

AccessOne

Software voor toegangscontrole



Systeembeschrijving en handleiding

 Nederlands

Versie VA1

BRO2262

Inhoudsopgave

1	Over deze handleiding	4
1.1	Fabrikant en service.....	5
1.2	Doelgroepen van deze handleiding	5
2	Voor uw veiligheid	6
2.1	Veiligheidsvoorschriften.....	6
2.2	Juridische informatie	6
2.3	Systeemvoorwaarden.....	6
2.4	Gegevensbescherming in AccessOne	6
3	Over AccessOne.....	8
3.1	Functie-uitbreidingen.....	9
3.2	Aanbevolen procedure voor de eerste configuratie van AccessOne	10
4	Algemeen gebruik van dialoogvensters.....	12
4.1	Kijkmodus – wijzigingsmodus.....	13
4.2	Taakbalk.....	13
5	Aanmelding	16
6	Configuratie van AccessOne	17
6.1	Systeemconfiguratie	17
6.1.1	Parameter.....	17
6.1.2	Gebieden.....	19
6.1.3	Parkeergroepen	19
6.1.4	Werkstations	20
6.1.5	Lezerformaten	20
6.1.6	Kaart analyseren.....	21
6.1.7	Licenties.....	22
6.1.8	Kaartformaten.....	23
6.2	Gebruikersgegevens	27
6.2.1	Gebruikersgroepen.....	27
6.2.2	Stamgegevens gebruiker.....	28
6.2.3	Gebruiker ACL (klantenmogelijkheden).....	29
6.2.4	Gegevensrecords toewijzen aan de toegangslijsten – ACL	30
6.2.5	Web-gebruikersgroepen.....	31
6.3	Locatiegegevens	32
6.3.1	Locatie aanmaken	32
7	Apparaten configureren	33
7.1	Apparaatgegevens online-apparaten	34
7.1.1	Apparaatoverzicht weergeven	34
7.1.2	Mastercontroller (MAC) aanmaken	35
7.1.3	Deurbesturing (LAC) aanmaken.....	37
7.1.4	Een deur aanmaken	40
7.1.5	Apparaatstatus weergeven.....	54

7.2	Apparaatgegevens offline-apparaten (OSS-SO).....	55
7.2.1	Facility data.....	55
7.2.2	Cilinders (en beslag).....	56
7.2.3	Offline-apparaten programmeren.....	57
7.2.4	Toegangsrechten.....	58
7.2.5	Gegevens importeren.....	59
7.2.6	Tijdmodellen.....	60
8	Toegangsrechten configureren.....	61
8.1	Toegangsrechten.....	61
8.1.1	Overzicht van de toegangsrechten.....	61
8.1.2	Algemene informatie over tijd- en dagmodellen.....	62
8.1.3	Dagmodellen.....	62
8.1.4	Speciale en feestdagen.....	63
8.1.5	Tijdmodellen.....	66
8.1.6	Toegangsmaskers.....	68
8.2	Toegangsrechtprofielen.....	69
8.2.1	Overzicht van online-toegangsrechten.....	69
8.2.2	Overzicht van offline-toegangsrechten.....	70
9	Persoonsgegevens aanmaken.....	71
9.1	Persoonsgegevens.....	71
9.1.1	Overzicht van persoonsgegevens.....	71
9.1.2	Stamgegevens.....	73
9.1.3	Verdere stamgegevens.....	75
9.1.4	Kaarten (toegangsmidia).....	76
9.1.5	Toegangsrechten.....	78
9.1.6	Capture picture.....	80
9.1.7	Blokkeringen.....	81
9.1.8	OSS-SO.....	82
9.1.9	Instructions.....	83
9.2	Verandering in groepen.....	84
9.2.1	Persoonsgegevens.....	84
9.2.2	Personenblokkeringen toevoegen of wissen.....	84
9.2.3	Persoonstoegangsrechten aanpassen.....	85
10	Systeemdocumentatie.....	86
10.1	Rapporten.....	86
10.2	Logboek.....	87
10.2.1	Berichten.....	87
10.2.2	Filter.....	87
11	Probleemoplossing.....	89

1 Over deze handleiding
2 Deze handleiding bevat fundamentele informatie over de configuratie en het beheer van een systeem voor toegangsbesturing met het toegangscontrolesysteem AccessOne.

De handleiding dient te worden beschouwd als onderdeel van het product en tijdens de volledige gebruiks- en levensduur van het product te worden bewaard. Geef de handleiding door aan alle volgende gebruikers.

Aanvullende documenten

Activeren licentie >	BRO2307_NL_Informatieblad_Activering-licentiemodule-AccessOne
Installatie >	BRO2313_NL_Informatieblad_Installatie-AccessOne

Eigenschappen



Verwijst naar verdere documentatie.



Markeert aanvullende informatie en tips.



Markeert waarschuwingen in stappenplannen en belangrijke informatie.

Gebruikelijke notaties

In dit document worden bedieningselementen van de dialooginterface, zoals knoppen, in vetgedrukte tekst weergegeven (voorbeeld: Klik op **Gebruiker aanmaken**). Knoppen op de werkbalk worden bovendien in hoofdletters weergegeven (voorbeeld: klik op AFBREKEN). Namen van dataobjecten, selectievelden, tekstvelden en selectievakjes worden getoond tussen aanhalingstekens (voorbeeld: in het veld "Opmerkingen" voert u aanvullende informatie in).

Afbeeldingen

De dialoogvensters die in de handleiding zijn afgebeeld, omvatten niet alle opties die het systeem heeft. Afhankelijk van de licentie en de geactiveerde opties kunnen de schermafbeeldingen en de beschrijving afwijken.

Merksnaambescherming

MIFARE, MIFARE Classic en MIFARE DESFire zijn geregistreerde merken van NXP BV en worden gebruikt onder licentie.

De informatie en gegevens in deze handleiding kunnen zonder voorafgaande kennisgeving worden gewijzigd of technisch worden doorontwikkeld. Niets uit deze handleiding mag voor welke doeleinden dan ook worden verveelvoudigd of verspreid zonder uitdrukkelijke schriftelijke toestemming van C.Ed. Schulte GmbH Zylinderschlossfabrik.

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

BRO2316-1 Versie: VA1



Gebruik altijd de nieuwste versie van deze handleiding. Geactualiseerde versies kunt u gratis aanvragen op www.ces.eu.

2.1 Fabrikant en service

De auteursrechten van AccessOne behoren toe aan ACcesstronic GmbH. Service en support worden verzorgd door C.Ed. Schulte GmbH, gevestigd te Velbert. Voor ondersteuning en service kunt u contact opnemen met de klantenservice van CES. U bereikt de CES-service via +49(0)2051 204 222 of via e-mail: hotline@ces.eu

Fabrikant

ACcesstronic GmbH
Gartenstr. 38
D-52249 Eschweiler

Service en 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

2.2 Doelgroepen van deze handleiding

Voor de configuratie van AccessOne geeft de exploitant van de systeem de opdracht. De configuratie wordt uitgevoerd door eigen vakmensen of dienstverleners van IT/systeembeheer. Alleen voor het product opgeleid personeel mag de toegangsbesturingssysteem bedienen. De informatie in deze handleiding is daarom bestemd voor verschillende doelgroepen. De doelgroepen worden aan het begin van elk hoofdstuk vermeld. Neem onze adviezen in acht over de procedures bij installatie, configuratie en bediening van AccessOne (zie "Algemeen" op de volgende pagina).

Doelgroep	Competenties
Vakmensen IT/systeembeheer	hebben jarenlange beroepservaring op het gebied van IT-structuren, systeembeheer en netwerken. Bijzonder eigenschappen van de doelgroep: Kennis van IT-vaktermen Kennis omtrent de opbouw en het onderhoud van netwerken, met name kennis van het netwerk dat door hen wordt beheerd
Systeemexploitanten	beschikken over ervaring met het beheer van sluitsystemen. Dit kunnen zowel meerdere systemen zijn alsook diepgaande kennis van een afzonderlijk sluitsysteem. Bijzonder eigenschappen van de doelgroep: Kennis van vaktermen rondom sluitsystemen Kennis over de omgang met een pc en software
Voor het product opgeleid personeel	is door CES of een CES-leverancier voor het product opgeleid. Daarbij is het personeel gericht en intensief op de betreffende taak voorbereid. Bijzonder eigenschappen van de doelgroep: Kennis van het CEStronics-product en ervaring met de omgang met deze producten (montage, bediening enz.)

3 Voor uw veiligheid

3.1 Veiligheidsvoorschriften

Het in dit handboek beschreven systeem voor toegangscontrole, AccessOne, mag alleen door personen worden bediend die voor deze taken zijn bevoegd en gekwalificeerd. Gekwalificeerd personeel beschikt over jarenlange beroepservaring op het gebied van IT-structuren, systeembeheer en netwerken, en kan vanwege zijn ervaring met het beheer van sluitsystemen of door de grondige kennis van een individueel sluitsysteem risico's herkennen en mogelijke gevaarlijke situaties vermijden.



Geblokkeerde deur belemmert hulp of leidt tot materiële schade

Verkeerd geprogrammeerde componenten kunnen tot een ongewenst geblokkeerde toegang leiden. Wanneer door een geblokkeerde deur de toegang tot personen in nood niet mogelijk is of de geblokkeerde deur tot materiële schade of andere schade leidt, is C.Ed. Schulte Zylinderschloss-fabrik GmbH daarvoor niet aansprakelijk!

3.2 Juridische informatie

Hierbij wordt de koper er uitdrukkelijk op gewezen dat het gebruik van het toegangscontrolesysteem AccessOne kan zijn onderworpen aan wettelijke bepalingen, en hier in het bijzonder, rechten met verplichte vergunning betreffende gegevensbescherming en medezeggenschap van het personeel. De koper en eindgebruiker zijn ervoor verantwoordelijk dat het product volgens de wet wordt gebruikt.

3.3 Systeemvoorwaarden

De minimale systeemvoorwaarden voor AccessOne zijn gerelateerd aan de aanbevolen systeemvoorwaarden voor de Microsoft SQL-server.

- Besturingssysteem (server): vanaf Windows Server 2016
- Besturingssysteem (pc): vanaf Windows 10 Professional
- Werkgeheugen: min. 8 GB
- SQL-server: vanaf MS SQL Server 2016, express-variant toepasbaar
- Harde schijf: min. 1 x 500 GB, 2 x 500 GB geadviseerd
- Netwerkkkaart

3.4 Gegevensbescherming in AccessOne

Naleving van de wistermijnen

AccessOne beschikt over een parametreerbaar wisproces dat dagelijks kort na middernacht start en gegevens uit het systeem verwijdert, waarvan de bewaartermijn is verstreken. Dat heeft met name betrekking op bewegingsgegevens. De gebruiker van het systeem kan de parameters instellen.



Om te voldoen aan de AVG, kan het wissen van persoonsgebonden logboekmeldingen worden geconfigureerd. Met de parameter 'LogbookRewriteOffset' wordt het aantal dagen ingesteld waarna dit dient plaats te vinden.

Parameter	Beschrijving	Standaardinstelling
DateDeletedOffset	Vertraging waarna persoonsgegevensrecords met de ingevoerde 'dateDeleted'-datum definitief uit de databank worden gewist.	3 dagen
VistorDeleteOffset	Vertraging waarna de bezoekers worden gewist.	183 dagen
EventDeleteOffset	Vertraging waarna de behandelde gebeurtenissen worden verwijderd.	183 dagen
AppointmentDelOffset	Aantal dagen waarna de afspraken en alle afhankelijk gegevens worden gewist.	365 dagen
LogbookRewriteOffset	Aantal dagen waarna de persoonsgebonden logboekmeldingen uit logboeken worden gewist.	0 (niet wissen)
LogbookDelMessages	De nummers van de persoonsgebonden logboekmeldingen die dienen te worden gewist. Er kunnen individuele nummers en nummerbereiken worden opgegeven.	Alle controlemeldingen
LogbookLastRunTime	Datum waarop het wisproces als laatste met succes werd uitgevoerd.	Datum van de laatste uitvoering

Gegevens minimaliseren

De gebruiker bepaalt welke gegevens noodzakelijk zijn voor het bedrijf en de taken. Voor het dagelijkse gebruik van AccessOne zijn per persoon alleen de achternaam en een personeels-ID (eigen/extern/bezoeker) noodzakelijk. De achternaam hoeft niet de daadwerkelijke naam van de kaarthouder te zijn. Er kan ook een pseudoniem (bijvoorbeeld "MA_001") worden gebruikt. Over het algemeen dient het gebruik van de naam met betrekking tot de AVG als niet-kritisch te worden beoordeeld.

Invoercontrole

AccessOne legt iedere gegevenswijziging in een logboek vast met werkstation, gebruiker en tijdstempel alsmede de oude en nieuwe waarde van het betreffende gegevensveld.

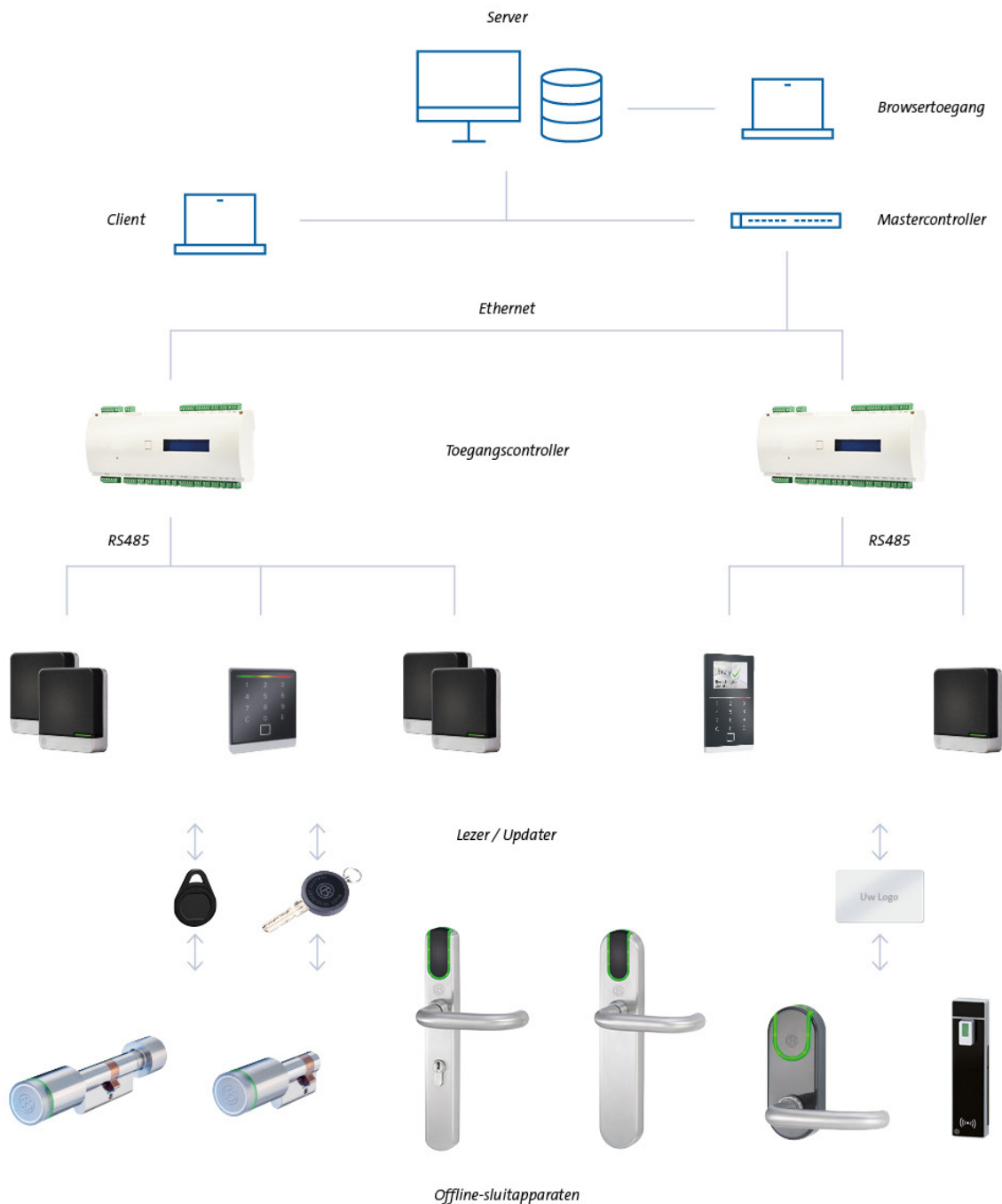
Toegangscontrole – Openingscontrole – Controle op toegang tot apparatuur

Als toegang geldt volgens DIN EN 50133-1 het proces van het betreden of verlaten van een beveiligd gebied. AccessOne verzorgt de besturing en de regeling. Opening omschrijft het logische gebruik van gegevens op computers in de betekenis van lezen, schrijven, wijzigen en wissen. Toegang tot apparatuur is het logistische begin van het gebruik van een informatiesysteem of communicatienetwerk. Dienovereenkomstig is de controle op toegang tot apparatuur de machinale controle van de toegangsbevoegdheid tot een informatiesysteem of netwerk.

Voor de bewaking en controle dient de opdrachtgever te voldoen aan overeenkomstige technisch-organisatorische maatregelen door het configureren of beschikbaar houden van de IT-infrastructuur (USB-poort, wachtwoordrichtlijnen, LDAP enz.). AccessOne ondersteunt dit door de mogelijkheid van overeenkomstige toewijzingen van gebruikersrechten in de gebruikersinterface.

4 Over AccessOne

Het toegangscontrolesysteem AccessOne is in de volledige versie flexibel schaalbare toegangscontrolemanagementsoftware voor grote systemen met maximaal 200.000 gebruikers, 16.000 ID-kaartlezers en maximaal 100.000 offline sluitapparaten. Een versie voor het mkb is met de licentie AccessOne KMU beschikbaar. Het toegangscontrolesysteem bestuurt deuren, kasten en andere sluitinrichtingen. De kern van de software is een gebruikers- en bevoegdhedenbeheer dat alle activiteiten op de aangesloten apparaten in een logboek vastlegt en lopende processen bewaakt. AccessOne is ontwikkeld als open systeem en kan zowel online- als offline-apparaten beheren en besturen. De communicatie is met 128 bit AES, end-to-end gecodeerd. Optionele USV- en serverredundantieconcepten staan in voor een hoge uitval- en systeemveiligheid.



4.1 Functie-uitbreidingen

Voor AccessOne in de basislicentie zijn de volgende functie-uitbreidingen verkrijgbaar:

ID-kaart creatie Art.nr. 348120V	Uitbreiding van de AccessOne met de mogelijkheid om een eigen kaart-lay-out met een grafische editor vorm te geven.
Multi-user-functie Art.nr. 348121V	De multi-user-functie maakt de logische toekenning mogelijk van gedefinieerde delen van het systeem, zoals deuren en personen, aan verschillende, onafhankelijke multi-users. Deze multi-users kunnen de aan hen toegekende systeemdelen zelfstandig beheren, maar hebben geen invloed op de systeemdelen van een andere multi-user. De mogelijkheid bestaat echter dat systeemdelen, zoals toegangsdeuren, gemeenschappelijk worden gebruikt.
Bezoekersbeheer Art.nr. 348122V	Breidt de AccessOne uit met de mogelijkheid om bezoekers in het systeem aan te melden en het uitgeven van dag-ID-kaarten met beperkte toegangsmogelijkheden. Aanmelding gebeurt via een webbrowser.
Parkeerbeheer Art.nr. 348123V	Breidt de AccessOne uit met de mogelijkheid om parkeerplaatsen te beheren. Aan bepaalde huurders kan een aantal "n" huurplaatsen worden toegewezen, terwijl de overige parkeerplaatsen worden geteld, maar voor andere, geautoriseerde gebruikers ter beschikking staan. Voor het gebruik van deze functie is een telling via een in- en uitgangsleder absoluut noodzakelijk.
Tijdregistratie Art.nr. 348124V	Breidt de AccessOne uit met de mogelijkheid via toegangslezers en/of separate tijdregistratielezers aankomst- en vertrekboekingen te genereren en deze dagelijks in CSV-formaat aan een bovengeschild werktijdmanagementsysteem beschikbaar te stellen.
Serverredundantie Art.nr. 348125V	Breidt de AccessOne uit met een hot-stand-by-functie.
Beheer externe firma Art.nr. 348126V	Breidt de AccessOne uit met een module voor het beheer van stamgegevens van medewerkers van externe bedrijven, zonder de stamgegevens van het eigen personeel te benaderen. De module maakt de vrijgave van monteurs mogelijk, die in gebouwen werkzaamheden moeten verrichten en daarvoor materialen en/of een ID-kaart nodig hebben. Speciale vergunningen of noodzakelijke instructies kunnen met geldigheid worden opgenomen en gecontroleerd. De medewerker van de externe firma bevestigt de ontvangst van materialen en het ter kennis nemen van overhandigde documenten met een handtekening op een elektronische pad.

4.2 Aanbevolen procedure voor de eerste configuratie van AccessOne

Om voor u als gebruiker het invoeren van veel gegevens voor de eerste configuratie van het toegangscontrole-systeem AccessOne te vergemakkelijken, adviseren wij om de afzonderlijke stappen in een bepaalde volgorde uit te voeren. Daarbij maken wij een onderscheid tussen de systeemconfiguratie van AccessOne door de systeemexploitant en/of een gemachtigde vakman van IT/systeembeheer en het aanmaken van apparaten, toegangsrechten en persoonsgegevens door voor het product opgeleid personeel.

De eerste stappen wordt uitgevoerd door de systeemexploitant en/of een gemachtigde vakman van IT/systeembeheer:

Stap	Nr.	Activiteit
Configuratie van AccessOne		Start de toepassing en meld u aan als gebruiker (zie „5 Aanmelding“ op pagina 16).
		Voordat u begint met de configuratie van uw AccessOne-systeem, moet u uw licentie activeren in de systeeminstellingen (zie „6.1 Systeemconfiguratie“ op pagina 17).
		Maak na de systeemconfiguratie de verschillende gebruikers aan, zodat aansluitend iedere AccessOne-gebruiker met zijn individuele toewijzingsrechten het systeem kan configureren (zie „6.2 Gebruikersgegevens“ op pagina 27).
		Definieer de locatiegegevens van uw AccessOne-systeem. Dan kunnen bij de configuratie van de apparaten de locatiegegevens direct worden toegewezen (zie „6.3 Locatiegegevens“ op pagina 32).

