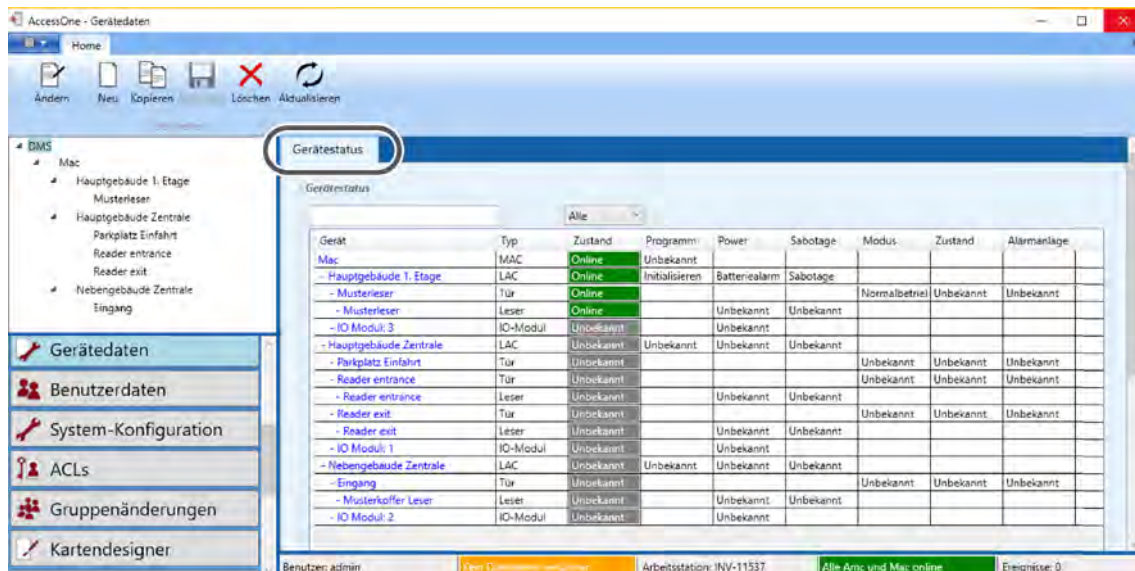


Die AccessOne basiert hardwareseitig auf einem Vier-Ebenen Konzept als Grundlage für praktisch unbegrenzte Skalierbarkeit. Die Serverprozesse Anwendung und Datenbank laufen auf Windows-Server-Betriebssystemen sowie einem installierten SQL-Server. Die Serversoftware läuft in den meisten Fällen in einer virtuellen Umgebung (Level 1). Der Mastercontroller verteilt die Daten an die Türsteuerungen (Door Control Unit) und stellt alle türsteuerungsübergreifenden Funktionen zur Verfügung (Level 2). Der Mastercontroller muss nicht physisch als eigenständige Komponente vorhanden sein, er kann ebenso wie die Serversoftware auch virtualisiert werden. Der Mastercontroller ist per Netzwerk lokal mit den Türsteuerungen verbunden (Level 3). Jede der angeschlossenen Türsteuerungen ist autark und verfügt, wenn die Daten einmal geladen wurden, über

alle Berechtigungsdaten einer Person inklusive der Offline-Daten. Alle Zutrittsentscheidungen werden somit lokal getroffen (Level 3). Die Leser werden über eine RS485-Schnittstelle angeschlossen (Level 4). Jeder Leser kann dabei auch als Updater für die Offline Geräte eingesetzt werden.

7.1 Gerätedaten Online-Geräte

7.1.1 Geräteübersicht anzeigen



Zum Anlegen und Parametrieren von Geräten stellt die AccessOne den Gerätedaten-Editor bereit. Dieser zeigt die Geräte in einem Strukturbaum in der Objektauswahl auf der linken Seite. Der oberste Eintrag ist das Data Management System(DMS) unter dem die Geräte angeordnet sind. Alle Datenänderungen und alle Meldungen der Türcontroller (TSG1, TSG8, AMC oder LAC*) erfolgen dort. Hier werden daher auch die Statusmeldungen interpretiert, im Speicher gesammelt und angezeigt.

Klicken Sie auf den Eintrag „DMS“, wenn Sie den Status aller Geräte in der Übersicht sehen möchten. Sie können den DMS Eintrag nicht löschen und auch keinen zweiten anlegen.



Den Status eines einzelnen Geräts (Online oder Offline) sehen Sie auch in der Detailansicht zum Gerät.

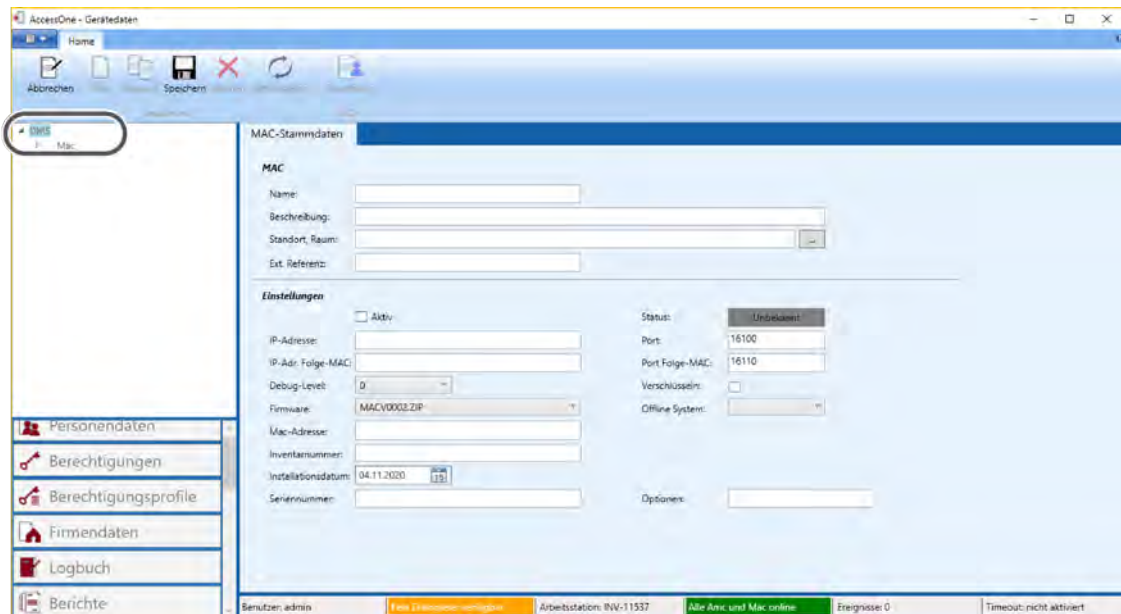
Im Dialogfenster wird der Status aller verfügbaren Geräte in Form einer Liste angezeigt. Diese Ansicht wird nicht automatisch aktualisiert. Für eine Aktualisierung klicken Sie bitte auf den Button AKTUALISIEREN. Über der Objektauswahl links gibt es ein Suchfenster. Werden hier Buchstaben eingegeben, wird die darunterliegende Liste nach allen Geräten gefiltert, die diese Buchstaben enthalten, sie müssen nicht damit beginnen. Auch die Groß- und Kleinschreibung wird ignoriert, um die Suche zu vereinfachen. Die Namen der Geräte sind in blauer Schrift dargestellt, was in der AccessOne generell bedeutet, dass hier durch einen Doppelklick auf den Namen eine direkte Navigation zum Tab dieses Eintrags möglich ist. In der Mitte gibt es eine zusätzliche Filtermöglichkeit nach Gerätestatus. Möchte man z. B. nur diejenigen Geräte sehen, die gerade online sind, wählt man im Drop-down-Menü den Eintrag „Online“ aus. Ein Klick mit der rechten Maustaste auf den Namen einer Tür zeigt die möglichen Steuerkommandos an, die für eine Tür zugelassen sind.

* TSG = Türsteuergerät, AMC = Access Modular Controller, LAC = Local Access Controller

7.1.2 Mastercontroller (MAC) anlegen

Zum Anlegen eines neuen Master-Controllers (MAC) wählen Sie den Eintrag „DMS“ im Strukturbaum und klicken Sie auf den Button NEU.

7.1.2.1 MAC-Stammdaten



Auf der rechten Seite wird daraufhin ein nicht ausgefüllter Tab zum MAC angezeigt, in die Sie die Daten eingeben können. Jeder MAC benötigt einen Namen, der so gewählt sein sollte, dass er den Zuständigkeitsbereich dieses Geräts beschreibt. In einer kleinen Installation genügt in der Regel ein MAC. Bei größeren Installationen ist häufig ein MAC je Gebäudekomplex vorhanden. Es bietet sich daher an, den Mastercontroller nach diesem Gebäude zu benennen. Ein einzelner MAC kann bis zu 32 Access Modular Controller (AMC) verwalten. Sie haben die Möglichkeit zusätzlich noch eine „Beschreibung“ anzugeben, z. B. den genauen Aufstellort. Die Auswahlliste „Standort“ bietet die Liste der zuvor konfigurierten Standorte an. Bei einem neuen System ist nur den Standort „unbekannt“ verfügbar. Sie können diese Liste über den Dialog „System-Konfiguration > Standorte“ mit zusätzlichen Standorten füllen (siehe „6.1 System-Konfiguration“ auf Seite 17). Bei Anwendungen, in denen sich die Zutrittskontrollanlage über viele Standorte verteilt, empfehlen wir, diese Standorte vorher anzulegen und bei der Anlage von Geräten nur noch aus der Liste auszuwählen. Die Standortdaten enthalten je nach Typ weitere Informationen, wie z. B. die Adresse eines Ansprechpartners mit Telefonnummer und sind damit im Störfall hilfreich.



Zu jedem MAC muss eine IP-Adresse und eine Portnummer angegeben werden. Die IP-Adresse des MACs kann der Netzwerkkonfiguration auf dem MAC entnommen werden. Sie können auf dem Mastercontroller auch ein Kommandofenster öffnen (cmd.exe) und den Befehl „ipconfig“ eingeben. Die zum LAN-Adapter angezeigte IP4 Adresse ist die IP-Adresse des MACs. Bei Fragen wenden Sie sich an den Systemadministrator Ihres Netzwerkes.

Die Portadresse ist bei neu installierten Mastercontrollern auf 50100 eingestellt. Diese Adresse kann beliebig geändert werden, muss aber in der Konfiguration beim MAC (Datasec\Mac\config\MacConfig.ini) und hier in den Gerätedaten übereinstimmen, da ansonsten keine Kommunikation aufgebaut werden kann.

Das Feld „Debug-Level“ ist ein Hilfsmittel für den Hersteller, um im Störfall ausführliche Fehlerprotokolle erzeugen zu können. Je größer der Debug-Level, desto umfangreicher sind die Aufzeichnungen, die der Mastercontroller bei allen Aktionen mitschreibt. Achten Sie darauf, dass der Wert nicht größer als 1 ist, da dies

Auswirkungen auf die Leistung des Geräts haben kann.

Über die Checkbox „Verschlüsseln“ stellen Sie ein, ob die Kommunikation zwischen DMS und MAC AES-verschlüsselt erfolgen soll. Die Verschlüsselung von Daten verlangsamt die Geschwindigkeit beim Verbindungsaufbau und wirkt sich danach geringfügig auch auf den Durchsatz beim Datenaustausch aus.

Das Feld „Firmware“ dient dazu, hier bei einem Upgrade die neue Softwareversion einzutragen. Diese wird automatisch an alle Mastercontroller verteilt und aktiviert. Wichtig: Jeder MAC besitzt seine eigene Firmware.



Ändern Sie den voreingestellten Wert nur, wenn Sie von CES ein entsprechendes Update bekommen haben! Wenn von Ihrem MAC Kartenleser mit Update-Funktion für Offline-Systeme bedient werden, müssen Sie dies beim Anlegen des MAC einstellen. In diesem Fall ändert sich die Auswahl der zu verwendenden Firmware(s) für den MAC. Eine **nachträgliche** Änderung dieser MAC-Funktion ist **nicht möglich**. In diesem Fall muss ein neuer MAC in dem DMS angelegt und die bereits zugewiesenen LACs zum neu angelegten MAC portiert werden.

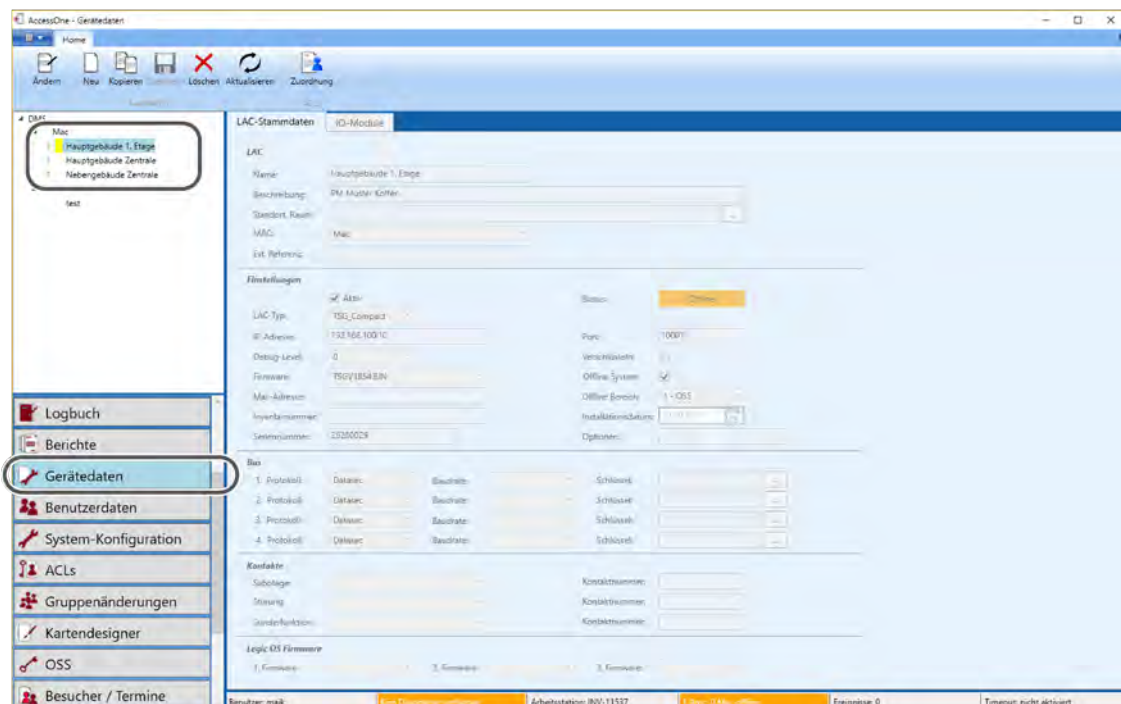
Optional können Sie zum Gerät auch die Mac-Adresse, eine Inventarnummer und das Installationsdatum eingeben. Bitte beachten: Die Mac-Adresse kann wichtig sein, wenn Ihr Netzwerk nur konfigurierte Mac-Adressen bedient, um zu verhindern, dass sich Unbefugte mit Ihrem Netzwerk verbinden.



Zu jedem Gerät und zu jeder Tür gibt es eine Checkbox, über die das Gerät aktiviert wird. Erst wenn dieser Haken gesetzt ist, wird das Gerät mit Daten geladen und gestartet. Die Geräte können somit schon konfiguriert werden und erst nach der Installation aktiv gesetzt werden. Vorteil: nicht aktivierte Geräte werden vom System nicht überwacht. Vorkonfigurierte, aber nicht aktivierte Geräte, werden daher auch nicht als gestörte Geräte gemeldet. Insgesamt können bis zu 32 lokale Türsteuerungen pro MAC angeschlossen werden.

7.1.3 Türsteuerung (LAC) anlegen

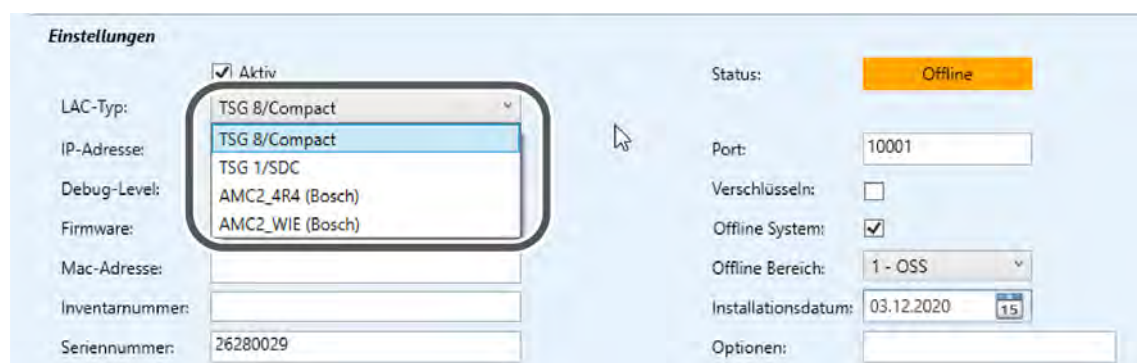
7.1.3.1 LAC-Stammdaten



Lokale Türsteuerungen, Local Access Controller (LAC), werden jeweils unter dem MAC angelegt, an dem sie auch angeschlossen sind. Wählen Sie mit der Maus den gewünschten Mastercontroller und klicken Sie auf **Neu**.

Im Dialogfenster wird daraufhin der Tab für eine Türsteuerung angezeigt.

Jeder LAC benötigt einen Namen und eine Beschreibung. Gehen Sie hier wie beim Mastercontroller MAC vor. Auch hier ist es sinnvoll einen Namen zu wählen, der Aufschluss über den Zuständigkeitsbereich gibt. Die Beschreibung gibt Ihnen zusätzlich die Möglichkeit, den genauen Montageort anzugeben.



Die AccessOne unterstützt Türsteuerungen verschiedener Hersteller. Wählen Sie unter LAC-Typ, die von Ihnen verwendete Hardware aus. Die Steuerungen können innerhalb einer Installation gemischt betrieben werden.

- TSG 8/Compact (Art. Nr. 348007V) Zutrittskontrollzentrale für bis zu 8 Türen mit bis zu 16 Lesern
- TSG 1/SDC (Art. Nr. 348008V) Zutrittskontrollzentrale für 1 Tür mit bis zu 2 Lesern
- AMC2_4R4 mit 4 RS485 Steckern für bis zu 8 Türen
- AMC2_WIE mit 4 Wiegand Schnittstellen für bis zu 8 Türen

Geben Sie zum LAC eine IP-Adresse an, die vom MAC aus erreichbar ist. Die Portadresse ist voreingestellt auf

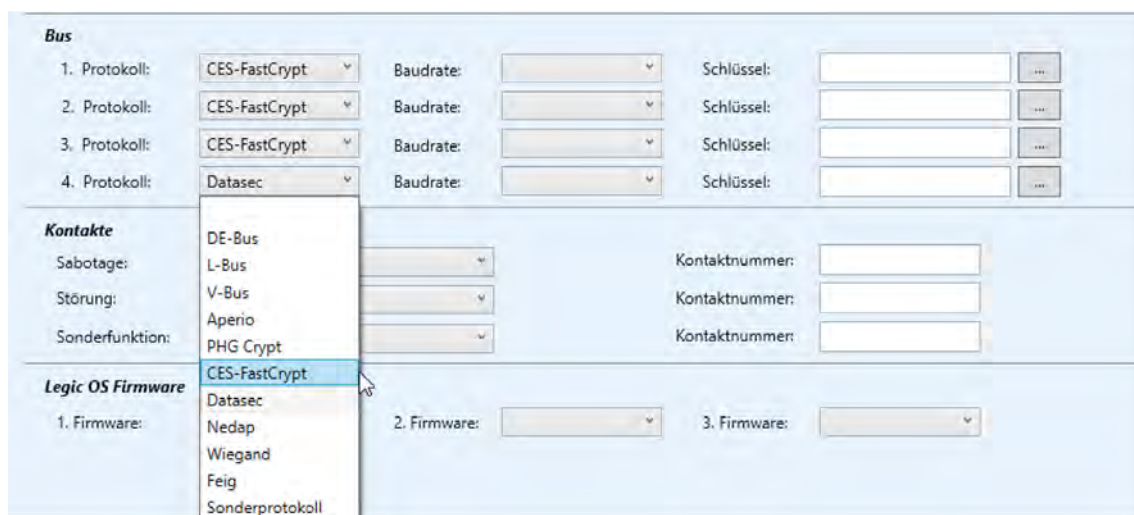
10001 und sollte nicht verändert werden. Zum Einstellen der IP-Adresse auf der Türsteuerung, wählen Sie die zur Türsteuerung passende Konfiguration.

Optional können Sie zum Gerät auch die Mac-Adresse, eine Inventarnummer und das Installationsdatum eingeben.

Über die Checkbox „Verschlüsseln“ stellen Sie ein, ob die Kommunikation AES-verschlüsselt erfolgen soll. Die Verschlüsselung von Daten verlangsamt die Geschwindigkeit beim Verbindungsaufbau und wirkt sich danach auch geringfügig auf den Durchsatz beim Datenaustausch aus.

Die Checkbox „Offline System“ bedeutet, dass der AMC erkennt, wenn Offlinesysteme betrieben werden und ein Updater vorhanden ist.

Je nach Hardware und Schnittstelle können hier die entsprechenden Protokolle angegeben werden.



The screenshot shows a software configuration window with three main sections: **Bus**, **Kontakte**, and **Legic OS Firmware**.
Bus section: Contains four rows for protocol configuration. Each row has a 'Protokoll' dropdown (all set to 'CES-FastCrypt'), a 'Baudrate' dropdown, and a 'Schlüssel' field with a '...' button.
Kontakte section: Contains a 'Sonderfunktion' dropdown (set to 'PHG Crypt') and three 'Kontakt' entries, each with a 'Kontakt' dropdown and a 'Kontaktnummer' field.
Legic OS Firmware section: Contains a '1. Firmware' dropdown (set to 'CES-FastCrypt') and two other firmware options, '2. Firmware' and '3. Firmware', each with a dropdown menu.



Zu jedem Gerät und zu jeder Tür gibt es eine Checkbox, über die das Gerät aktiviert wird. Erst wenn dieser Haken gesetzt ist, wird das Gerät mit Daten geladen und gestartet. Die Geräte können somit schon konfiguriert werden und erst nach der Installation aktiv gesetzt werden. Vorteil: nicht aktivierte Geräte werden vom System nicht überwacht. Vorkonfigurierte, aber nicht aktivierte Geräte, werden daher auch nicht als gestörte Geräte gemeldet. Insgesamt können bis zu 32 lokale Türsteuerungen pro MAC angeschlossen werden.

In der Dialogauswahl „Berichte“ gibt es eine Geräteliste, die zu allen Geräten die relevanten Daten zur Hardwareokumentation ausgibt. Sind alle Daten angegeben, kann das System jederzeit eine vollständige Anlagendokumentation ausgeben.

7.1.3.2 IO-Module

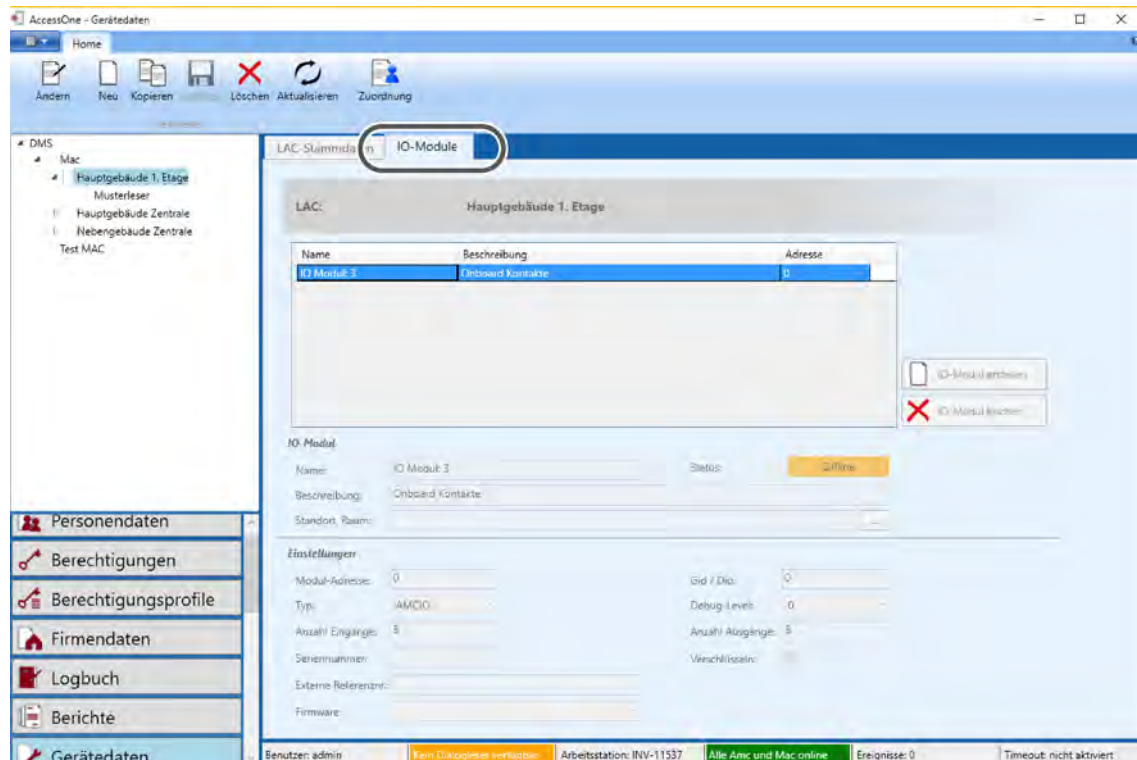
Bei den Eigenschaften zur Türsteuerung gibt es zusätzlich einen Tab für IO-Module. Jede lokale Türsteuerung benötigt für die Überwachung von Eingangssignalen (z. B. Signale zum Türzustand) und für die Ausgabe von Steuerbefehlen Hardwarekomponenten. Das sind die sogenannten IO-Module (Input-Output-Module) des LAC. Ein IO-Modul hat mehrere Eingangsschaltkreise, um zu prüfen, ob ein externer Kontakt geöffnet oder geschlossen ist.



In der AccessOne werden IO-Module grundsätzlich getrennt behandelt, selbst wenn die entsprechende Hardware in der Türsteuerung oder im Ausweisleser enthalten ist. Dies ermöglicht eine freie Zuordnung von Signalen über alle vorhandenen IO-Module.

Die AccessOne unterscheidet, ob es sich um onboard befindliche IO-Module des LAC handelt oder um abgesetzte separate IO-Module. Das onboard befindliche IO-Modul wird standardmäßig beim Anlegen des LAC mit angelegt. Abgesetzte IO-Module müssen manuell mit ihrer jeweiligen Busadresse hinzugefügt werden. Die Signalprogrammierung der IO-Module wird später in der Konfiguration der jeweiligen Türen individuell vorgenommen.