De volgende stappen kunnen worden uitgevoerd door voor het product opgeleid personeel:

Stap	Nr.	Activiteit
Apparaten aanmaken	1	Maak eerst uw online-apparaten aan, zoals deurbesturingen en lezers. Iedere lezer kan ook als updater voor toegangsmedia worden gebruikt. Dat is de voorwaarde voor de configuratie van de offline-apparaten (zie „7.1 Apparaatgegevens online-apparaten“ op pagina 34).
	2	Nadat de online-apparaten zijn geconfigureerd, maakt u de offline-apparaten aan. Deze stap is de voorwaarde dat u in het verdere verloop de toegangsrechten met alle aangemaakte apparaten kunt definiëren (zie „7.2 Apparaatgegevens offline-apparaten (OSS-SO)“ op pagina 55).
Toegangsrechtgroepen en -profielen aanmaken	3	Configureer eerst de toegangsrechtgroepen voor de online- en offline-apparaten (zie „8.1 Toegangsrechten“ op pagina 61).
	4	De toegangsrechtgroepen worden samengevoegd in toegangsrechtprofielen. Daarmee zijn alle noodzakelijke stappen voor uw toegangsrechtconcept uitgevoerd (zie „8.2 Toegangsrechtprofielen“ op pagina 69).
Persoonsgegevens aanmaken	5	Nu kunt u de reeds geconfigureerde toegangsrechten van de online-/offline-apparaten direct toewijzen aan personen (zie „9.1 Persoonsgegevens“ op pagina 71).
	6	Gebruik de kaartontwerper voor het afdrukken van ID-kaarten. De kaart-lay-outs worden dan aan de persoon toegewezen (Uitbreiding van de AccessOne met de mogelijkheid om een eigen kaart-lay-out met een grafische editor vorm te geven).
	7	U kunt bovendien een bedrijf aan de persoon toewijzen (Breidt de AccessOne uit met een module voor het beheer van stamgegevens van medewerkers van externe bedrijven, zonder de stamgegevens van het eigen personeel te benaderen).
Latere aanpassingen	>	Alle aangemaakte gegevens kunnen bij noodzakelijke veranderingen ook achteraf eenvoudig worden aangepast (zie „9.2 Verandering in groepen“ op pagina 84).

5 Algemeen gebruik van dialoogvensters

Doelgroep van dit hoofdstuk:

- Voor het product opgeleid personeel
- Vakmensen IT/systeembeheer
- Systeemexploitanten

AccessOne wordt bediend via een dialoogvensterinterface met een gebruikelijk bedieningsconcept. Alle dialoogvensters zijn volgens hetzelfde schema opgebouwd. Een nieuwe gebruiker kan zich daarom snel oriënteren in het systeem.

De gebruikersinterface is hetzelfde opgebouwd als bij de bekende Microsoft Office-producten. Linksonder vindt u de knoppen voor het oproepen van de dialoogvensters (1). Daarboven bevindt zich, afhankelijk van het betreffende opgeroepen dialoogvenster, een lijst van beschikbare dataobjecten in de objectselectie (2). Als een vermelding uit de dialoogselectie (1) wordt gekozen, worden in het dialoogvenster (4) de details hiervan op een tabblad in een of meerdere gebieden (5) weergegeven. De gegevens van een dataobject (bijvoorbeeld personen of apparaten) worden, afhankelijk van de omvang, op meerdere tabbladen samengevoegd. Knoppen in de taakbalk (3) bieden fundamentele functies voor het telkens actuele tabblad.

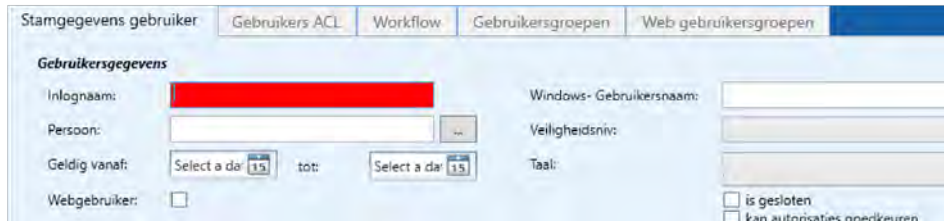


Voor elk dialoogvenster kan worden vastgelegd of een gebruiker toegang heeft en met welk toegangsrecht (Lezen – Schrijven – Wissen). Als een gebruiker voor een dialoogvenster geen toegangsrecht heeft, dan is de betreffende knop niet zichtbaar in de interface. Hetzelfde geldt ook voor de tabbladpagina's in het dialoogvenster.





Lege verplichte velden worden bij het opslaan rood gearcheveerd. Tooltips bieden aanvullende gegevens over het bijbehorende element, wanneer de cursor erover wordt bewogen.



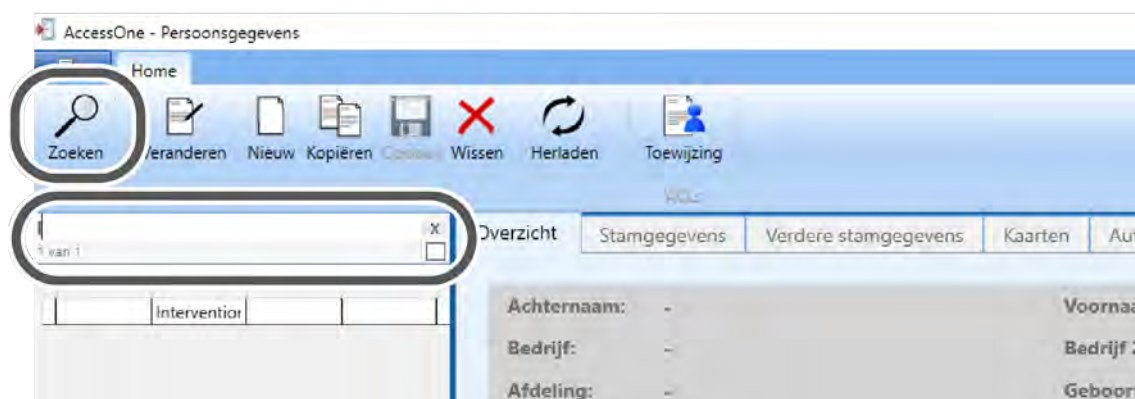
5.1 Kijkmodus – wijzigingsmodus

AccessOne maakt een onderscheid tussen de kijkmodus en de wijzigingsmodus. In de kijkmodus kunnen gegevens alleen worden bekeken, maar niet worden gewijzigd. De gegevens zijn grijs gemaakt. In de wijzigingsmodus worden de knoppen en invoervelden in het dialoogvenster geactiveerd. In de wijzigingsmodus wordt de geselecteerde gegevensrecord intern voor alle andere dialooggebruikers geblokkeerd.

5.2 Taakbalk

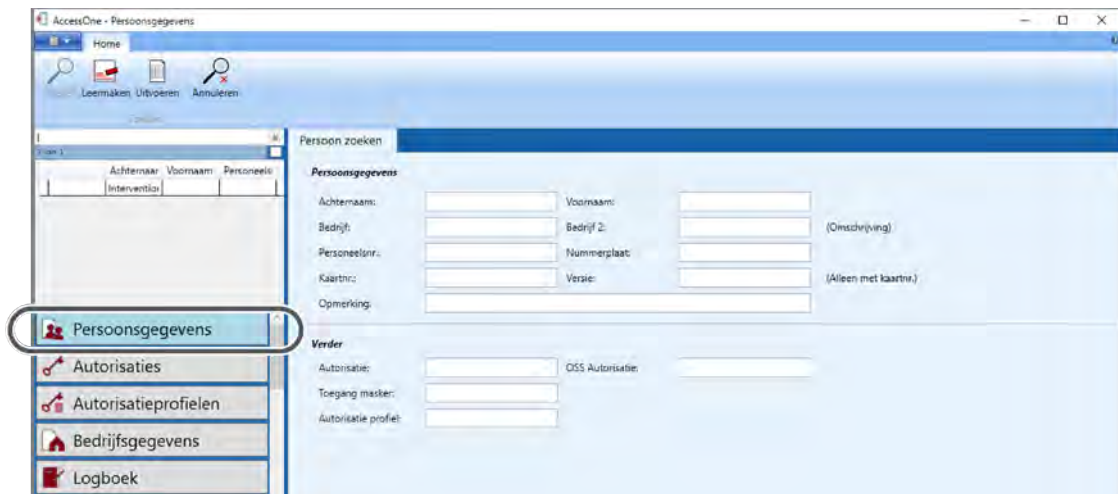
Zoeken

Via de objectselectie aan de linkerzijde bevindt zich in de taakbalk het invoerveld voor het zoeken.



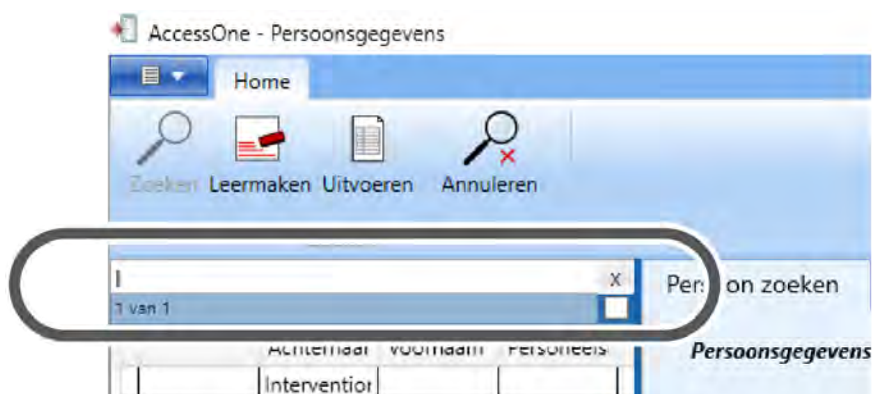

De knop ZOEKEN in de menubalk is alleen actief wanneer het dialoogvenster "Persoonsgegevens" wordt gekozen.

Door te klikken op de knop ZOEKEN, opent u in het dialoogvenster het tabblad "Persoon zoeken". Hier zijn andere zoekcriteria beschikbaar (bijvoorbeeld naam, voornaam, bedrijf, personeelsnummer, toegangsrecht, toegangsrechtprofiel, ID-nummer). De selectielijst in het invoerveld wordt met elk ingevoerd teken geactualiseerd.



Voor het tabblad "Persoon zoeken" zijn alleen de knoppen LEEGMAKEN, UITVOEREN en AFBREKEN van de zoekopdracht beschikbaar.

Door te klikken op UITVOEREN, wordt de gefilterde selectielijst geactualiseerd. Gegevensrecords kunnen individueel worden opgeroepen en bewerkt. De zoektermen blijven actief, totdat er op AFBREKEN wordt geklikt. Als u bijvoorbeeld in de zoekdialoogvenster een bedrijf hebt gekozen, worden in de selectielijst alleen personen van dit bedrijf weergegeven, onafhankelijk of u via de selectielijst extra gegevens invoert in het zoekveld. Pas door het zoekdialoogvenster opnieuw op te roepen en vervolgens de zoekopdracht af te breken, wordt dit zoekcriterium weer gewist. LEEGMAKEN wist de inhoud van het zoekdialoogvenster. Daarna kunt u nieuwe zoekcriteria invoeren.



In het voorbeeld zijn er precies 2 gegevensrecords die beide met een "T" beginnen. Als u bijvoorbeeld geen zoekcriterium opgeeft, dan is de weergave beperkt tot maximaal 150 vermeldingen. Deze waarde kan worden ingesteld via de systeemp parameters van AccessOne. Via het knopje in de hoek rechtsonder in het zoekvenster kunt u de beperking tijdelijk uitschakelen. Dan worden alle gegevensrecords die bij het zoekcriterium passen, in de selectielijst geladen. Wanneer u geen zoekterm invoert, worden alle gegevensrecords geladen die in de databank aanwezig zijn.

Wijzigen

Door te klikken op WIJZIGEN of te dubbelklikken op de gegevensrecord in de selectielijst, activeert u de invoervelden en knoppen in het dialoogvenster aan de rechterzijde. De geselecteerde gegevensrecord wordt intern geblokkeerd voor alle andere dialooggebruikers.

Nieuw

Maakt een nieuwe, lege gegevensrecord aan.

Kopiëren

Dupliceert een bestaande gegevensrecord. Velden die per gegevensrecord eenduidig moeten zijn, worden automatisch leeggemaakt.

Opslaan

Slaat de gegevensrecord in de databank op en actualiseert deze. Vervolgens is de gegevensrecord weer vrijgegeven voor wijzigingen door andere dialooggebruikers.



Het actuele dialoogvenster wordt automatisch opgeslagen zodra u de dialoogpagina verlaat.

Wissen

Wist de opgeroepen gegevensrecord (met blauwe achtergrond). Na het bevestigen van een veiligheidsvraag wordt de bewerking uitgevoerd.

Actualiseren

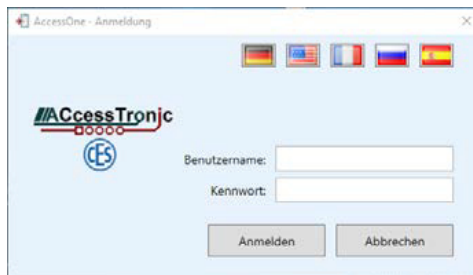
Laadt actuele gegevens uit de databank en actualiseert de weergave.

Toewijzing

Wijst de actuele gegevensrecord toe aan een cliënt. Is alleen actief wanneer de mogelijkheid voor cliënten is geactiveerd.

6 Aanmelding

Nadat het installeren van de software is gelukt, meldt u zich aan als gebruiker. Start het programma op door te dubbelklikken op het pictogram dat de installatie automatisch op uw pc aanmaakt.

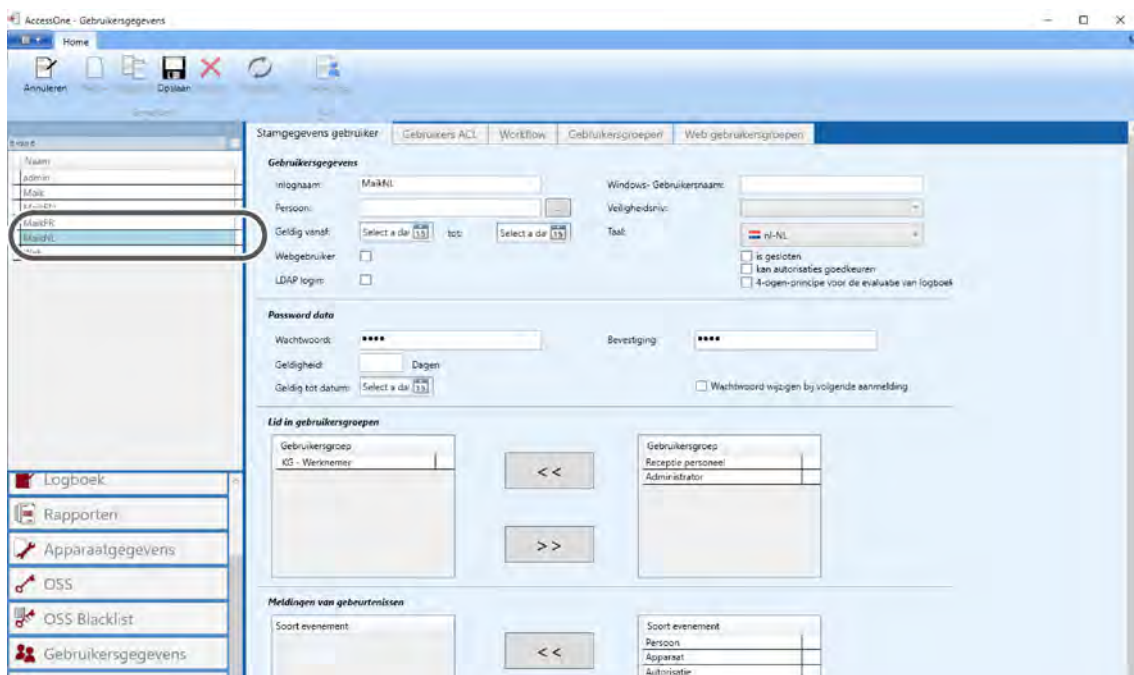


Voor de eerste aanmelding na de installatie zijn de volgende inloggegevens vooraf ingesteld:

Gebruikersnaam: admin

Wachtwoord: admin

Wijzig het wachtwoord om veiligheidsredenen direct na het invoeren. Ga daarvoor naar het dialoogvenster "Gebruikersgegevens".



Kies in de objectselectie de inlognaam "admin" en klik daarna in de taakbalk linksboven in het venster op de knop WIJZIGEN. Geef een eigen wachtwoord op. Een heel veilig wachtwoord is een zo lang mogelijk wachtwoord dat uit letters en cijfers bestaat. De lengte van het wachtwoord kunt u zelf kiezen. Herhaal het wachtwoord opnieuw in het veld "Bevestiging" om het in te stellen.

Als u een wachtwoord met beperkte geldigheid wilt instellen, dan kunt u dat doen op deze plaats. Bevestig de wijziging met de knop OPSLAAN.

Het aanmaken van andere gebruikers wordt verderop in het handboek uitvoerig beschreven (zie „6.2 Gebruikersgegevens“ op pagina 27).

7 Configuratie van AccessOne

Doelgroep van dit hoofdstuk:

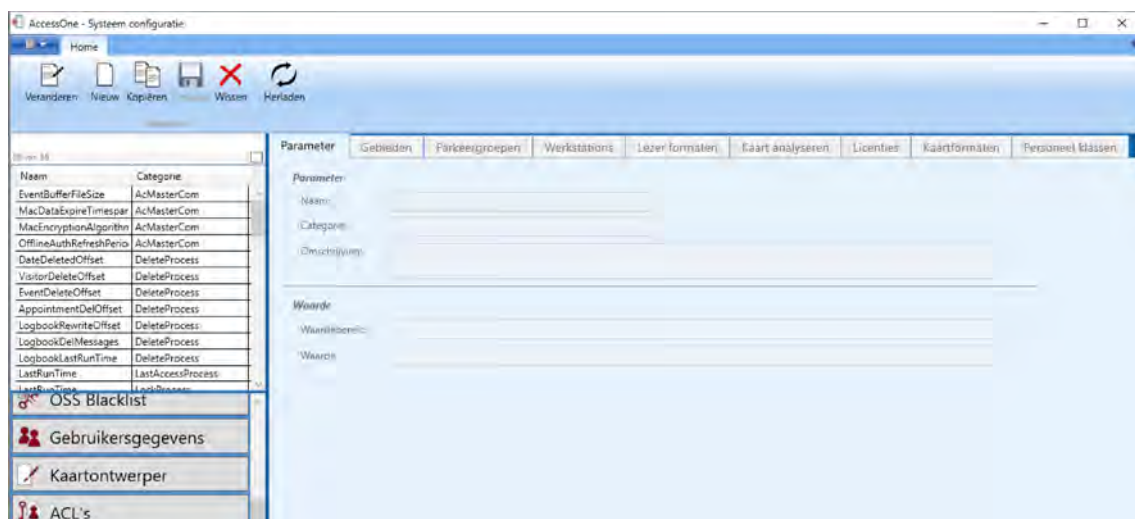
- Vakmensen IT/systeembeheer
- Systeemexploitanten

Om de voorwaarden te scheppen voor het configureren van het toegangscontrolesysteem, moet u enkele systeemparameters aanpassen. Leg de gebieden vast en configureer de werkstations. Definieer bovendien de gebruikte lezer- en kaartformaten. Met de invoer van de gebruikers- en locatiegegevens scheidt u de voorwaarden voor de configuratie van de apparaten en de toegangsrechten.

7.1 Systeemconfiguratie

7.1.1 Parameter

Geeft de systeemparameters voor uw systeem aan.

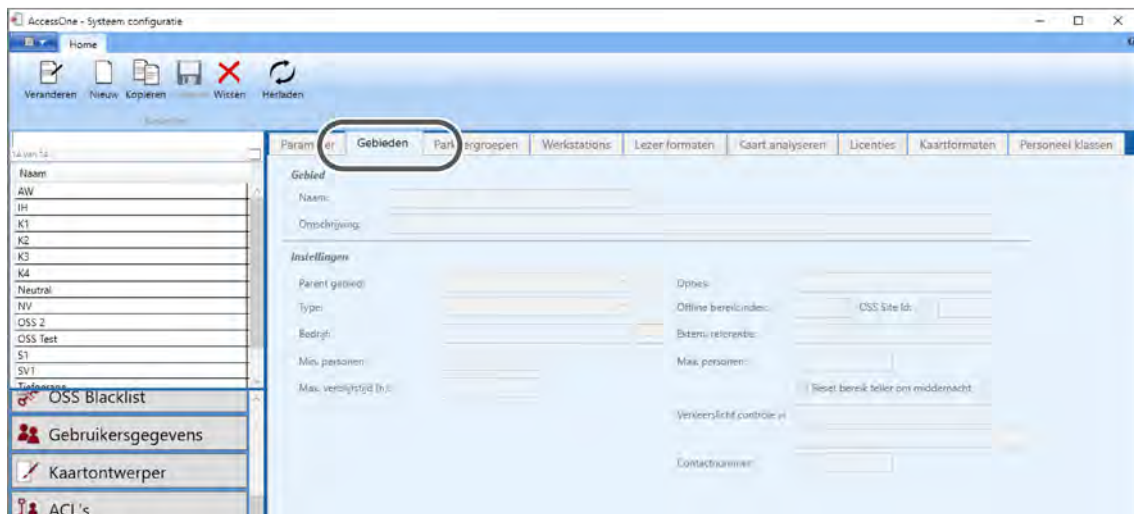


Uitleg over de parameters

Naam	Vertaling	Toelichting
EventBufferFileSize	Grootte bestandsbuffer	Grootte bestandsbuffer (Mb) om gebeurtenissen voor een individuele MAC op te slaan.
MacDataExpireTimespan	Tijd waarna de gegevens verstrijken	Tijd in minuten zonder verbinding met de MAC, waarna de gegevens in de gebeurtenisbuffer ongeldig worden.
MacEncryptionAlgorithm	Versleutelingsalgoritme	Versleutelingsalgoritme voor de communicatie tussen AccessOne en MAC's (voorinstelling: geen).
DateDeletedOffset	Gegevensrecords wissen	Tijd in dagen waarna personeegegevensrecords na het wissen uit het dialoogvenster definitief uit de databank worden gewist.
EventDeleteOffset	Gebeurtenissen wissen	Aantal dagen waarna de gebeurtenissen uit de databank worden gewist.
VisitorDeleteOffset	Bezoeker wissen	Aantal dagen waarna de gewiste bezoekers uit de databank worden gewist.