Wechseln Sie auf den Tab „IO-Module“ um die Hardware für Ein- und Ausgänge der Türsteuerung zu konfigurieren.



Haben Sie eine Türsteuerung ausgewählt, die schon über im Gerät enthaltene Ein- und Ausgänge verfügt, wird dieses IO-Modul automatisch beim Wechsel auf diese Seite angelegt.

Um ein neues IO-Modul zu erstellen, klicken Sie auf die Schaltfläche IO-Modul erstellen und füllen Sie die zugehörigen Eingabefelder aus. Die Modul-Adresse ist bei internen Kontakten 0.

Als Typ wählen Sie „AMC-IO“, falls Sie als Türsteuerung einen AMC gewählt haben. Wenn Sie eine TSG Zutrittskontrollzentrale verwenden, wählen Sie als Typ „TS2“ für ein Türsteuermodul mit 4 Ein- und Ausgängen und 2 Leserschnittstellen oder „IO8“ für ein Relaisboard mit 8 Ein- und Ausgängen. Bei abgesetzten Türsteuermodulen, die am Leserbus angeschlossen werden, geben Sie die eingestellte Busadresse ein und wählen als Typ „TSM“. TSM Türsteuermodule haben zwei Eingänge und zwei Ausgänge (Hinweis: Das variiert je nach Ausführung/Typ). Geben Sie hier nur die tatsächlich vorhandene Anzahl an, da ansonsten Steuerbefehle für nicht vorhandene Relais zu Fehlermeldungen führen können.

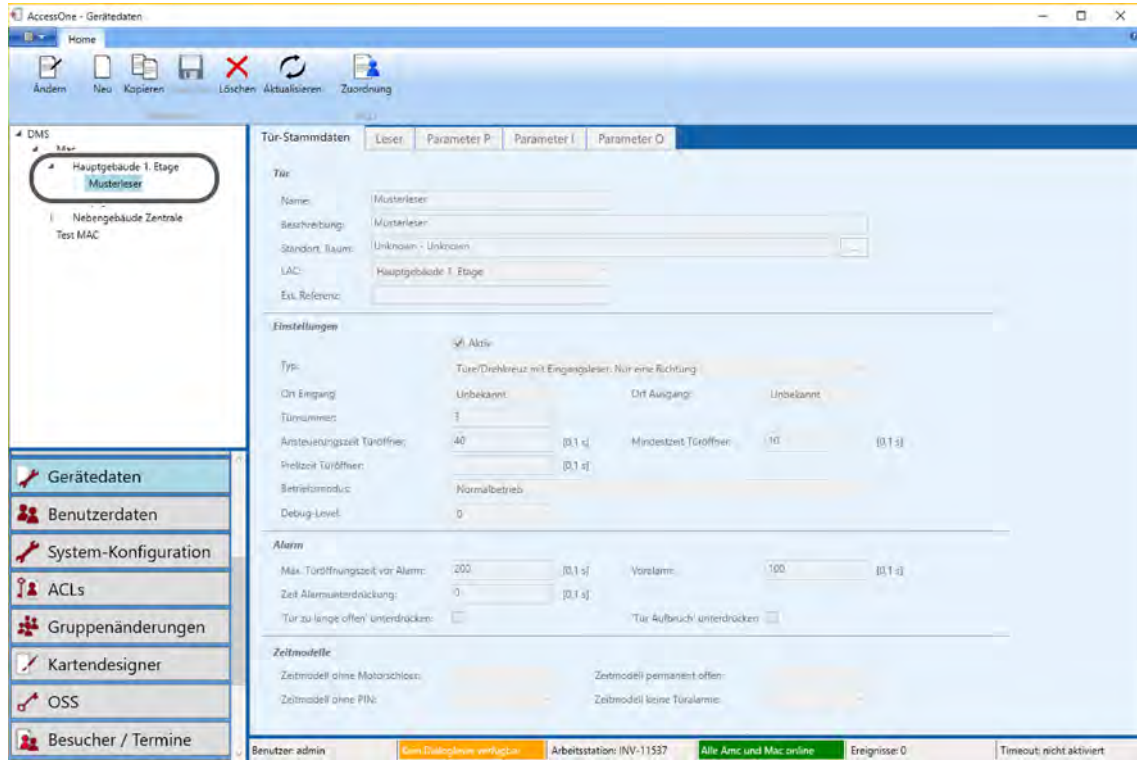


Pro Türsteuerung können bis zu 64 Eingangssignale und 64 Ausgangssignale angesteuert werden. Die Aufteilung auf IO-Module ist dabei nicht relevant, sofern der Adressbereich des Leserbusses mit maximal 16 Teilnehmern nicht überschritten wird.

7.1.4 Eine Tür anlegen

7.1.4.1 Tür-Stammdaten

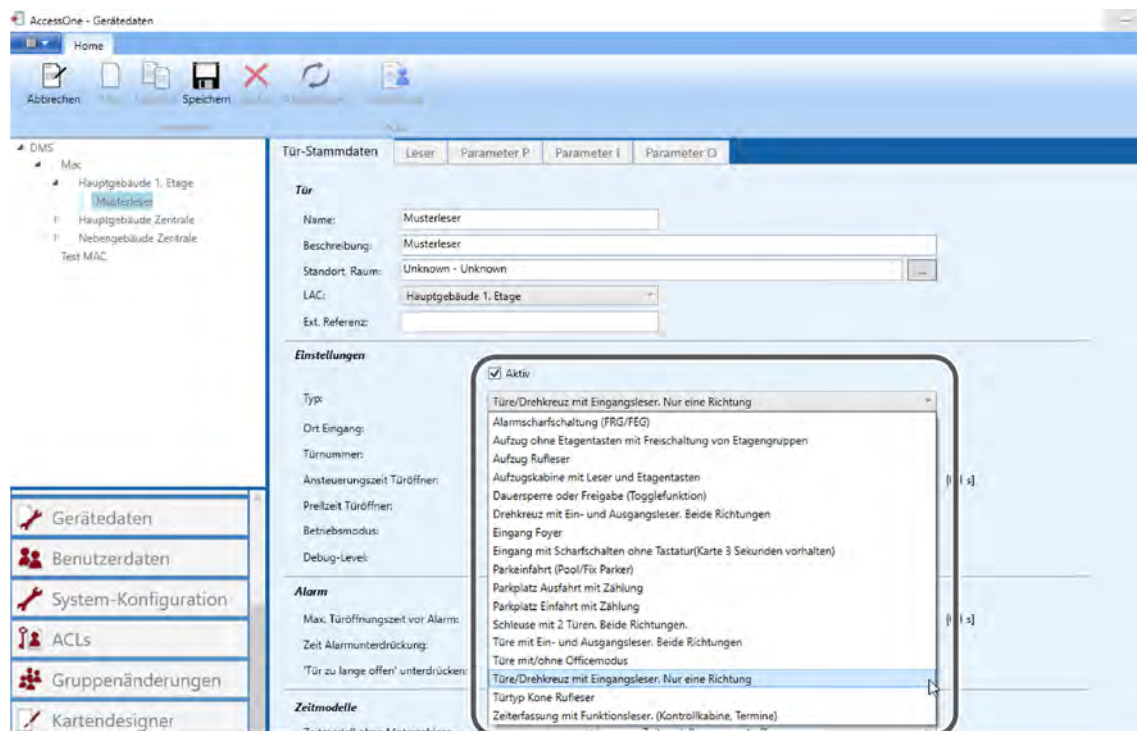
Um auf einer Türsteuerung (LAC) eine Tür anzulegen, wählen Sie die entsprechende Türsteuerung in der linken Auswahlliste an und klicken Sie auf den Button NEU. Im Fenster wird daraufhin rechts die Eigenschaftenseite für eine Türsteuerung angezeigt.



The screenshot shows the 'AccessOne - Gerätedaten' application window. The left sidebar contains a tree view with 'Hauptgebäude 1. Etage' selected, and a list of navigation buttons including 'Gerätedaten', 'Benutzerdaten', 'System-Konfiguration', 'ACLs', 'Gruppenänderungen', 'Kartendesigner', 'OSS', and 'Besucher / Termine'. The main window has a tabbed interface with 'Tür-Stammdaten' selected. The 'Tür' section contains fields for Name, Beschreibung, Standort, LAC, and Ex. Referenz. The 'Einstellungen' section includes checkboxes for 'Aktiv', dropdowns for 'Typ', 'Ort Eingang', and 'Ort Ausgang', and input fields for 'Türnummer', 'Ansteuerungszeit', 'Prellzeit', 'Mindestzeit', and 'Betriebsmodus'. The 'Alarm' section has input fields for 'Mx. Türöffnungszeit', 'Zeit Alarmunterdrückung', and checkboxes for 'Tür zu lange offen' and 'Tür Außenbruch'. The 'Zeitmodelle' section has four checkboxes for different door models. The bottom status bar shows 'Benutzer: admin', 'Zum Testplaner verfügbar', 'Arbeitsstation: INV-11537', 'Alle Ams und Mac online', 'Ereignisse: 0', and 'Timeout: nicht aktiviert'.

In diesem Tab werden die generellen Eigenschaften einer Tür festgelegt. Hierzu gehören neben einem aussagekräftigen Namen und der Angabe des Standorts auch der Typ der gewünschten Tür. Der Typ entscheidet darüber, wie der Begehungsablauf gestaltet ist und welche Ein- und Ausgabesignale Verwendung finden.

Die AccessOne stellt vorkonfigurierte Türmodelle zur Verfügung, die alle gängigen Aufgabenstellungen an einer Tür abdecken. Auf Wunsch können weitere, spezielle Türmodelle ergänzt werden, die kundenspezifische Anforderungen erfüllen. Wählen Sie den für Ihre Anwendung passenden Typ aus. Im folgenden Beispiel ist eine einfache Eingangstür mit nur einer Richtung gewählt.



Nachdem der Türtyp ausgewählt wurde, können über die Eingabefelder die grundsätzlichen Parameter dieses Zugangs eingestellt werden.

Bereich „Einstellungen“

Zu jedem Gerät gibt es die Checkbox „Aktiv“, über die das Gerät aktiviert wird. Erst wenn dieser Haken gesetzt ist, wird das Gerät mit Daten geladen und gestartet. Die Geräte können somit schon konfiguriert werden und erst nach der Installation aktiv gesetzt werden. Vorteil: nicht aktivierte Geräte werden vom System nicht überwacht. Vorkonfigurierte, aber nicht aktivierte Geräte, werden daher auch nicht als gestörte Geräte gemeldet.

Mit „Ort Eingang“ und „Ort Ausgang“ wählen Sie den Quell- und Zielbereich aus. Jede Tür in der AccessOne führt von einem Quellbereich in einen Zielbereich. Diese Bereiche können, müssen aber nicht unterschiedlich sein.

Beispiel: Wenn ihr Gebäude in mehrere Sicherheitsbereiche aufgeteilt ist, könnte z. B. ein Eingang vom Äußeren Sicherheitsbereich (ASB) in den Inneren Sicherheitsbereich (ISB) führen. Eine Zwischentür kann aber auch von ISB nach ISB führen.

Die Bereiche werden in der Dialogauswahl „System-Konfiguration“ im Tab „Bereiche“ angelegt. Für einen Bereich im Gebäude kann das System mitzählen, wie viele Personen sich dort momentan aufhalten und z. B. prüfen, ob die maximale Anzahl Personen erreicht ist. In diesem Fall würde kein weiterer Zutritt gewährt. Voraussetzung dafür ist, dass eine Person ohne Ausweis nicht in den jeweiligen Bereich gelangen kann und die Ein- und Ausgänge mit Vereinzelungsanlagen, z. B. Drehkreuzen, ausgestattet sind, so dass nicht gleichzeitig mehrere Personen mit einer Zutritts-Berechtigung den Bereich betreten.

Jede Tür benötigt an der Türsteuerung eine eindeutige Türnummer. Diese muss zwischen 1 und 8 liegen, da pro Türsteuerung maximal 8 Türen unterstützt werden.

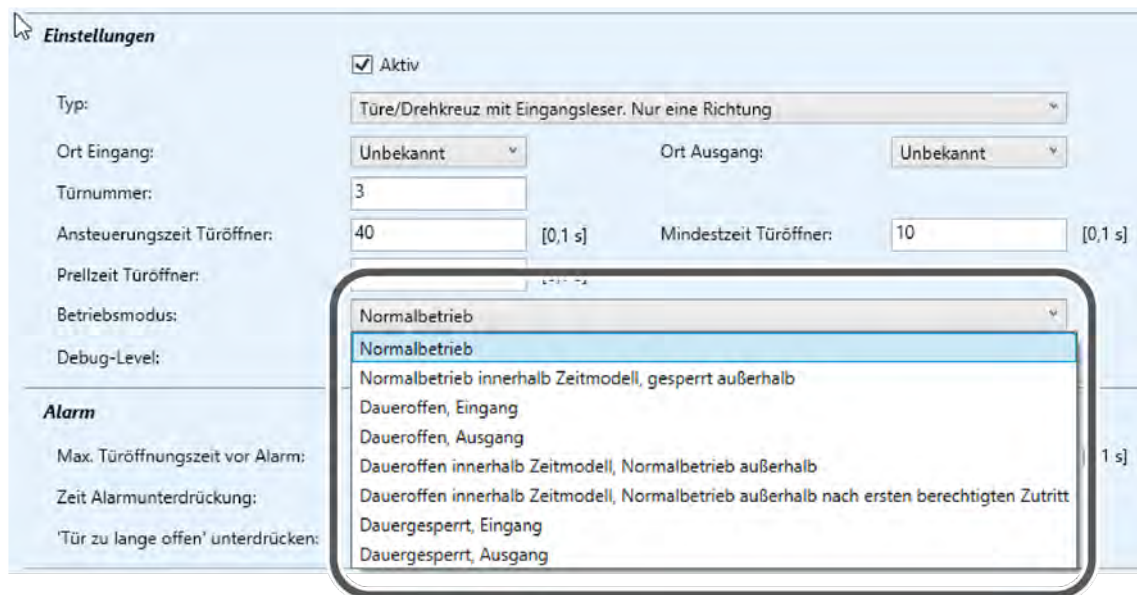
Der Wert im Feld „Ansteuerungszeit Türöffner“ legt fest, wie lange der Türöffner bei einem berechtigten Zu-

tritts-Medium maximal angesteuert wird. Die Angabe erfolgt in Zehntelsekunden. Die Eingabe 40 bedeutet im Beispiel also $40 \times 0,1 \text{ s} = 4 \text{ Sekunden}$. Wenn die Tür über einen Türkontakt verfügt, kann die Türsteuerung feststellen, dass die Tür geöffnet wurde. In diesem Fall wird die Freigabe in dem Moment zurückgenommen, sobald die Tür als geöffnet erkannt wird. Der Wert im Feld „Mindestzeit Türöffner“ ermöglicht es, in diesem Fall sicher zu stellen, dass der Türöffner lange genug betätigt wird, so dass eine sichere Öffnung gewährleistet ist.

 Es gibt Türöffnungskontakte, die im Schloss oder in der magnetischen Zuhaltvorrichtung integriert sind, und die die Tür als bereits geöffnet melden, wenn sie nur wenige Millimeter bewegt wurde. In diesem Fall würde ohne eine Angabe für die Mindestöffnungszeit die Türe direkt wieder verriegelt und ein Zugang wäre dann unter Umständen nicht möglich.

Der Wert im Eingabefeld „Prellzeit Türöffner“ gibt an, wie lange der AMC nach einer Begehung und dem Erkennen, dass eine Tür wieder geschlossen wurde, wartet, bevor er die Einbruchsüberwachung der Tür wieder aktiviert. Bei schweren Türen kann es vorkommen, dass ein Türflügel beim Zufallen im Rahmen etwas federt, so dass für die Türsteuerung die Tür erst einmal kurz geschlossen ist, dann wieder für den Bruchteil einer Sekunde offen und erst dann als dauerhaft geschlossen erkannt wird. Ohne diese Prellzeit gäbe es dann unter Umständen nach einer Begehung immer die Meldung über einen Türaufbruch.

Im Betriebsmodus kann unter folgenden Alternativen gewählt werden:



„Normalbetrieb“ (Standard): In diesem Modus kann die Tür nur mit der zugehörigen Berechtigung und einem gültigen Ausweis begangen werden.

„Daueroffen“: Der Türöffner ist immer aktiv, die grüne LED am Ausweisleser leuchtet permanent und jeder kann ohne Ausweis diese Tür öffnen.

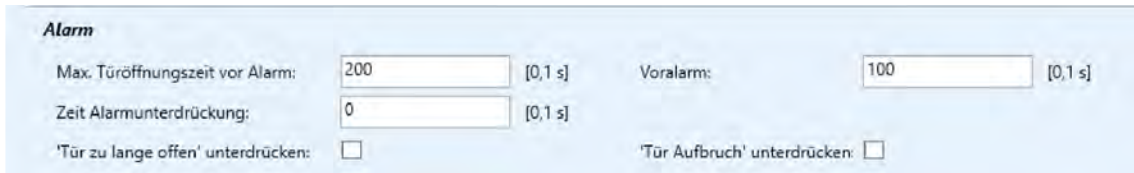
„Daueroffen innerhalb Zeitmodell, Normalbetrieb außerhalb“: Die Tür kann zu normalen Bürozeiten ohne Ausweis geöffnet werden, aber nach dieser frei definierbaren Zeit sollen nur noch berechtigte Personen Zutritt haben.

„Daueroffen innerhalb Zeitmodell, Normalbetrieb außerhalb nach ersten berechtigten Zutritt“: Nach der ersten berechtigten Öffnung bleibt die Tür offen. Die Tür wechselt innerhalb des gewählten Zeitmodells in den Zustand „daueroffen“. So wird sichergestellt, dass mindestens ein berechtigter Mitarbeiter anwesend ist.

„Normalbetrieb innerhalb Zeitmodell, gesperrt außerhalb“: Außerhalb des zugewiesenen Zeitmodells kann diese Tür nicht benutzt werden, auch nicht mit einem berechtigten Ausweis. Innerhalb des Zeitmodells sind zum Öffnen ein gültiger Ausweis und die entsprechende Berechtigung notwendig.

Alarm

Im Bereich „Alarm“ werden die Parameter für den Türalarm eingestellt.



„Maximale Türöffnungszeit vor Alarm“: Angabe, wie lange das System wartet, bis die Tür wieder geschlossen ist, bevor ein Alarm gemeldet wird. Dieser Wert wird in Zehntelsekunden angegeben. Wird die eingetragene Zeit überschritten, erzeugt das System eine Logbuchmeldung mit dem Text „Tür zu lange auf“.

„Voralarm“: Der Wert im Feld sollte kleiner sein, als der Wert im Feld davor. Er gibt an, wann ein Aufmerksamkeitssignal am Leser erzeugt werden soll. Somit kann die Person die Tür noch schließen, bevor es zur Alarmmeldung kommt. Ist die Tür länger offen als in diesem Wert angegeben, erzeugt der an der Tür montierte Ausweisleser wiederholt einen Piepton, bis die Tür wieder geschlossen wird oder die Alarmmeldung erzeugt wurde.

„Zeit Alarmunterdrückung“: Die Angabe ist erforderlich bei Türen, die permanent von einer zusätzlichen Einbruchmeldeanlage überwacht werden. Hier kann es erforderlich sein, dieser Anlage über ein Ausgangssignal mitzuteilen, dass die Tür jetzt berechtigt geöffnet wird. Dieses Signal wird zurückgenommen, kurz nachdem die Tür wieder geschlossen wurde, spätestens aber nach der Zeit, die dem Wert in diesem Feld entspricht.

„Tür zu lange offen unterdrücken“: Hier steuern Sie, ob das System eine Einbruchmeldung erzeugen soll oder nicht, wenn die Tür ohne Ausweis geöffnet wurde.

„Tür Aufbruch unterdrücken“: Mit dieser Checkbox steuern Sie das Alarmsignal vor Ort.



Das System erzeugt keine separaten Türzustandsmeldungen. Die Information, ob die Tür geöffnet wurde oder nicht, ergibt sich aus der entsprechenden Logbuchmeldung zum Zutritt.

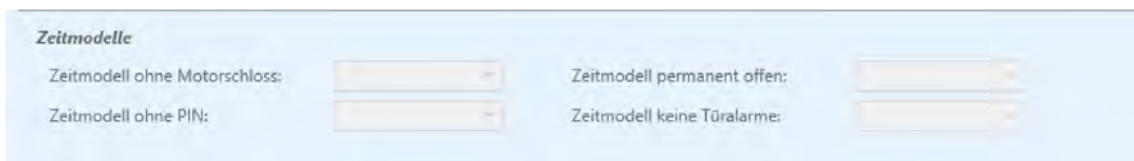
Logbuch-Einträge:

„Berechtigt, Zutritt“: Die Tür wurde nach berechtigter Buchung geöffnet.

„Berechtigt, kein Zutritt“: Die Tür wurde nicht geöffnet, obwohl sie freigegeben wurde.

Zeitmodelle

Im diesem Abschnitt können die zum generellen Verhalten ggf. gewünschten Zeitmodelle ausgewählt werden:



Insgesamt stehen vier Zeitmodelle zur Verfügung:

„Zeitmodell ohne Motorschloss“: Verfügt die Tür über ein Motorschloss, so wird die mechanische Beanspruchung reduziert, indem das Motorschloss nur vor und nach dem eingetragenen Zeitmodell aktiviert ist.

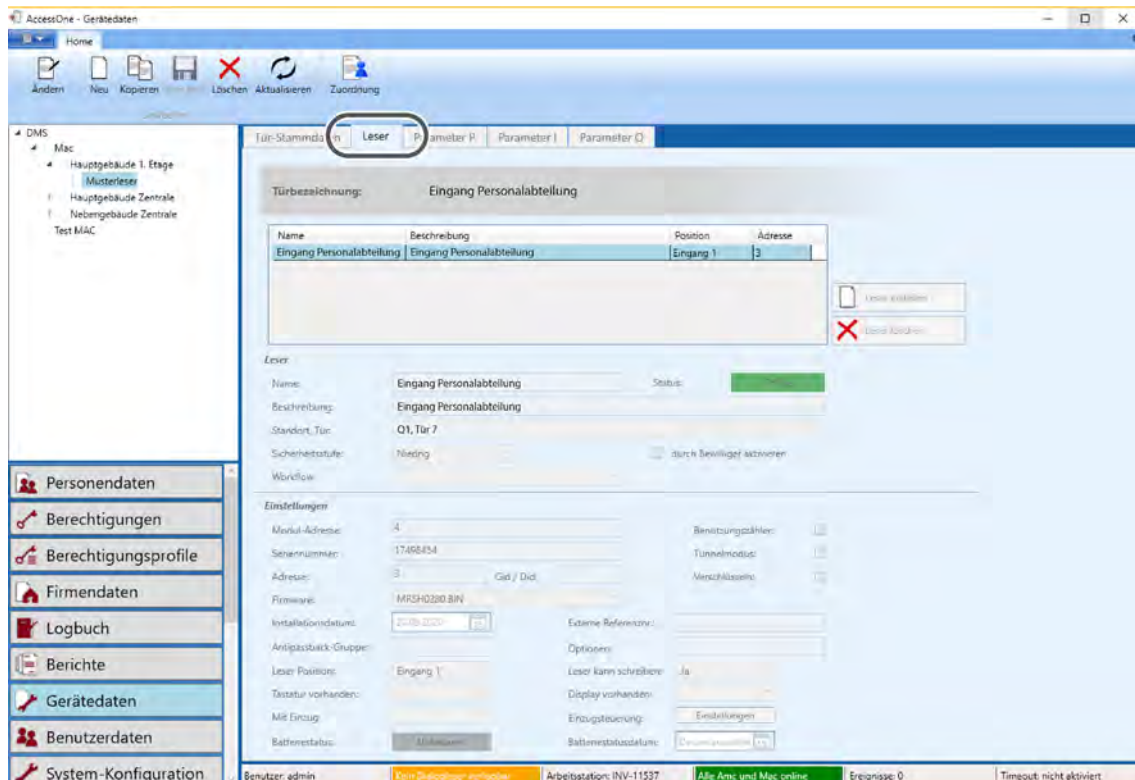
„Zeitmodell ohne PIN“: Die Eingabe des PIN-Codes am Ausweisleser wird auf Zeiten außerhalb des eingetragenen Zeitmodells eingeschränkt werden.

„Permanent offen“: Der Türöffner ist immer aktiv und die Tür kann ohne Ausweis passiert werden (Diese Einstellung entspricht dem Zeitmodell „Daueroffen“).

„Zeitmodell keine Türalarme“: Türalarme erfolgen nur außerhalb des eingetragenen Zeitmodells.

7.1.4.2 Leser

Auf dem Tab „Leser“ werden die zur Tür gehörenden Ausweisleser definiert.



Um einen neuen Leser zu erstellen, klicken Sie auf die Schaltfläche Leser erstellen. Das System fügt daraufhin eine neue Zeile in die Übersichtsliste ein und gibt Ihnen die Möglichkeit, die zum Leser gehörenden Parameter in die darunter stehenden Felder einzugeben.

Bereich „Leser“

Im Bereich „Leser“ machen Sie Angaben zu Name, Beschreibung, Standort, Sicherheitsstufe und Workflow.



Sicherheitsstufe

Bei der Sicherheitsstufe kann zwischen fünf verschiedenen Stufen von „sehr niedrig“ bis „sehr hoch“ gewählt werden. Dieser Leser darf nur in eine Berechtigung oder bei einer Person eingetragen werden, wenn der Benutzer an der Dialogstation eine mindestens gleichwertige oder höhere Sicherheitsstufe hat. Sie können über die Sicherheitsstufen steuern, dass nicht jeder AccessOne Benutzer die Zugangsberechtigung zu sensiblen Bereichen vergeben kann.

Die Checkbox „durch Bewilliger aktivieren“ macht eine zusätzliche Aktivierung durch einen Benutzer mit entsprechender Berechtigung nötig.

Workflow

Hier können Sie bestimmte Arbeitsschritte erstellen, die von einem Vorgesetzten genehmigt werden müssen, zum Beispiel die Vergabe von Berechtigungen für einen bestimmten Bereich.

Bereich „Einstellungen“

Im Bereich „Einstellungen“ geben Sie die technischen Eigenschaften des Ausweislesers an.

Modul-Adresse

Das erste Feld ist ein reines Anzeigefeld und gibt den vom System vergebenen internen Leserindex an. Dieser wird für die Zusammenstellung der Berechtigungen verwendet und kann nicht verändert werden.

Seriennummer des Kartenlesers

Die Seriennummer des Lesers wird benötigt, um die interne Busadressierung des Lesers durchzuführen. Bei diesen Lesern kann die Busadresse nicht per Dip-Schalter eingestellt werden, sondern wird über eine Konfigurationssoftware gesteuert. Die AccessOne ordnet die Adresse automatisch zu, wenn die Seriennummer des Lesers eingetragen wurde. Meldet sich z. B. ein auf Adresse 3 konfigurierter Leser nicht, versucht die Türsteuerung diesen Leser an Hand der Seriennummer zu identifizieren. Bei erfolgreicher Identifizierung wird ihm die entsprechende Adresse, hier: 3, zugewiesen.

Adresse (manuelle Eintragung)

Jeder Leser muss eine Busadresse zwischen 1 und 8 haben.



Abhängig vom Leserprotokoll wird auf die Busadresse noch ein fester Zahlenwert addiert, da in einigen Leserprotokollen die Adressen von A bis H vergeben sind. Dies erfolgt automatisch, da in der Türsteuerung die Konventionen der verschiedenen Leserprotokolle hinterlegt sind.

Firmware

Auswahlfeld für die Firmware-Version. Angezeigt wird die jeweils aktuelle Version.

GID/DID

Sind an der Türsteuerung Leser mit einem alten V-Protokoll oder 9er-Protokoll angeschlossen, muss zusätzlich zur logischen Busadresse noch eine Gruppen ID (GID) und eine Device ID (DID) angegeben werden. Die GID bildet dabei die Zehnerstelle und die DID die Einerstelle. Beide Werte müssen zwischen 1 und 8 liegen. Beispiel: Der Wert „12“ beschreibt eine Leseradresse mit GID 1 und DID 2.

Benutzungszähler

Der Leser prüft, ob der Ausweis die für diesen Tag maximale Nutzung erreicht hat.

Tunnelmode

Nur bei LEGIC-Lesern mit DE-Bus relevant. Deister Ausweisleser können, wie die meisten anderen Leser auch, bei LEGIC-Karten nur einen Stamp auswerten. Hat die Karte mehr als ein Segment und sollen alle Segmente ausgewertet werden, muss daher die Intelligenz des Lesers abgeschaltet und der so genannte Tunnelmode benutzt werden. Hierbei werden die Kommandos an den LEGIC-Chip zum Suchen und Lesen eines Segments vom Leser an den Mastercontroller weitergegeben. Die Firmware des AMC kann dann die Segmente die in den

Leserformaten der AccessOne aktiviert sind, nacheinander lesen.

Bei DE-Bus und Datasec-Bus kann die Kommunikation zum Ausweisleser auch AES-verschlüsselt betrieben werden.

Verschlüsseln

Die Verbindung zwischen MAC und Controller ist extra verschlüsselt.

Installationsdatum

Wird bei Anlegen des Lesers automatisch mit dem aktuellen Tag vorbesetzt, kann aber beliebig geändert werden. Das Installationsdatum dient der Anlagendokumentation.

Externe Referenznummer

Für kundeninterne Bezeichnung.

Optionen

Für kundeninterne Bezeichnung.

Antipassback-Gruppe (zeitbezogen)

Verhindert, dass ein Zutritts-Medium nach der Begehung an eine andere Person weitergegeben wird und dieser mit demselben Zutritts-Medium ebenfalls eintritt. Um nebeneinander befindliche Türen gleich zu behandeln, können diese in einer Gruppe zusammengefasst werden. Leser mit gleicher Antipassback-Gruppe werden so behandelt, als ob sie nebeneinander montiert sind und den gleichen Zugang bedienen. Ein Zutritts-Medium, das an einem Leser dieser Gruppe genutzt wurde, ist an allen anderen Leser derselben Gruppe für eine bestimmte Zeit gesperrt (Die Zeitspanne ist in den Tür-Parametern einstellbar). Der eingetragene Wert ist eine Zahl zwischen 1 und 99. Es können bis zu 99 Türgruppen gebildet werden.

Leser Position

Eine Tür kann in der AccessOne mit bis zu vier Lesern ausgestattet sein: je zwei für Eingangs- und Ausgangsrichtung. Beispiel: Bei KFZ-Einfahrten kann es sinnvoll sein, über dem Leser für PKWs auch einen in einer höheren Position für LKWs zu montieren.

Leser kann schreiben

Der Leser kann Karten beschreiben. Beispiel: Aktualisierung von Zutrittsrechten bei Offline-Schließgeräten. Bei einigen Lesern kann die Software das automatisch erkennen, bei anderen muss dies explizit angegeben werden. Wird kein Wert angegeben, wird die eventuell vorhandene Schreibfunktion des Lesers nicht verwendet.

Tastatur vorhanden

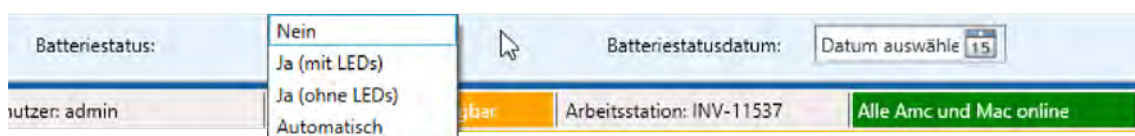
Bei einigen Zugängen ist die Eingabe eines PIN-Codes zum Scharfschalten der Einbruchmeldeanlage (EMA) oder zusätzlich zum biometrischen Merkmal beim Zutritt notwendig. Da bei einigen Lesern die Tastatur über einen Steuerbefehl von der Türsteuerung aktiviert werden muss, ist hier die Möglichkeit geschaffen, dies explizit anzugeben. In den meisten Fällen erkennt die Türsteuerung das Vorhandensein einer Tastatur automatisch.

Display vorhanden

Ein Display am Leser wird nur dann angesteuert, wenn hier ein entsprechender Eintrag erfolgt.

Mit Einzug

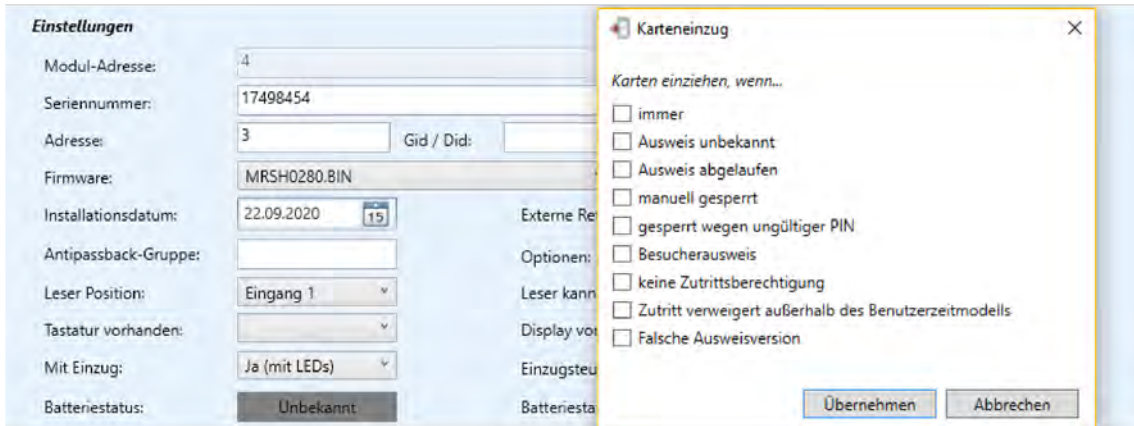
Hier kann eingetragen werden, ob der Leser mit einem Motoreinzug ausgestattet ist.



Ist der Motoreinzugsschacht mit LEDs ausgestattet, müssen diese an Stelle der LEDs am Leser angesteuert werden. In diesem Fall wählen Sie „Ja (mit LEDs)“. Bei der Auswahl „Ja (ohne LEDs)“ werden die Leuchtdioden des Lesers angesteuert.

Einzugssteuerung

Bei vorhandenem Motoreinzug, wird hier festgelegt, ob die Karte nach dem Lesen wieder ausgegeben wird bzw. unter welchen Bedingungen sie eingezogen werden soll.



Einstellungen

Modul-Adresse: 4

Seriennummer: 17498454

Adresse: 3 Gid / Did:

Firmware: MRS_H0280.BIN

Installationsdatum: 22.09.2020 15

Antipassback-Gruppe:

Leser Position: Eingang 1

Tastatur vorhanden:

Mit Einzug: Ja (mit LEDs)

Batteriestatus: Unbekannt

Karteneinzug

Karten einziehen, wenn...

- ☒ immer
- ☐ Ausweis unbekannt
- ☐ Ausweis abgelaufen
- ☐ manuell gesperrt
- ☐ gesperrt wegen ungültiger PIN
- ☐ Besucherausweis
- ☐ keine Zutrittsberechtigung
- ☐ Zutritt verweigert außerhalb des Benutzerzeitmodells
- ☐ Falsche Ausweisversion

Übernehmen Abbrechen

7.1.4.3 Parameter P

Tür-Stammdaten

Leser

Parameter P

Parameter I

Parameter O

Türbezeichnung: Eingang Personalabteilung

Allgemeine Parameter

Parameter	Richtung	Wert
Optionen	Eingang	0
Vereinzelung	Eingang	Nein
Bereichüberprüfung	Eingang	0
AntiPassBack Zeit	Eingang	0
Bereichüberprüfung	Eingang	0
Begleiter erforderlich	Eingang	Nein
Gruppenbegehung	Eingang	
Benutzungszähler	Eingang	Nein
Offline Schreibfehler ignorieren	Eingang	Nein
Offline Daten immer aktualisieren	Eingang	Nein
Pincode erforderlich	Eingang	Nein
Impulszeit Scharfschaltung	Eingang	0
Automatische Scharfschaltung	Eingang	0
Impulszeit Freigabe Bedienteil	Eingang	0
Zeit für Pressalarm	Eingang	0
Taste für Pressalarm	Eingang	0

Dieser Tab enthält die Parameter, die die Ablaufsteuerung der Tür betreffen. Abhängig von der Komplexität des gewählten Türtyps, werden auf dieser Seite mehr oder weniger Parameter aufgeführt. Im Folgenden wird beispielhaft die Standardtür mit einer Durchgangsrichtung betrachtet. Bei Türen, die in beide Richtungen begangen werden können, sind die Parameter jeweils für die Eingangs- und Ausgangsrichtung vorhanden.

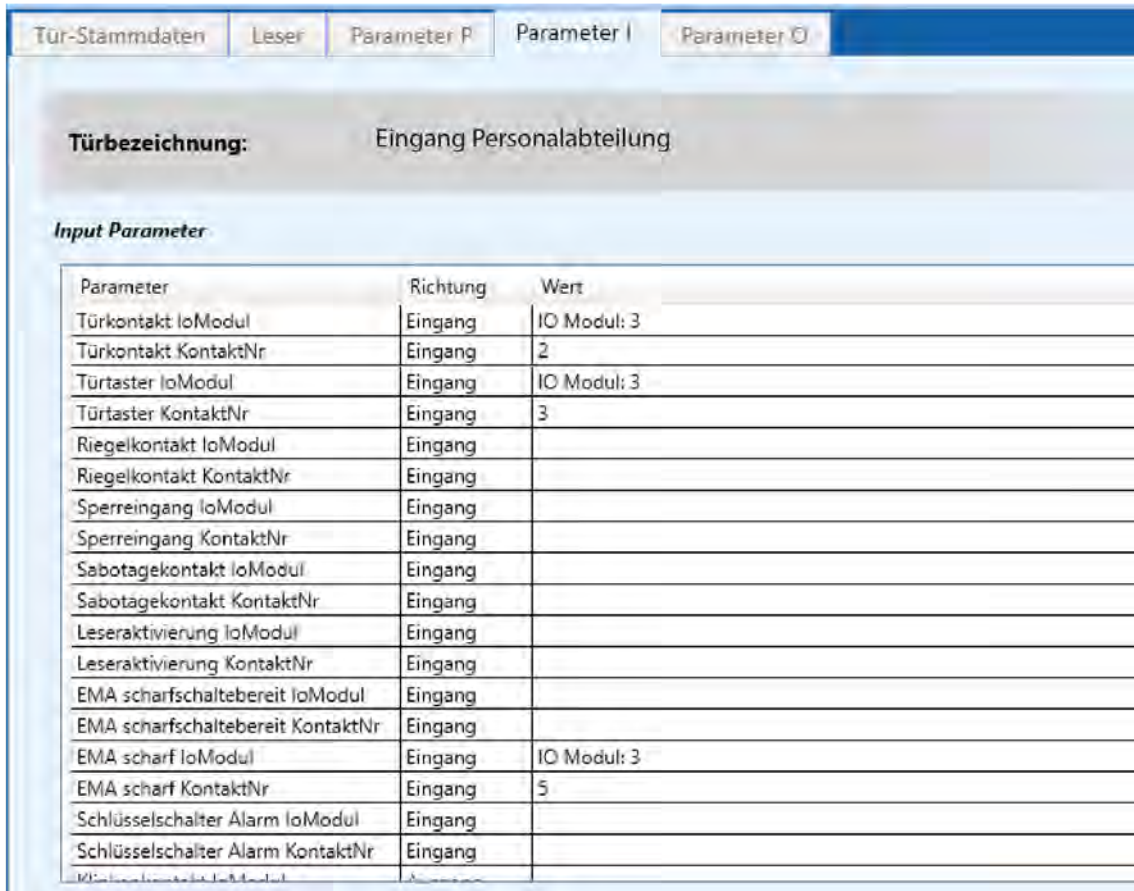
Optionen	Optionen werden verwendet, um kundenspezifische Sonderbehandlungen zu ermöglichen. Bei jedem Türtyp bewirkt der Wert 1, dass an dieser Tür das Zeitmodell zur Berechtigung ignoriert wird. Eine sinnvolle Anwendung dafür ist z. B. der Ausgangsleser. Beispiel: Eine Person soll nach 17 Uhr das Gebäude nicht mehr betreten aber dennoch verlassen können. Der Eingangsleser würde nach 17 Uhr die Person mit der Meldung „Nicht berechtigt, außerhalb des gültigen Zeitmodells“ abweisen. Der Ausgangsleser prüft mit gesetzter Option 1 nur, ob für diesen Leser eine Berechtigung existiert und ignoriert das Zeitmodell.
Vereinzelung	Hier wird festgelegt, ob die Steuerung verlangt, dass nach jedem berechtigten Zutritt die Türe erst wieder geschlossen werden muss, bevor die nächste Karte akzeptiert wird.

Zufallsgeber Rate in %	Wenn gewünscht wird, dass eine Taschenkontrolle zufällig durchgeführt werden soll, kann hier über einen Wert zwischen 0–100 der Prozentsatz eingestellt werden. Die Software nutzt einen Zufallsgenerator. Beispiel: Ein Wert von 50 bedeutet, dass bei 100 Durchtritten genau 50 Personen mit der Meldung „Berechtigt zur Kontrolle“ abgewiesen werden. In der Folge wird eine Sperre für diese Person gesetzt, die nach der Kontrolle vom Sicherheitspersonal wieder gelöscht werden muss. Die Sperre bewirkt, dass ein Zutritt auch an anderen Zugängen abgewiesen wird.
Antipassback-Zeit	Angabe, wie lange eine Karte nach erfolgter Benutzung an Lesern derselben Antipassbackgruppe gesperrt ist (Zeit in Sekunden).
Bereichskontrolle	Der Aufenthaltsort (= Bereich) einer Person wird von der AccessOne bei jeder Ausweisnutzung an einem Leser mitgeführt. Daher kann die Türsteuerung auch prüfen, ob die Person, die gerade ihre Karte vor den Leser gehalten hat, überhaupt im gleichen Bereich gemeldet ist, in dem der Leser positioniert ist. Ist das nicht der Fall, ist die Person ohne die Karte an einem Leser zu benutzen durch eine offene Tür gegangen, oder die Karte wurde entwendet. Ist die Bereichskontrolle eingeschaltet, kann nur dann eine Tür passiert werden, wenn der Aufenthaltsort mit dem Ort des Ausweislesers übereinstimmt. Voraussetzung dafür ist eine saubere Trennung der Zutrittsbereiche und eine ständige Ein- und Ausgangskontrolle über das Zutrittskontrollsystem.
Begleiter erforderlich	Besucher dürfen bestimmte Bereiche nicht ohne Begleitung betreten. Die Türsteuerung verhält sich so, dass nach der Erkennung einer Besucherkarte für maximal 10 Sekunden auf eine zweite Karte, die eine Eigenpersonalkarte sein muss, gewartet wird. Erst wenn dies erfolgt ist und die begleitende Person die für diese Tür notwendige Berechtigung hat, wird die Tür freigegeben. Während der Wartezeit blinkt die grüne LED am Leser um zu signalisieren, dass zwar eine Berechtigung vorhanden ist, aber eine weitere Karte erwartet wird.
Gruppenbegehung	Wenn es erforderlich ist, dass mehrere Personen nötig sind, um einen Bereich betreten zu dürfen, kann dies über diesen Parameter eingestellt werden. Wird z. B. der Wert 3 eingetragen, müssen mind. drei Ausweise von verschiedenen berechtigten Personen hintereinander vor den Leser gehalten werden, bevor die Tür freigegeben wird.
Benutzungszähler	In der AccessOne kann ein Ausweis mit einer maximalen Nutzung angelegt werden. Wird dieser Wert beim Ausweis auf den Wert 1 gesetzt, ist dies vergleichbar mit einer einmalig nutzbaren Eintrittskarte. Jeder Leser, der diesen Parameter gesetzt hat, prüft, ob die maximale Nutzung beim Ausweis noch größer als Null ist. Falls ja, und wenn die Person die notwendige Berechtigung hat, wird die Tür freigegeben und zählt die Nutzung herunter. Ist der Zähler bei Null angekommen, öffnet sich keine Tür mehr, bei der dieser Parameter ebenfalls gesetzt ist. Wird dieser Parameter am Leser des Gebäudeeingangs gesetzt, wird erreicht, dass der Besucher das Gebäude genau einmal betreten kann. Innerhalb des Gebäudes wird der Zähler nicht geprüft und der Besucher wird hier nicht eingeschränkt.

Offline Schreibfehler ignorieren	Dieser Parameter ist nur bei einem vorhandenen Offline-Schließsystem sinnvoll und steuert, ob ein Zugang auch dann freigegeben werden soll, wenn das Schreiben der Zutrittsberechtigung für die Offlinetüren ohne Fehler durchgeführt werden konnte. Im Normalfall öffnet sich die Tür nur dann, wenn der Karteninhaber seine Karte so lange vor den Leser gehalten hat, dass diese erfolgreich beschrieben werden konnte.
Offline Daten immer aktualisieren	Um zu viele Schreibvorgänge zu vermeiden, aktualisiert die Türsteuerung die Karte nur, wenn mindestens die Hälfte der Gültigkeitszeit abgelaufen ist. Diese Aktualisierung findet jedoch nur bei Offline-Schließsystemen statt.
PIN Code erforderlich	Dieser Wert legt fest, ob ein PIN-Code für den Zutritt eingegeben werden muss. Setzt voraus, dass der Leser über eine Tastatur verfügt.

7.1.4.4 Parameter I

Auf dieser Seite werden die Eingabesignale (Inputs) festgelegt, d.h. mit welchem Eingang am jeweiligen IO-Board die Rückmeldekontakte der angeschlossenen Peripherie verbunden sind.



Parameter	Richtung	Wert
Türkontakt IoModul	Eingang	IO Modul: 3
Türkontakt KontaktNr	Eingang	2
Türtaster IoModul	Eingang	IO Modul: 3
Türtaster KontaktNr	Eingang	3
Riegelkontakt IoModul	Eingang	
Riegelkontakt KontaktNr	Eingang	
Sperreingang IoModul	Eingang	
Sperreingang KontaktNr	Eingang	
Sabotagekontakt IoModul	Eingang	
Sabotagekontakt KontaktNr	Eingang	
Leseraktivierung IoModul	Eingang	
Leseraktivierung KontaktNr	Eingang	
EMA scharfschaltebereit IoModul	Eingang	
EMA scharfschaltebereit KontaktNr	Eingang	
EMA scharf IoModul	Eingang	IO Modul: 3
EMA scharf KontaktNr	Eingang	5
Schlüsselschalter Alarm IoModul	Eingang	
Schlüsselschalter Alarm KontaktNr	Eingang	

Die Bedeutung der einzelnen Eingangssignale, unabhängig vom Türtyp:

Türkontakt IoModul	IO-Modul, an dem der Türkontakt angeschlossen ist (Input).
Türkontakt KontaktNr	Nummer des Kontaktes auf diesem Modul.
Türtaster IoModul	IO-Modul, an dem der Request to Exit (Handfreigabe) Kontakt angeschlossen ist.
Riegelkontakt IoModul	Ein zusätzliches Signal, das angibt, ob die Tür nicht nur geschlossen, sondern auch der Sperriegel ausgefahren ist.
Sperreingang IoModul	IO-Modul an dem der Kontakt zum Sperren des Durchtritts angeschlossen ist.
Sabotagekontakt IoModul	Wird dieses Signal erkannt, wird eine Sabotagemeldung erzeugt und das Sabotagerelais gesetzt.
Gruppenbegehung	Wenn es erforderlich ist, dass mehrere Personen nötig sind, um einen Bereich betreten zu dürfen, kann dies über diesen Parameter eingestellt werden. Wird z. B. der Wert 3 eingetragen, müssen mind. drei Ausweise von verschiedenen berechtigten Personen hintereinander vor den Leser gehalten werden, bevor die Tür freigegeben wird.
Leseraktivierung IoModul	IO-Modul an dem der Schleifenkontakt/Lichtschranke angeschlossen ist.
EMA scharfschaltebereit IoModul	IO-Modul an dem der Kontakt „Alarmanlage bereit“ angeschlossen ist.

EMA scharf IoModul	IO-Modul an dem der Kontakt „Alarmanlage scharf“ angeschlossen ist.
Schlüsselschalter Alarm IoModul	IO-Modul an dem der (Schlüssel-)Kontakt „bitte Alarmanlage scharfschalten“ angeschlossen ist.
Klinkenkontakt IoModul	Wird ausgelöst, wenn bei einer Tür von der Innenseite, die keinen Ausweiser hat, der Drücker (Türklinke) betätigt wird. Dadurch wird eine Einbruchmeldung bei der Öffnung mit dem Drücker vermieden.
Schlüsselkontakt IoModul	Analog zum Klinkenkontakt bedeutet ein gesetztes Signal, dass die Tür mit einem Schlüssel geöffnet wird.

7.1.4.5 Parameter O

Auf dieser Seite werden die Ausgangssignale (Outputs) festgelegt, d.h. mit welchem Relaisausgang am jeweiligen IO-Board die Aktoren der angeschlossenen Peripherie verbunden sind.

Tür-Stammdaten
Leser
Parameter P
Parameter I
Parameter O

Türbezeichnung: Eingang Personalabteilung

Output Parameter

Parameter	Richtung	Wert
Türöffner IoModul	Eingang	IO Modul: 3
Türöffner RelaisNr	Eingang	1
Alarmunterdrückung IoModul	Eingang	
Alarmunterdrückung RelaisNr	Eingang	
Motorschloss IoModul	Eingang	
Motorschloss RelaisNr	Eingang	
Türalarm IoModul	Eingang	
Türalarm RelaisNr	Eingang	
Voralarm IoModul	Eingang	
Voralarm RelaisNr	Eingang	
EMA scharfschalten IoModul	Eingang	
EMA scharfschalten RelaisNr	Eingang	
Zusatzrelais-1 IoModul	Eingang	
Zusatzrelais-1 RelaisNr	Eingang	
Zusatzrelais-2 IoModul	Eingang	
Zusatzrelais-2 RelaisNr	Eingang	
Licht IoModul	Eingang	
Licht RelaisNr	Eingang	
Kontaktschaltung IoModul	Eingang	

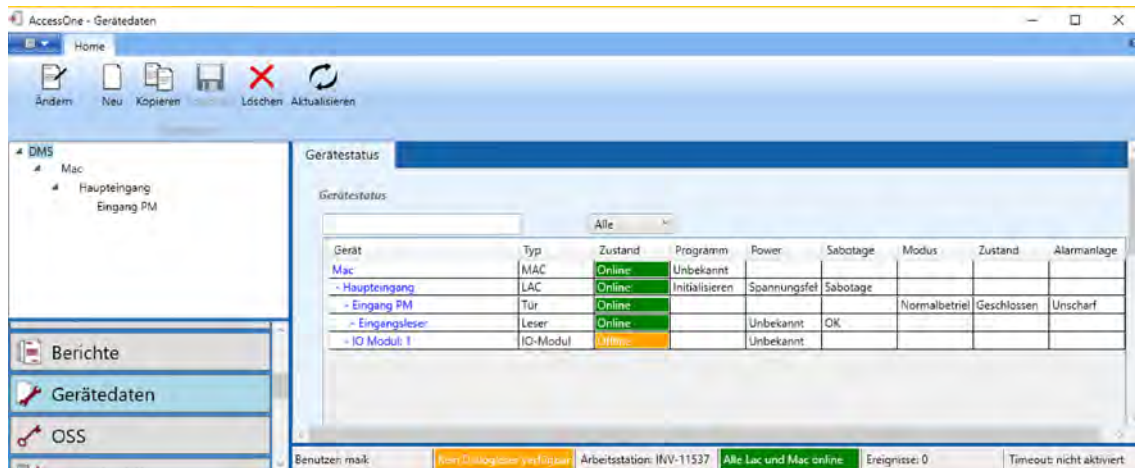
Die Bedeutung der einzelnen Ausgangssignale:

Türöffner IoModul	IO-Modul, an dem das Türöffnerrelais angeschlossen ist (Output).
Alarmunterdrückung IoModul	IO-Modul, an dem das Relais für die Alarmunterdrückung angeschlossen ist (Output).
Motorschloss IoModul	Bei selbstverriegelnden Türen muss zusätzlich zum Türöffner auch das Motorschloss angesteuert werden, um den Riegel einzufahren. Dieses Ausgangssignal kann mit einem Zeitmodell kombiniert werden. Ist die Tür im Zustand „Daueroffen“ wird dieses Signal permanent gesetzt.
Türalarm IoModul	Ausgangssignal für die EMA. Es wird immer dann gesetzt, wenn eine Tür unberechtigt geöffnet wurde oder zu lange offen ist. Das Setzen dieses Signals kann über Parameter unterdrückt werden.
Voralarm IoModul	Ist für eine Tür eine Voralarmzeit eingetragen, wird nach der Türöffnung und Ablauf der eingestellten Zeit dieses Signal gesetzt.
EMA scharfschalten IoModul	IO-Modul an dem das Relais zum Scharfschalten der Alarmanlage angeschlossen ist (Output).
Zusatzrelais-1 IoModul	IO-Modul an dem das Relais zur Sonderfunktion 1 angeschlossen ist (Output).

Zusatzrelais-2 IoModul

IO-Modul an dem das Relais zur Sonderfunktion 2 angeschlossen ist (Output).

7.1.5 Gerätestatus anzeigen



Klicken Sie mit der linken Maustaste auf den Eintrag „DMS“ im Strukturbaum, wenn Sie den Status aller Geräte in der Übersicht sehen möchten. Den Status eines einzelnen Gerätes (Online oder Offline) sehen Sie in der Detailansicht zum Gerät. Sie können diesen Eintrag nicht löschen und auch keinen zweiten anlegen.