Naam	Vertaling	Toelichting
LastRunTime (LastAccessProcess)	Laatste keer dat het proces werd uitgevoerd	Tijdstip van de laatste procesuitvoering
LastRunTime (LockProcess)	Laatste keer dat het proces werd uitgevoerd	Tijdstip van de laatste procesuitvoering
CardNoRecycling	Kaartnummers opnieuw gebruiken	1= hergebruik van kaartnummers doordat naar hiaten in gewiste kaarten wordt gezocht. 0 = kaartnummers doorlopend verstrekken.
DatabaseNumber	Databanknummer	ID in de gegevensrecord wanneer er verschillende databanken aanwezig zijn (tot dusver 00)
LockingTimeout	Blokkeringstijd gegevensrecord	Tijd in seconden voor de blokkering van gegevensrecords die in bewerking zijn. Indien binnen deze tijd de blokkering door de client niet wordt vernieuwd, wordt de blokkering opgeheven door het masterproces.
LogonTimeout	Tijdsbestek waarna opnieuw moet worden aangemeld	Tijd in seconden waarbinnen een client zijn inlog bij de master moet vernieuwen, voordat deze automatisch wordt aangemeld.
NumberLogonFailures	Aantal foutieve aanmeldingen	Max. aantal pogingen met foutieve aanmelding
ProcessLogfileAge	Leeftijd van de debug-logbestanden	Max. leeftijd in dagen van de debug-logbestanden
ProcessLogfileSize	Grootte van de debug-logbestanden	Max. grootte in MB van de debug-logbestanden
XmlDoorDataDir	Directory van deurgegevens	Directory voor de OSS-uitwisseling van deurgegevens
CardNoZeroes	Kaartnummers	Aanvullen van gedrukte kaartnummers met nullen tot aan de aangegeven totale lengte.
CardToCodeAlgorithm	Codealgoritme	Algoritme voor het bepalen van kaartnummers uit de codegegevens. Standaard: 0 = kaartnummer voldoet aan de codegegevens.
DialogTimeout	Tijdsoverschrijding van dialoogvenster	Standaard time-out in seconden, omdat een dialoogvenster niet werd gebruikt. Als deze tijd wordt overschreden, wordt de gebruiker automatisch afgemeld.
EntitiesToTake	Entiteiten	Aantal gegevensrecords dat in de selectielijst wordt weergegeven.
MaxPinLength	Maximale lengte pincode	Max. lengte van de pincode (PIN, EMA1, EMA2)
MaxPinValidity	Maximale geldigheid van de pincode	Max. geldigheid van de pincode in dagen
OfflineValidityTime	Offline-geldigheidsduur	Standaard geldigheid van een offline-ID-kaart in uren, minuten (standaard: 24,0).

7.1.2 Gebieden



Elke deur in AccessOne leidt van een brongebied naar een doelgebied. Deze gebieden hoeven niet per se verschillend te zijn. Wanneer uw gebouw is onderverdeeld in verschillende veiligheidszones, kunt u bijvoorbeeld een ingang vanaf de buitenste veiligheidszone (ASB) naar de inwendige veiligheidszone (ISB) leiden. Een tussendeur kan echter ook leiden van ISB naar ISB.

Met "Ingang locatie" en "Uitgang locatie" selecteert u het bron- en doelgebied.

Instellingen

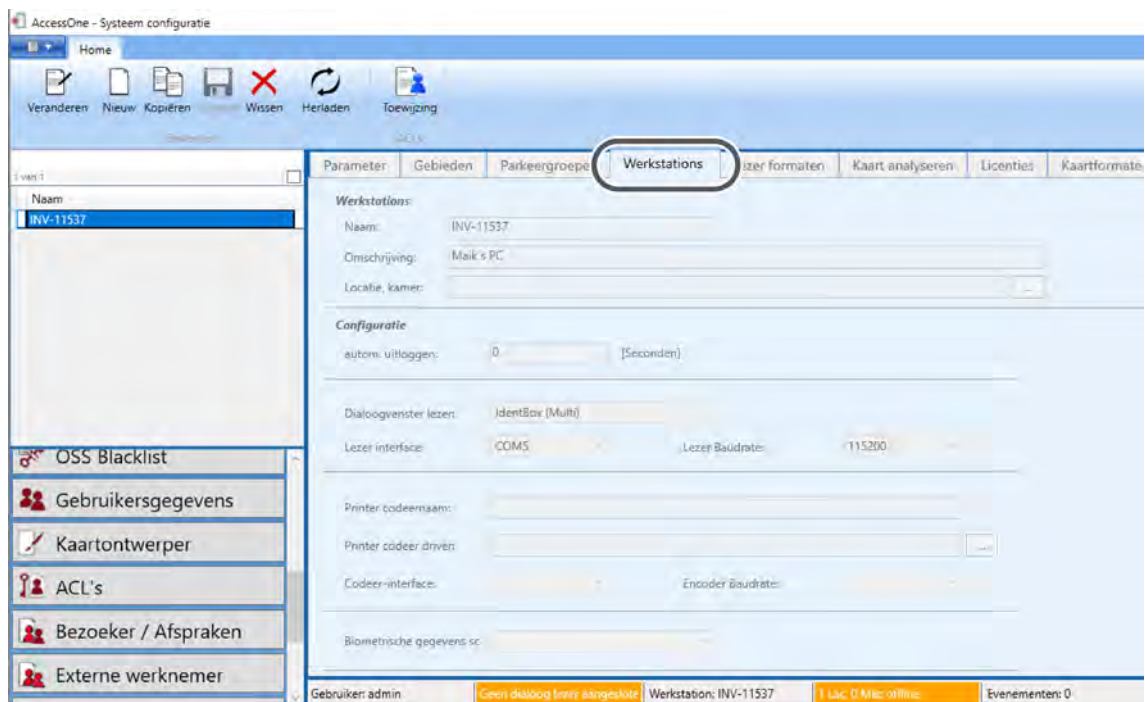
Onder "Instellingen" kan een gebied verder worden onderverdeeld. Bij "Normaal gebied" is de richtlijn van een minimaal en maximaal toegelaten aantal personen binnen het gebied mogelijk. Voor een "Parkeerplaats" kan bijvoorbeeld het maximale aantal beschikbare parkeerplaatsen worden opgegeven.

7.1.3 Parkeergroepen

(Alleen actief bij het gebruik van de aanvullende module Parkeerbeheer, art.nr. 348123V)

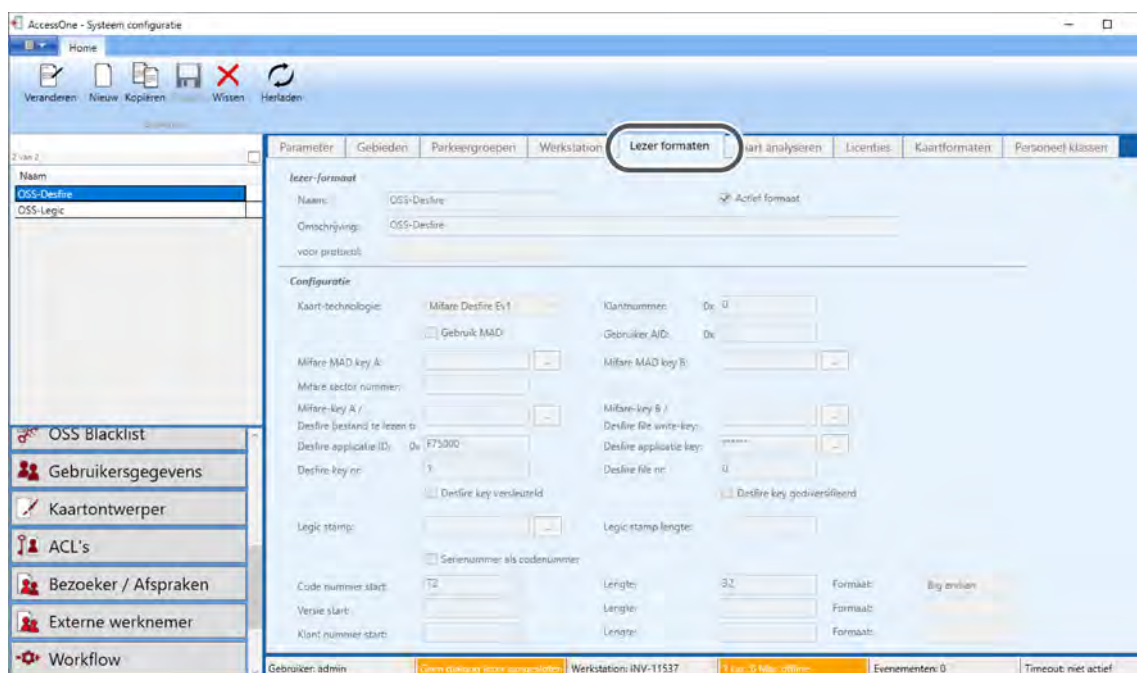
Biedt de mogelijkheid om personen voor een parkeergroep samen te voegen. Deze kunnen dan worden toegewezen aan een bepaalde parkeerplaats.

7.1.4 Werkstations



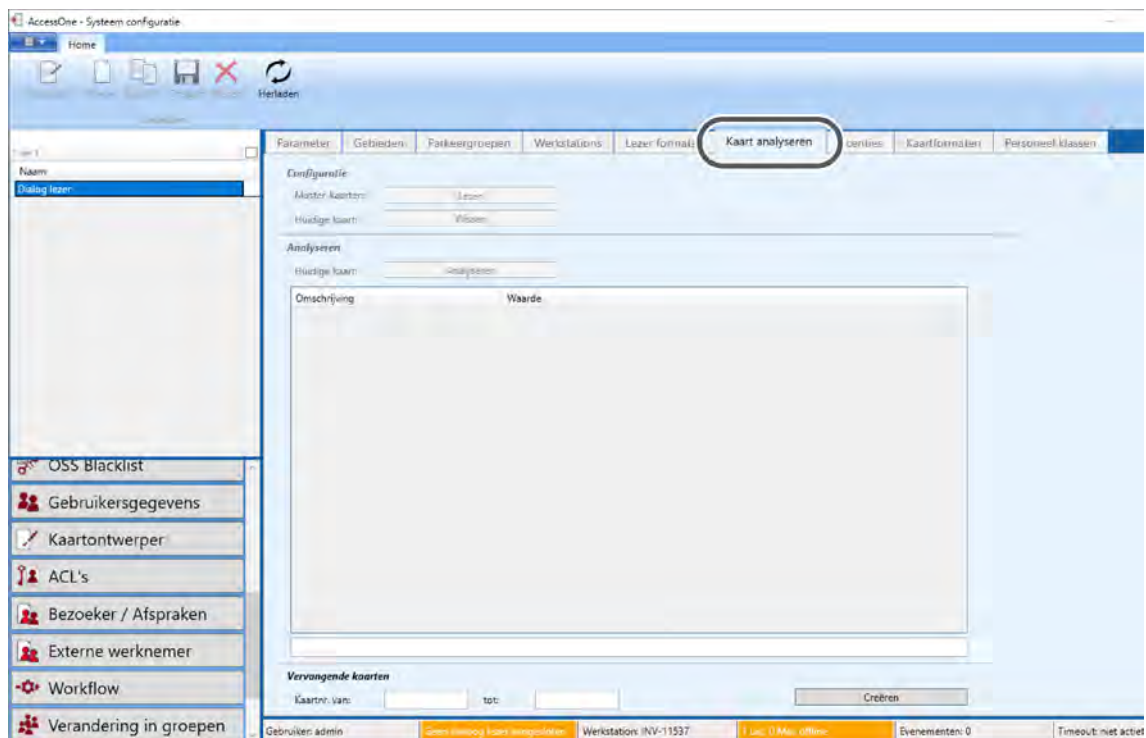
In het tabblad "Werkstations" worden de betreffende AccessOne-clients met hun exacte Windows-computernamen aangemaakt. Hier wordt voor het betreffende werkstation lokaal vastgelegd of een dialooglezer (bijvoorbeeld een Identbox) of een kaartprinter samen met het codeerstation is geïnstalleerd. Voor het eindapparaat moeten telkens de juiste ComPorts worden ingesteld. De ComPorts kunt u in uw Windows-apparaatmanager aflezen.

7.1.5 Lezerformaten



Hier stelt u de lezerformaten in die door de kaartlezer van de deurcontroller dienen te worden gelezen.

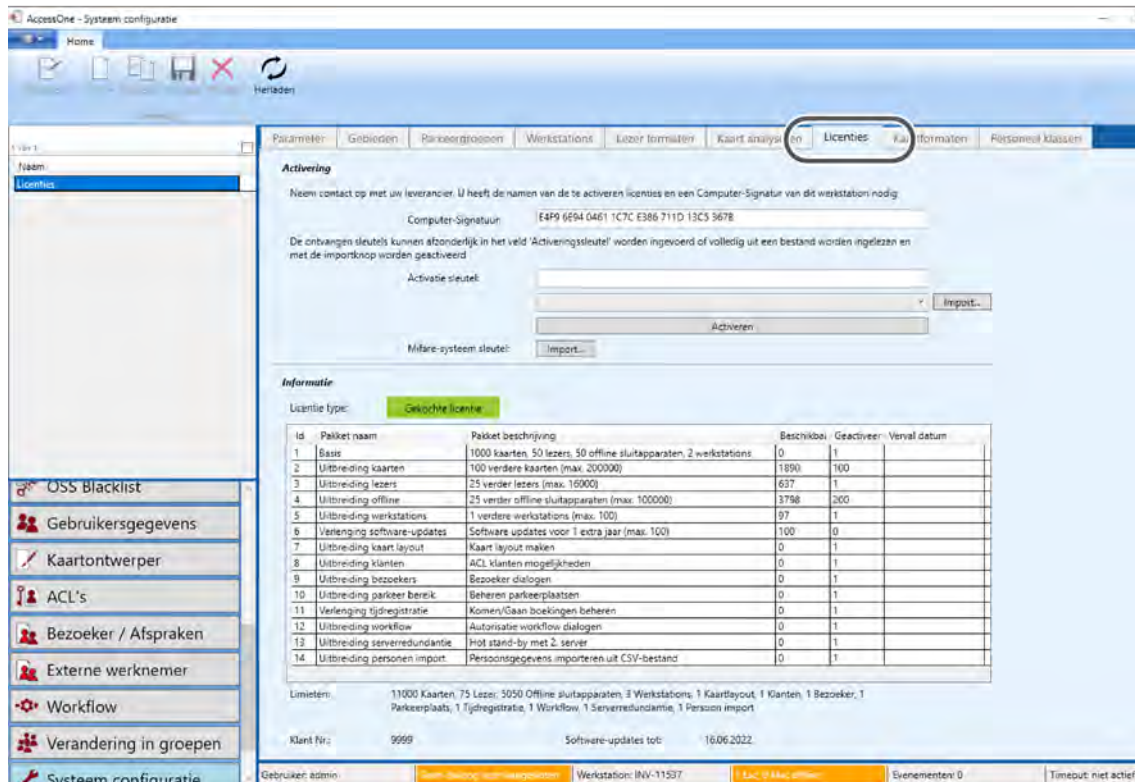
7.1.6 Kaart analyseren



In het tabblad "Kaart analyseren" kunnen master-kaarten (bijvoorbeeld LEGIC-, IAM-kaarten) die voor het gebruik van de schrijffunctie van uw dialooglezer (Identbox) belangrijk zijn, worden ingelezen of gewist. Via de knop Analyseren worden via de aangesloten dialooglezer transponderkaarten van een eerder aangemaakt kaartformaat in detail uitgelezen.

In het gebied "Vervangende kaarten" kan een gedefinieerde hoeveelheid vervangende kaarten in het betreffende kaartnummerbereik worden aangemaakt in de databank.

7.1.7 Licenties



Het tabblad "Licenties" geeft een opsomming van de betreffende programmalicenties en hun inhoud.



Voor de vrijgave van de licentie is de computer-signatuur van uw AccessOne server-pc nodig. Zonder vrijgave van de licentie kan uw AccessOne-installatie alleen als demolicentie met beperkingen worden gebruikt.

Er zijn drie licentietypes:

- Een testlicentie met een minimale systeemomvang die direct na de installatie van de AccessOne-software actief is.
- Een demolicentie die een tijdelijke geldigheid heeft en volgens de wensen van de klant wordt gemaakt. Dit licentietype kan twee keer worden verlengd. Na het verstrijken van deze periode wordt de demolicentie automatisch omgezet in een "Testlicentie".
- De gekochte licentie biedt alle standaardfuncties.

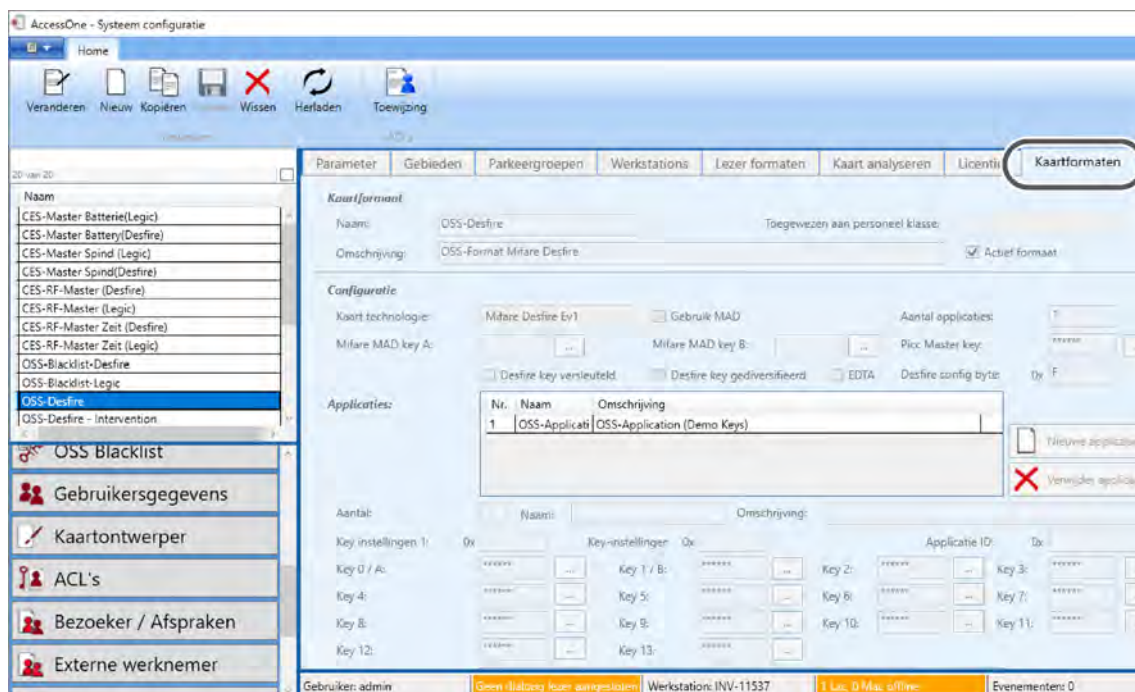
7.1.8 Kaartformaten

In het tabblad "Kaartformaten" worden de formaten gedefinieerd die voor het beschrijven van een kaart aan een dialooglezer, codeerstation (eventueel in de kaartprinter) of een ZK-wandlezer (updater voor toegangsmedia) nodig zijn.

Er mag per kaarttechnologie (Mifare, LEGIC enz.) slechts één kaartformaat actief zijn. Er kunnen echter zeker verschillende inactieve kaartformaten van dezelfde kaarttechnologie zijn aangemaakt.



De definitie van een kaartformaat stelt echter als voorwaarde dat de AccessOne-gebruiker de mogelijke instellingen van de betreffende kaarttechnologie kent. Aangezien met name Mifare-DESFire de gebruiker zeer veel vrijheden geeft bij het definiëren van toegangsrechten, kunnen daardoor ook kaarten worden gegenereerd die niet meer bruikbaar zijn wanneer de instellingen tegenstrijdig zijn. De volgende tekst geeft aanwijzingen over welke parameters op welke eigenschappen van de kaart invloed hebben. Desondanks moet de betreffende NXP- en LEGIC-documentatie toch nog worden gelezen.



De parameters worden op verschillende structuurniveaus aangemaakt:

- Parameters op kaartniveau
- Parameters op applicatieniveau
- Parameters op bestandsniveau

7.1.8.1 Parameters op kaartniveau

Bij het aanmaken van een nieuwe kaart wordt eerst de PICC-masterkey vanaf de standaardwaarde naar de hier gedefinieerde waarde uitgevoerd. Daarna worden de eigenschappen ingesteld, die betrekking hebben op het gebruik van deze PICC-masterkey. De instellingen worden in de waarde van "Desfire config byte" opgeslagen.

De waarde is bit-gecodeerd en dient als volgt te worden geïnterpreteerd:

Bit 4 tot 7 moeten 0 zijn.

Bit 3 bepaalt of deze configuratie ooit weer mag worden gewijzigd (ook niet door het formatteren van de kaart).

- 0: de configuratie mag nooit meer worden gewijzigd;

- 1: de configuratie mag worden gewijzigd, wanneer men zich eerder met de PICC-masterkey heeft geauthenticeerd.

Bit 2 bepaalt of het aanmaken of wissen van een applicatie van de PICC-masterkey is vereist of niet.

- 0: aanmaken en wissen van een app werkt alleen met de PICC-masterkey;
- 1: aanmaken gebeurt zonder, wissen van een app gebeurt met de PICC-masterkey of applicatie-masterkey.

Bit 1 bepaalt of voor het oproepen van de inhoudsopgave van de kaart de PICC-masterkey vereist is of niet.

- 0: oproepen werkt alleen met de PICC-masterkey;
- 1: voor het oproepen is geen PICC-masterkey nodig.



De PICC-masterkey mag niet worden doorgegeven. Wanneer u derden wilt toestaan om eigen applicaties aan te maken, is voor "Desfire config byte" bijvoorbeeld 0x0f een nuttige instelling. Met deze definitie hoeft u de PICC-masterkey niet door te geven.

7.1.8.2 Parameters op applicatieniveau

Volgens de DESFire-standaard is de sleutel 0 altijd de applicatie-masterkey (APMK). Alle andere sleutels kunnen, maar hoeven niet te worden gedefinieerd. Het is raadzaam om ten minste één extra sleutel te definiëren om eventuele derden toegang te verlenen zonder de APMK te hoeven doorgeven.

Sleutelinstellingen 1 bepaalt wat via de applicatie-masterkey wordt gecontroleerd. 0xE1 is bijvoorbeeld een nuttige waarde.

Instellingen van de toepassing van de APMK:

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Wijzigen van de sleuteltoegangsrechten				Configuratie kan worden gewijzigd	Vrij aanmaken/wissen zonder APMK	Vrije toegang tot directorylijsten zonder APMK	Wijziging van de APMK toegelaten
Bit3	Bit2	Bit1	Bit0				

Op toepassingsniveau wordt de codering geïnterpreteerd als (de geselecteerde AID is niet 0x00):

Bit 7 – bit 4 Bepaal de toegangsrechten voor het wijzigen van applicatiesleutels (commando Change-Key).

0x0: de authenticatie van de APMK is vereist om iedere gewenste sleutel te wijzigen (standaard).

0x1...0xD: de authenticatie met de opgegeven sleutel is vereist om iedere gewenste sleutel te wijzigen. Een wijzigingssleutel en een PICC-masterkey kunnen alleen worden gewijzigd na authenticatie met de APMK. Voor andere sleutels is een authenticatie met dezelfde sleutel nodig.

0xE: de authenticatie met de te wijzigen sleutel (hetzelfde KeyNo) is vereist om een sleutel te wijzigen.

0xF: alle sleutels (behalve APMK, zie bit 0) binnen deze toepassing zijn bevroren.

Bit 3 Geeft aan of een wijziging van de instellingen van de APMK is toegelaten:

0: configuratie kan niet meer worden gewijzigd (bevroren)

1: deze configuratie kan worden gewijzigd wanneer met de APMK wordt geauthenticeerd (standaardinstelling).

- Bit 2** Geeft aan of de authenticatie van de APMK voor CreateFile/DeleteFile is vereist.
 0: CreateFile/DeleteFile is alleen toegelaten met de authenticatie van de APMK.
 1: CreateFile/DeleteFile is ook toegelaten zonder de authenticatie van de APMK.
- Bit 1** Geeft aan of voor de toegang tot de bestandsdirectory de master-sleutel-authenticatie is vereist:
 0: voor de uitvoering van de commando's GetFileIDs, GetFileSettings en GetKeySettings is een succesvolle master-sleutel-authenticatie vereist.
 1: De commando's GetFileIDs, GetISOFileIDs, GetFileSettings en GetKeySettings zijn onafhankelijk van een eerdere master-sleutel-authenticatie (standaardinstelling) succesvol.
- Bit 0** Geeft aan of de APMK kan worden gewijzigd:
 0: de APMK kan niet meer worden gewijzigd (bevroren).
 1: de APMK kan worden gewijzigd (authenticatie met de actuele APMK is vereist (standaardinstelling)).

Via "Key-instellingen 2" wordt het aantal voor deze applicatie geldige sleutels en het type versleuteling voor de toegang tot deze applicatie gedefinieerd.

De parameter "Key-instellingen 2" definieert verschillende instellingen:

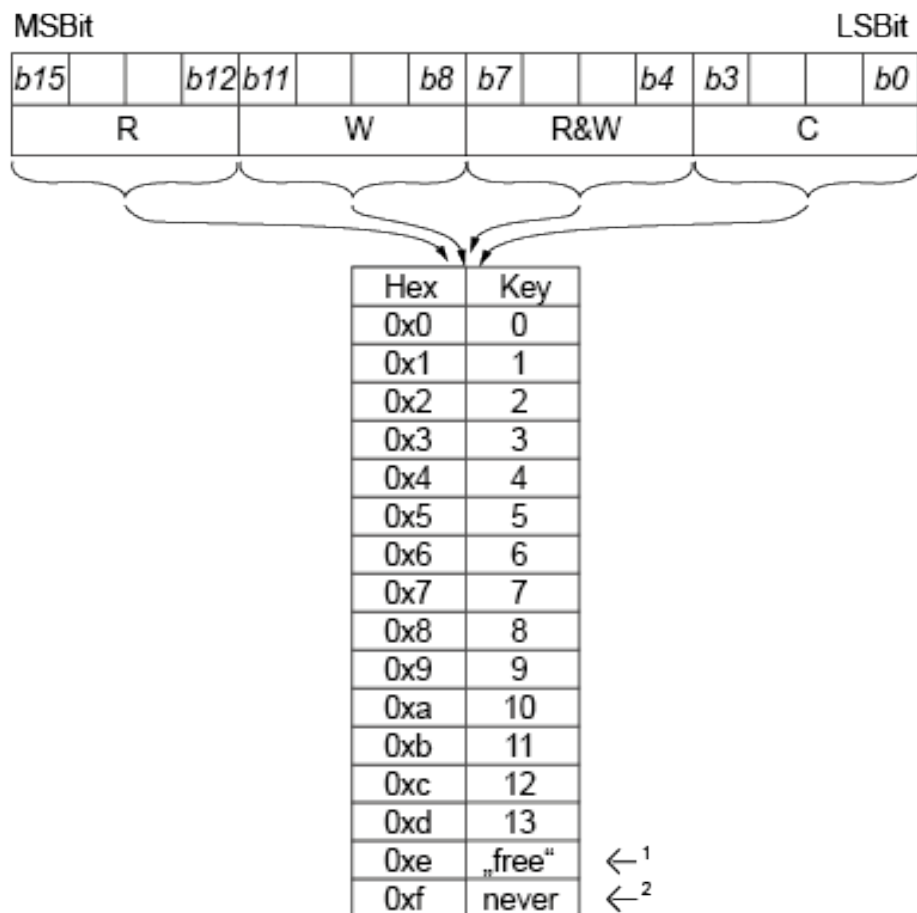
- Bit 0...3** Aantal sleutels dat binnen de toepassing voor cryptografische doeleinden kan worden opgeslagen. Er kunnen maximaal 14 sleutels binnen een toepassing van MIFARE DESFire EV1 worden opgeslagen. Er kan ook een toepassing worden aangemaakt zonder sleutel!
- Bit 4** RFU moet zijn ingesteld op 0.
- Bit 5** Geeft het gebruik van 2 byte ISO/IEC 7816-4-bestandsnummers voor bestanden binnen de toepassing weer:
 0: er worden geen 2 byte-bestandsnummers binnen de toepassing ondersteund.
 1: er worden 2 byte-bestandsnummers binnen de toepassing ondersteund.
- Bit 6...7** Geeft de crypto-methode van de toepassing weer:
 00: geeft DES- en 2K3DES-bewerkingen voor de volledige toepassing aan.
 01: geeft 3K3DES-bewerkingen voor de volledige toepassing aan.
 10: geeft AES-bewerkingen voor de volledige toepassing weer.
 Een geldige waarde is bijvoorbeeld 0x82, wanneer twee sleutels voor de applicatie zijn ingevoerd. ISO/IEC 7816-4 wordt niet ondersteund. Bit 4 en 5 moeten daarom 0 zijn. In het algemeen wordt AES gebruikt voor de versleuteling.

7.1.8.3 Parameters op bestandsniveau

Voor de Comm- en File-instellingen zijn er overeenkomstig voorbereide, handige selectievakjes. Bij de Access Rights moet voor het bestand telkens worden ingesteld welke applicatiesleutel lees- of schrijftoegang heeft en welke sleutel eventueel precies deze (toegangsrecht-) instelling mag wijzigen (zie tabel).

Wanneer de wens bijvoorbeeld is dat met sleutel 1 kan worden gelezen en geschreven, maar alleen met sleutel 0 (APMK) deze instellingen kunnen worden gewijzigd, dan zou de waarde voor de rechten er zo uitzien: 0x1110.

Wanneer u een waarde op 0xe instelt, heeft dat als gevolg dat de communicatie van "Gecodeerde" naar "Platte tekst" wisselt. Dat kan op zijn beurt eventueel botsen met de instellingen van de applicatie.



¹ geen verificatie mogelijk

² geen toegang

7.2 Gebruikersgegevens

In een eerste stap maakt u naar wens verschillende gebruikersgroepen met individuele dialoogrechten aan. De aangemaakte gebruikersgroepen worden daarna op het tabblad "Stamgegevens gebruiker" aan afzonderlijke gebruikers toegewezen.

7.2.1 Gebruikersgroepen

Op het tabblad "Gebruikersgroepen" worden dialoogrechten in groepen aangemaakt en samengevoegd. De dialoogrechten in de kolommen Lezen – Wijzigen – Opslaan – ACL (optioneel) kunnen eenvoudig met een muisklik worden geactiveerd/gedeactiveerd.

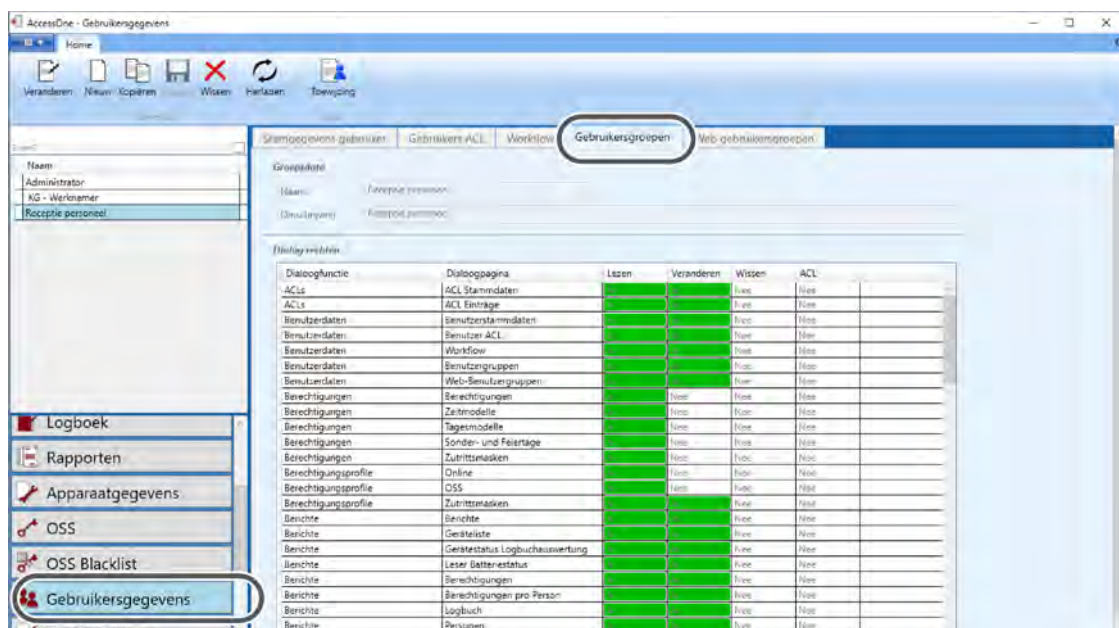


Om het werk te vergemakkelijken, kunt u meerdere cellen tegelijkertijd met een ingedrukte muisknop selecteren en erop klikken. De betreffende vermeldingen in de afzonderlijke cellen worden dan omgeschakeld (Ja>Nee en Nee>Ja).

Geef de groep een duidelijke naam en beschrijving.

Door te klikken op de knop WIJZIGEN wordt de betreffende functie geselecteerd en groen gemarkeerd. Als er op de knop OPSLAAN wordt geklikt, worden de opgegeven toegangsrechten in het systeem opgeslagen.

In het volgende voorbeeld is de gebruikersgroep "Medewerker ontvangst" aangemaakt en zijn de rechten van een medewerker bij de ontvangst van het hoofdgebouw beperkt tot het aanmaken en wijzigen van persoonsgegevens. De medewerker kan bijvoorbeeld de personeelsstamgegevens wijzigen en de kaart- en blokkeringsfuncties in het overzichtsdialogvenster gebruiken.



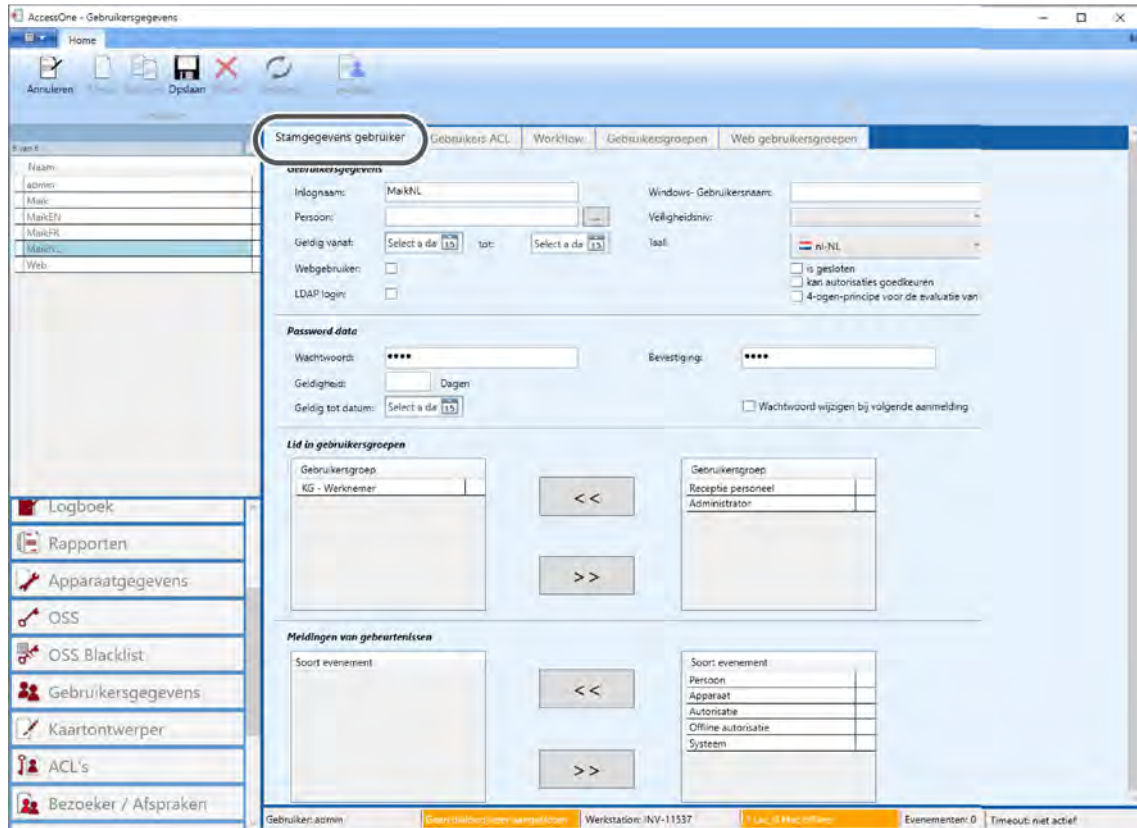
Voor de leden van de groep "Medewerker ontvangst" dient hiervoor geen toegang tot de ACL te worden voorzien om te voorkomen dat ze personen in andere toegangslijsten kunnen plakken. De leden van deze groep hebben alleen leestoeegang tot alle stamgegevens om eventuele vragen over de kaart en toegangsrechten te kunnen beantwoorden.



Medewerkers van het management en/of systeembeheer dienen te worden geautoriseerd om de persoonsgegevens van de medewerkers die het gebouw mogen betreden, in de toegang in te voeren.

7.2.2 Stamgegevens gebruiker

Maak nu gebruikers aan die zich in AccessOne mogen aanmelden.



Gebruikersgegevens

Geef een naam voor de aanmelding op. Als een Windows-gebruikersnaam wordt opgegeven, gebruikt de AccessOne-software deze voor de automatische aanmelding (Single Sign-on). De persoon kan worden geselecteerd uit een lijst. Als het gebruikersprofiel slechts beperkt geldig is, kan een van/tot-datum worden opgegeven. Als deze geldigheid verstrijkt, wordt de gebruiker automatisch geblokkeerd. Een gebruiker kan te allen tijde ook onmiddellijk handmatig worden geblokkeerd (schakel daarvoor het selectievakje in).

In het masker kan aan de gebruiker bovendien het attribuut "4-ogen-principe voor de evaluatie van logboeken" worden toegewezen, wat wil zeggen dat de weergave van meer gedetailleerde gegevens uit het logboek het inloggen van een andere gebruiker dit toegangsrecht als voorwaarde stelt.

Op dezelfde wijze kan aan de gebruiker het recht "Toegangsrechten activeren" worden toegewezen. Dit recht is nodig bij bepaalde toegangsrechten die een eigen activering vereisen.

Password data

Ken aan de gebruiker een wachtwoord toe. Een beperkte geldigheid kunt u voor een bepaalde periode vastleggen of alleen met een "Geldig tot datum" opgeven.

Activeer "Wachtwoord wijzigen bij volgende aanmelding": nadat de gebruiker in het invoermasker zijn inlognaam en het toegewezen wachtwoord voor het eerst heeft ingevoerd, krijgt deze de opdracht om een nieuw wachtwoord in te voeren en dit te bevestigen. Bij het invoeren van het wachtwoord kunt u een willekeurig aantal tekens kiezen. De maximale wachtwoordlengte kan worden ingesteld in het systeem.

Lid in gebruikersgroepen

Wijs aan de AccessOne-gebruiker de dialoogpagina's en de functies toe die deze na het inloggen mag bekijken

of bewerken. Deze dialoogrechten worden van tevoren voor zogenaamde gebruikersgroepen gedefinieerd. Verdere informatie vindt u bij "6.2 Gebruikersgegevens" op pagina 28.

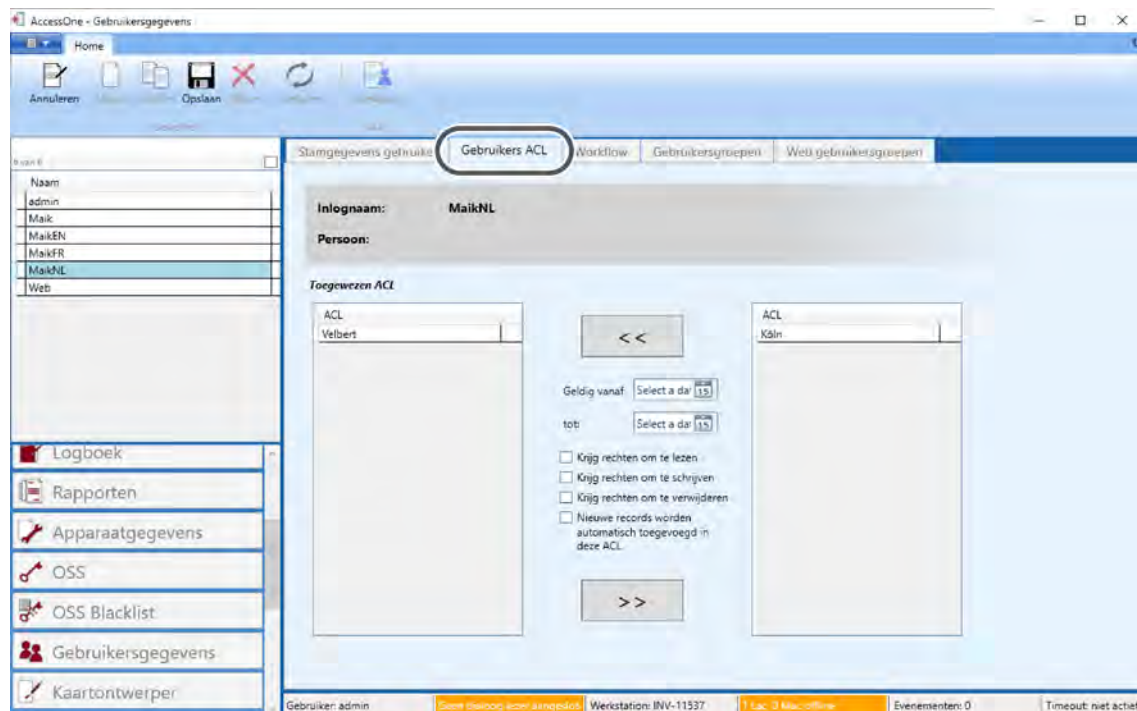
Toegangsrechten voor gebeurtenissen

Wijs aan de AccessOne-gebruiker de gebeurtenissen toe die deze na het inloggen mag bekijken of bewerken.

7.2.3 Gebruiker ACL (klantenmogelijkheden)

(Alleen bij gegevensscheiding beschikbaar.)

Hier kunnen Access Control-lijsten (ACL) aan dialooggebruikers worden toegewezen. De ACL's kunnen worden ingesteld en gewijzigd. Voorwaarde: de systeembeheerder heeft de ACL-functie vrijgegeven.



Klantenmogelijkheden zijn raadzaam wanneer een AccessOne-installatie/databank verschillende klanten (multi-users) bedient en daarbij iedere klant dan alleen zijn eigen gegevens kan bekijken en bewerken. Gegevensrecords waaraan geen multi-user-module is toegewezen, zijn voor alle gebruikers beschikbaar. Een bovengeschatte persoon (systeembeheerder) is verantwoordelijk voor de bewerking van dergelijke parameters. Het management en de systeembeheerder dienen altijd master- of aanvullende bevoegdheden te krijgen. Voor medewerkers, zoals personen bij de ontvangst, dienen eigen deelsystemen van het toegangscontrolesysteem te worden geconfigureerd om stamgegevens te kunnen bekijken, bewerken en wissen. Gebruikers van een deelsysteem, zoals de groep "Medewerker ontvangst", dienen bijvoorbeeld geen toegang te hebben tot ACL, omdat deze anders ook personen in andere toegangslijsten kunnen plakken. Het toegangsrecht voor het uitlezen van stamgegevens is voor gebruikers van dit deelsysteem voldoende.