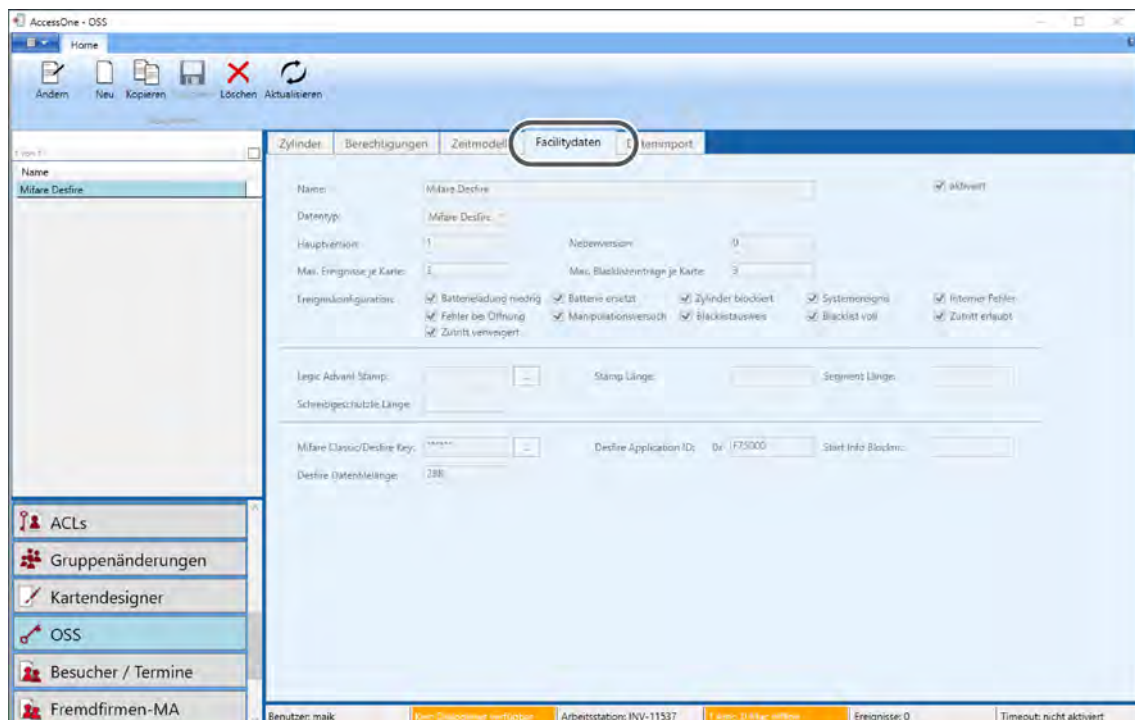
Rechtsklicken auf „DMS“ erzeugt eine weitere Auswahlmöglichkeit. Hier kann ein neuer MAC, ein neuer EMC oder ein neuer PS-Online (Schlüsselkabinett) angelegt werden.

7.2 Gerätedaten Offline-Geräte (OSS-SO)

Zu jeder Installation von OSS Standard Offline müssen Facilitydaten angelegt werden. Hier werden die Grunddaten für die Offline-Geräte wie Zylinder und Beschläge eingegeben. Über diese Daten wird unter anderem festgelegt, wie groß der Speicher für die Offline-Daten auf dem Transponder ist und wie viel Platz für Ereignisse und Sperrlisteneinträge reserviert werden soll. Bei Mifare enthalten die Facilitydaten die Zugriffsschlüssel auf die Offline Segmente der Karte und die Applikations-ID, bei LEGIC wird hier der Stamp hinterlegt.

7.2.1 Facilitydaten

Die Facilitydaten sind im Regelfall von CES vorinstalliert, sie können aber auch vom Benutzer eingetragen oder verändert werden. Es gibt einen Datensatz pro System. Um einen neuen Eintrag anzulegen, klicken sie in der Werkzeugeiste auf Neu.



Vergeben Sie einen Namen und wählen Sie den Datentyp. Tragen Sie die Haupt- und Nebenversionsnummer ein (z. B. die Ziffern 1 und 0 für die Version 1.0). Die Versionsnummer ist als Unterscheidungsmerkmal notwendig.

Im Bereich der „Ereigniskonfiguration“ wird eingestellt, welche Ereignisse vom Zylinder auf die Karte zurückgeschrieben werden sollen. Diese Einstellungen gelten systemweit, sie werden also am Updater für alle Transponder auf die gleiche Art geschrieben.

Für ein LEGIC advant System tragen Sie den Stamp und die Stamplänge ein. Klicken Sie für die Eingabe des Stamps auf die Schaltfläche hinter dem Eingabefeld. Sowohl Stamp als auch Schlüssel werden üblicherweise in hexadezimaler Schreibweise angegeben, d.h. es sind die Zahlen von 0–9 und die Buchstaben von A bis F zulässig. Insgesamt muss der Schlüsselwert für Mifare DESFire 32 Stellen lang sein (Mifare Classic 12 Stellen).



Die Zugriffsschlüssel werden verschlüsselt in der Datenbank abgelegt. Einmal eingegeben, wird dieser Wert aus Sicherheitsgründen niemals (!) mehr im Klartext angezeigt, es kann nur ein neuer Wert angegeben werden.



Wenn Sie den Schlüssel ändern, wird diese Änderung sofort aktiv. Das kann bedeuten, dass ab diesem Zeitpunkt kein Transponder mehr aktualisiert werden kann.

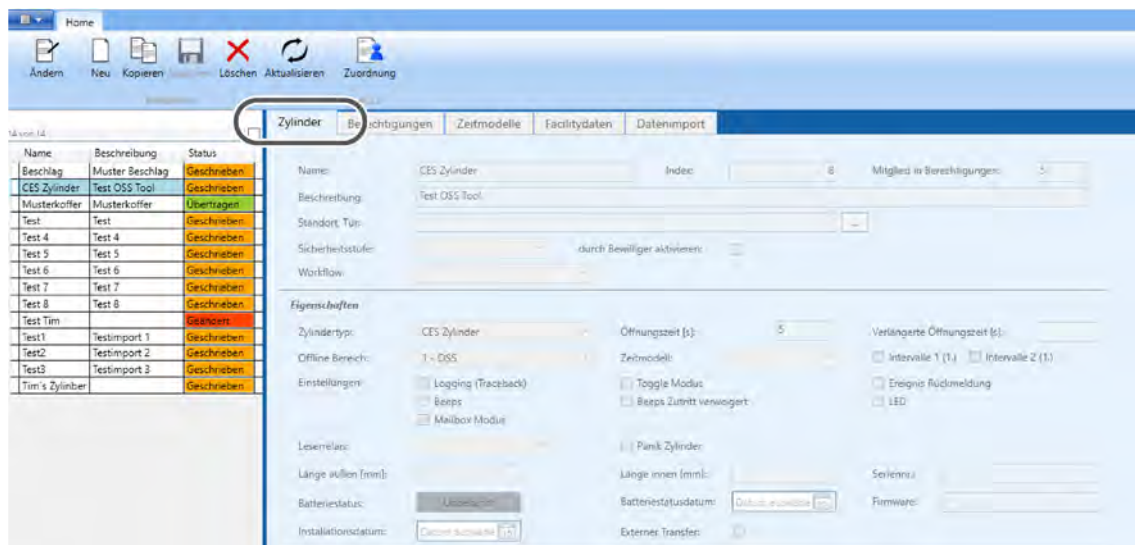
Klicken Sie auf **SPEICHERN** in der Werkzeugleiste, wenn die Angaben vollständig sind.

7.2.2 Zylinder (und Beschläge)

Auf diesem Tab werden die Offline Komponenten angelegt. Klicken Sie in der Werkzeugleiste auf **NEU** und tragen Sie die Daten für den Zylinder ein.



Geben Sie im Feld „Beschreibung“ den genauen Einbauort an. Offline-Systeme sind batteriebetrieben und als Standard Offline Komponenten in der Lage, den Batteriestatus auf den Transponder zurückzuschreiben, wenn die Batterie einen bestimmten Spannungswert unterschreitet. Für den Austausch einer schwachen Batterie muss der Einbauort bekannt sein.



Name	Beschreibung	Status
Beschlag	Muster Beschlag	Geschrieben
CES Zylinder	Test OSS Tool	Geschrieben
Musterkoffer	Musterkoffer	Übertragen
Test	Test	Geschrieben
Test 4	Test 4	Geschrieben
Test 5	Test 5	Geschrieben
Test 6	Test 6	Geschrieben
Test 7	Test 7	Geschrieben
Test 8	Test 8	Geschrieben
Test Tim	Test Tim	Geschrieben
Test1	Testimport 1	Geschrieben
Test2	Testimport 2	Geschrieben
Test3	Testimport 3	Geschrieben
Tim's Zylinder	Testimport 3	Geschrieben

Name:	CES Zylinder	Index:	8	Mitglied in Berechtigungen:	5
Beschreibung:	Test OSS Tool				
Standort Tür:					
Sicherheitsstufe:	durch Bewilliger aktivieren				
Workflow:					

Eigenschaften		
Zylindertyp:	CES Zylinder	Öffnungszeit (s):
Offline Bereich:	1 - OSS	Verlängerte Öffnungszeit (s):
Einstellungen:	☐ Logging (Traceback) ☐ Beeps ☐ Mailbox Module	Zeitmodell: ☐ Toggle Modus ☐ Beeps Zutritt verweigert ☐ Ereignis Rückmeldung ☐ LED
Leserrelais:		
Länge außen (mm):	Länge innen (mm):	Plank Zylinder:
Batteriestatus:	Batteriestatusdatum:	Seitenansicht:
Installationsdatum:	Externes Transfer:	Firmware:

Die Zylinder und Beschläge werden über die Nummer eindeutig unterschieden. Die AccessOne vergibt die Nummer beim Anlegen und Speichern eines neuen Zylinders automatisch (Anzeige im Feld „Index“).

Bereich „Eigenschaften“

Machen Sie weitere Angaben zum verbauten Gerät.

Zylindertyp

Auswahl zwischen Zylinder, Beschlag und Wandterminal. Die Geräte können unterschiedliche Batterien benötigen.

Öffnungszeit

Gibt an, wie lange der Zylinder bei einem berechtigten Zutritt eingekuppelt bleibt. Ein Wert von 5–10 Sekunden ist allgemein ausreichend (Standardeinstellung: 5).

verlängerte Öffnungszeit

Für bestimmte Personengruppen kann die Standard-Öffnungszeit verlängert werden.

Offline-Bereich

Die Offline Bereichsnummer (Site-ID) muss bei Standard Offline immer angegeben werden. Eine 0 ist hier nicht zulässig. Über die Bereichsnummer kann eine Installation in mehrere Bereiche geteilt werden. In diesem Fall gibt es den Zylinder mit der Nummer 1 dann mehrfach, nämlich einmal für jeden Bereich. Dies bedeutet, dass die Zylinder Nummer nur in Verbindung mit der Bereichsnummer eindeutig ist. Beim Wechsel, von einem Bereich in den anderen löscht der Updater die Daten des vorherigen Bereichs und ersetzt sie durch die des aktuellen Bereichs. Durch Aufteilung in mehrere Bereiche, kann die Anzahl der Offline-Schließgeräte in einer Installation theoretisch beliebig groß werden.

Zeitmodell

Auswahlmöglichkeiten zum Zeitmodell. Funktion ist abhängig von Gerätetyp und Hersteller.

Intervalle 1 und 2

Funktion ist abhängig von Gerätetyp und Hersteller.

Einstellungen

Einstellungsmöglichkeiten sind abhängig von Gerätetyp und Hersteller.

Leserrelais

Funktion ist abhängig von Gerätetyp und Hersteller.

Panikzylinder

Angabe zum Gerätetyp.

Länge

Angabe zu Länge Innen und Außen.

Seriennummer

Angabe der Seriennummer.

Batteriestatus

Im Feld „Batteriestatus“ wird angezeigt, ob ein Offline-Gerät eine schwache Batterie gemeldet hat. Das Feld Batteriestatusdatum zeigt an, wann diese Meldung erzeugt wurde. Wird die Batterie gewechselt, erzeugt das Offline-Gerät bei der nächsten Buchung eine „Batterie gewechselt“ Meldung, die über die Ausweiskarte ins System zurückkommt und die Daten entsprechend aktualisiert werden. Über den Bericht „Leser Batteriestatus“, kann jederzeit eine Liste der Geräte mit schwacher Batterie erzeugt werden.

Abschließend übertragen Sie die Daten über die Schaltfläche **Übertragen**.

7.2.3 Offline Geräte programmieren

Die Programmierung der Daten auf die Offline-Geräte erfolgt direkt aus dem Tab. Dazu wird folgendes benötigt:

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

Vorgehensweise:

1. RF-Stick in den PC stecken.
2. Auf ÜBERTRAGEN klicken.
3. A-Lizenz in die AccessOne einlesen (einmaliger Vorgang beim ersten Gerät, das programmiert wird)
4. RF-Stick-Master vor das Gerät halten.

7.2.4 Berechtigungen

Fassen Sie mehrere Türen zu einer Türgruppe zusammen.



Wenn Sie einem Zylinder eine neue Berechtigung zuweisen, müssen Sie diese Daten auch auf das Offline-Gerät übertragen.



Berechtigungen sollten so gebildet werden, dass sie nur Räume gleicher Sicherheitsstufe zusammenfassen. Wenn es in einem Raum oder Flur mehrere Zugänge gibt, dann sollten die entsprechenden Zylinder in einer Berechtigung zusammengefasst werden. Über die Berechtigungsprofile fassen Sie dann die Türgruppen je nach Nutzerprofil zusammen.

AccessOne - OSS

Home | **Zylinder** | **Berechtigungen** | Zeitmodelle | Facilitydaten | Datenimport

Ändern | Neu | Kopieren | Löschen | Aktualisieren | Zuordnung

Name	Beschreibung
Musterkoffer	
Produktion	Offline Geräte in der Pro.
Service	Offline Geräte im Service

Name: Produktion | Video: 4 | Anzahl Benutzer aktiviert: 0

Beschreibung: Offline Geräte in der Produktion

Offline Bereich: 1 - OSS | Sicherheitsstufe: | Workflow:

Zugeordnete Zylinder:

Name	Beschreibung	Sicherheitsst.
CES Zylinder	Test OSS Tool	Ohne
Musterkoffer	Musterkoffer	Ohne
Raum E124	Raum E124	Ohne

<< >>

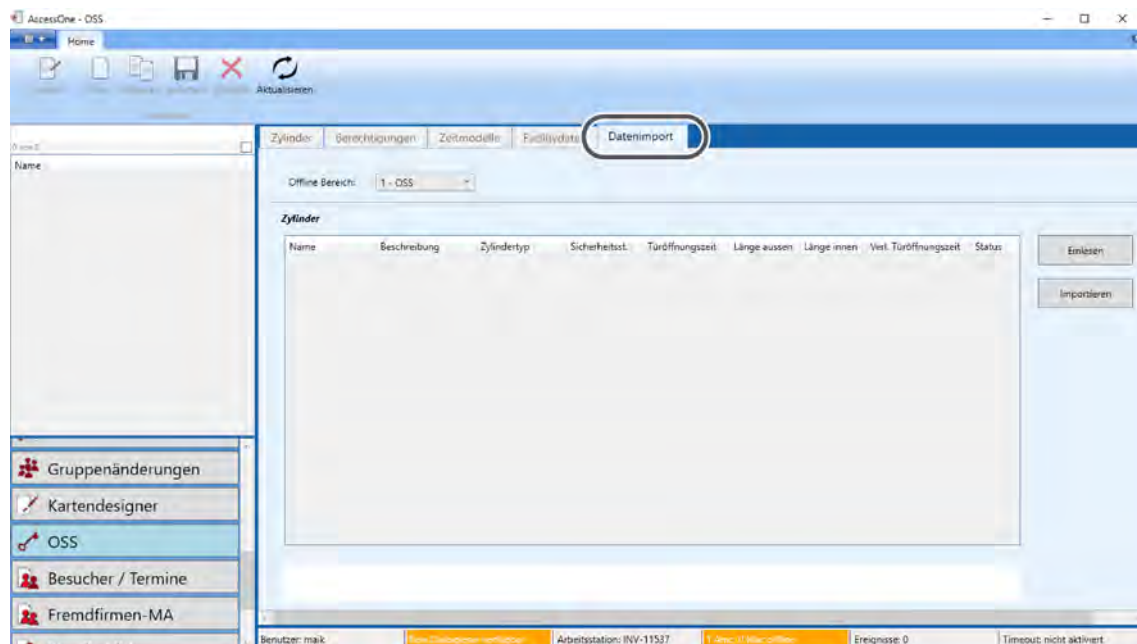
Zugeordnete Räume:

Name	Beschreibung	Sicherheitsst.
Beschlag	Muster Beschlag	Ohne
Raum E123	Raum E123	Ohne
Raum E125	Raum E125	Ohne
Test	Test	Ohne
Tim's Zylinder		Ohne

Kartendesigner | **OSS** | Besucher / Termine | Fremdfirmen-MA | Standortdaten | Workflow | OSS Blacklist

Benutzer: maik | 1 Netz: 0AAA: offline | Arbeitsstation: INV-11537 | Ereignisse: 0 | Timeout: nicht aktiviert

7.2.5 Datenimport

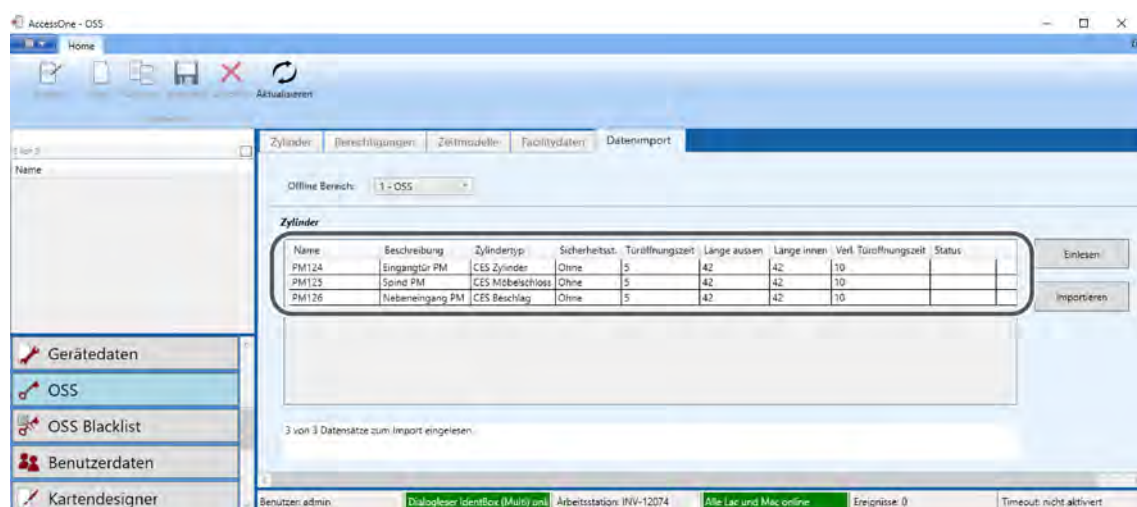


Ermöglicht den Import einer *.csv-Türenliste. Wählen Sie den Offline-Bereich und klicken Sie auf **Einlesen**. Wählen Sie die entsprechende Türliste aus dem Verzeichnisordner.



Die Türenliste wird in der Regel bei der Anlageneinrichtung von CES angelegt. Die Liste kann auch vom Kunden bearbeitet werden.

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

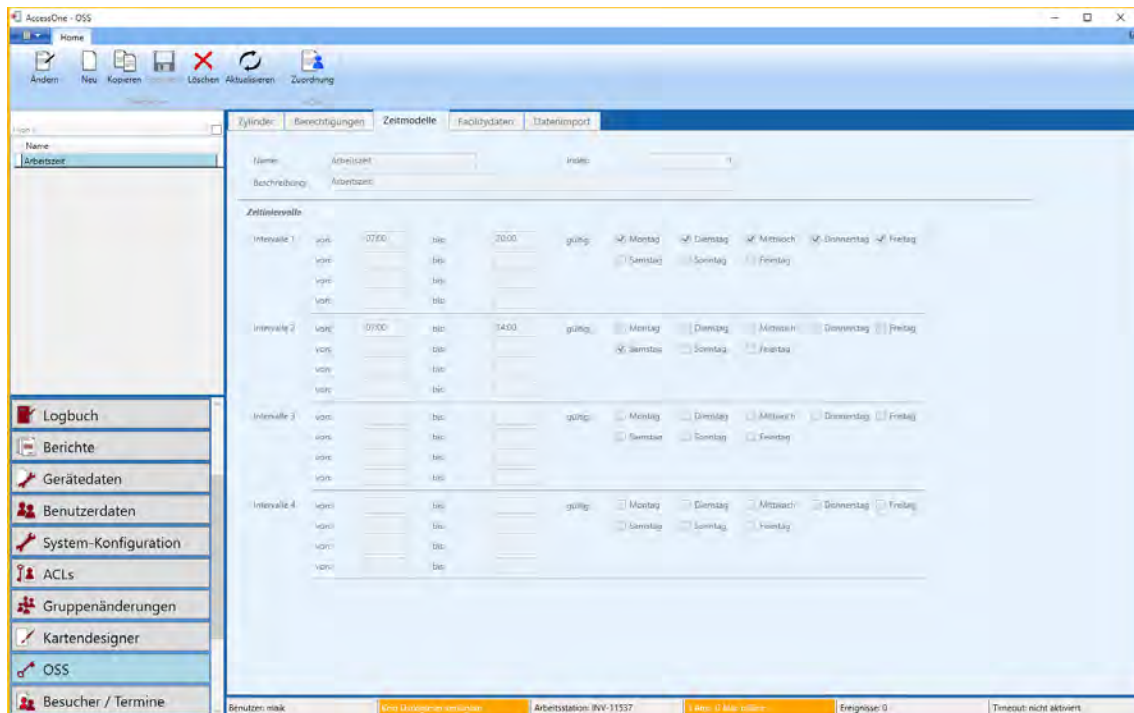


Die eingelesene Datei kann jetzt in der Listenansicht im Feld „Zylinder“ noch einmal geprüft werden. Drücken Sie auf die Schaltfläche Importieren um die Liste in die Datenbank zu importieren. Die Bestätigung erfolgt im Textfeld unterhalb des Felds.

7.2.6 Zeitmodelle

 OSS Standard Offline verwendet ein anderes Format für die Zeitmodelle und ist nicht so flexibel, wie es die AccessOne für die Online-Komponenten ist. Daher können die Online-Zeitmodelle nicht durchgängig verwendet werden und es gibt einen eigenen Tab für die OSS Standard Offline-Zeitmodelle.

Ein Zeitmodell bei OSS Standard Offline besteht aus bis zu vier Intervallen. Für jede Intervallgruppe können Tage ausgewählt werden, an denen es gültig ist. Ist bei der Berechtigung für eine Person kein Zeitmodell eingetragen, gilt sie für den ganzen Tag.



Im Beispiel ist von Montags bis Freitags von 7:00 – 20:00 und am Samstag von 7:00 bis 14:00 der Zutritt erlaubt. An Sonn- und Feiertagen ist kein Zutritt möglich.

8 Konfiguration der Berechtigungen

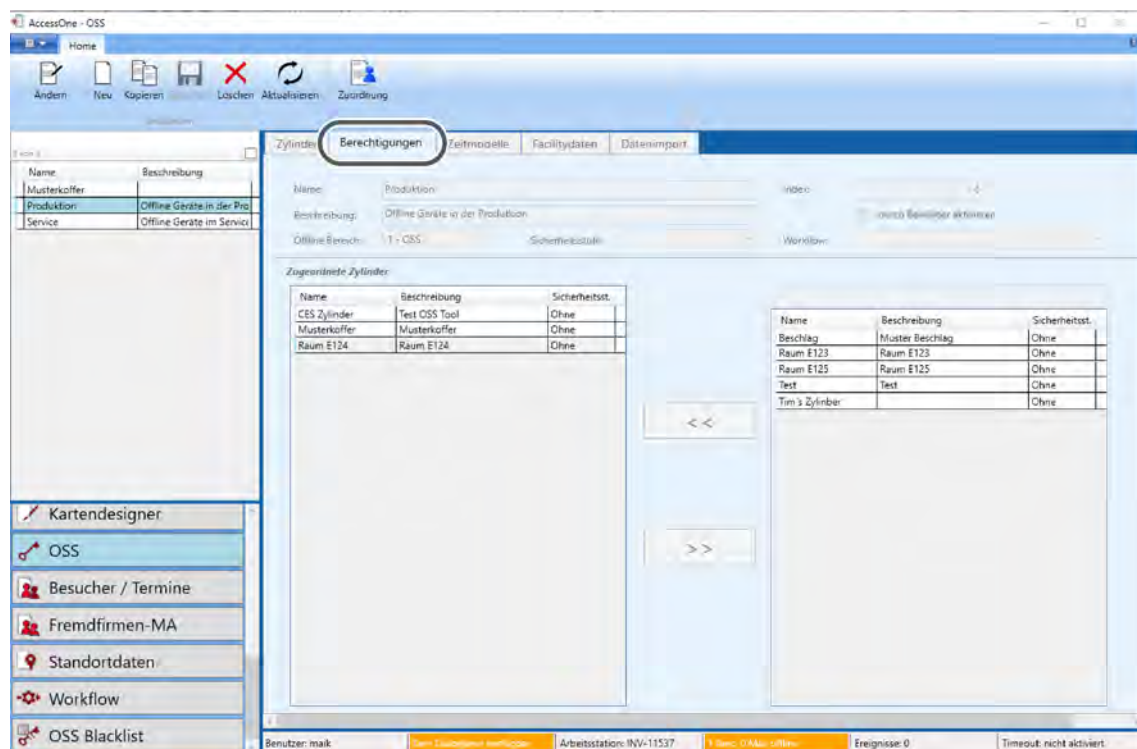
Zielgruppe dieses Kapitels:

- produktgeschultes Personal

8.1 Berechtigungen

Richten Sie zuerst Berechtigungsgruppen für Online und Offline Geräte ein. Dann bestimmen Sie über Tages- und Zeitmodelle weitere Einschränkungen bzw. Türfunktionen (z. B. Öffnungsfunktionen zu bestimmten Tageszeiten) unter Berücksichtigung von Sonder- und Feiertagen.

8.1.1 Berechtigungen in der Übersicht



Die Dialogauswahl „Berechtigungen“ öffnet im Dialogfenster mehrere Tabs.

Im Tab „Berechtigungen“ können mehrere Leser zu einer Gruppe zusammengefasst werden. Die Leser werden aus der Liste der nicht zugeordneten Leser (rechte Liste) ausgewählt und mit der Schaltfläche „<<“ der aktuellen Gruppe zugeordnet.



Berechtigungsgruppen bestehen aus zusammengefassten Berechtigungen. Die auf der rechten Seite des Fensters angelegten Berechtigungen (nicht zugeordnet) können wiederum Einzelberechtigungen oder Gruppenberechtigungen sein.

8.1.2 Generelles zu Zeit- und Tagesmodellen

Zeitmodelle werden in der AccessOne an verschiedenen Stellen verwendet.

- Für die Einschränkung des Zutritts. Hier kann ein Zeitmodell personenbezogen hinterlegt werden, als Zeitmodell für einen Mitarbeiter. Ist bei einer Berechtigung kein eigenes Zeitmodell angegeben, gilt immer das personenbezogene Zeitmodell.
- Zeitmodelle werden bei Türen verwendet, um z. B. eine Daueröffnungsfunktion zu bestimmten Tageszeiten festzulegen.

In der AccessOne entspricht ein Zeitmodell entweder einem Wochenplan und besteht aus einzelnen Tagesmodellen für jeden einzelnen Wochentag oder aus zusätzlichen Tagesmodellen für Sonder- oder Feiertage.

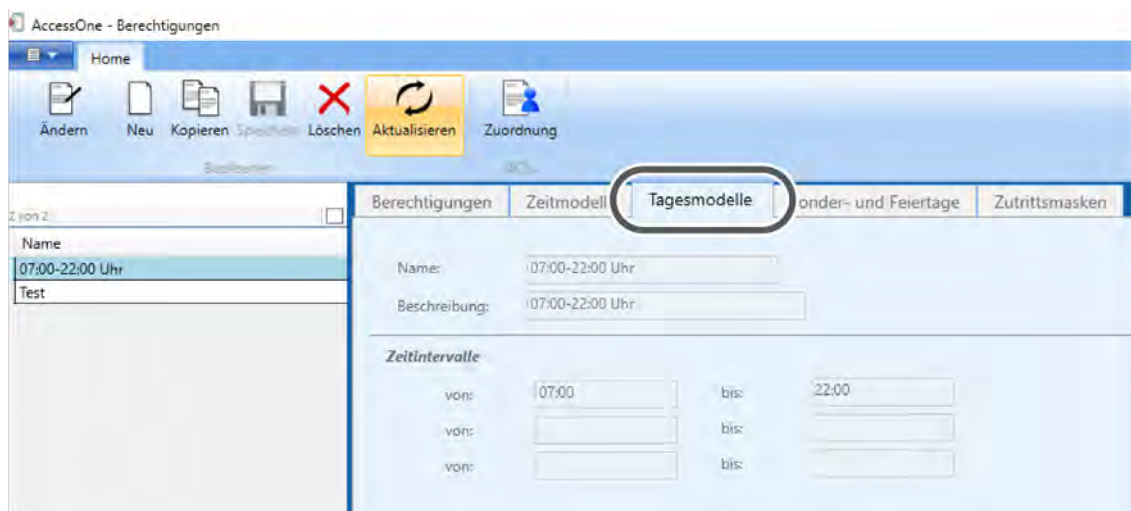


Jedes Tagesmodell kann drei Intervalle beinhalten und legt die Zutrittszeiten für genau einen Tag fest.

Wir empfehlen beim Definieren der Pläne folgende Vorgehensweise:

1. Tagesmodelle anlegen
2. Sonder- und Feiertage in Gruppen zusammenfassen
3. Zeitmodelle für Türen anlegen

8.1.3 Tagesmodelle



Klicken Sie in der Werkzeugleiste auf NEU. Vergeben Sie einen Namen für Ihr Tagesmodell, optional können Sie eine Beschreibung ergänzen.

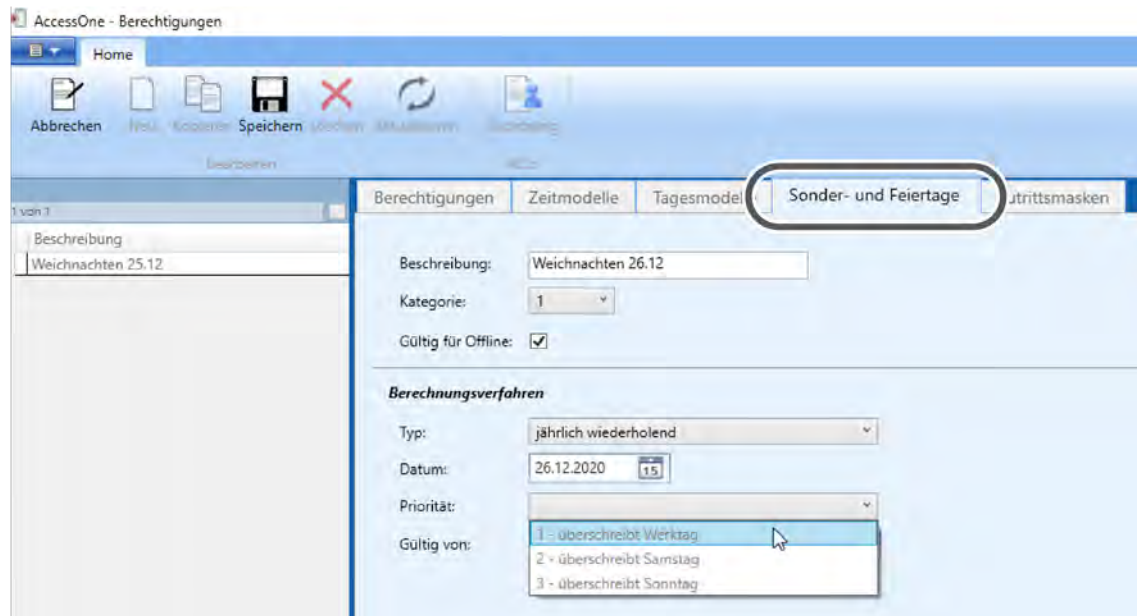
Bei den „Zeitintervallen“ geben Sie mindestens 1 an. Diese müssen Sie mit einer „von“/„bis“-Zeit definieren. Abschließend klicken Sie auf SPEICHERN.

TIPP Legen Sie auch das Zeitmodell „Kein Zutritt“ an. Das Zeitmodell eignet sich z. B. für Mitarbeiter, die nur an bestimmten Tagen berechtigt sind und an anderen Tagen nicht. Auch Feiertage können so einfach berücksichtigt werden.

8.1.4 Sonder- und Feiertage

Klicken Sie auf NEU und geben Sie eine „Bezeichnung“ für Ihren Sondertag ein. Die Kategorien dienen dazu, die Sondertage in Gruppen zusammenzufassen und damit für eine solche Gruppe dann ein Tagesmodell festlegen zu können.

TIPP Fassen Sie die bundesweiten Feiertage in einer Kategorie zusammen. Für diese Tage gilt dann das Tagesmodell „Kein Zutritt“ (Alternativ: kein Eintrag in dieser Kategorie ist wie ein Tagesmodell mit einem Intervall von 0:00 bis 0:00). Durch Verteilung der Feiertage auf entsprechende Kategorien, kann man erreichen, dass für die Zeitmodelle die Feiertage des jeweiligen Bundeslandes berücksichtigt und die anderen ignoriert werden.



Weiter unten wird das Berechnungsverfahren gewählt:

Die meisten beweglichen Gedenk- und Feiertage des Kirchenjahrs hängen vom Datum des Ostersonntags ab:

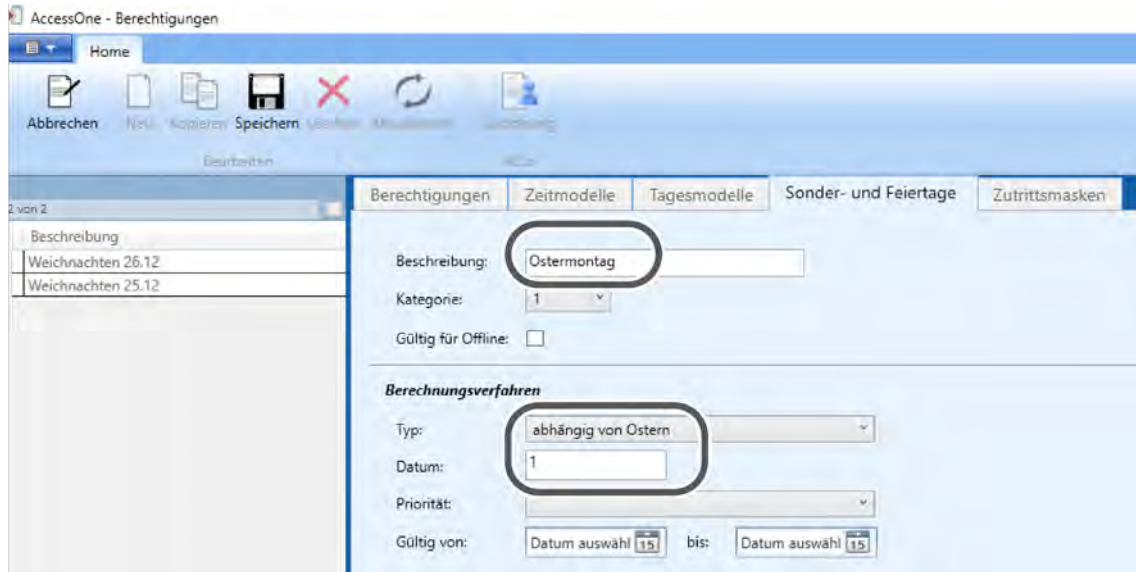
- Aschermittwoch = 46 Tage vor Ostern
- Palmsonntag = 7 Tage vor Ostern
- Gründonnerstag = 3 Tage vor Ostern
- Karfreitag = 2 Tage vor Ostern
- Ostermontag = 1 Tag nach Ostern
- Christi Himmelfahrt = 39 Tage nach Ostern (der 40. Tag)
- Pfingstsonntag = 49 Tage nach Ostern (der 50. Tag)

In der katholischen Kirche gelten zusätzlich

- Fronleichnam = 60 Tage nach Ostern
- Heiligstes Herz Jesu, 68 Tage nach Ostern

Die Türsteuerung berechnet das Datum von Ostersonntag automatisch und kann daher diese von Ostern abhängigen Feiertage bestimmen, wenn sie im System angelegt sind. Bei Tagen, die abhängig von Ostern berechnet werden, wird in das Datumsfeld die Anzahl der Tage eingetragen, die auf das berechnete Datum addiert werden müssen.

Im Beispiel wird Ostermontag (= 1 Tag nach Ostern) wie folgt definiert:



Liegt der Feiertag vor Ostern, kann auch ein negativer Wert angegeben werden. Beispiel: Für Karfreitag (2 Tage vor Ostern) lautet der Eintrag „-2“.

- festes Datum

Sondertage, die jedes Jahr erneut angelegt werden müssen, oder einmalige Ereignisse, wie Firmenfeier werden mit einem festen Datum angelegt. Sie gelten dann genau einmal.

- jährlich wiederholend

Es gibt Daten, die sich jährlich als Sonder- oder Feiertag wiederholen: z. B. der 1. Mai oder der 24. Dezember. Wählen Sie hierfür ein Datum aus dem Kalender aus. Die Jahreszahl wird dabei bei der Prüfung ignoriert.

- Priorität/Kategorie

Die Priorität eines Sondertages bestimmt seine Relevanz. Ein normaler Feiertag hat die Priorität 1, d.h. wenn er auf einen Werktag fällt, gilt nicht das Tagesmodell dieses Werktages, sondern das Tagesmodell des Sondertages.

Beispiel 1: Heiligabend sei der Kategorie 8 zugeordnet und allen Sondertagen der Kategorie 8 ist in Ihrem Zeitmodell ein Tagesmodell von einem halben Arbeitstag (07:00– 12:00 Uhr) eingetragen. Wenn nun Heiligabend auf einen Montag fällt, kann man von 7:00–12:00 Uhr die gesicherten Bereiche betreten. Fällt Heiligabend auf einen Samstag oder Sonntag, soll kein Zutritt gewährt werden. In diesem Fall ist die Priorität für Heiligabend auf 1 zu setzen, denn Samstag und Sonntag haben eine höherwertige Priorität.

Beispiel 2: Für die Inventur am Wochenende soll bestimmten Mitarbeitern Zutritt gewährt werden. Für diesen Sondertag muss eine Priorität 2 oder sogar 3 eingestellt werden, damit das normale Tagesmodell des Samstags bzw. Sonntags überschrieben wird.

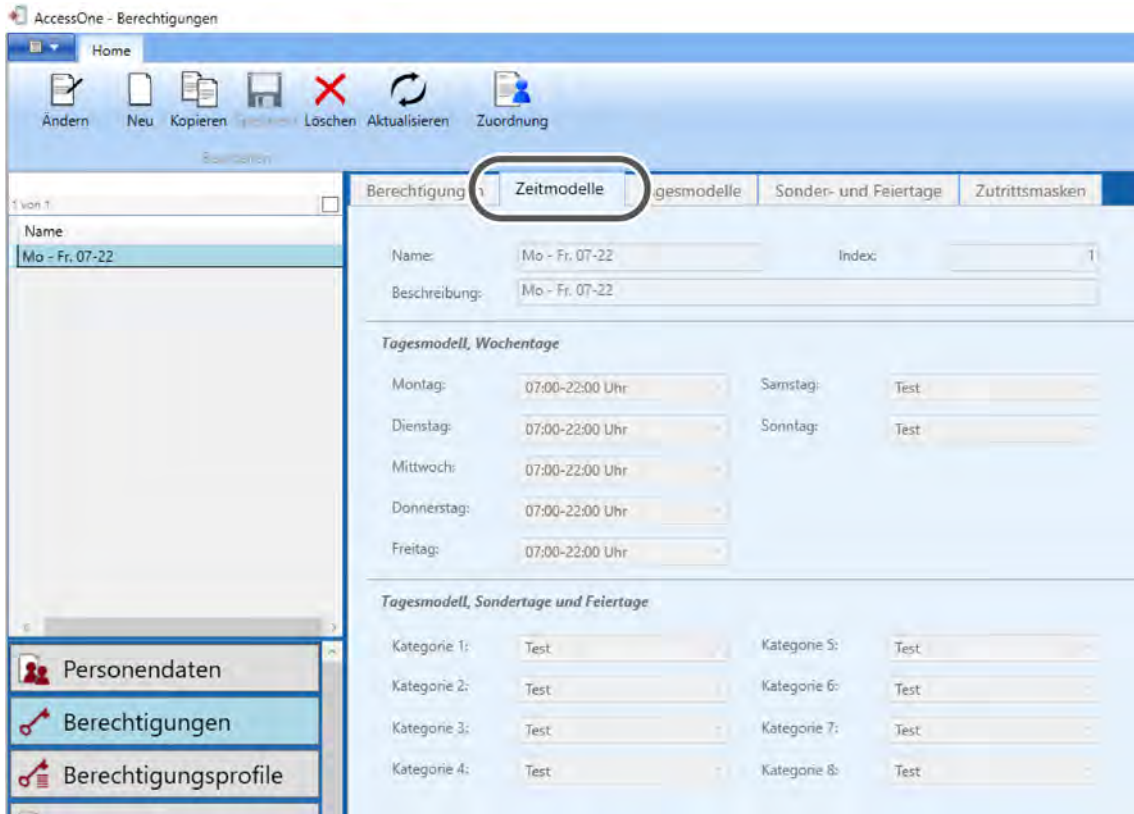
Die folgende Tabelle gibt eine Übersicht über die Feiertage in Deutschland:

Feiertag	Geltungsbereich
Neujahr	bundesweit
Heilige Drei Könige	Baden-Württemberg, Bayern, Sachsen-Anhalt
Karfreitag	bundesweit
Ostersonntag	bundesweit
Ostermontag	bundesweit
Tag der Arbeit / 1.Mai	bundesweit
Christi Himmelfahrt	bundesweit
Pfingstsonntag	bundesweit
Pfingstmontag	bundesweit
Fronleichnam	Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland
Mariä Himmelfahrt	Bayern (in katholischen Gebieten), Saarland
Tag der Deutschen Einheit	bundesweit
Reformationstag	Brandenburg, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt, Thüringen
Allerheiligen	Baden-Württemberg, Bayern, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland
Buß- und Bettag	Sachsen
1. Weihnachtstag	bundesweit
2. Weihnachtstag	bundesweit

Es empfiehlt sich, die Sondertagekategorien so zu wählen, dass Feiertage, die im gleichen Bundesland Gültigkeit haben auch in derselben Kategorie liegen.

Bundesweite Feiertage	Kategorie 1
Heilige Drei Könige	Kategorie 2
Fronleichnam	Kategorie 3
Maria Himmelfahrt	Kategorie 4
Reformationstag	Kategorie 5
Allerheiligen	Kategorie 6
Buß- und Bettag	Kategorie 7
sonstige Sondertage	Kategorie 8

8.1.5 Zeitmodelle



AccessOne - Berechtigungen

Home

Ändern Neu Kopieren Löschen Aktualisieren Zuordnung

Berechtigungen

1 von 1

Name

Mo - Fr, 07-22

Berechtigungen

Berechtigungsprofile

Berechtigung Zeitmodelle Tagesmodelle Sonder- und Feiertage Zutrittsmasken

Name: Mo - Fr, 07-22 Index: 1

Beschreibung: Mo - Fr, 07-22

Tagesmodell, Wochentage

Montag: 07:00-22:00 Uhr Samstag: Test

Dienstag: 07:00-22:00 Uhr Sonntag: Test

Mittwoch: 07:00-22:00 Uhr

Donnerstag: 07:00-22:00 Uhr

Freitag: 07:00-22:00 Uhr

Tagesmodell, Sonertage und Feiertage

Kategorie 1: Test Kategorie 5: Test

Kategorie 2: Test Kategorie 6: Test

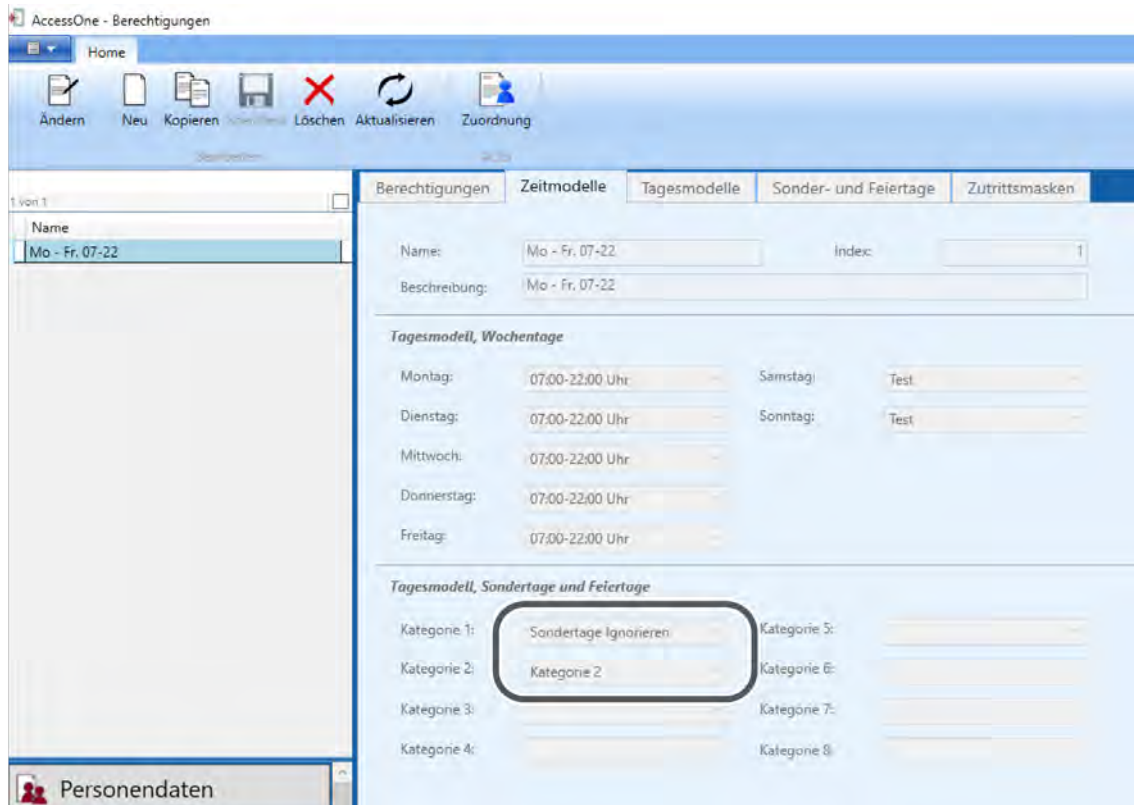
Kategorie 3: Test Kategorie 7: Test

Kategorie 4: Test Kategorie 8: Test

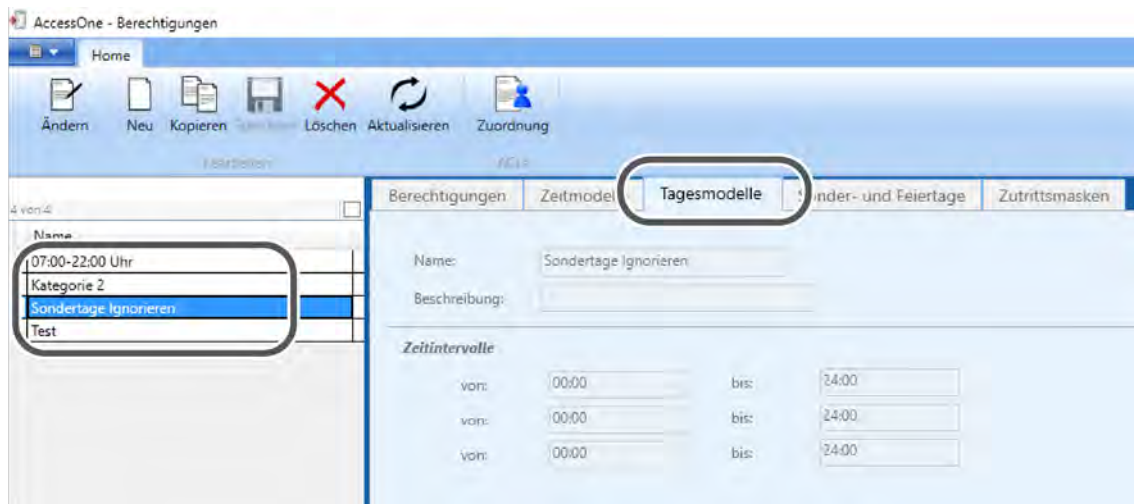
Ist im System kein Sondertag hinterlegt, wird an diesem Datum kein Zutritt erlaubt. Klicken Sie auf NEU und nehmen Sie die entsprechenden Eingaben vor. Speichern Sie das Zeitmodell. Wechseln Sie die Seite ohne zu speichern, macht das in diesem Fall die AccessOne automatisch.

Das Eingabefeld „Beschreibung“ dient zur firmeninternen Zuordnung.

Die Angabe im Feld „Index“ bezeichnet eine fortlaufende Kontroll-Nummer, in welcher Reihenfolge die Zeitmodelle angelegt wurden.

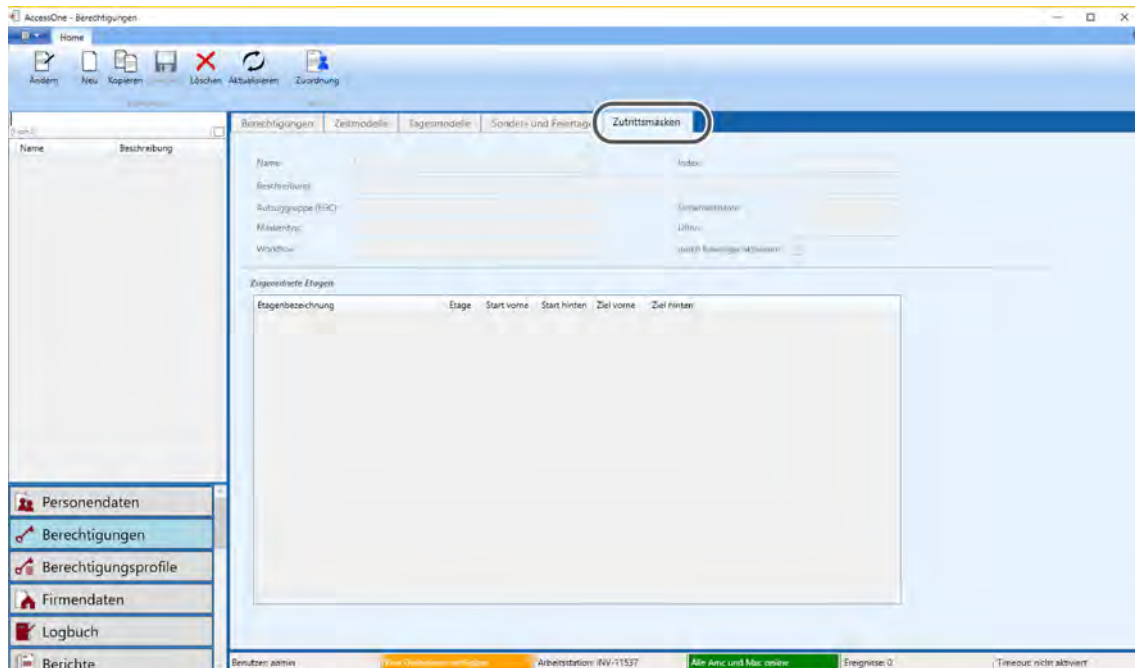


In diesem Beispiel gilt von Montag bis Freitag jeweils dasselbe Tagesmodell. Die Feiertage der Kategorie 1 werden in diesem Zeitmodell ignoriert, d.h. es gilt hier das jeweilige Tagesmodell des Wochentages auf den dieser Feiertag fällt. Für die Sonder- und Feiertage der Kategorie 2 gibt es ein entsprechendes Tagesmodell, bei allen anderen Sonder- und Feiertagen der Kategorien 3 bis 8 ist kein Tagesmodell eingetragen und damit der Zutritt gesperrt.



Um zu erreichen, dass ein Sonder- und Feiertag ignoriert wird, also das normale Tagesmodell des entsprechenden Werk- tags gilt, muss ein spezielles Tagesmodell angelegt werden, sofern es nicht bei der Installation automatisch angelegt wurde (z.B. „Sonder- und Feiertage ignorieren“).