Wanneer aan een AccessOne-gebruiker slechts één toegangslijst (ACL) is toegewezen, kan deze alleen de toegangsrechten toewijzen die in dezelfde ACL zijn opgenomen. Daardoor kan de AccessOne-gebruiker leden van de groep "Medewerker ontvangst" alleen toegangsrechten geven voor de deuren die zijn vrijgegeven voor het gebouwgedeelte Ontvangst. Andere deuren worden niet weergegeven in de selectielijst.

De leden van de groep "Medewerker ontvangst" kunnen de toegangsrechten bekijken, wijzigen en wissen, maar niet opnieuw toevoegen. Dat gebeurt alleen via de systeembeheerder of een persoon met het betreffende toegangs- of toewijzingsrecht. Het is ter vrije beoordeling en verantwoordelijkheid van de gebruiker om de gegevens nuttig en volgens zijn (veiligheids-)vereisten in te delen.

Workflow

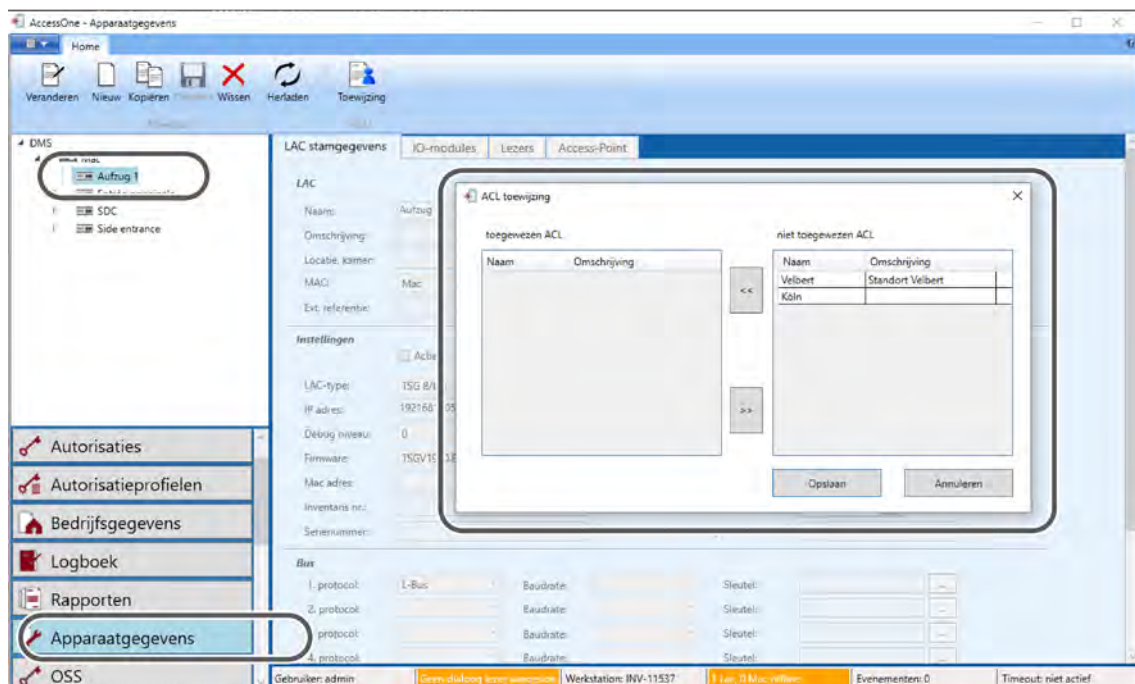
Via het tabblad Workflow kunnen voor bepaalde uit te voeren acties werkprocessen worden aangemaakt, bijvoorbeeld wanneer een goedkeuring van een leidinggevende is vereist.

7.2.4 Gegevensrecords toewijzen aan de toegangslijsten – ACL

Als het systeem reeds gegevens bevat waarvan de toegang op een later tijdstip dient te worden beperkt, moeten deze gegevens via de knop TOEWIJZING aan een ACL worden toegewezen.



Let altijd op het volgende: gegevens die niet aan een ACL zijn toegewezen, zijn voor iedereen zichtbaar!



Aanbevolen procedure en volgorde

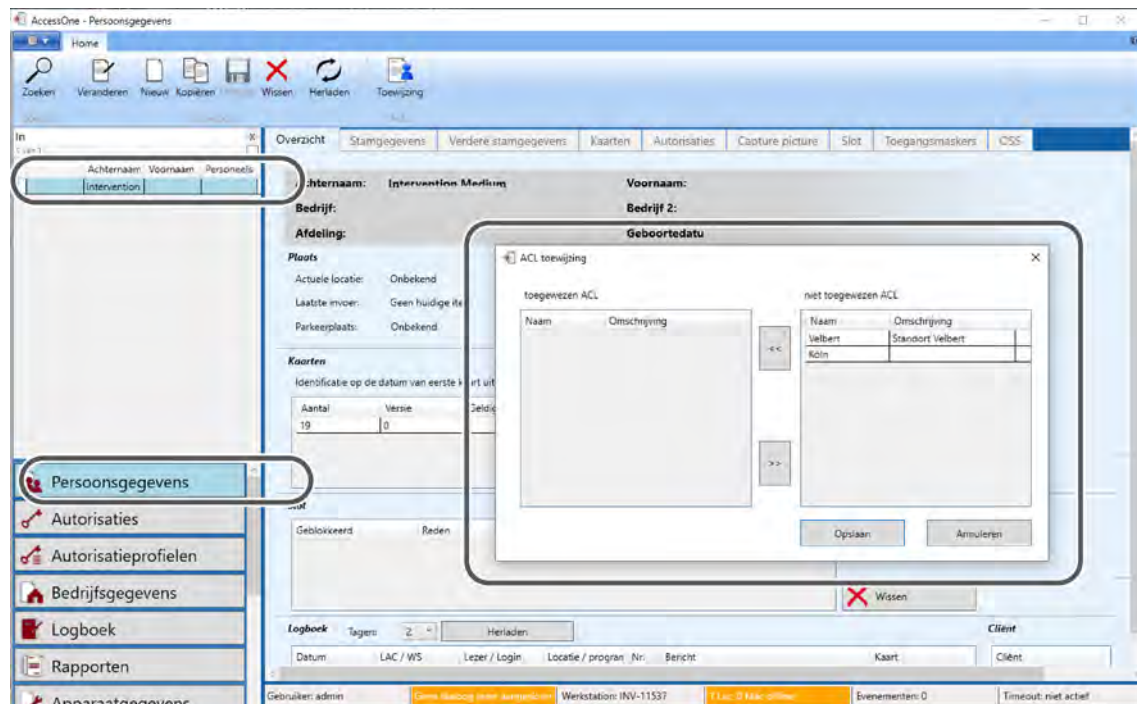
Begin met de deuren in het dialoogvenster "Apparaatgegevens". Klik daarvoor op de knop TOEWIJZING in de taakbalk.

Selecteer een deur in de selectielijst aan de linkerzijde en wijs deze toe aan de betreffende ACL. Klik vervolgens op de knop WIJZIGINGEN OPSLAAN. Het gekozen object wordt dan met een gekleurde balk dienovereenkomstig gemarkeerd.

Ga op dezelfde manier te werk voor de dialoogvensters "Persoonsgegevens" en "Toegangsrechten".

7.2.5 Web-gebruikersgroepen

(Alleen beschikbaar in combinatie met licentiemodule Bezoekersbeheer, art.nr. 348122V.)



Hier worden webpagina's voor de webgebaseerde bezoekersaanmelding en het beheer van werknemers van externe bedrijven aan web-gebruikersgroepen samengevoegd.

Op dezelfde manier kunnen via het Lightweight Directory Access Protocol (LDAP) gegevens over gebruikers en tot welke groep ze behoren, ter beschikking worden gesteld en aan het systeem worden toegevoegd. LDAP maakt het mogelijk om gegevens van een LDAP-directory op te roepen.

7.3 Locatiegegevens

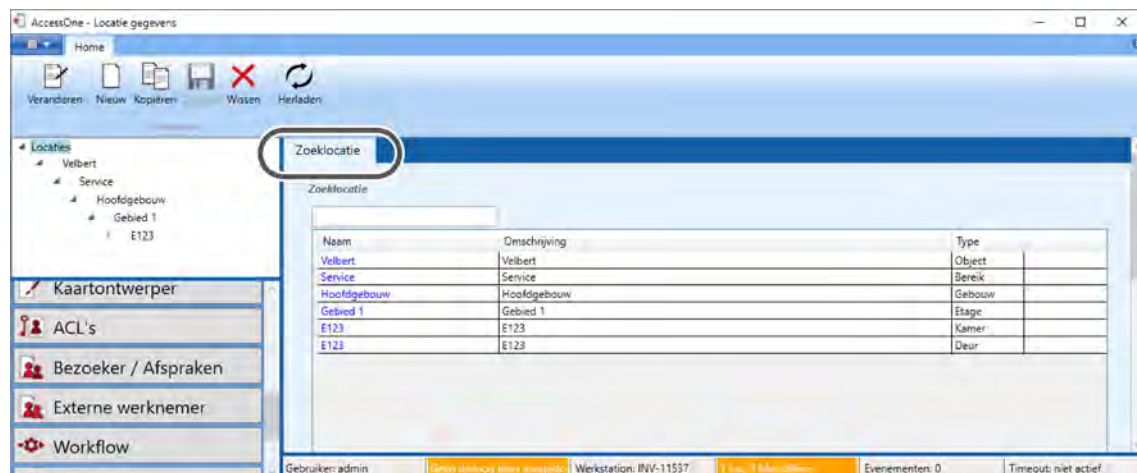
Met de locatiegegevens beeldt u alle objectstructuren af die relevant zijn voor het toegangscontrolesysteem. De weergave gebeurt overzichtelijk in de vorm van een structuurboom.



Geef de locatiegegevens zo compleet en gedetailleerd mogelijk op, omdat deze later worden gebruikt wanneer hardwarecomponenten worden aangemaakt.

Als er verschillende locaties zijn aangemaakt, helpt het tabblad "Zoeklocatie" verder. Door te klikken op "Locaties" in de structuurboom, worden alle aangemaakte locaties weergegeven, gesorteerd op type. Door te dubbelklikken op een locatie in de lijst, wordt de locatie in de linker structuurboom geopend.

7.3.1 Locatie aanmaken



Kies "Locatiegegevens" in de dialoogselectie. Het tabblad "Zoeklocatie" wordt geopend en in de structuurboom links worden de gegevens van objecten, gebieden, gebouwen, etages, ruimten en deuren hiërarchisch weergegeven.

Door te klikken op het betreffende niveau, kan er met de knoppen NIEUW en WIJZIGEN iets worden ingevoerd of aangepast.

Object

Geef de locatie waar de gebieden, gebouwen, deuren, cilinders, lezers en offline-apparaten zich bevinden, een objectnaam. Op objectniveau kunnen verschillende locaties worden aangemaakt.

Gebied

Geef namen aan gebieden die zich in het object bevinden (bijvoorbeeld "Productie", "Ontwikkeling", "Boekhouding" enz.).

Gebouw

Geef een naam aan het gebouw waar alle gebieden van het object zich bevinden (bijvoorbeeld "Gebouw 3.1.") en maak daarvoor adres- en contactgegevens aan.

Etage

Voer de etagenam en het etagenummer in waar de deuren, cilinders, lezers en offline-apparaten van het bovengesikte gebouw van uw object zich bevinden, bijvoorbeeld "BG".

Ruimte

Geef hier namen aan ruimten op dezelfde etage, bijvoorbeeld "0.12", en configureer de ruimten volgens de verantwoordelijke personen, het gebruik en de techniek.

Deur

Voer de naam van de deur van een ruimte in, bijvoorbeeld "Deur 0.12 buiten".

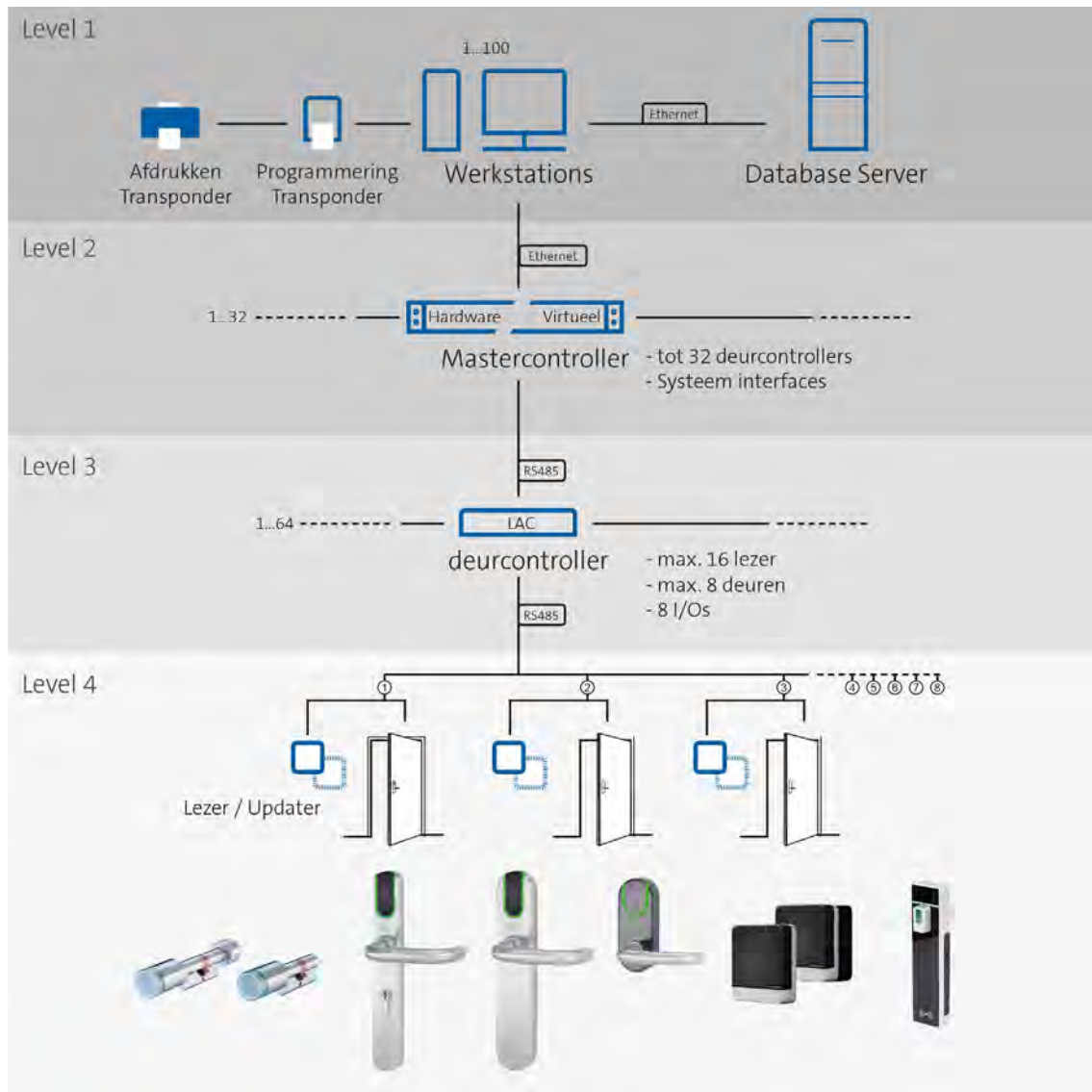
8 Apparaten configureren

Doelgroep van dit hoofdstuk:

- Voor het product opgeleid personeel

De configuratie van de apparaten begint met de mastercontrollers op niveau 2. Dan worden de deurcontrollers op niveau 3 geconfigureerd en worden de I/O-modulen aangemaakt. Als laatste configureert u de aangesloten online- en offline-apparaten op niveau 4.

AccessOne – het 4-niveaus-concept

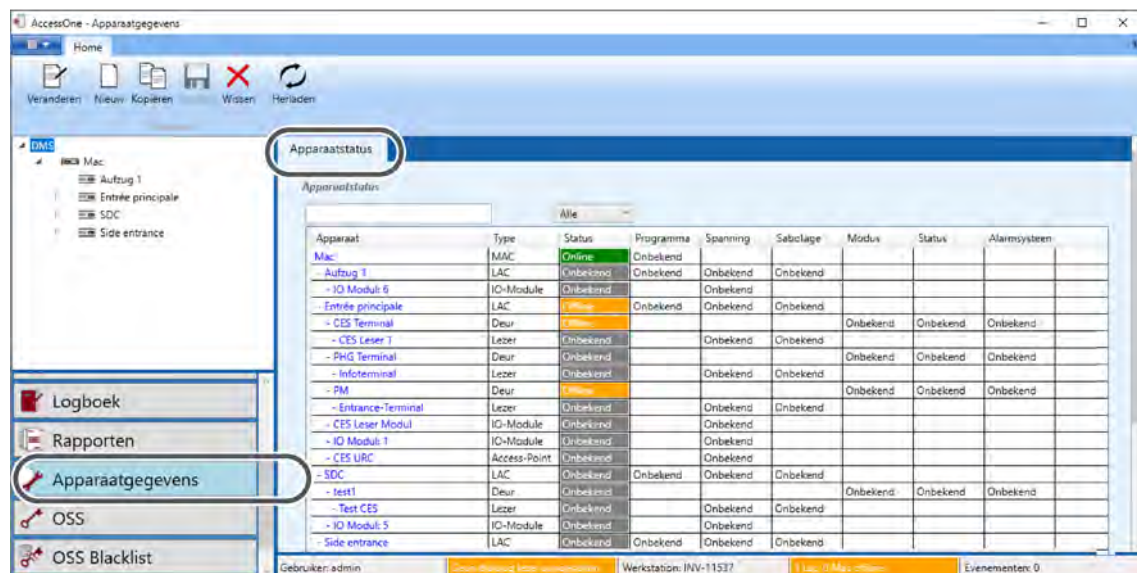


AccessOne is aan hardwarezijde gebaseerd op een vier-niveaus-concept als basis voor een vrijwel onbeperkte schaalbaarheid. De serverprocessen Toepassing en Databank werken op Windows-server-besturingssystemen alsmede een geïnstalleerde SQL-server. De serversoftware werkt in de meeste gevallen in een virtuele omgeving (niveau 1). De mastercontroller verstrekt de gegevens aan de deurbesturingen (Door Control Unit) en stelt alle deurbesturings-overkoepelende functies ter beschikking (niveau 2). De mastercontroller hoeft niet fysiek als autonome component aanwezig te zijn. Deze kan, net zoals de serversoftware, ook worden gevirtualiseerd. De mastercontroller is via het netwerk lokaal met de deurbesturingen verbonden (niveau 3). Elke aangesloten deurbesturing is autonoom en beschikt over alle toegangsrechtgegevens van een persoon

inclusief de offline-gegevens wanneer de gegevens eenmaal zijn geladen. Daardoor worden alle toegangsbeslissingen lokaal genomen (niveau 3). De lezers worden aangesloten via een RS485-interface (niveau 4). Iedere lezer kan daarbij ook als updater voor de offline-apparaten worden gebruikt.

8.1 Apparaatgegevens online-apparaten

8.1.1 Apparaatoverzicht weergeven



AccessOne stelt de apparaatgegevens-editor ter beschikking voor het aanmaken en parametriseren van apparaten. Deze toont de apparaten in een structuurboom in de objectselectie aan de linkerzijde. De bovenste vermelding is het Data Management System (DMS) en daaronder zijn de apparaten gerangschikt. Daar vinden alle gegevenswijzigingen en alle meldingen van de deurcontrollers (TSG1, TSG8, AMC of LAC*) plaats. Daarom worden hier ook de statusmeldingen geïnterpreteerd, in het geheugen verzameld en weergegeven.

Klik op "DMS" wanneer u de status van alle apparaten wilt zien in het overzicht. U kunt de DMS-vermelding niet wissen en ook geen tweede aanmaken.



De status van een individueel apparaat (online of offline) ziet u ook in de detailweergave van het apparaat.

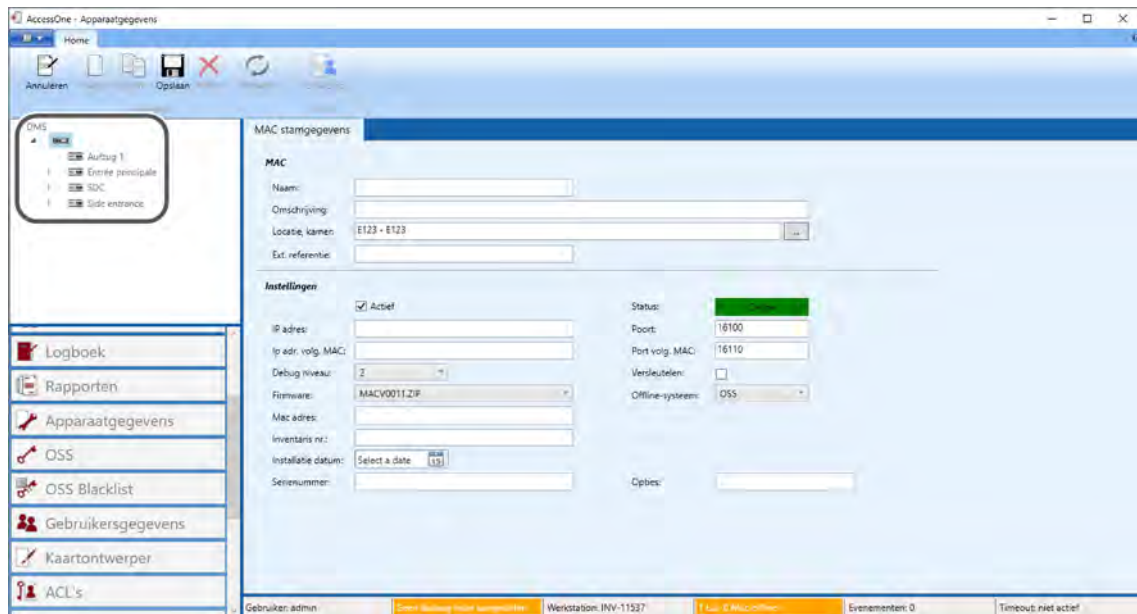
In het dialoogvenster wordt de status van alle beschikbare apparaten weergegeven in de vorm van een lijst. Deze weergave wordt niet automatisch geactualiseerd. Voor een actualisering klikt u op de knop ACTUALISEREN. Via de objectselectie links is er een zoekvenster beschikbaar. Als hier letters worden ingevoerd, wordt de ondergeschikte lijst op alle apparaten gefilterd die deze letters bevatten. Deze hoeven daar niet mee te beginnen. Ook hoofdletters en kleine letters worden genegeerd om het zoeken te vereenvoudigen. De namen van de apparaten worden in blauwe tekst getoond, wat in AccessOne meestal betekent dat hier door te dubbelklikken op de naam, direct naar het tabblad van deze vermelding kan worden genavigeerd. In het midden is er een aanvullende filtermogelijkheid op apparaatstatus. Als u bijvoorbeeld alleen de apparaten wilt zien die op dat moment online zijn, selecteert u in de vervolgkeuzelijst "Online". Door met de rechtermuisknop op de naam van een deur te klikken, worden mogelijke stuurcommando's weergegeven die voor een deur zijn toegelaten.

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

8.1.2 Mastercontroller (MAC) aanmaken

Om een nieuwe mastercontroller (MAC) aan te maken, kiest u "DMS" in de structuurboom en klikt u op de knop NIEUW.

8.1.2.1 MAC-stamgegevens



Vervolgens wordt aan de rechterzijde een niet ingevuld tabblad voor de MAC weergegeven, waarin u de gegevens kunt invoeren. Iedere MAC heeft een naam nodig, die zo dient te zijn gekozen dat deze het verantwoordelijkheidsgebied van dat apparaat beschrijft. In een klein systeem is over het algemeen één MAC voldoende. Bij grotere systemen is vaak één MAC per gebouwencomplex aanwezig. Daarom is het raadzaam om de mastercontroller naar dit gebouw te noemen. Een individuele MAC kan tot 32 Access Modular Controllers (AMC) beheren.

U hebt de mogelijkheid om aanvullend nog een "Omschrijving" op te geven, bijvoorbeeld de precieze opstellocatie. Het selectievakje "Locatie" biedt de lijst aan van de eerder geconfigureerde locaties. Bij een nieuw systeem is alleen de locatie "onbekend" beschikbaar. U kunt deze lijst via het dialoogvenster "Systeemconfiguratie > Locaties" vullen met extra locaties (zie „6.1 Systeemconfiguratie“ op pagina 17). Bij toepassingen waar het toegangscontrolesysteem over veel locaties is verdeeld, raden wij aan om deze locaties van tevoren aan te maken en bij het aanmaken van apparaten alleen nog uit de lijst te selecteren. De locatiegegevens omvatten, afhankelijk van het type, verdere informatie, zoals het adres van een contactpersoon met telefoonnummer, en zijn daardoor nuttig in geval van een storing.



Voor iedere MAC moet een IP-adres en een poortnummer worden opgegeven. Het IP-adres van de MAC treft u aan in de netwerkconfiguratie op de MAC. U kunt op de mastercontroller ook een commando venster openen (cmd.exe) en het commando "ipconfig" invoeren. Het voor de LAN-adapter weergegeven IP4-adres is het IP-adres van de MAC. Neem bij vragen contact op met de systeembeheerder van uw netwerk.

Het poortadres is bij nieuw geïnstalleerde mastercontrollers ingesteld op 50100. Dit adres kan naar wens worden gewijzigd, maar moet in de configuratie bij de MAC (Datasec\Mac\config\MacConfig.ini) en hier in de apparaatgegevens overeenkomen, omdat er anders geen communicatie kan worden opgebouwd.

Het veld "Debug-niveau" is een hulpmiddel voor de fabrikant om in het geval van een storing uitgebreide fout-

protocollen te kunnen genereren. Hoe groter het Debug-niveau is, des te uitgebreider zijn de registraties die de mastercontroller bij alle acties meeschrijft. Let erop dat de waarde niet groter is dan 1, omdat dit gevolgen voor de prestaties van het apparaat kan hebben.

Via het selectievakje "Versleutelen" stelt u in of de communicatie tussen DMS en MAC AES-versleuteld dient plaats te vinden. De versleuteling van gegevens vertraagt de snelheid bij het opbouwen van de verbinding en is daarna ook enigszins van invloed op de doorvoercapaciteit bij de gegevensuitwisseling.

Het veld "Firmware" is bestemd om hier bij een upgrade de nieuwe softwareversie in te voeren. Deze wordt automatisch aan alle mastercontrollers verstrekt en geactiveerd. Belangrijk: iedere MAC beschikt over zijn eigen firmware.



Wijzig de vooraf ingestelde waarde alleen wanneer u van CES een overeenkomstige update hebt ontvangen! Wanneer uw MAC-kaartlezers met updatefunctie voor offline-systemen bedient, moet u dit instellen wanneer u de MAC aanmaakt. In dat geval wijzigt de selectie van de te gebruiken firmware voor de MAC. Wijziging **achteraf** van deze MAC-functie is **niet mogelijk**. In dat geval moet een nieuwe MAC in de DMS worden aangemaakt en moeten de reeds toegewezen LAC's aan de nieuw aangemaakte MAC worden overgedragen.

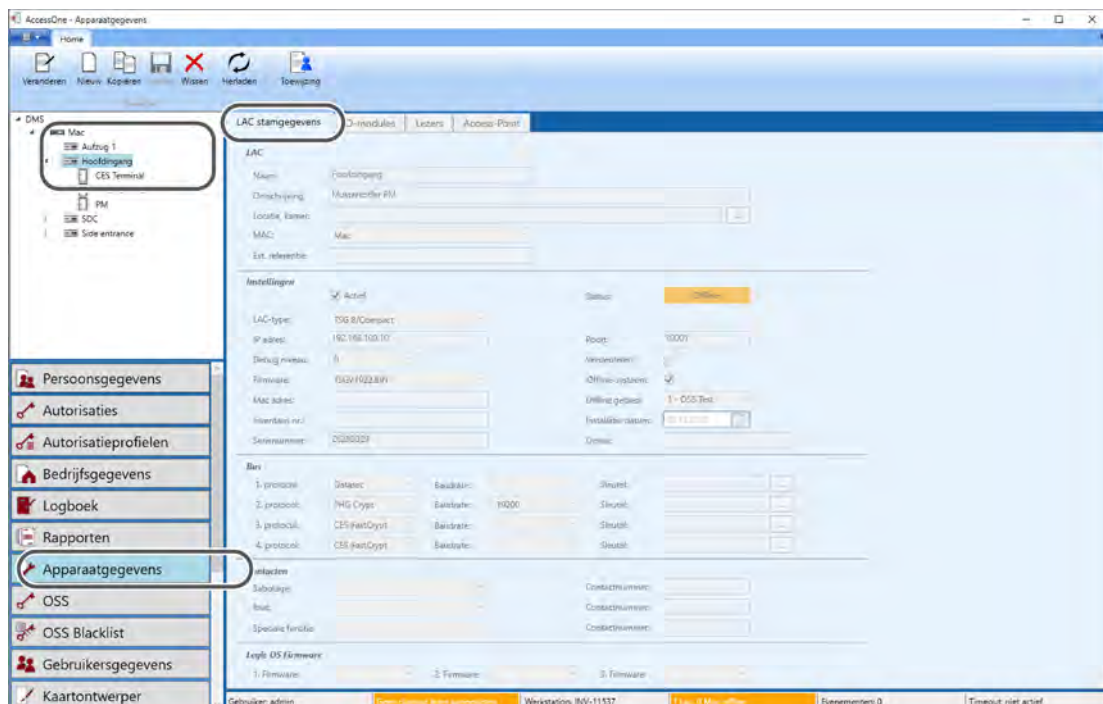
Optioneel kunt u voor het apparaat ook het Mac-adres, een inventarisnummer en de installatiedatum invoeren. Let op het volgende: het Mac-adres kan belangrijk zijn wanneer uw netwerk alleen geconfigureerde Mac-adressen bedient om te voorkomen dat onbevoegden een verbinding tot stand brengen met uw netwerk.



Voor elk apparaat en elke deur is er een selectievakje om het apparaat te activeren. Pas wanneer dit vakje is aangevinkt, wordt het apparaat met gegevens geladen en gestart. Daardoor kunnen de apparaten al worden geconfigureerd en pas na de installatie op actief worden ingesteld. Voordeel: niet geactiveerde apparaten worden niet bewaakt door het systeem. Daarom worden vooraf geconfigureerde, maar niet geactiveerde apparaten niet als apparaten met een storing gemeld. In totaal kunnen tot 32 lokale deurbesturingen per MAC worden aangesloten.

8.1.3 Deurbesturing (LAC) aanmaken

8.1.3.1 LAC-stamgegevens

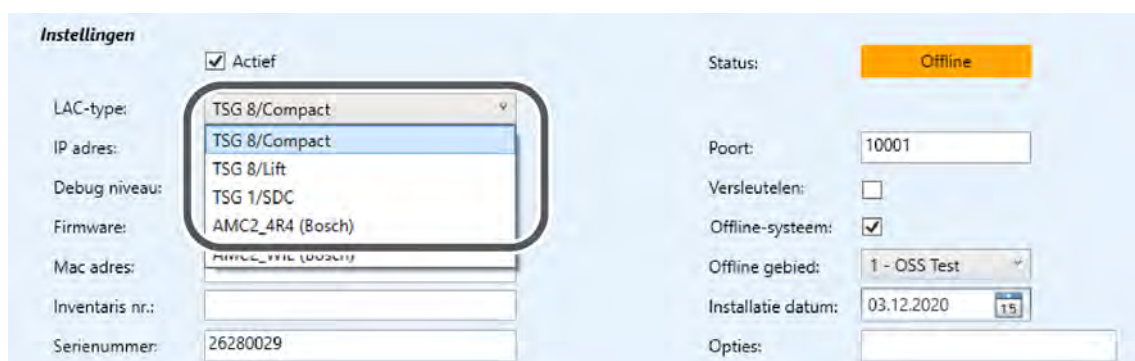


Lokale deurbesturingen, Local Access Controllers (LAC), worden telkens onder de MAC aangemaakt waarop deze ook zijn aangesloten. Kies met de muis de gewenste mastercontroller en klik op

Nieuw.

In het dialoogvenster wordt vervolgens een tabblad voor een deurbesturing weergegeven.

Iedere LAC heeft een naam en een omschrijving nodig. Ga hier te werk zoals bij de mastercontroller (MAC). Ook hier is het nuttig om een naam te kiezen die uitsluitend geeft over het verantwoordelijkheidsgebied. De omschrijving biedt u bovendien de mogelijkheid om de precieze montage locatie op te geven.



AccessOne ondersteunt deurbesturingen van verschillende fabrikanten. Selecteer onder LAC-type de hardware die u gebruikt. De besturingen kunnen binnen één systeem gemengd worden gebruikt.

- TSG 8/Compact (art.nr. 348007V) toegangscontrolecentrale voor tot 8 deuren met max. 16 lezers
- TSG 1/SDC (art.nr. 348008V) toegangscontrolecentrale voor 1 deur met max. 2 lezers
- AMC2_4R4 met 4 RS485-connectoren voor tot 8 deuren
- AMC2_WIE met 4 Wiegand-interfaces voor tot 8 deuren

Geef voor de LAC een IP-adres op dat vanaf de MAC bereikbaar is. Het poortadres is vooraf ingesteld op

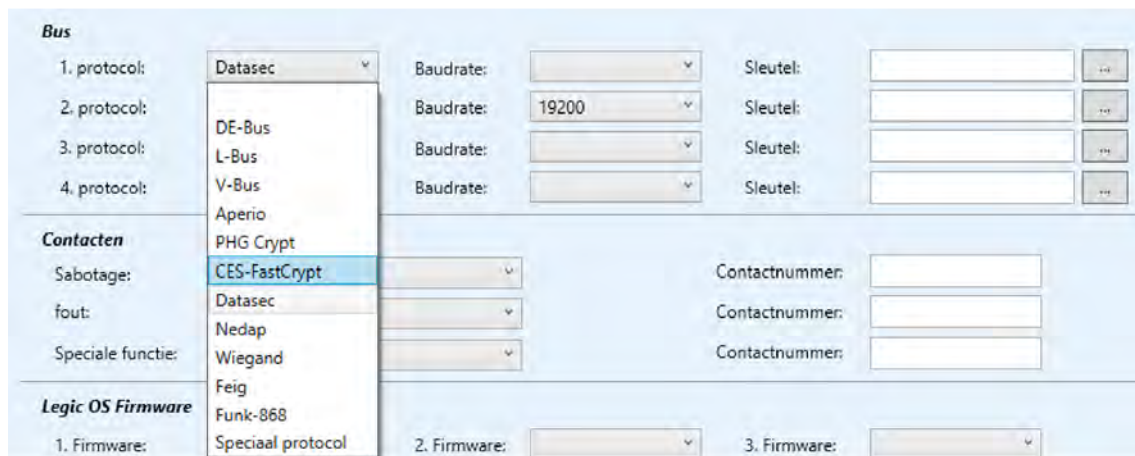
10001 en mag niet worden gewijzigd. Kies de bij de deurbesturing passende configuratie voor het instellen van het IP-adres op de deurbesturing.

Optioneel kunt u voor het apparaat ook het Mac-adres, een inventarisnummer en de installatiedatum invoeren.

Via het selectievakje "Versleutelen" stelt u in of de communicatie AES-versleuteld dient plaats te vinden. De versleuteling van gegevens vertraagt de snelheid bij het opbouwen van de verbinding en is daarna ook enigszins van invloed op de doorvoercapaciteit bij de gegevensuitwisseling.

Het selectievakje "Offline-systeem" betekent dat de AMC herkent wanneer er offline-systemen worden gebruikt en of er een updater beschikbaar is.

Afhankelijk van de hardware en de interface kunnen hier de betreffende protocollen worden opgegeven.



The screenshot shows a configuration window with several sections:

- Bus:** Contains four rows for protocol configuration. Each row has a '1. protocol:' dropdown (currently showing 'Datasec'), a 'Baudrate:' dropdown (showing '19200'), and a 'Sleutel:' text field with a 'Generate' button.
- Contacten:** Contains three rows for contact configuration. Each row has a 'Sabotage:' dropdown (showing 'CES-FastCrypt'), a 'fout:' dropdown (showing 'Datasec'), a 'Speciale functie:' dropdown (showing 'Wiegand'), and a 'Contactnummer:' text field.
- Legic OS Firmware:** Contains three rows for firmware configuration. Each row has a '1. Firmware:', '2. Firmware:', and '3. Firmware:' dropdown.

 Voor elk apparaat en elke deur is er een selectievakje om het apparaat te activeren. Pas wanneer dit vakje is aangevinkt, wordt het apparaat met gegevens geladen en gestart. Daardoor kunnen de apparaten al worden geconfigureerd en pas na de installatie op actief worden ingesteld. Voordeel: niet geactiveerde apparaten worden niet bewaakt door het systeem. Daarom worden vooraf geconfigureerde, maar niet geactiveerde apparaten niet als apparaten met een storing gemeld. In totaal kunnen tot 32 lokale deurbesturingen per MAC worden aangesloten.

In de dialoogselectie "Rapporten" is er een apparatenlijst die voor alle apparaten de relevante gegevens voor de hardwaredocumentatie verstrekt. Als alle gegevens zijn vermeld, kan het systeem te allen tijde een volledige systeemdokumentatie verstrekken.

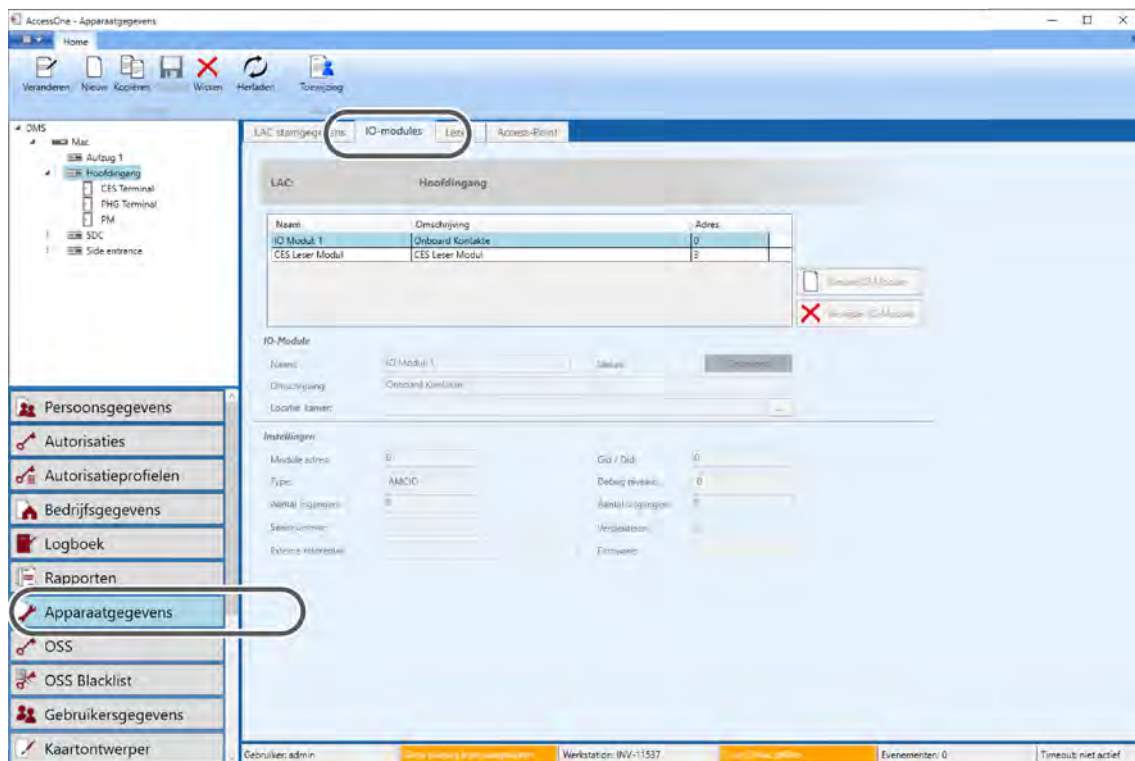
8.1.3.2 IO-modules

Bij de eigenschappen voor de deurbesturing is er bovendien een tabblad voor IO-modules. Iedere lokale deurbesturing heeft hardwarecomponenten nodig voor het bewaken van ingangssignalen (bijvoorbeeld signalen over de deurstatus) en voor het geven van stuurcommando's. Dat zijn zogenoemde IO-modules (Input-Output-modules) van de LAC. Een IO-module heeft meerdere ingangsschakelcircuits om te controleren of een extern contact is geopend of gesloten.

 In AccessOne worden IO-modules in principe gescheiden behandeld, zelfs wanneer de betreffende hardware in de deurbesturing of in de ID-kaartlezer is opgenomen. Dat maakt een vrije toewijzing van signalen mogelijk over alle beschikbare IO-modules.

AccessOne onderscheidt of het om onboard IO-modules van de LAC gaat of om uitgezette, aparte IO-modules. De onboard IO-module wordt bij het aanmaken van de LAC ook standaard aangemaakt. Uitgezette IO-modules moeten handmatig met hun betreffende busadres worden toegevoegd. De signaalprogrammering van de IO-modules wordt later in de configuratie van de betreffende deuren afzonderlijk uitgevoerd.

Ga naar het tabblad "IO-modules" om de hardware voor in- en uitgangen van de deurbesturing te configureren.



Als u een deurbesturing hebt geselecteerd, die al over de in het apparaat opgenomen in- en uitgangen beschikt, wordt deze IO-module automatisch aangemaakt bij het wisselen naar deze pagina.

Klik op de knop Nieuwe IO-module en vul de bijbehorende invoervelden in om een nieuwe IO-module aan te maken. Het module-adres bij interne contacten is 0.

Als type kiest u "AMC-IO" indien u als deurbesturing een AMC hebt gekozen. Wanneer u een TSG-toegangscontrolecentrale gebruikt, kiest u als type "TS2" voor een deurbesturingsmodule met 4 in- en uitgangen en 2 lezerinterfaces, of "IO8" voor een relaisboard met 8 in- en uitgangen. Bij uitgezette deurbesturingsmodules die op de lezerbus worden aangesloten, voert u het ingestelde busadres in en kiest u als type "TSM". TSM-deurbesturingsmodules hebben twee ingangen en twee uitgangen (aanwijzing: dat varieert afhankelijk van uitvoering/type). Geef hier alleen het daadwerkelijk aanwezige aantal op, omdat anders besturingscommando's voor niet beschikbare relais kunnen leiden tot foutmeldingen.

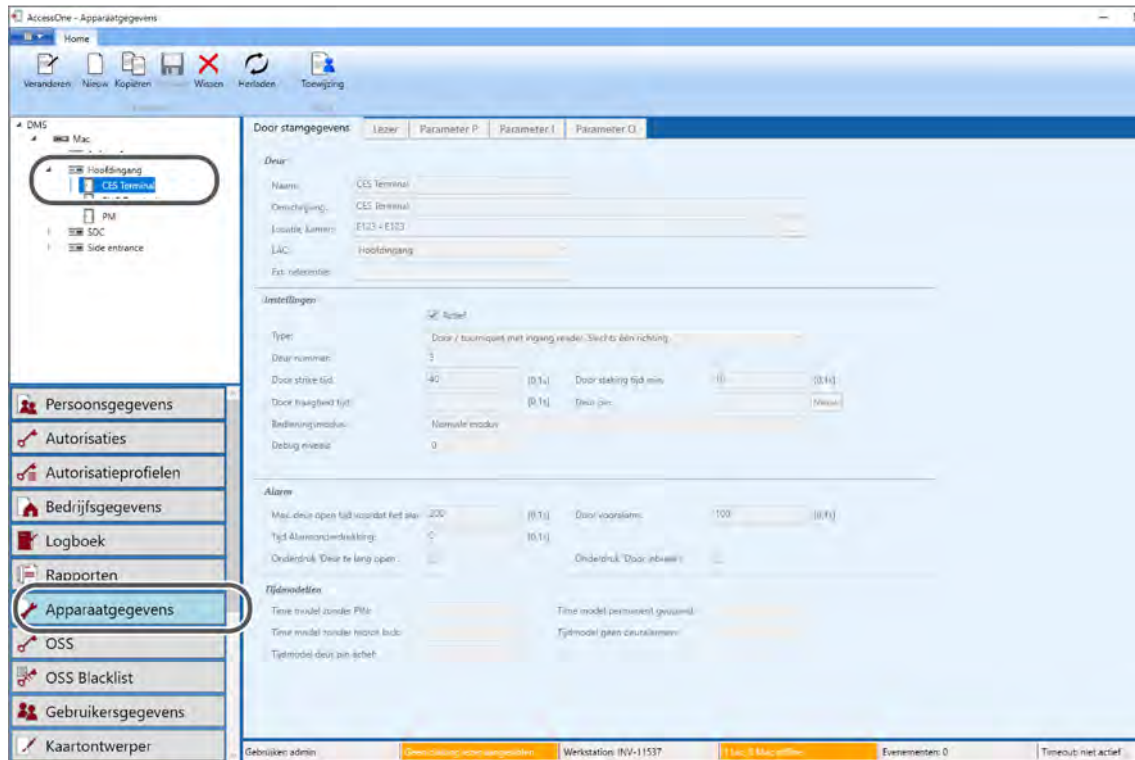


Per deurbesturing kunnen maximaal 64 ingangssignalen en 64 uitgangssignalen worden aangestuurd. De verdeling over de IO-modules is daarbij niet relevant, mits het adresbereik van de lezerbus met maximaal 16 deelnemers niet wordt overschreden.