8.1.6 Zutrittsmasken

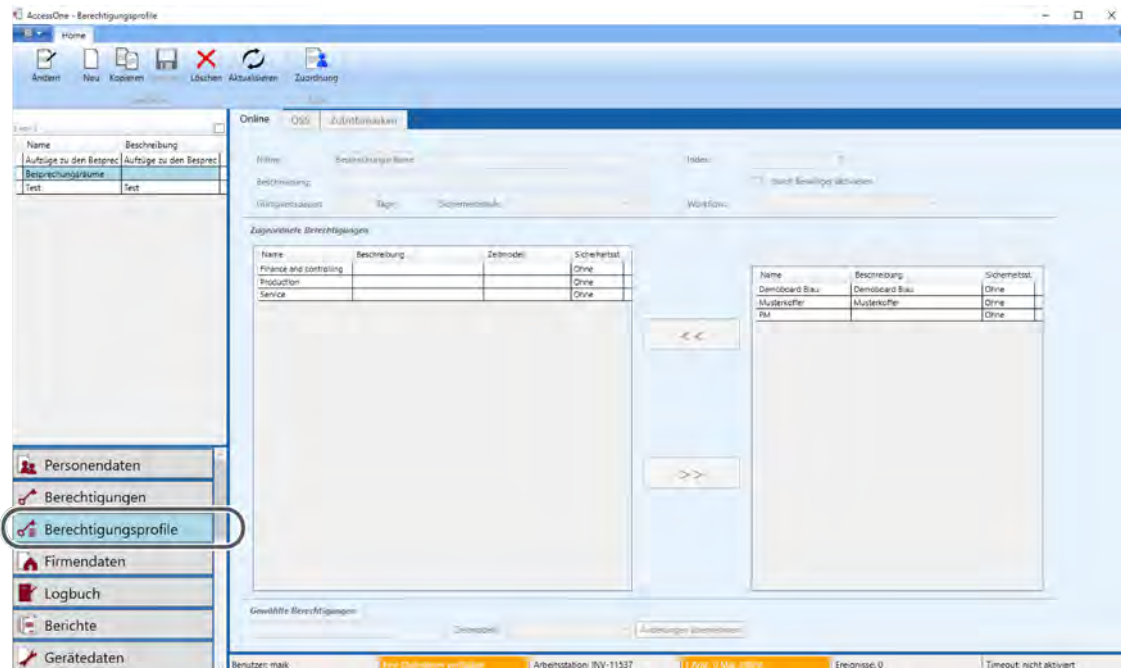


Im Dialog „Zutrittsmasken“ können Zutrittsberechtigungen auf einer zuvor angelegten Aufzuggruppe erstellt werden. Dazu legen Sie mit NEU eine leere Zutrittsmaske an. Geben Sie Name und Beschreibung ein und wählen Sie eine Aufzuggruppe, um die Etagen dieser Gruppe angezeigt zu bekommen. Anschließend bestimmen Sie den Maskentyp („Benutzer“ oder „Notfall“) . Für berechnete Zutritte in den Etagen schalten oder ziehen Sie die „Start-“ und „Ziel“-Türen von „Nein“ auf „Ja“. Speichern Sie die Eingaben.

8.2 Berechtigungsprofile

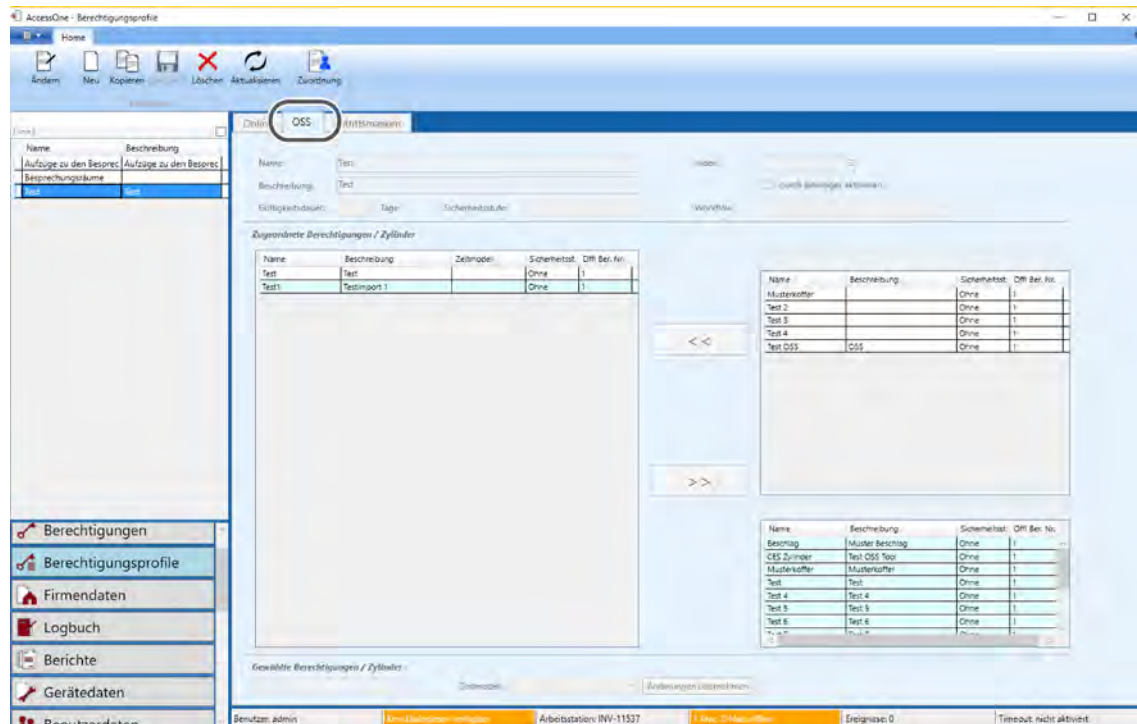
Im Dialog „Berechtigungsprofil“ hat der Nutzer die Möglichkeit, aus mehreren Berechtigungsgruppen ein Berechtigungsprofil zu erstellen. Dabei besteht die Möglichkeit, Berechtigungen für die Online- und Offline-Geräte miteinander zu verbinden und in einem Profil zusammenzufassen.

8.2.1 Online-Berechtigungen in der Übersicht



Im Tab „Online“ können Berechtigungsgruppen zu einem Berechtigungsprofil zusammengefasst werden. Die Gruppen werden aus der Liste der nicht zugeordneten Gruppen (rechte Liste), ausgewählt und mit der Schaltfläche „<<“ dem aktuellen Profil (linke Liste) zugeordnet.

8.2.2 Offline-Berechtigungen in der Übersicht



In dem Tab „OSS“ können die Offline-Geräte ebenfalls zu dem ausgewählten Profil zusammengefasst werden. Sie haben die Möglichkeit aus der Liste von der rechten Seite (nicht zugeordnete Gruppen und Geräte) sowohl eine Berechtigungsgruppe als auch ein einzelnes Offline-Gerät über die Schaltfläche „<<“ dem aktuellen Profil zuzuordnen.



Voraussetzung für die Einbindung von Offline-Geräten ist die Einrichtung der Offline-Geräte (siehe „7.2 Gerätedaten Offline-Geräte (OSS-SO)“ auf Seite 55).

9 Anlegen von Personendaten

Zielgruppe dieses Kapitels:

- produktgeschultes Personal

Der Dialog „Personendaten“ bietet Ihnen die Möglichkeit, Berechtigungen zu vergeben und alle notwendigen Daten zur Person zu erfassen. Ordnen Sie die zuvor konfigurierten Berechtigungen der Online- und Offline-Geräte den Personen direkt zu.

9.1 Personendaten

9.1.1 Personendaten in der Übersicht

Auf dem ersten Tab werden alle wesentlichen Daten zur Person angezeigt und es gibt die Möglichkeit, eine Sperre zu löschen bzw. bei Personen, die ihren Ausweis vergessen haben, einen neuen Ausweis zuzuweisen (Schaltfläche Ausweis wechseln). Der bisher aktive Ausweis wird dadurch deaktiviert.



Diese Übersicht ist für die schnelle Erfassung von Eigenschaften, die einer Person zugeordnet sind, geeignet (z. B. für den Objektschutz).

Bereich „Aufenthaltort“

Im Bereich „Aufenthaltort“ werden „Aktueller Ort“, „Letzte Begehung“ und „Parkbereich“ angezeigt.

Aktueller Ort

Passiert eine Person mit berechtigtem Ausweis eine mit AccessOne gesicherte Tür, wird der Aufenthaltsort erfasst. Für jede Tür ist definiert, an welche Bereiche sie angrenzt. Der betretene Bereich zum Zeitpunkt der Erfassung wird hier angezeigt.

Letzte Begehung

Jeden Tag um Mitternacht wird das Logbuch des aktuellen Tages gelesen und die letzte Begehung im Datensatz zur Person eingetragen. Diese Information wird unter „Letzte Begehung“ angezeigt. Es kann vorkommen, dass eine Begehung einige Wochen zurückliegt. In diesem Fall ist der aktuelle Aufenthaltsort nicht bekannt.

Das Datum der letzten zur Person gespeicherten Begehung bleibt aber erhalten.



Dieses Datum kann in der AccessOne auch dazu verwendet werden, Personen, die eine einstellbare Zeit nicht anwesend waren, automatisch zu sperren. Dies wird über den Sperrentyp „Abwesenheitszeit“ gesteuert (siehe „9.1.7 Sperren“ auf Seite 81).

Ausweise

Die Liste ist eine Übersicht über die Zutritts-Medien, die einer Person zugeordnet sind. Gespeichert sind der jeweilige Status und die Gültigkeit. Mit der Schaltfläche „Ausweis wechseln“ ändern Sie das zugehörige Zutritts-Medium der Person. Für den Fall, dass die Person ihren Ausweis verloren hat, muss eine Wechselkarte aktiviert werden.

Sperren

Zeigt an, ob zu dieser Person eine Sperre eingetragen ist. Sperren können auch für die Zukunft gelten und werden dann erst zu einem späteren Zeitpunkt aktiv. Sperren, die zum aktuellen Zeitpunkt aktiv sind, werden orange hinterlegt.

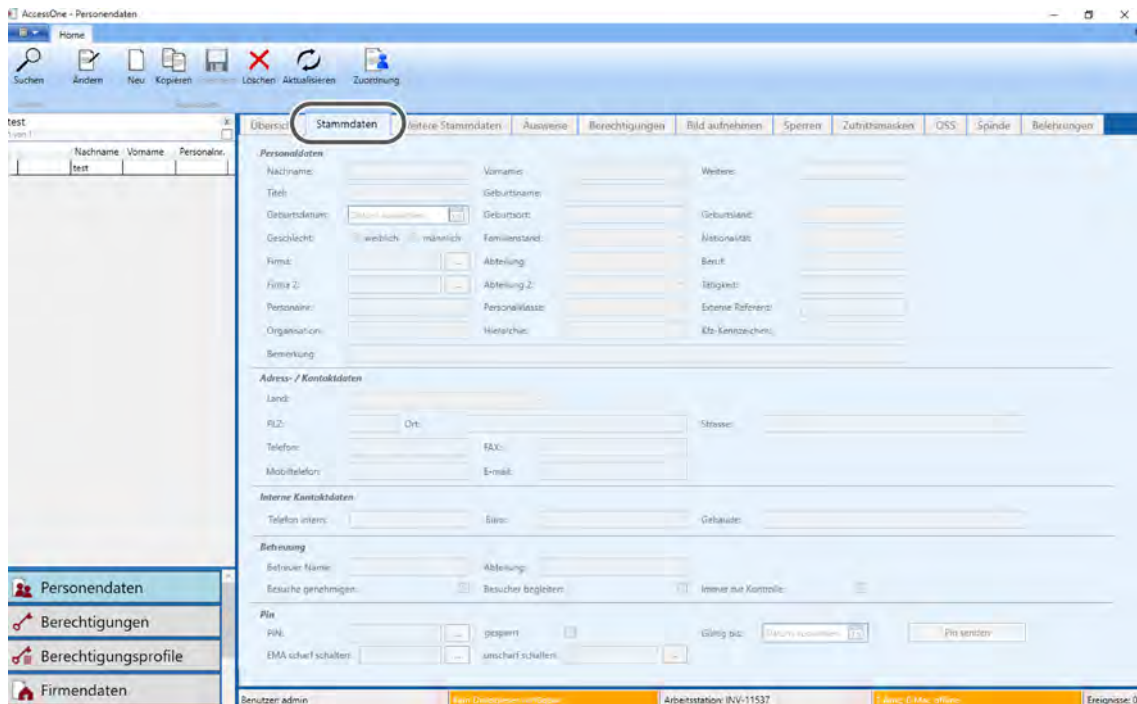
Sperren können in diesem Dialog auch markiert und gelöscht werden. Wird ein verloren gegangener Ausweis wiedergefunden, kann hier die entsprechende Sperre gelöscht werden. Wählen Sie dazu einfach die aktive Sperre aus und betätigen Sie die Schaltfläche Löschen.

Logbuch

Klicken auf die Schaltfläche Aktualisieren zeigt die Logbuch-Meldungen der letzten zwei Tage zur Person. Sie können den Wert zwischen 2–7 Tagen einstellen.

Beispiel: Einer Person wird kein Zutritt mehr gewährt und sie informiert den Objektschutz. Der Sicherheitsdienst kann dann einsehen, an welcher Tür die Person abgewiesen wurde und ob Änderungen an den Daten zur Person vorgenommen wurden, z. B. ob eine Berechtigung entzogen oder ein Zeitmodell geändert wurde.

9.1.2 Stammdaten



Um neue Personaldaten anzulegen, klicken Sie auf den Button NEU. Der Tab „Stammdaten“ öffnet sich automatisch. Wollen Sie diesen Tab verlassen, müssen Sie die zwei rot hinterlegten Pflichtfelder „Name“ und „Personalklasse“ ausfüllen.

Personaldaten

Es gibt in diesem Bereich Pflichtfelder, die zu jeder Person eingetragen werden müssen („Name“ und „Personalklasse“). Die AccessOne unterscheidet prinzipiell zwischen Eigenpersonal, Fremdpersonal und Besuchern. Zusätzliche Personalklassen können vom Administrator in der Datenbank angelegt werden, müssen aber den drei vordefinierten Basisklassen (Eigenpersonal, Fremdpersonal, Besucher) zugeordnet werden. Der Nutzer kann das Fremdpersonal z. B. in „Fremdfirmen mit Arbeitnehmerüberlassung“ oder „Fremdfirmen“ unterteilen. Einige Sperren werden abhängig von der Personalklasse gesetzt. So kann eingestellt werden, dass bei Eigenpersonal eine Sperre für zu lange Abwesenheit erst nach sechs Wochen gesetzt wird und bei Fremdpersonal bereits nach zwei Wochen. Auch an den Zugängen wird die Personalklasse ausgewertet.

Beispiel: Für Taschenkontrollen kann die Einstellung so erfolgen, dass Besucher immer kontrolliert werden, während Eigenpersonal nur nach einstellbarem Zufallsgeber kontrolliert wird.

Die Personalnummer ist ein externes Ordnungskriterium, das üblicherweise von einem externen Personalverwaltungssystem (z. B. SAP) kommt. Dies dient der Zuordnung von Personen aus dem Zutrittskontrollsystem mit den Daten der Personalabteilung. Die Personalnummer ist auch als Suchkriterium zugelassen.

Firma und Abteilung definieren Sie im Dialog „Firmendaten“. Bei den Firmen ist definiert, ob es eine Eigenfirma oder eine Fremdfirma ist. Im Eingabefeld „Firma“ können nur Eigenfirmen ausgewählt werden, im Feld „Firma 2“ nur Fremdfirmen. Die Abteilungen werden zuvor bei den Firmendaten definiert und können hier nur ausgewählt werden. In der Eingabereihenfolge sollten daher zuerst die Firmen und dann die Personen angelegt werden.

Adresse

Tragen Sie an dieser Stelle alle relevanten Adressdaten der Person ein.

Kontaktdaten

Tragen Sie an dieser Stelle alle relevanten Kontaktdaten der Person ein.

Betreuer

Für Fremdfirmenmitarbeiter kann ein Betreuer eingetragen werden. Dies muss zwingend eine Person des

Eigenpersonals sein. Der Betreuer ist der zuständige Ansprechpartner für die von ihm betreuten Personen.

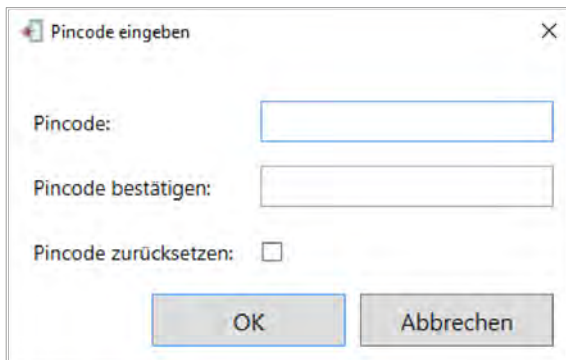
PIN-Codes

In der AccessOne werden drei PIN-Codes geführt. Ein PIN ist der persönliche Nummerncode für die Zutrittskontrolle. Es gibt Türen, die nur nach Eingabe des PIN-Codes begangen werden können. Die Mindestlänge des PINs ist über einen Systemparameter einstellbar (Standard 4 Stellen, maximal 6 Stellen).

Der PIN kann eine beschränkte Gültigkeit aufweisen und auch gesperrt sein. Wenn drei mal der falsche PIN-Code eingegeben wurde, wird dieser PIN-Code automatisch gesperrt und muss im System geändert werden. Für die Scharf- und Unscharfschaltung der Einbruchmeldeanlage (EMA) werden zwei weitere PIN-Codes im System geführt. Der PIN darf für Scharf- und Unscharfschaltung identisch sein, er muss sich jedoch vom PIN für die Zutrittskontrolle unterscheiden.



Es ist eine Forderung des VDS*1, dass es zwei verschiedene PIN-Codes sind. Diese PIN-Codes haben keine zeitlich begrenzte Gültigkeit. Bei einer Tür kann in der Berechtigung zur Person gewählt werden, ob die Person scharf schalten darf, unscharf schalten oder beides. Nur wenn diese Berechtigung existiert, ist eine PIN-Code Eingabe möglich.



Alle PIN-Codes sollten verdeckt eingegeben werden. Der vier- bis sechststellige PIN-Code muss zweimal eingegeben werden und aus mindestens drei verschiedenen Ziffern bestehen. Die Eingabe erfolgt durch den jeweiligen Ausweisinhaber über eine separate Nummerntastatur.

9.1.3 Weitere Stammdaten

Übersicht	Stammdaten	Weitere Stammdaten	Ausweise	Berechtigungen	Bild aufnehmen	Sperren	Zutrittsmasken	OSS	Spinde	Belehrungen
Nachname: test Vorname: Firma: Firma 2: Abteilung: Geboren am:										
Personalausweis / Reisepass Ausweisnr.: Art: Gültig bis: Datum auswählen 15										
Zutritt Tätigkeitsbeginn: Datum auswählen 15 Tätigkeitsende: Datum auswählen 15 Erlaubt von: Datum auswählen 15 Erlaubnis bis: Datum auswählen 15 ☐ Verlängerte Türöffnungszeiten										
Fremdsystemdaten ☐ Importsperre ☐ Teilnahme Zeiterfassung aktueller Zeitsaldo: 00:00 ☐ Aufzug Sonderfahrt Aufzug Vorzugsetage: ☐ Dienstgang unterdrücken ☐ Erstes Kommen/Letztes Gehen unterdrücken										
Aufenthalts- und Arbeitserlaubnis ☐ Aufenthaltserlaubnis Gültig bis: Datum auswählen 15 ☐ Permanent ☐ Arbeitserlaubnis Gültig bis: Datum auswählen 15 ☐ Permanent										
Einwanderung Datum: Datum auswählen 15 Geburtsland: Geburtsstadt:										
Parkplatz Parkgruppe: Parkbereich: Parkplatz-Nr.: freie Nummer: Suchen Nummernbereich: Berechtigt bis: Datum auswählen 15 00:00 Preiskategorie:										
Sonstiges Verkaufskategorie: Statusbericht: Erstellen										

Geben Sie alle Daten ein, die Sie zur Person hinterlegen möchten.

Personalausweis/Reisepass

An dieser Stelle haben Sie die Möglichkeit, die Nummer des Personalausweises oder Reisepasses und dessen Dauer und Gültigkeit einzutragen. Diese Eingabe erfolgt nur zu dokumentierenden Zwecken.

Zutritt

Tätigkeitsbeginn und Tätigkeitsende (z. B. bei befristeten Verträgen) werden hier eingetragen, um automatisch entsprechende Sperren zu setzen. Diese Daten werden z. B. bei Eigenpersonal verwendet, um das Eintrittsdatum bei Neuanfängern bzw. das Austrittsdatum bei Kündigung festzuhalten. Vor dem Tätigkeitsbeginn und bei Erreichen des Enddatums wird eine entsprechende Sperre gesetzt. Man kann so Personen im System anlegen, bevor diese den ersten Arbeitstag antreten. Teilweise geschieht das durch die Schnittstelle zum Personal- datenverwaltungssystem der Personalabteilung automatisch. Mit Erreichen des Kündigungsdatums wird der Ausweis automatisch gesperrt.

Fremdsystemdaten

Hier kann eine Importsperre ausgewählt werden, d.h., dass das System keine täglichen Datenabgleiche von externen SAP-Quellen abrufen. Wenn Daten in der AccessOne geändert wurden, sollten sie nicht erneut überschrieben werden können.

Unterweisung

Wenn es im Unternehmen eine Pflicht für verbindliche Unterweisungen für neue Mitarbeiter gibt, können Sie an dieser Stelle das Datum der ersten und zweiten Unterweisung eintragen. Ebenso das Datum, wann die nächste Unterweisung stattfinden muss.

Aufenthalts- und Arbeitserlaubnis

Eine gültige Arbeits- und Aufenthaltserlaubnis ist gesetzliche Voraussetzung für die Arbeitsaufnahme. Bei Personen mit begrenzter Aufenthalts-und/oder Arbeitserlaubnis überwacht das System die Einhaltung, wenn hier entsprechende Daten eingegeben werden. Die Eingabe ist im Sinne des Auftraggebers, der sich strafbar

macht, wenn Personen ohne diese Erlaubnis auf seiner Anlage arbeiten.

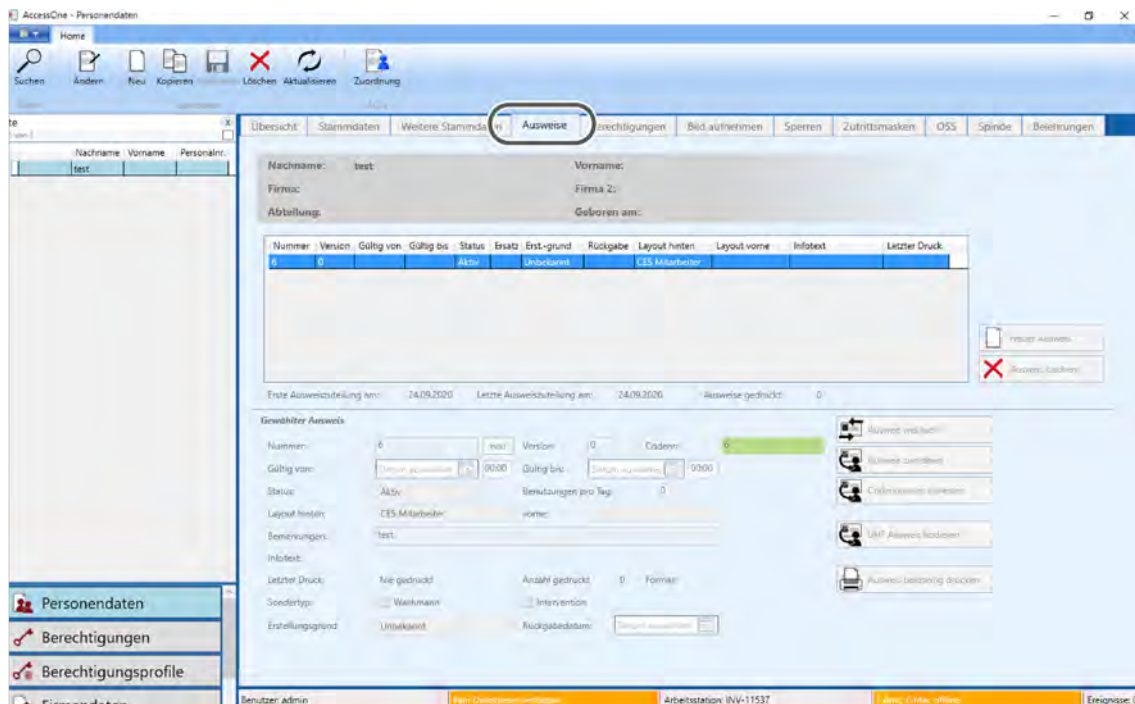
Einwanderung

Diese Eingabe ist nur zu dokumentierenden Zwecken und kann optional eingetragen werden.

Sonstiges

Die „Verkaufskategorie“ wird verwendet, um eine Ausweiskarte für die Nutzung an Verkaufsautomaten freizuschalten. Voraussetzung ist, dass die Karten mit der AccessOne kodiert werden.

9.1.4 Ausweise (Zutritts-Medien)



Auf diesem Tab können Sie Ausweise anlegen, wechseln, zuordnen oder drucken. In der tabellarischen Übersicht sehen Sie alle zu dieser Person definierten Ausweise.



Eine Person kann mehrere Ausweise besitzen. Das ist insbesondere bei der Verwendung von unterschiedlichen Ausweistechnologien notwendig.

Um einen neuen Ausweis anzulegen, wählen Sie eine Person aus, betätigen Sie in der oberen Menüleiste den Button ÄNDERN und klicken Sie auf die Schaltfläche Neuer Ausweis.

Ein Ausweis wird gelöscht, indem er in der Liste ausgewählt und dann auf Ausweis löschen geklickt wird.



ACHTUNG: Hier gibt es keine Sicherheitsabfrage vor dem endgültigen Löschen! Wurde die Schaltfläche versehentlich gedrückt, muss in der Werkzeugleiste auf den Button ABBRECHEN geklickt werden. Die Änderungen auf dem aktuellen Tab werden dann verworfen.

Gewählter Ausweis

Hier können alle Daten zum Ausweis eingegeben oder geändert werden. Die Ausweisnummer dient nur als Ordnungskriterium. Im Normalfall hat sie nichts mit der im Ausweis kodierten Nummer zu tun, kann aber mit der im Ausweis kodierten Nummer identisch sein.

Die Angabe zur Version ist einstellig und geht von 0–9, bzw. A bis Z. Ist ein Ausweis defekt, so kann ein identi-

scher Ausweis mit gleicher Karten- und Codenummer wieder produziert werden, wobei die Versionsnummer dann um eins erhöht und zusammen mit der im Ausweis kodierten Nummer gespeichert wird. Daher ist immer nur der Ausweis mit der aktuellen Versionsnummer gültig. Diese Nummer wird an der Tür überprüft. Stimmt sie nicht überein, wird eine entsprechende Meldung generiert und der Zutritt wird abgewiesen.

Gültig von/bis

Ausweise können eine begrenzte Gültigkeit haben. Dieser Gültigkeitszeitraum wird vom System überwacht. Außerhalb der Gültigkeit wird die Karte abgewiesen. Ist kein Wert gesetzt, bedeutet das unbegrenzte Gültigkeit.

Status

Nur aktive Ausweise werden an die Türsteuerungen geladen. Ein inaktiver Ausweis wird dementsprechend nicht funktionieren. Das System meldet dann: „unbekannter Ausweis“. Für einen Ausweis, der auch gültig sein soll, wählen Sie hier den Eintrag „Aktiv“.