8.1.4 Een deur aanmaken

8.1.4.1 Deurstamgegevens

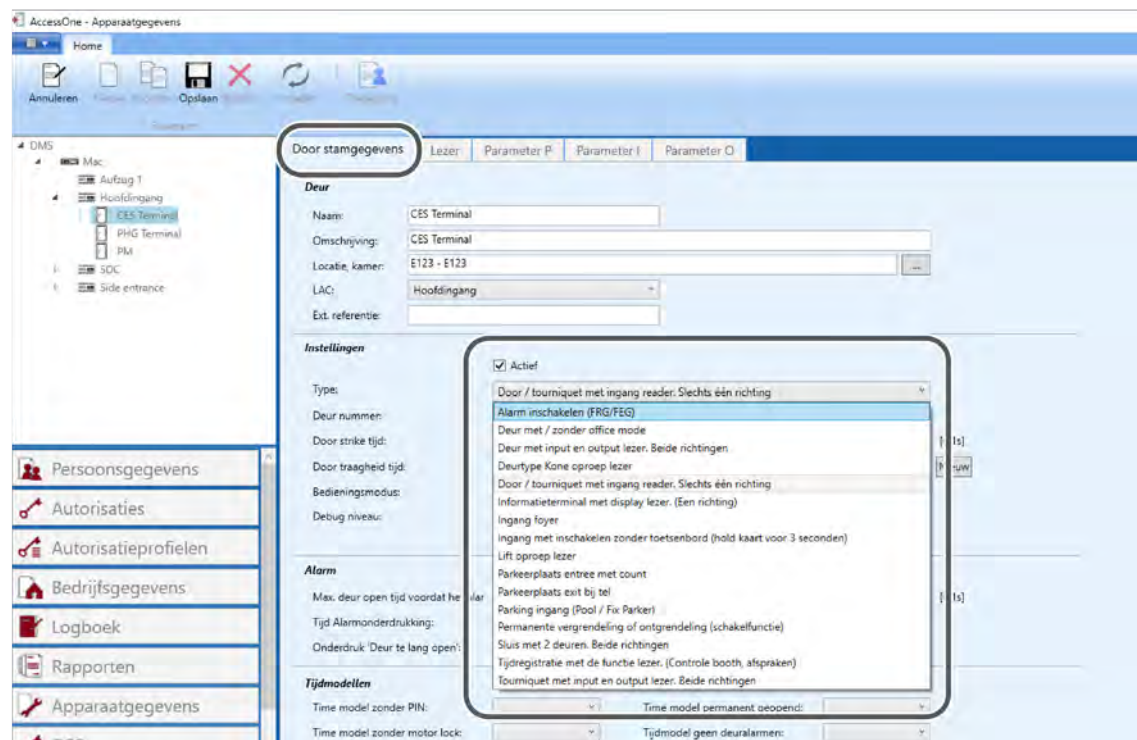
Om op een deurbesturing (LAC) een deur aan te maken, klikt u op de betreffende deurbesturing in de linkerselectielijst en daarna op de knop NIEUW. Daarna wordt recht in het venster de eigenschappenpagina voor een deurbesturing weergegeven.



The screenshot shows the 'AccessOne - Apparaatgegevens' window. On the left, a sidebar contains a tree view with 'Hoofdingang' selected. The main area is titled 'Deur' and contains several sections: 'Deur' (Door) with fields for Name, Description, Location, LAC, and Ext. reference; 'Instellingen' (Settings) with a 'Type' dropdown, 'Deur nummer' (Door number), 'Doorklootijd' (Door stroke time), 'Doorklootijd' (Door stroke time), 'Bedieningsmodus' (Control mode), and 'Deurbreuk' (Door break); 'Alarm' with 'Max. deur open tijd voordat het alarm' (Max. door open time before alarm), 'Tijd alarmoverdekking' (Alarm overlap time), 'Onderdruk. Deur te lang open' (Door pressure too long open), and 'Onderdruk. Deur afwaarts' (Door pressure down); and 'Tijdschema's' (Timetables) with 'Time model zonder PIR' (Time model without PIR), 'Time model permanent gesloten' (Time model permanently closed), 'Time model zonder handreik bod' (Time model without hand reach bottom), 'Tijdschema piken draaitaken' (Timetable pick up tasks), and 'Tijdschema deur pin bereik' (Timetable door pin reach). The bottom status bar shows 'Gebruiker: admin', 'Overzicht: Apparaatgegevens', 'Workstation: (HV-11537)', '11.01.2014 14:00', 'Evenementen: 0', and 'Time-out: niet actief'.

In dit tabblad worden de algemene eigenschappen van een deur vastgelegd. Hiertoe behoren, naast een duidelijke naam en de opgave van de locatie, ook het type van de gewenste deur. Het type beslist hoe het betredingsproces is vormgegeven en welke in- en uitgangssignalen worden gebruikt.

AccessOne stelt vooraf geconfigureerde deurmodellen ter beschikking die alle gangbare taken bij een deur dekken. Naar wens kunnen andere, speciale deurmodellen worden aangevuld die voldoen aan klantspecifieke vereisten. Selecteer het type dat voor uw toepassing geschikt is. In het volgende voorbeeld is een eenvoudige toegangsdeur gekozen met slechts één richting.



Nadat het deurtype is geselecteerd, kunnen via de invoervelden de fundamentele parameters van deze toegang worden ingesteld.

Gebied "Instellingen"

Bij elk apparaat hoort het selectievakje "Actief", waarmee het apparaat wordt geactiveerd. Pas wanneer dit vakje is aangevinkt, wordt het apparaat met gegevens geladen en gestart. Daardoor kunnen de apparaten al worden geconfigureerd en pas na de installatie op actief worden ingesteld. Voordeel: niet geactiveerde apparaten worden niet bewaakt door het systeem. Daarom worden vooraf geconfigureerde, maar niet geactiveerde apparaten niet als apparaten met een storing gemeld.

Met "Ingang locatie" en "Uitgang locatie" selecteert u het bron- en doelgebied. Elke deur in AccessOne leidt van een brongebied naar een doelgebied. Deze gebieden kunnen, maar hoeven niet verschillend te zijn.

Voorbeeld: wanneer uw gebouw is onderverdeeld in verschillende veiligheidszones, kunt u bijvoorbeeld een ingang vanaf de buitenste veiligheidszone (ASB) naar de inwendige veiligheidszone (ISB) leiden. Een tussendeur kan echter ook leiden van ISB naar ISB.

De gebieden worden in de dialoogselectie "Systeemconfiguratie" in het tabblad "Gebieden" aangemaakt. Voor een gebied in het gebouw kan het systeem meetellen hoeveel personen daar momenteel verblijven en bijvoorbeeld controleren of het maximale aantal personen is bereikt. In dat geval zou geen verdere toegang worden verleend. De voorwaarde daarvoor is dat een persoon zonder kaart niet in het betreffende gebied terecht kan komen en dat de in- en uitgangen met isolatiesystemen, bijvoorbeeld tourniquets, zijn uitgerust, zodat niet verschillende personen tegelijkertijd met één toegangsrecht het gebied betreden.

Elke deur heeft bij de deurbesturing een eenduidig deurnummer nodig. Dat moet tussen 1 en 8 liggen, omdat per deurbesturing maximaal 8 deuren worden ondersteund.

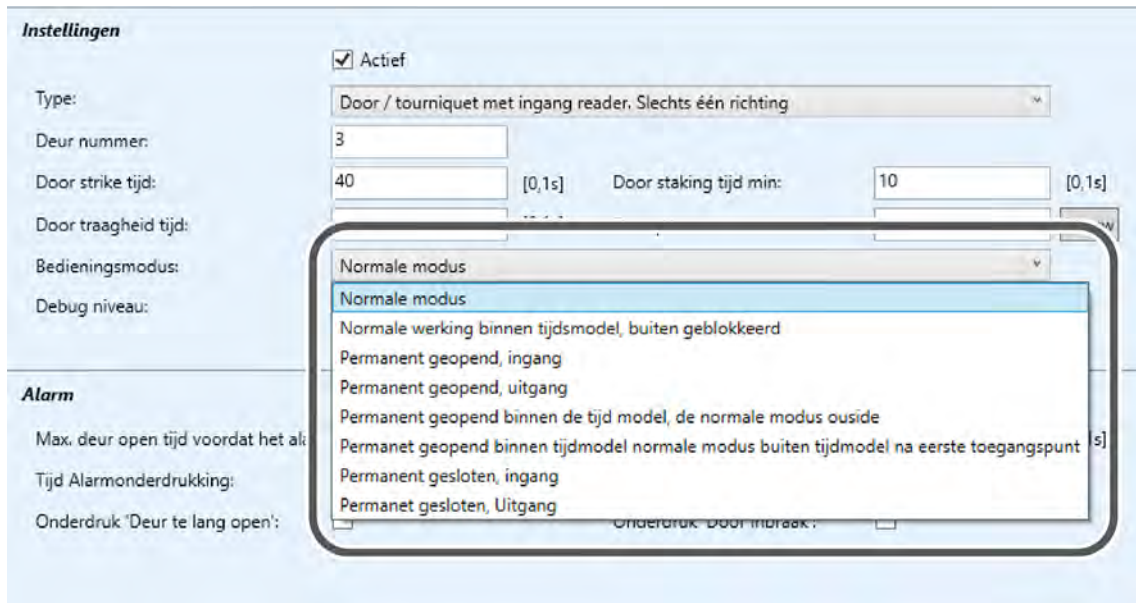
De waarde in het veld "Aansturingstijd deuropener" legt vast hoelang de deuropener bij een geautoriseerd toegangsmedium maximaal wordt aangestuurd. Dit wordt in tienden van seconden gedaan. 40 betekent in

het voorbeeld dus $40 \times 0,1 \text{ sec} = 4 \text{ seconden}$. Wanneer de deur over een deurcontact beschikt, kan de deurbesturing vaststellen dat de deur is geopend. In dat geval wordt de vrijgave ingetrokken zodra de deur als geopend wordt herkend. De waarde in het veld "Minimumtijd deuropener" maakt het mogelijk om in dit geval ervoor te zorgen dat de deuropener lang genoeg wordt bediend, zodat een veilige opening is gewaarborgd.

 Er zijn deuropeningscontacten die in het slot of in de magnetische sluitinrichting zijn geïntegreerd en die de deur als Reeds geopend melden, wanneer deze slechts enkele millimeters heeft bewogen. In dat geval zouden zonder een ingestelde minimumopeningstijd de deuren direct weer zijn vergrendeld en zou een toegang onder bepaalde omstandigheden niet mogelijk zijn.

De waarde in het invoerveld "Deur traagheidstijd" geeft aan hoelang de AMC na het betreden en het herkennen dat een deur weer gesloten is, wacht tot deze de inbraakbewaking van de deur weer activeert. Bij zware deuren kan het voorkomen dat een deurvleugel bij het dichtvallen in het kozijn iets veert, zodat voor de deurbesturing de deur eerst één keer kort is gesloten, dan weer voor een fractie van een seconde is geopend en deze de deur pas weer herkent als deze goed is gesloten. Zonder deze traagheidstijd zou dan onder bepaalde omstandigheden na het betreden telkens weer de melding over een geforceerde deur verschijnen.

In de bedieningsmodus kan uit de volgende opties worden gekozen:



"Normale modus" (standaard): in deze modus kan de deur alleen met het bijbehorende toegangsrecht en een geldige kaart worden binnengegaan.

"Permanent open": de deuropener is altijd actief, de groene led op de ID-kaartlezer brandt permanent en iedereen kan deze deur zonder kaart openen.

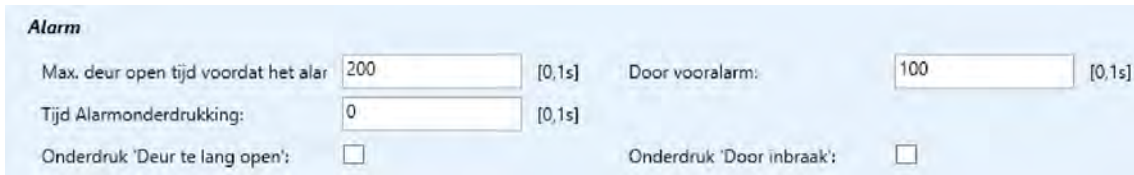
"Permanent geopend binnen het tijdsmodel, de normale modus outside": de deur kan tijdens normale kantoor tijden zonder kaart worden geopend, maar na deze vrij definieerbare tijd dienen alleen nog geautoriseerde personen toegang te hebben.

"Permanent geopend binnen tijdsmodel, normale modus buiten tijdsmodel, behalve na eerste geautoriseerde toegang": na de eerste geautoriseerde opening blijft de deur geopend. De deur schakelt binnen het gekozen tijdsmodel over op de toestand "Permanent open". Zo wordt gewaarborgd dat er ten minste één geautoriseerde medewerker aanwezig is.

"Normale werking binnen tijdsmodel, buiten geblokkeerd": Buiten het toegewezen tijdsmodel kan deze deur niet worden gebruikt, ook niet met een geautoriseerde kaart. Binnen het tijdsmodel zijn voor het openen een geldige kaart en de betreffende toegangsrecht nodig.

Alarm

In het gedeelte "Alarm" worden de parameters ingesteld voor het deuralarm.



"Maximale deuropeningstijd vóór alarm": Hoelang het systeem wacht tot de deur weer is gesloten, voordat er een alarm wordt gemeld. Deze waarde wordt in tienden van seconden opgegeven. Als de ingevoerde tijd wordt overschreden, genereert het systeem een logboekmelding met de tekst "Deur te lang open".

"Vooralarm": De waarde in het veld dient kleiner te zijn dan de waarde in het veld ervoor. Deze geeft aan wanneer een aandachtsignaal aan de lezer dient te worden gegenereerd. Daardoor kan de persoon de deur nog sluiten, voordat er een alarmmelding wordt uitgegeven. Als de deur langer open is dan in deze waarde is opgegeven, geeft de op de deur gemonteerde ID-kaartlezer herhaaldelijk een pieptoon af tot de deur weer wordt gesloten of de alarmmelding is gegenereerd.

"Tijd alarmonderdrukking": De opgave is vereist bij deuren die permanent worden bewaakt door een aanvullende inbraakalarmering. Hier kan het zijn vereist om dit systeem via een uitgangssignaal mee te delen dat de deur nu geautoriseerd wordt geopend. Dit signaal wordt ingetrokken kort nadat de deur weer is gesloten, maar uiterlijk na de tijd die overeenkomt met de waarde in dit veld.

"Deur te lang open onderdrukken": Hier regelt u of het systeem een inbraakmelding dient te genereren of niet wanneer de deur zonder kaart wordt geopend.

"Deurinbraak onderdrukken": Met dit selectievakje bestuurt u het alarmsignaal ter plaatse.



Het systeem genereert geen aparte meldingen over de deurtoestand. De informatie of de deur is geopend of niet, resulteert uit de betreffende logboekmelding over de toegang.

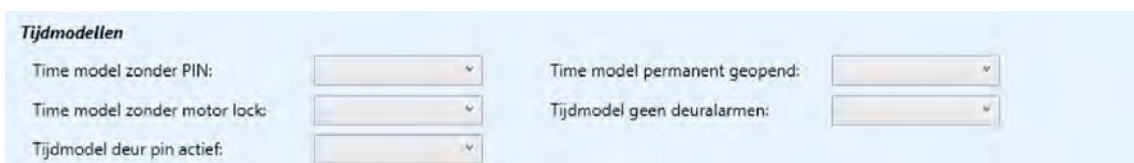
Logboekvermeldingen:

"Geautoriseerde toegang": de deur is na een geautoriseerde boeking geopend.

"Geen geautoriseerde toegang": de deur is niet geopend, hoewel deze werd vrijgegeven.

Tijdmodellen

In deze paragraaf kunnen de voor het algemene gedrag eventueel gewenste tijdmodellen worden geselecteerd:



Er zijn in totaal vier tijdmodellen beschikbaar:

"Tijdmodel zonder motor lock": als de deur over een motorslot beschikt, dan wordt de mechanische belasting vermindert, doordat het motorslot alleen voor en na het ingevoerde tijdmodel geactiveerd is.

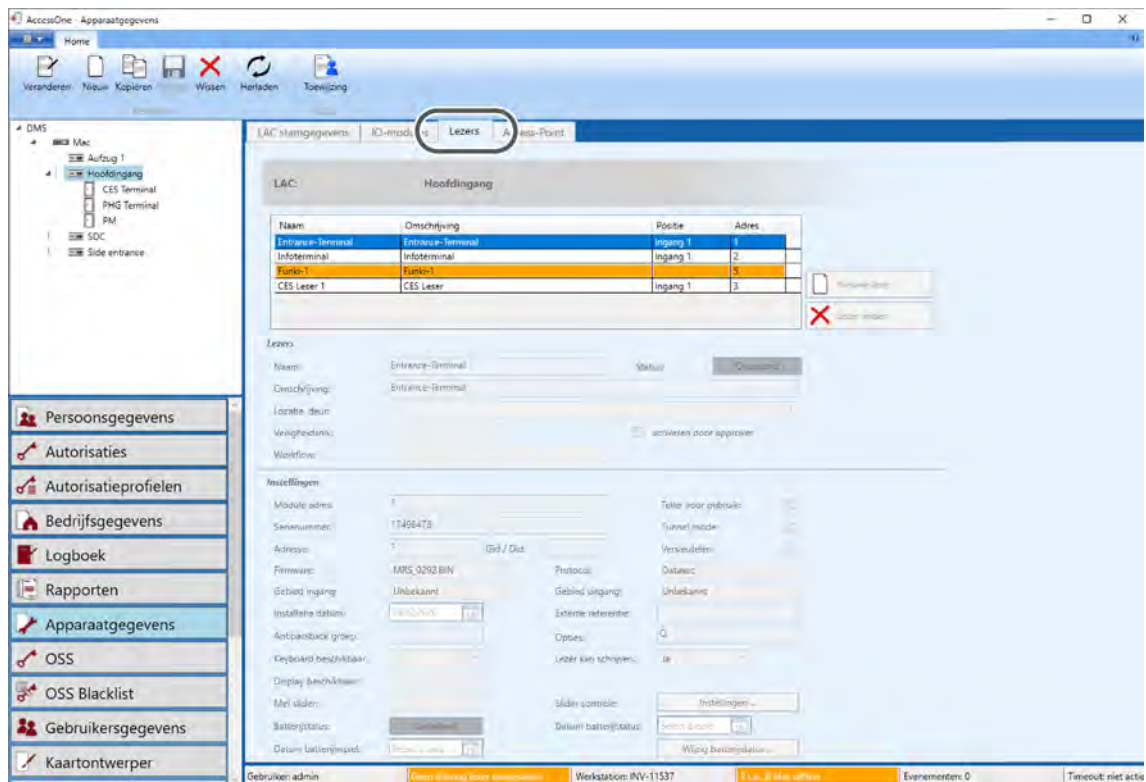
"Tijdmodel zonder PIN": de invoer van de pincode op de ID-kaartlezer wordt beperkt tot tijden buiten het ingevoerde tijdmodel.

"Permanent open": de deuropener is altijd actief en de deur kan zonder kaart worden gepasseerd (deze instelling komt overeen met het tijdmodel "Permanent open").

"Tijdmodel geen deuralarmen": deuralarmen worden alleen gegeven buiten het ingevoerde tijdmodel.

8.1.4.2 Lezer

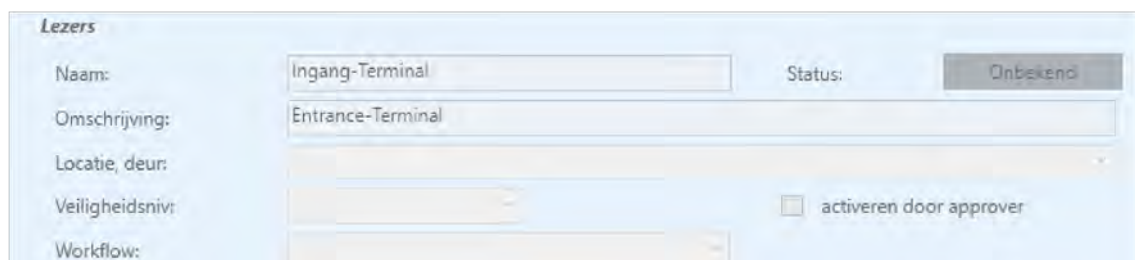
Op het tabblad "Lezer" worden de ID-kaartlezers gedefinieerd die bij de deur horen.



Klik op de knop Nieuwe lezer om een nieuwe lezer aan te maken. Het systeem voegt vervolgens een nieuwe regel in de overzichtslijst in en biedt u de mogelijkheid om de parameters die bij de lezer behoren, in de eronder staande velden in te voeren.

Gebied "Lezer"

In het gebied "Lezer" geeft u naam, omschrijving, locatie, veiligheidsniveau en workflow op.