Layout hinten/vorne

Im Dialog „Kartendesigner“ (Nur mit Modul Ausweiserstellung Art.-Nr. 348120V) wird beschrieben, wie Sie Karten bedrucken. Dort haben Sie auch die Möglichkeit verschiedene Layouts auszuwählen, die zuvor definiert wurden. Wenn Sie einen Ausweis neu anlegen, stellen Sie hier ein, welches Layout verwendet werden soll. Layouts können für jeden Ausweis separat festgelegt werden.



Eine Voreinstellung der Layouts kann über die Personalklasse der Person erfolgen, indem bei der Personalklasse die entsprechenden Layouts durch den Administrator hinterlegt werden (siehe „9.1.2 Stammdaten“ auf Seite 73).

Codedaten vorhanden

Wenn der Ausweis angelegt wurde, muss die zugehörige im Ausweis gespeicherte Information hinterlegt werden. Im Fall, dass vorkodierte Ausweise Verwendung finden, geschieht das über die Schaltfläche **Ausweis zuordnen**. Es folgt die Aufforderung, einen Ausweis an den Dialogleser zu halten, womit die Ausweisinformation ausgelesen und zum Datensatz gespeichert wird. Die Anzeige wechselt auf grün „Codedaten vorhanden“.

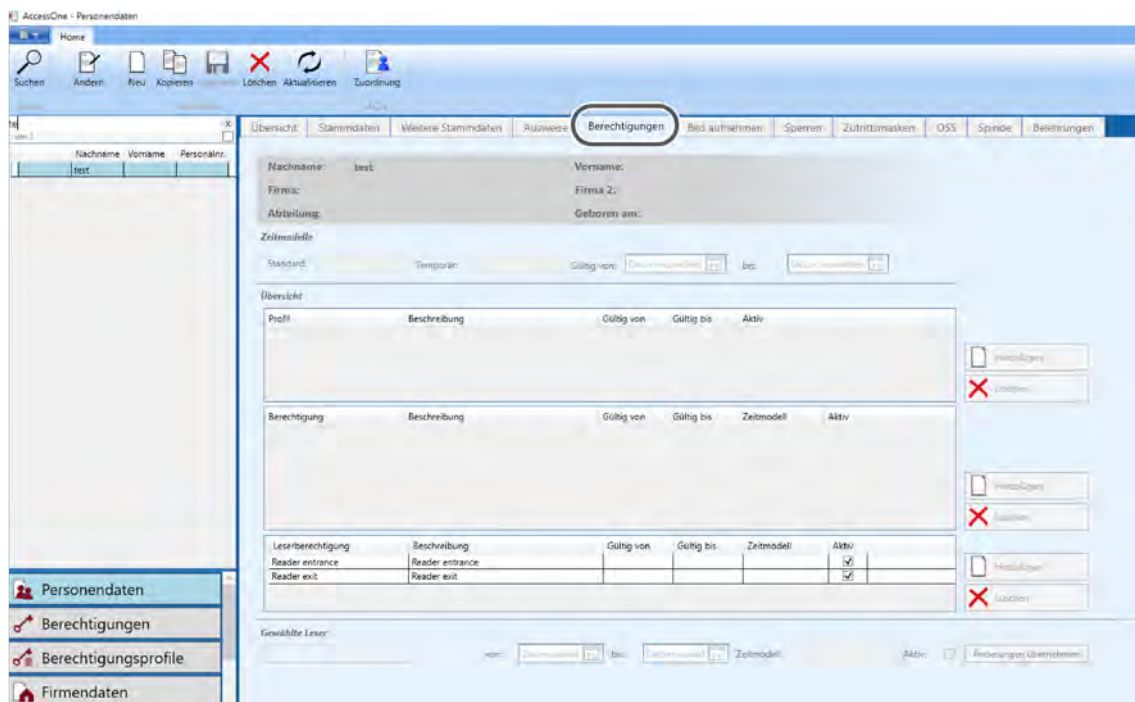
Werden die Ausweise von der AccessOne kodiert, ist alternativ die Schaltfläche **Codenummer zuweisen** aktiv. In diesem Fall wird von der AccessOne eine dem Ausweisformat des Kunden entsprechende Vorschrift angewendet und eine eindeutige freie Codenummer bestimmt. Diese wird dem Ausweis zugewiesen. Über die Schaltfläche **UHF Ausweis Kodieren** wird der Ausweis über den Dialogleser programmiert. Alternativ kann über die Schaltfläche **Ausweis beidseitig drucken** in einem Arbeitsgang kodiert und gedruckt werden. Voraussetzung dafür ist, dass in dem Drucker eine Kodiereinheit installiert ist.

Ausweis beidseitig drucken

Zeigt den Ausweis mit dem aufbereiteten Layout in einer Druckvorschau an. Nach Bestätigung wird der Ausweis gedruckt und je nach Möglichkeit des Druckers im gleichen Arbeitsschritt auch kodiert.

- „Letzter Druck“ zeigt das Datum und die Uhrzeit an, wann diese Karte zuletzt gedruckt wurde.
- „Anzahl gedruckt“ zeigt die Anzahl der gedruckten Ausweise der gewählten Person an.
- „Erstellungsgrund“ bietet die Möglichkeit, einen Grund für die (Neu-)Erstellung auszuwählen.
- „Rückgabedatum“ legt den Tag der Rückgabe fest. Mit Ablauf dieses Tages ist die Karte gesperrt.

9.1.5 Berechtigungen



In diesem Menü werden der Person definierte Zeitmodelle zugeordnet. Diese müssen im Dialog „Berechtigungen“ angelegt worden sein (siehe „9.1.5 Berechtigungen“ auf Seite 78).

Hier sind alle für die Zutrittsberechtigungen relevanten Informationen zusammengefasst:

Zeitmodelle

Für jede Person kann ein Standard-Zeitmodell festgelegt werden. Dieses gilt dann, wenn es zu einer Berechtigung kein eigenes Zeitmodell gibt. Sie können so z. B. festlegen, dass eine Person im Normalfall täglich von 09–17 Uhr Zutritt haben soll, aber die Tiefgarage auch nach Ablauf dieser Zeit noch nutzen darf. Alternativ kann man auch den Zutritt in bestimmte Bereiche stärker einschränken.



Ist kein Zeitmodell angegeben, so ist der Zutritt zeitlich nicht eingeschränkt.

Zusätzlich kann man ein temporäres Zeitmodell angeben, welches das Standard-Zeitmodell für einen festgelegten Zeitraum überschreibt. Das Zeitmodell kann ein kleineres Zeitfenster aufweisen (z. B. bei Kurzarbeit) oder ein größeres Zeitfenster (z. B. bei Wochenendarbeit).

Darunter stehen die beiden Listen mit den zur Person gewählten Profilen bzw. Berechtigungen.

Profile

Ein Profil umfasst eine Gruppe von Berechtigungen. Man kann mehrere Berechtigungen unter einem Profil zusammenfassen. Profile ermöglichen es, die Berechtigungen nach der Funktion der Person zusammenzustellen. So kann man z. B. ein Profil für Reinigungskräfte und eines für Techniker erstellen. Dieses Vorgehen erleichtert die Auswahl der Berechtigungen, die der jeweilige Mitarbeiter zur Erfüllung seiner Aufgaben benötigt.

Beispiel: Die Gebäudeeingänge werden in einer Berechtigung zusammengefasst und ein Profil für Gebäudeeingänge beinhaltet dann die Berechtigungen je Gebäude.

 Änderungen in den Berechtigungen, die in Profilen enthalten sind, wirken sich sofort auf die Profile aus. Die AccessOne überträgt die Profile unmittelbar an die Türsteuerungen, so dass sich die Änderung in einer Berechtigung oder in einem Profil auf alle Personen auswirkt, die dieses Profil zugewiesen bekommen haben, ohne dass dafür zusätzliche Datensätze übertragen werden müssen.

Zu jedem Profil kann eine begrenzte Gültigkeit und ein Zeitmodell angegeben werden. Ist kein Zeitmodell angegeben, gilt das zur Person hinterlegte Zeitmodell. Ist keine Gültigkeit eingetragen, ist dieses Profil unbegrenzt gültig. Ist nur ein Startdatum, aber kein Enddatum vorhanden, gilt das Profil ab Startdatum unbegrenzt. Ein eingetragenes Enddatum beendet die Gültigkeit.

Ein Profil wird aus der Liste entfernt, indem es ausgewählt wird und dann die Schaltfläche Löschen neben der Auswahlliste angeklickt wird. Ein neues Profil wird angelegt, indem über die Schaltfläche Hinzufügen eine Auswahlbox aufgerufen wird, aus der das gewünschte Profil ausgewählt werden kann. Mehrfachauswahl ist durch Klicken bei gedrückter STRG-Taste möglich.

Berechtigungen

Berechtigungen fassen Leser zu einer zusammengehörigen Gruppe zusammen. Siehe dazu auch den Dialog „Berechtigungen“ (siehe „9.1.5 Berechtigungen“ auf Seite 78). Für Berechtigungen gelten die gleichen Regeln wie für Profile.

Gewählte Berechtigung

Werden eine oder mehrere Berechtigungen oder Profile durch Anklicken ausgewählt, werden in diesen Feldern die Details angezeigt und können dort auch geändert werden. Mit Klicken der Schaltfläche

Änderungen übernehmen werden die geänderten Felder dann in die Berechtigung bzw. das Profil übernommen.



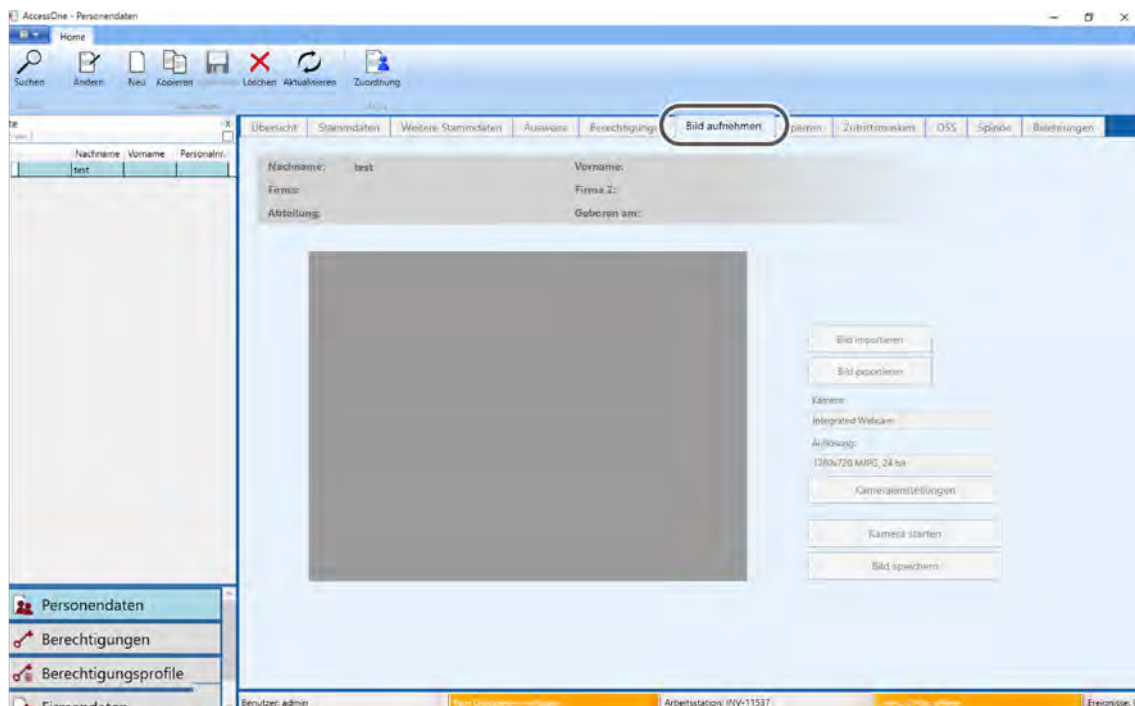
Für die Übernahme der Änderung muss die Schaltfläche **Änderungen übernehmen** betätigt werden, sonst werden die Änderungen nicht gespeichert.

Einer Person können bis zu 64 Berechtigungen und/oder Profile zugewiesen werden (z. B. 10 Profile und 22 Berechtigungen). Sind bei vielen Personen immer die gleichen Berechtigungen aufgeführt, empfehlen wir, diese Berechtigungen in einem eigenen Berechtigungsprofil zusammenzufassen.



Wenn einer Person eine Berechtigung zugewiesen wird, die bereits in einem Berechtigungsprofil enthalten ist, das der Person zugewiesen wurde, wird diese redundante Berechtigung im Rahmen der automatisierten Wartungsprozesse zum Tageswechsel gelöscht.

9.1.6 Bild aufnehmen



Auf dem Tab „Bild aufnehmen“ können Sie der Person ein Bild zuweisen, in dem Sie dieses Bild importieren oder direkt ein Foto machen.

Möchten Sie zur Person ein Bild importieren, wählen Sie die Person im Auswahlfenster links an und klicken Sie in der Werkzeugleiste oben auf den Button ÄNDERN. Betätigen Sie nun die Schaltfläche **Bild importieren**. Sie können Dateien im Format *.bmp, *.png oder *.jpg wählen. Um ein Foto aufzunehmen, muss eine Kamera an Ihrem PC/Laptop angeschlossen sein.

Wählen Sie in der Dropdown-Box „Kamera“ das entsprechende Gerät aus. Eine andere Auflösung und weitere Kamera-Einstellungen können je nach angeschlossenem Gerätetyp vorgenommen werden.

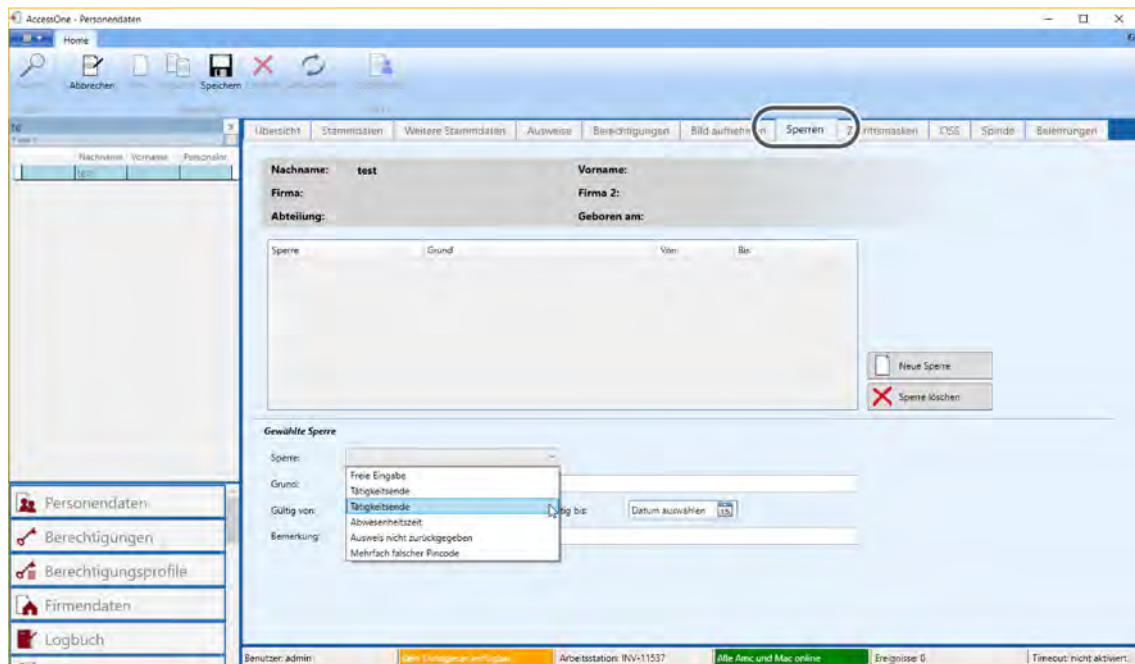
Mit der Schaltfläche **Kamera starten** nehmen Sie ein Foto von der Person auf.

Nachdem der passende Bildausschnitt (grüner Rahmen) gewählt wurde, wird dieser über die Schaltfläche **Bild speichern** in der Vorschau im oberen rechten Bereich angezeigt.



Beim Wechsel zu einem anderen Tab ohne zu speichern, steht die Aufnahme zur weiteren Bearbeitung nicht mehr zur Verfügung.

9.1.7 Sperren



Auf diesem Tab können Sie Personen sperren, wenn z. B. ein Mitarbeiter seinen Ausweis verloren hat. Doppelklicken Sie dazu im Auswahlfenster links auf die Person, die Sie sperren möchten, um in den Bearbeitungsmodus zu gelangen. Die Schaltfläche **Neue Sperre** ist nun aktiviert und Sie können der Person eine Sperre zuweisen.

Im Bereich „Gewählte Sperre“ nehmen Sie zusätzliche Einstellungen vor.

Soll die Sperre zeitlich befristet sein, z. B. vor einem „Tätigkeitsbeginn“, wählen Sie ein „Gültig von/bis“-Datum an.

Machen Sie Angaben zur Sperre im Eingabefeld „Bemerkung“. Mit dem Button **SPEICHERN** in der Werkzeugleiste speichern Sie die Sperre. Eine Sperre können Sie löschen, indem Sie sie in der Liste auswählen und die Schaltfläche **Sperre löschen** betätigen.

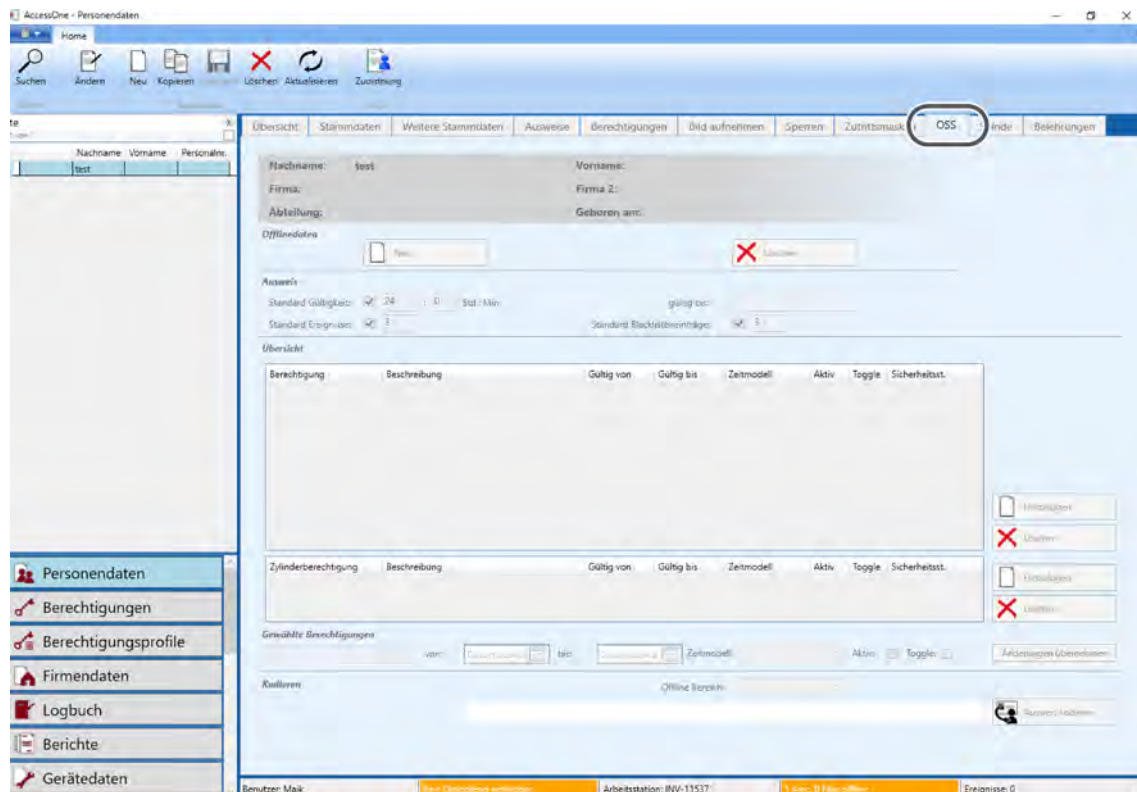
Die AccessOne unterscheidet zwischen automatischen und manuellen Sperren. Es können auf Wunsch zusätzliche Sperren im System vordefiniert werden.

Beispiel: Sperre vor Tätigkeitsbeginn und nach Tätigkeitsende

Diese Sperre kann auch per Hand gesetzt werden und ist sofort wirksam! In diesem Fall ist zu beachten, dass das System während der Nachtstunden die Sperre anhand der bei der Person eingetragenen Daten aktualisiert. Wenn eine Person z. B. wegen Tätigkeitsende gesperrt ist, aber am nächsten Tag noch einmal ins Büro muss, so kann diese Sperre zwar von Hand gelöscht werden, nach Mitternacht wird sie automatisch wieder gesetzt.

9.1.8 OSS-SO

Dank OSS Standard Offline können Zylinder und Beschlge unterschiedlicher Marken die gleichen Berechtigungen von der Karte lesen und sie in gleicher Weise interpretieren.



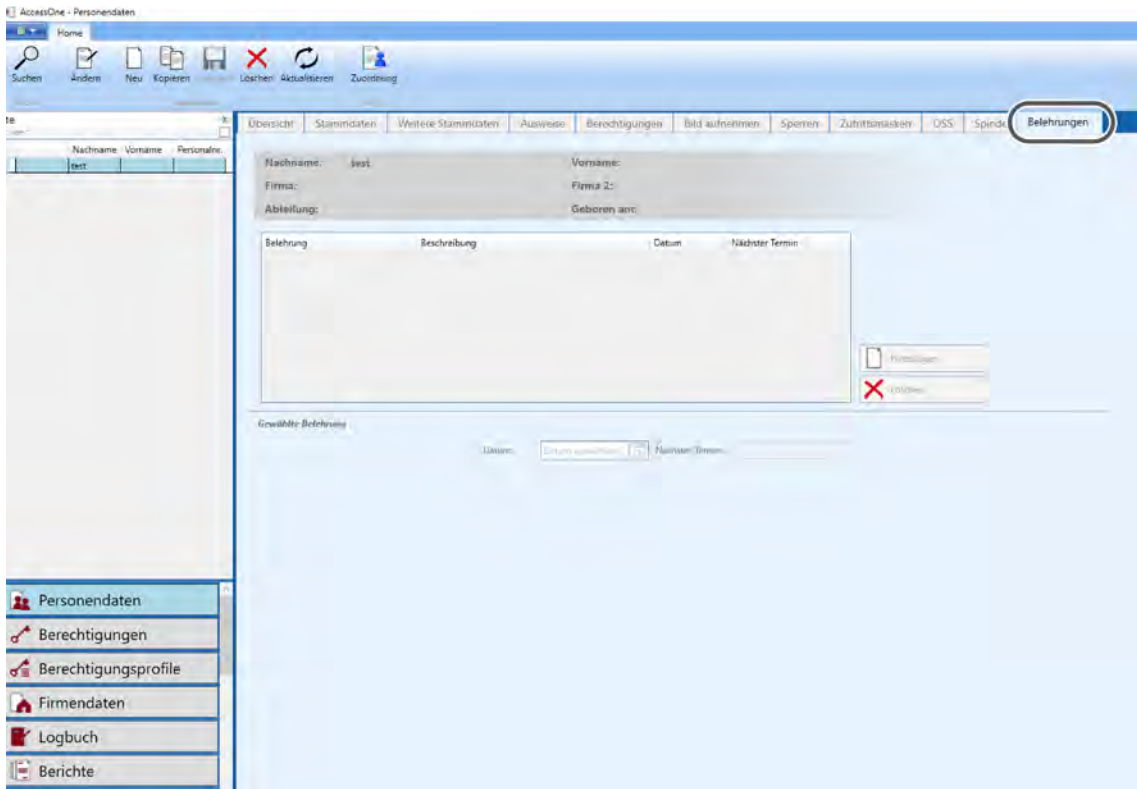
Die Einrichtung und Verwaltung von elektronischen Zylindern und Beschlgen, die zum OSS Standard kompatibel sind, ist vollstndig in die AccessOne integriert. Zur Einrichtung bentigen Sie zustzlich das vom jeweiligen Hersteller gelieferte Konfigurationstool, mit dem die Konfigurationsdaten in die Zylinder einprogrammiert werden.

Alle Konfigurationsdaten werden in der AccessOne erfasst. Aus der Bedienoberflche knnen Sie dann eine XML-Datei erzeugen, die von dem jeweiligen Konfigurationstool eingelesen wird. In dieser Datei sind alle Daten fr die Initialisierung der Zylinder enthalten.

Nach Installation der entsprechenden Lizenz steht in der Funktionsauswahl eine Schaltflche fr OSS zur Verfgung. Hierber erreichen Sie die Dialoge fr die Datenpflege der Offline-Komponenten. Dort legen Sie die Gultigkeit der Ausweise der Personen fest und fgen Profile, Berechtigungen und Zylinderberechtigungen hinzu.

Zum Schluss kodieren Sie den Ausweis.

9.1.9 Belehrungen



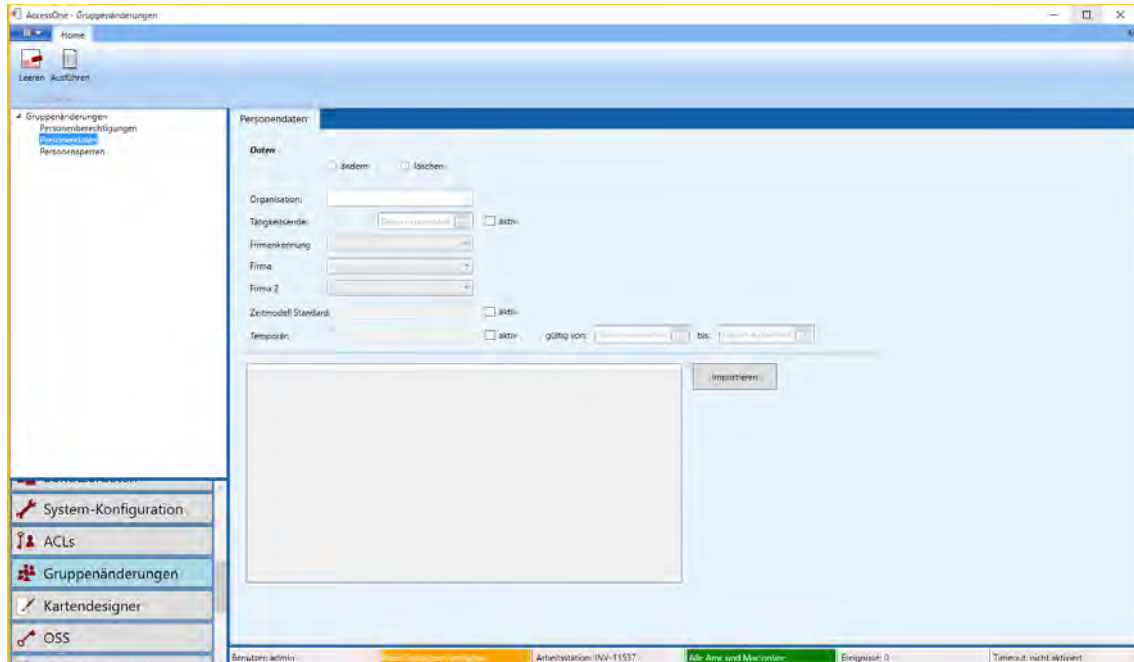
The screenshot shows the 'AccessOne - Personendaten' application. The 'Belehrungen' tab is active, displaying a form for entering instructions. The form includes fields for 'Nachname', 'Vorname', 'Firma', 'Geburtsort', 'Geburtsdatum', and 'Geburtsort'. Below the form is a table with columns 'Belehrung', 'Beschreibung', 'Datum', and 'Nächster Termin'. A sidebar on the left contains navigation links for 'Personendaten', 'Berechtigungen', 'Berechtigungsprofile', 'Firmendaten', 'Logbuch', and 'Berichte'.

Hier können Belehrungen, die in einem bestimmten Zeitraum erfolgen müssen, hinterlegt werden (z. B. UVV, DSGVO etc.). Über die Schaltfläche Hinzufügen können diese ausgewählt und mit Datum eingetragen werden.

9.2 Gruppenänderungen

Im Dialog „Gruppenänderungen“ können Änderungen an Personendaten, Personensperren und Berechtigungen auf ganze Gruppen per Datenimport angewendet werden.

9.2.1 Personendaten



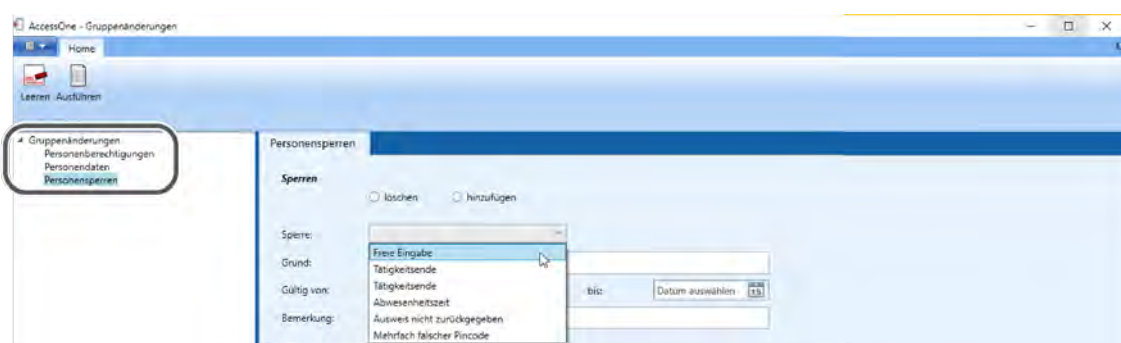
Im Tab „Personendaten“ können zuvor erstellte Daten für Personengruppen, die durch Klicken auf die Schaltfläche **Importieren** geladen worden sind, geändert oder gelöscht werden.

Die zu importierenden Daten müssen als *.csv-Datei vorliegen. Erzeugt werden kann diese Datei über die Dialogseite „Berichte > Personen > Personengruppen Export“. Auf dieser Dialogseite stehen vielfältige Filter zum Konfigurieren von Personengruppen zur Verfügung. Wird ein Bericht erstellt, kann die erzeugte Personengruppe als MS Excel-Datei auf der Festplatte gespeichert und weiter bearbeitet werden.



Die aus diesem Programm gespeicherte *.csv-Datei, dient als Importdatei für alle Gruppenänderungsdialoge.

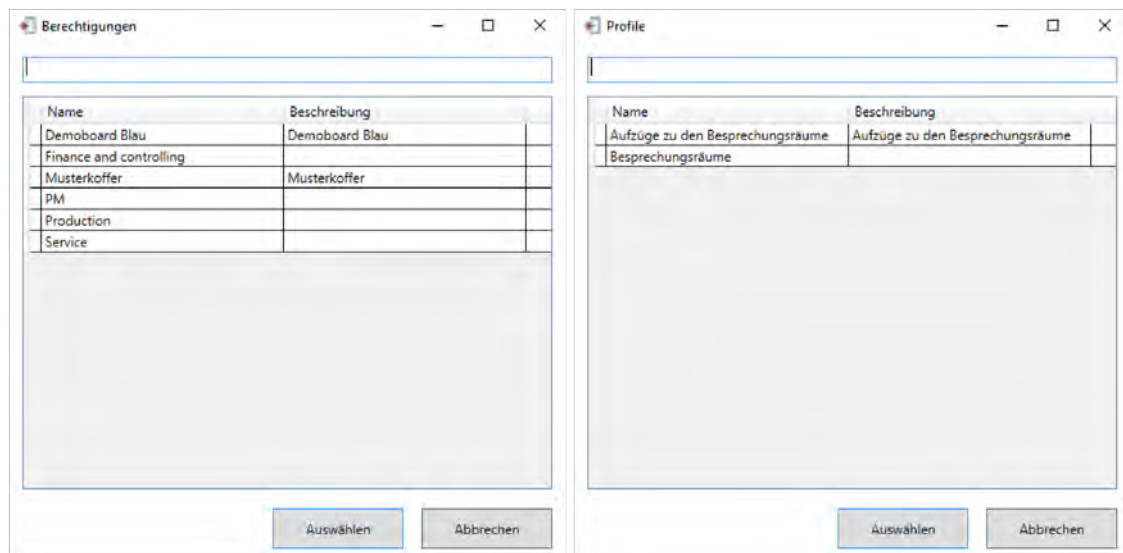
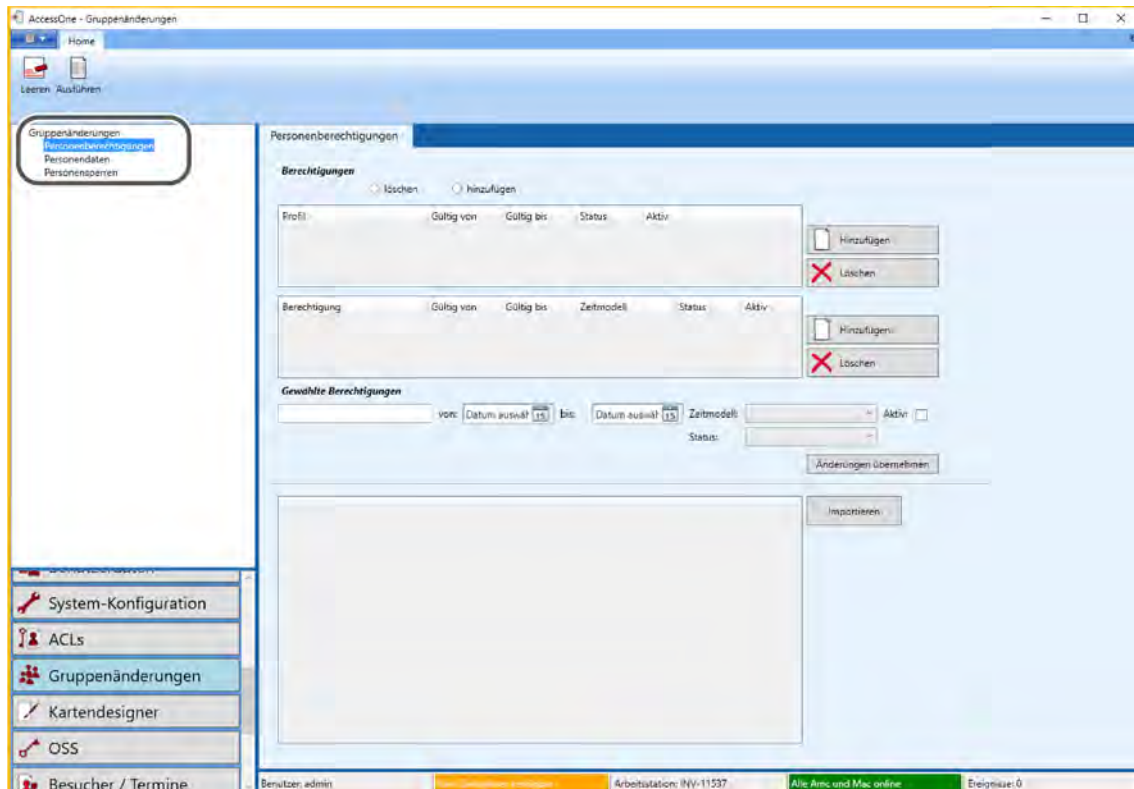
9.2.2 Personensperren hinzufügen oder löschen



Im Tab „Personensperren“ können für die jeweilige Personengruppe Sperrdaten durch Dateiimport hinzugefügt oder gelöscht werden.

Im Eingabefeld „Sperre“ haben Sie mehrere Sperrgründe zur Auswahl, die mit einer Gültigkeit eintragen werden können.

9.2.3 Personenberechtigungen anpassen



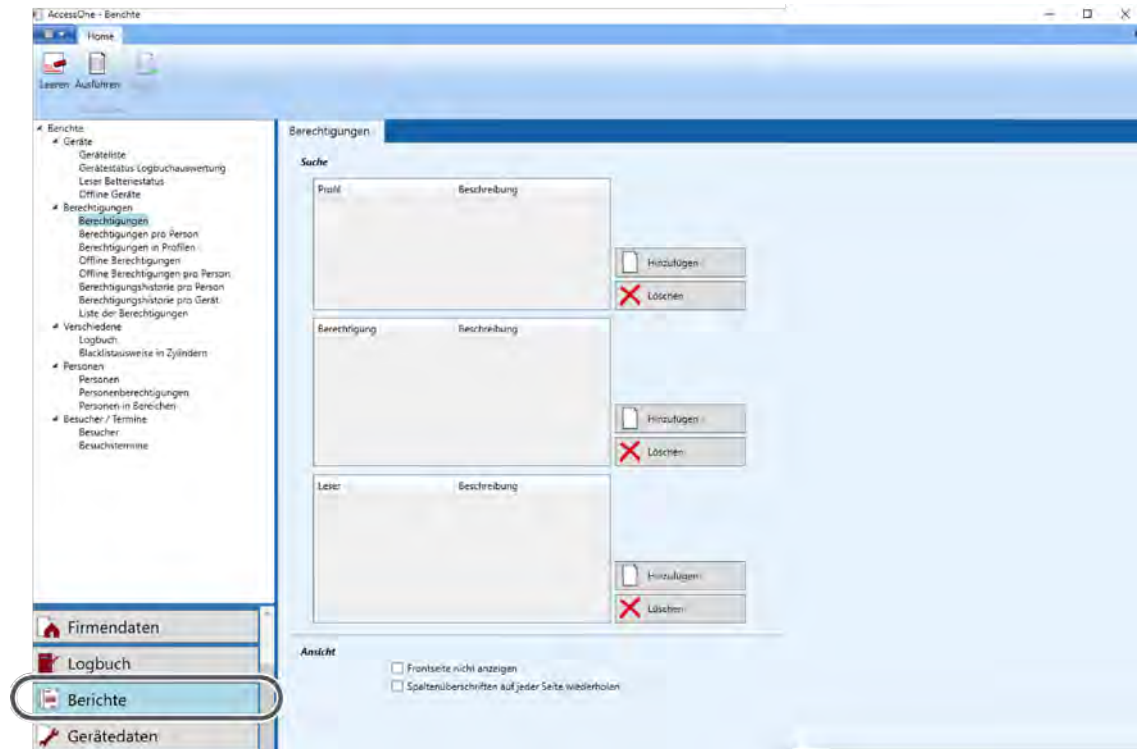
Im Tab „Personenberechtigungen“ können für die jeweilige Personengruppe Berechtigungen durch Dateiimport oder Eingabe von Profil und Berechtigung hinzugefügt und gelöscht werden. Änderungen immer mit **Änderungen übernehmen** bestätigen.

10 Anlagendokumentation

Für die Dokumentation der Anlage zu einem bestimmten Zeitpunkt können Berichte erzeugt und Logbucheintragen eingesehen und exportiert werden.

10.1 Berichte

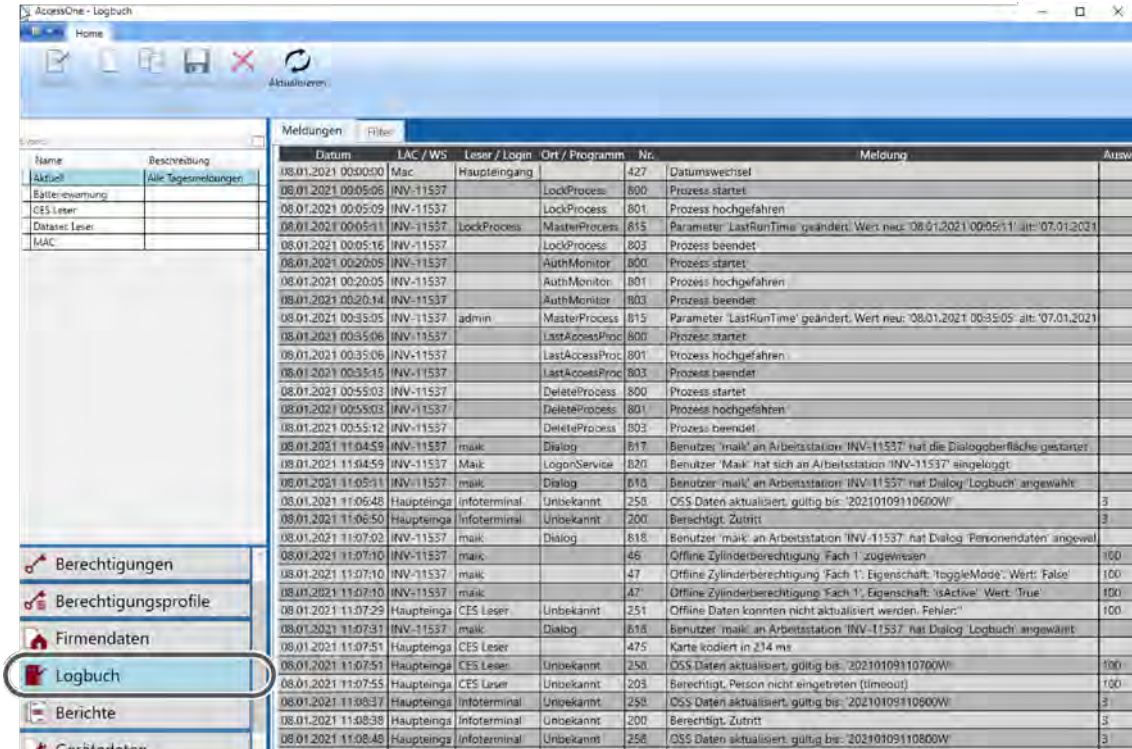
Über die Dialogauswahl „Berichte“ können alle vorgenommenen Eintragungen eingesehen und ausgegeben werden. Die AccessOne kann jederzeit eine vollständige Anlagendokumentation ausgeben.



10.2 Logbuch

Der Dialog „Logbuch“ ermöglicht die Abfrage aller aktuellen Tagesmeldungen und das Anlegen individueller Filter.

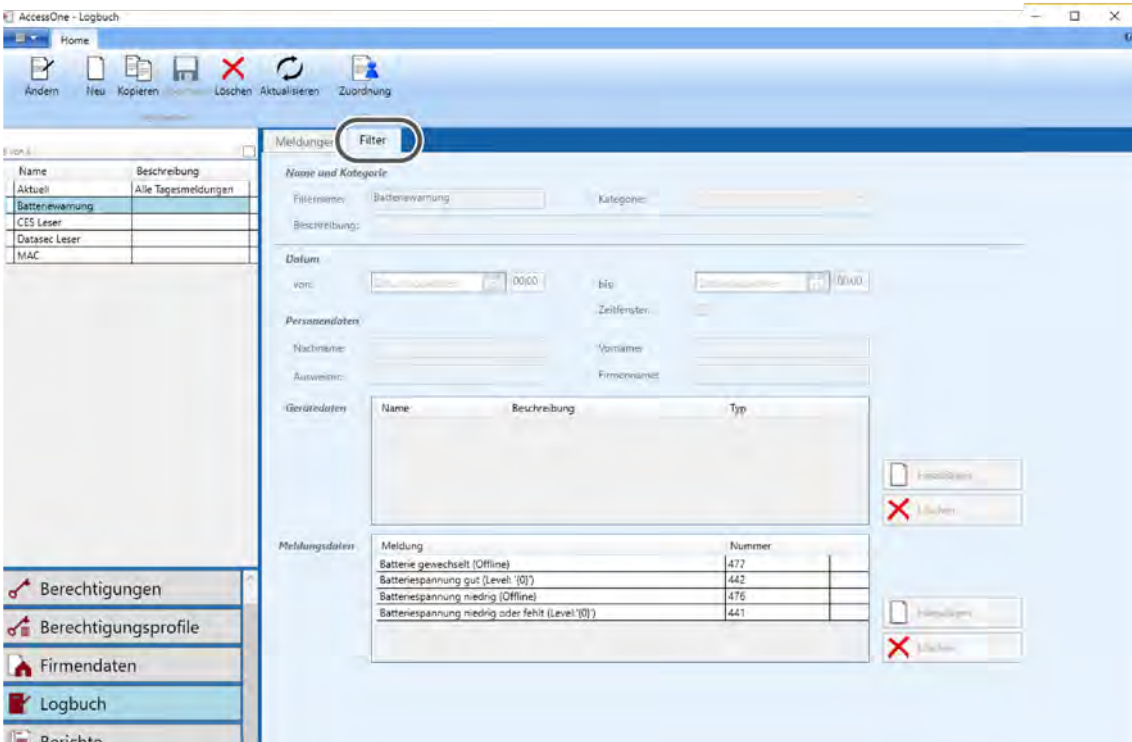
10.2.1 Meldungen



Name	Beschreibung	Datum	LAC / WS	Leser / Login	Ort / Programm	Nr.	Meldung	Anzeige
Aktuell	Alle Tagesmeldungen	08.01.2021 00:00:00	Mac	Haupteingang		427	Datumswechsel	
Batteriewarnung		08.01.2021 00:05:08	INV-11537		LockProcess	800	Prozess startet	
CES Leser		08.01.2021 00:05:09	INV-11537		LockProcess	801	Prozess hochgefahren	
Datasec Leser		08.01.2021 00:05:11	INV-11537		LockProcess	815	Parameter 'LastRunTime' geändert. Wert neu: '08.01.2021 00:05:11' alt: '07.01.2021	
MAC		08.01.2021 00:05:16	INV-11537		LockProcess	803	Prozess beendet	
		08.01.2021 00:20:05	INV-11537		AuthMonitor	800	Prozess startet	
		08.01.2021 00:20:05	INV-11537		AuthMonitor	801	Prozess hochgefahren	
		08.01.2021 00:20:14	INV-11537		AuthMonitor	803	Prozess beendet	
		08.01.2021 00:35:05	INV-11537	admin	MasterProcess	815	Parameter 'LastRunTime' geändert. Wert neu: '08.01.2021 00:35:05' alt: '07.01.2021	
		08.01.2021 00:35:06	INV-11537		LastAccessProc	800	Prozess startet	
		08.01.2021 00:35:06	INV-11537		LastAccessProc	801	Prozess hochgefahren	
		08.01.2021 00:35:15	INV-11537		LastAccessProc	803	Prozess beendet	
		08.01.2021 00:55:03	INV-11537		DeleteProcess	800	Prozess startet	
		08.01.2021 00:55:03	INV-11537		DeleteProcess	801	Prozess hochgefahren	
		08.01.2021 00:55:12	INV-11537		DeleteProcess	803	Prozess beendet	
		08.01.2021 11:04:59	INV-11537	maik	Dialog	817	Benutzer 'maik' an Arbeitsstation 'INV-11537' hat die Dialogoberfläche gestartet	
		08.01.2021 11:04:59	INV-11537	maik	LoginService	820	Benutzer 'maik' hat sich an Arbeitsstation 'INV-11537' eingeloggt	
		08.01.2021 11:05:11	INV-11537	maik	Dialog	818	Benutzer 'maik' an Arbeitsstation 'INV-11537' hat Dialog 'Logbuch' angewählt	
		08.01.2021 11:05:48	Haupteinga	Infoterminal	Unbekannt	250	OSS Daten aktualisiert, gültig bis: '20210109110600W'	3
		08.01.2021 11:06:50	Haupteinga	Infoterminal	Unbekannt	200	Berechtigt Zutritt	3
		08.01.2021 11:07:02	INV-11537	maik	Dialog	818	Benutzer 'maik' an Arbeitsstation 'INV-11537' hat Dialog 'Personendaten' angewel	
		08.01.2021 11:07:10	INV-11537	maik		46	Offline Zylinderberechtigung Fach 1 zugewiesen	100
		08.01.2021 11:07:10	INV-11537	maik		47	Offline Zylinderberechtigung Fach 1: Eigenschaft: 'toggleMode' Wert: False	100
		08.01.2021 11:07:10	INV-11537	maik		47	Offline Zylinderberechtigung Fach 1: Eigenschaft: 'isActive' Wert: True	100
		08.01.2021 11:07:29	Haupteinga	CES Leser	Unbekannt	251	Offline Daten konnten nicht aktualisiert werden. Fehler:	100
		08.01.2021 11:07:31	INV-11537	maik	Dialog	818	Benutzer 'maik' an Arbeitsstation 'INV-11537' hat Dialog 'Logbuch' angewählt	
		08.01.2021 11:07:51	Haupteinga	CES Leser		475	Karte kodiert in 214 ms	
		08.01.2021 11:07:51	Haupteinga	CES Leser	Unbekannt	250	OSS Daten aktualisiert, gültig bis: '20210109110700W'	100
		08.01.2021 11:07:55	Haupteinga	CES Leser	Unbekannt	203	Berechtigt, Person nicht eingetreten (timeout)	100
		08.01.2021 11:08:37	Haupteinga	Infoterminal	Unbekannt	250	OSS Daten aktualisiert, gültig bis: '20210109110800W'	3
		08.01.2021 11:08:38	Haupteinga	Infoterminal	Unbekannt	200	Berechtigt Zutritt	3
		08.01.2021 11:08:48	Haupteinga	Infoterminal	Unbekannt	250	OSS Daten aktualisiert, gültig bis: '20210109110800W'	3

10.2.2 Filter

Bestimmen Sie Ihre individuellen Filter. Die AccessOne bietet vielfältige Eingabemöglichkeiten.



Filter

Name und Kategorie

Filtername: Batteriewarnung Kategorie:

Beschreibung:

Datum

Von: 00:00 bis: 00:00

Personendaten

Nachname: Zeilenfilter: Vorname: Firmenname:

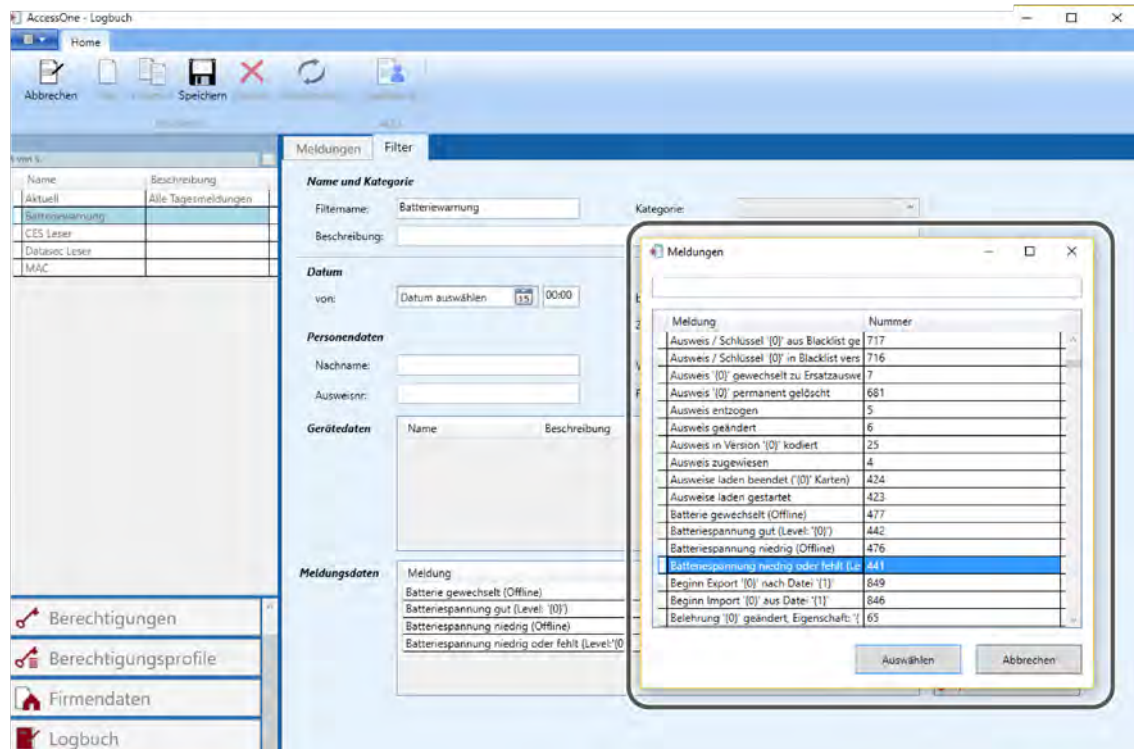
Gerätedaten

Name	Beschreibung	Typ

Meldungsdaten

Meldung	Nummer
Batterie gewechselt (Offline)	417
Batteriespannung gut (Level: '0')	442
Batteriespannung niedrig (Offline)	476
Batteriespannung niedrig oder fehlt (Level: '0')	441

Über die Schaltfläche **Hinzufügen** wird ein Fenster aufgerufen, das alle Geräte- und Meldungsdaten, nach denen gefiltert werden kann, auflistet.



11 Fehlerbehebung

Verbindung der Clients zum AccessOneServer funktioniert nicht	Im Installationsverzeichnis	Die Einträge in der Datei ClientConfig.xml im Installationsverzeichnis\AccessOne\config kontrollieren. Stimmen die Einträge für „MasterHost“ und „MasterPort“?
	Auf dem Server	- Sind SQL Server und SQL Browser Dienst gestartet und die Protokolle TCP/IP und Named Pipes aktiviert? - Firewallregeln kontrollieren. SQL Server Port (Standard: TCP 1433), SQL Browser Port (Standard: UDP 1434) und die konfigurierten AccessOnePorts (z. B. TCP 50000-500xx) zugreifbar?
	Zusammenspiel Server-Client	Ist die Uhrzeit auf Client und AccessOneServer synchron? Eine Zeitdifferenz kleiner als 5 Minuten ist erlaubt.



C.Ed. Schulte GmbH
Zylinderschlossfabrik

Friedrichstraße 243

D-42551 Velbert

☎ +49 2051 204 0

☎ +49 2051 204 229

✉ info@ces.eu