Veiligheidsniveau

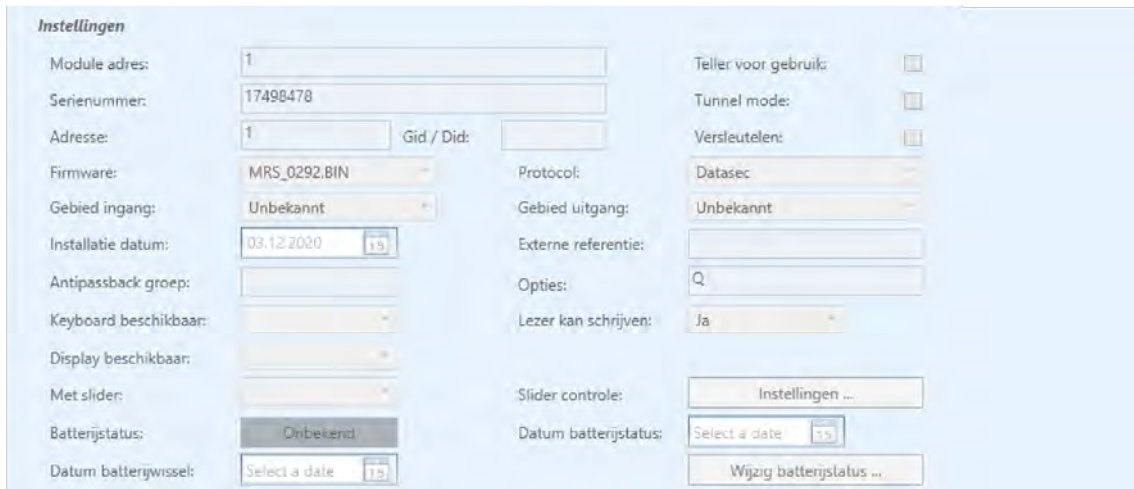
Bij het veiligheidsniveau kan worden gekozen tussen vijf verschillende niveaus van "zeer laag" tot "zeer hoog". Deze lezer mag alleen voor een toegangsrecht of bij een persoon worden ingevoerd wanneer de gebruiker bij het werkstations ten minste een gelijkwaardig of hoger veiligheidsniveau heeft. U kunt via de veiligheidsniveaus regelen dat niet elke AccessOne-gebruiker het toegangsrecht kan verlenen tot gevoelige gebieden. Het selectievakje "Door aaprover activeren" maakt een aanvullende activering noodzakelijk door een gebruiker met het overeenkomstige toegangsrecht.

Workflow

Hier kunt u bepaalde werkstappen aanmaken die door een leidinggevende moeten worden goedgekeurd, bijvoorbeeld het verlenen van toegangsrechten voor een bepaald gebied.

Gebied "Instellingen"

In het gebied "Instellingen" geeft u de technische eigenschappen van de ID-kaartlezer op.



Instellingen	
Module adres:	1
Serienummer:	17498478
Adresse:	1 Gid / Did:
Firmware:	MRS_0292.BIN
Gebied ingang:	Onbekannt
Installatie datum:	03.12.2020
Antipassback groep:	
Keyboard beschikbaar:	
Display beschikbaar:	
Met slider:	
Batterijstatus:	Onbekend
Datum batterijwissel:	Select a date
Teller voor gebruik:	☐
Tunnel mode:	☐
Versleutelen:	☐
Protocol:	Datasec
Gebied uitgang:	Onbekannt
Externe referentie:	
Opties:	Q
Lezer kan schrijven:	Ja
Slider controle:	Instellingen ...
Datum batterijstatus:	Select a date
	Wijzig batterijstatus ...

Module-adres

Het eerste veld is een weergaveveld. Het geeft de door het systeem verstrekte interne lezerindex weer. Deze wordt gebruikt voor de samenstelling van toegangsrechten en kan niet worden gewijzigd.

Serienummer van de kaartlezer

Het serienummer van de lezer is nodig om de interne busadressering van de lezer uit te voeren. Bij deze lezers kan het busadres niet via een tuimelschakelaar worden ingesteld, maar wordt via een configuratiesoftware gestuurd. AccessOne wijst het adres automatisch toe wanneer het serienummer van de lezer is ingevoerd. Als een lezer die op adres 3 is geconfigureerd, zich niet meldt, dan probeert de deurbesturing deze lezer aan de hand van het serienummer te identificeren. Als de identificatie is gelukt, wordt hier het betreffende adres, hier: 3, aan toegewezen.

Adres (handmatige invoer)

Elke lezer moet een busadres tussen 1 en 8 hebben.



Afhankelijk van het lezerprotocol wordt op het busadres nog een vaste getalswaarde opgeteld, omdat in enkele lezerprotocollen de adressen van A tot H zijn verstrekt. Dat gebeurt automatisch, omdat in de deurbesturing de conventies van de verschillende lezerprotocollen zijn opgeslagen.

Firmware

Selectieveld voor de firmwareversie. De telkens actuele versie wordt weergegeven.

GID/DID

Als op de deurbesturing lezers met een oud V-protocol of 9-serie protocol zijn aangesloten, moeten aanvullend op het logische busadres nog een groeps-ID (GID) en een device-ID (DID) worden opgegeven. De GID vormt daarbij de plaats van het tiental en de DID van de eenheid. Beide waarden moeten tussen 1 en 8 liggen. Voorbeeld: waarde "12" omschrijft een lezeradres met GID 1 en DID 2.

Gebruiksteller

De lezer controleert of de kaart het maximale gebruik heeft bereikt dat geldt voor deze dag.

Tunnel mode

Alleen relevant bij LEGIC-lezers met DE-bus. Deister-ID-kaartlezers kunnen, zoals de meeste andere lezers, bij LEGIC-kaarten alleen een stempel analyseren. Als de kaart meer dan één segment heeft en als alle segmenten dienen te worden geanalyseerd, moet daarom de intelligentie van de lezer worden uitgeschakeld en moet de zogenaamde Tunnel mode worden gebruikt. Hierbij worden de commando's aan de LEGIC-chip door de lezer aan de mastercontroller overgedragen voor het zoeken en lezen van een segment. De firmware van de AMC kan dan de segmenten die in de

lezerformaten van AccessOne zijn geactiveerd, achtereenvolgens lezen.

Bij DE-bus en Datasec-bus kan de communicatie met de ID-kaartlezer ook worden gebruikt met AES-versleuteling.

Versleutelen

De verbinding tussen MAC en controller is extra versleuteld.

Installatiedatum

Als bij het aanmaken van de lezer deze automatisch met de huidige dag wordt ingesteld, kan deze echter naar wens worden gewijzigd. De installatiedatum is bestemd voor de systeemdokumentatie.

Extern referentienummer

Voor interne benamingen bij de klant.

Opties

Voor interne benamingen bij de klant.

Antipassback-groep (tijdgerelateerd)

Voorkomt dat een toegangsmedium na het betreden aan een andere persoon wordt doorgegeven en dat deze ook naar binnen gaat met hetzelfde toegangsmedium. Om deuren die zich naast elkaar bevinden, op dezelfde manier te behandelen, kunnen deze in een groep worden samengevoegd. Lezers uit dezelfde antipassback-groep worden behandeld alsof ze naast elkaar zijn gemonteerd en dezelfde toegang bedienen. Een toegangsmedium dat op een lezer van deze groep is gebruikt, is op alle andere lezers van dezelfde groep gedurende een bepaalde periode geblokkeerd (het tijdsbestek kan worden ingesteld in de deurparameters). De ingevoerde waarde is een getal tussen 1 en 99. Er kunnen max. 99 deurgroepen worden gevormd.

Lezerspositie

In AccessOne kan een deur met maximaal vier lezers zijn uitgerust: telkens twee voor de ingangs- en uitgangsricting. Voorbeeld: bij auto-ingangen kan het nuttig zijn om via de lezer voor personenvoertuigen ook een hogere positie voor vrachtwagens te monteren.

Lezer kan schrijven

De lezer kan kaarten beschrijven. Voorbeeld: actualisering van toegangsrechten bij offline-sluitapparaten. Bij enkele lezers kan de software dat automatisch herkennen. Bij andere lezers moet dat uitdrukkelijk worden opgegeven. Als er geen waarde wordt opgegeven, wordt de eventueel beschikbare schrijffunctie van de lezer niet gebruikt.

Keyboard beschikbaar

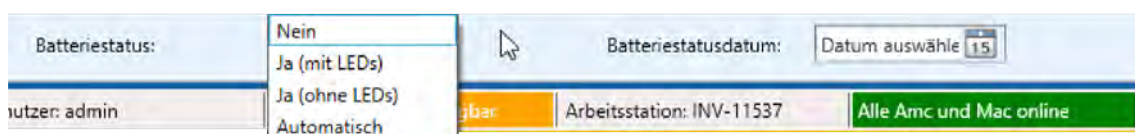
Bij enkele toegangen is het invoeren van een pincode noodzakelijk om de inbraakalarmering (EMA) te activeren, of als aanvulling op het biometrische kenmerk bij de toegang. Aangezien bij enkele lezers het toetsenbord moet worden geactiveerd via een stuurcommando door de deurbesturing, is hier de mogelijkheid gecreëerd om dit uitdrukkelijk op te geven. In de meeste gevallen herkent de deurbesturing automatisch dat er een toetsenbord aanwezig is.

Display beschikbaar

Een display op de lezer wordt alleen aangestuurd wanneer dat hier overeenkomstig wordt ingevoerd.

Met intrek

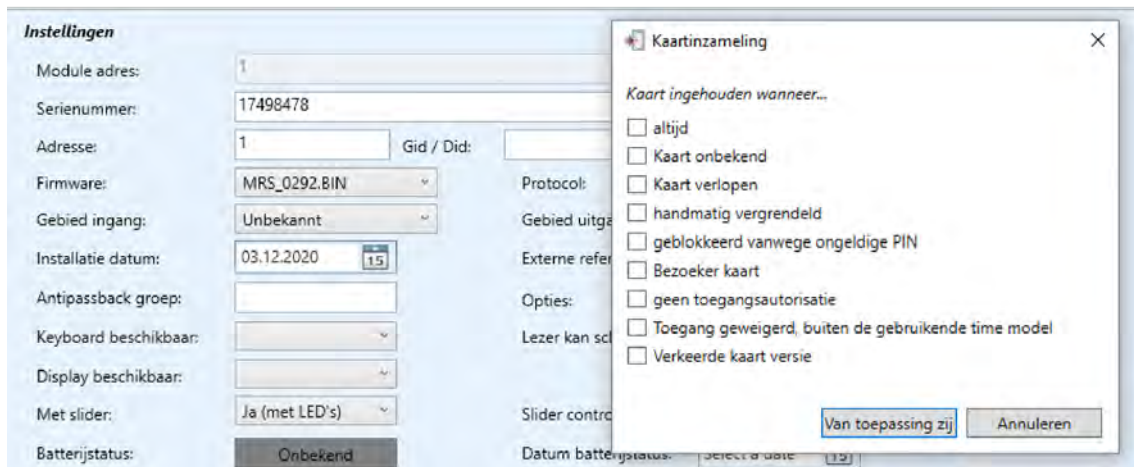
Hier kan worden ingevoerd of de lezer is uitgerust met een gemotoriseerd intreksysteem.



Als de gemotoriseerde intrekschacht is uitgerust met leds, moeten deze worden aangestuurd in plaats van de leds op de lezer. In dat geval kiest u "Ja (met leds)". Bij de selectie "Ja (zonder leds)" worden de leds van de lezer aangestuurd.

Intrekcontrole

Bij een aanwezig, gemotoriseerd intreksysteem wordt hier vastgelegd of de kaart na het lezen weer wordt teruggegeven of onder welke voorwaarden deze dient te worden ingetrokken.



The screenshot shows the 'Instellingen' (Settings) window for a CESTronics device. The 'Kaartinzameling' (Card Collection) dialog box is open, allowing configuration of card return settings.

Instellingen (Settings):

- Module adres: 1
- Serienummer: 17498478
- Adresse: 1
- Gid / Did:
- Firmware: MRS_0292.BIN
- Protocol:
- Gebied ingang: Unbekannt
- Gebied uitga:
- Externe refer:
- Opties:
- Lezer kan sch:
- Slider contro:
- Datum batterijstatus:
- Antipassback groep:
- Keyboard beschikbaar:
- Display beschikbaar:
- Met slider: Ja (met LED's)
- Batterijstatus: Onbekend

Kaartinzameling (Card Collection):

Kaart ingehouden wanneer...

- ☐ altijd
- ☐ Kaart onbekend
- ☐ Kaart verlopen
- ☐ handmatig vergrendeld
- ☐ geblokkeerd vanwege ongeldige PIN
- ☐ Bezoeker kaart
- ☐ geen toegangsautorisatie
- ☐ Toegang geweigerd, buiten de gebruikende time model
- ☐ Verkeerde kaart versie

Buttons: Van toepassing zij, Annuleren

8.1.4.3 Parameter P

Door stamgegevens
Lezer
Parameter P
Parameter I
Parameter O

Deurnaam:
CES Terminal

Algemene parameters

Parameter	Richting	Waarde
Opties	Ingang	0
Bumperkieven	Ingang	Nee
Willekeurig generator rate	Ingang	0
Antipassback tijd	Ingang	0
Area controle	Ingang	0
Companion vereist	Ingang	Nee
Toegang in groep	Ingang	
Gebruik teller	Ingang	Nee
Negeer offline schrijffouten	Ingang	Nee
Altijd update offline data	Ingang	Ja
Pincode vereist	Ingang	Nee
Pulse tijd bewapenen	Ingang	0
Automatische inschakeling	Ingang	0
Genereer tijdregistratie bericht	Ingang	0
Tijd voor persalarm	Ingang	0
Bedreiging alarmknop	Ingang	0

Dit tabblad bevat de parameters die gaan over de afloopbesturing van de deur. Afhankelijk van de complexiteit van het gekozen deurtje worden op deze pagina meer of minder parameters vermeld. Hierna wordt als voorbeeld de standaarddeur met één doorgangsrichting bekeken. Bij deuren die vanaf beide richtingen toegankelijk zijn, zijn de parameters telkens beschikbaar voor de ingangs- en uitgangsrichting.

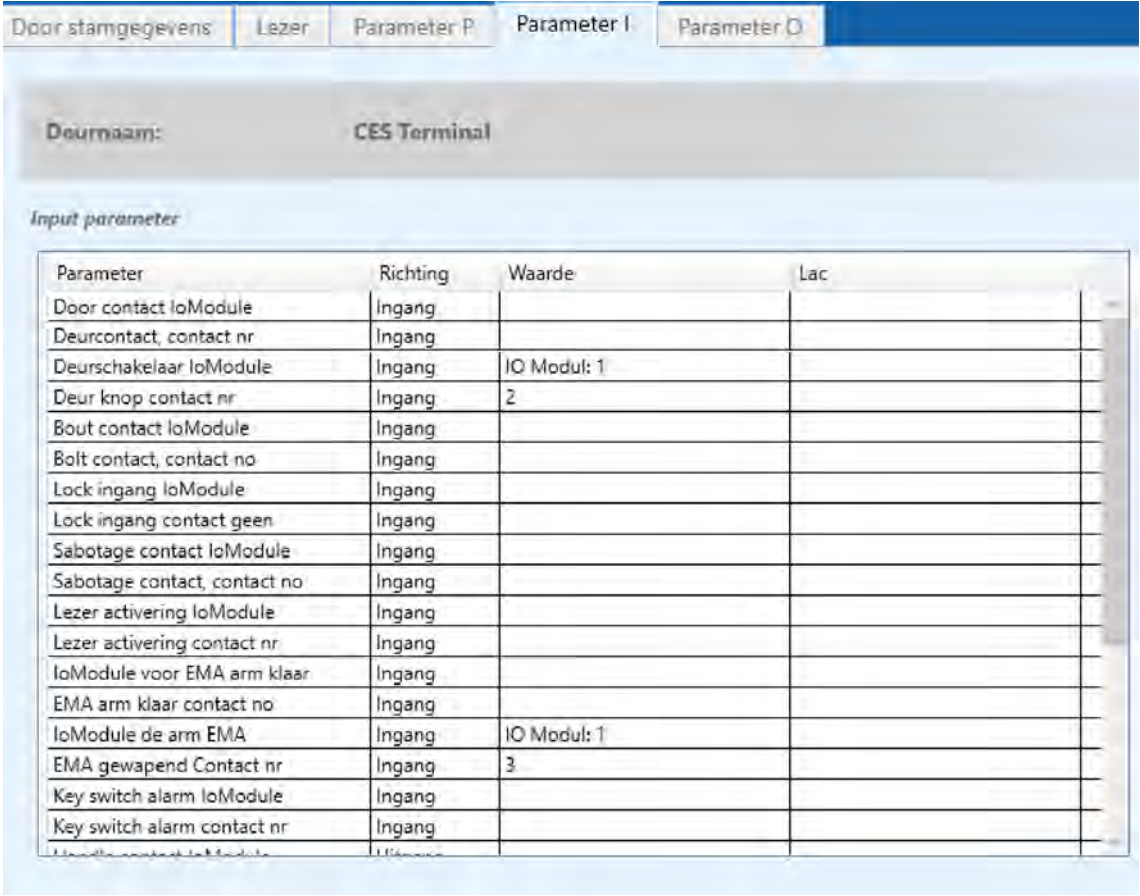
Opties	Opties worden gebruikt om klantspecifieke, speciale behandelingen mogelijk te maken. Bij elk deurtje zorgt Waarde 1 ervoor dat bij deze deur het tijdmodel voor het toegangsrecht wordt genegeerd. Een nuttige toepassing daarvoor is bijvoorbeeld de uitgangslezer. Voorbeeld: een persoon dient na 17.00 uur het gebouw niet meer te betreden, maar wel nog te kunnen verlaten. Een ingangsslezer zou de persoon na 17.00 uur weigeren met de melding "Niet geautoriseerd, buiten het geldige tijdmodel". De uitgangslezer controleert met de ingestelde optie 1 alleen of voor deze lezer een toegangsrecht bestaat en negeert het tijdmodel.
Isolatie	Hier wordt vastgelegd of de besturing vereist dat na elke geautoriseerde toegang de deur eerst weer moet worden gesloten, voordat de volgende kaart wordt geaccepteerd.

Generator van willekeurige getallen in %	Wanneer wordt gewenst dat een tassencontrole toevallig dient te worden uitgevoerd, kan hier via een waarde tussen 0 en 100 het percentage worden ingesteld. De software maakt gebruik van een generator van willekeurige getallen. Voorbeeld: een waarde van 50 betekent dat bij 100 doorgangen precies 50 personen worden afgewezen met de melding "Bevoegd tot controle". Daarna wordt een blokkering voor deze persoon ingesteld, die na de controle door het veiligheidspersoneel weer moet worden gewist. De blokkering zorgt ervoor dat toegang ook bij andere toegangen wordt geweigerd.
Antipassback-tijd	Hoelang een kaart na gebruik op lezers van dezelfde antipassback-groep is geblokkeerd (tijd in seconden).
Gebiedscontrole	De verblijfslocatie (= gebied) van een persoon wordt door AccessOne bij elk gebruik van een kaart op een lezer meegenomen. Daarom kan de deurbesturing ook controleren of de persoon die zojuist zijn kaart voor de lezer heeft gehouden, eigenlijk wel in hetzelfde gebied is aangemeld als waar deze lezer is geplaatst. Als dat niet het geval is, is de persoon zonder de kaart bij een lezer te gebruiken door een open deur gegaan, of werd de kaart onttrokken. Als de gebiedscontrole is ingeschakeld, kan een deur alleen dan worden gepasseerd, wanneer de verblijfslocatie overeenkomt met de locatie van de ID-kaartlezer. De voorwaarde daarvoor is een schone scheiding van de toegangsgebieden en een voortdurende in- en uitgangscontrole via het toegangscontrolesysteem.
Begeleider vereist	Bezoekers mogen bepaalde gebieden niet betreden zonder begeleiding. De deurbesturing gedraagt zich zo dat na het herkennen van een bezoekerskaart gedurende maximaal 10 seconden wordt gewacht op een tweede kaart die een eigen personeels-ID moet zijn. Pas wanneer dat is gebeurd en de begeleidende persoon het toegangsrecht heeft dat voor deze deur noodzakelijk is, wordt de deur vrijgegeven. Tijdens de wachttijd knippert de groene led op de lezer om te signaleren dat er weliswaar een toegangsrecht beschikbaar is, maar dat er nog een kaart wordt verwacht.
Toegang in groep	Wanneer het is vereist dat er verschillende personen nodig zijn om een gebied te mogen betreden, kan dat worden ingesteld via deze parameter. Als bijvoorbeeld waarde 3 wordt ingevoerd, moeten minstens drie kaarten van verschillende geautoriseerde personen na elkaar voor de lezer worden gehouden voordat de deur wordt vrijgegeven.
Gebruiksteller	In AccessOne kan een kaart worden aangemaakt met een maximaal gebruik. Als deze waarde bij de kaart op waarde 1 wordt ingesteld, is dit vergelijkbaar met een eenmalig bruikbare entreekaart. Elke lezer die deze parameter heeft ingesteld, controleert of het maximale gebruik bij de kaart nog groter is dan nul. Indien ja, en wanneer de persoon het noodzakelijke toegangsrecht heeft, wordt de deur vrijgegeven en telt het gebruik af. Als de teller bij nul is gearriveerd, wordt er geen deur meer geopend, waarbij deze parameter ook is ingesteld. Als deze parameter op de lezer van de gebouwingang wordt ingesteld, wordt bereikt dat de bezoeker het gebouw precies één keer mag betreden. Binnen het gebouw wordt de teller niet gecontroleerd en wordt de bezoeker hier niet beperkt.

Offline-schrijffout negeren	Deze parameter is alleen nuttig bij een beschikbaar offline-sluitsysteem en stuurt of een toegang ook dient te worden vrijgegeven wanneer het schrijven van het toegangsrecht voor de offlinedeuren zonder fout is uitgevoerd. In een normale situatie gaat de deur alleen open wanneer de kaarteigenaar zijn kaart zo lang voor de lezer heeft gehouden dat deze succesvol kon worden beschreven.
Offline gegevens altijd actualiseren	Om te veel schrijfprocessen te vermijden, actualiseert de deurbesturing de kaart alleen wanneer ten minste de helft van de geldigheidsperiode is verstreken. Deze actualisering vindt echter alleen plaats bij offline-sluitsystemen.
Pincode vereist	Deze waarde legt vast of een pincode moet worden ingevoerd voor de toegang. Voorwaarde daarvoor is dat de lezer een toetsenbord heeft.

8.1.4.4 Parameter I

Op deze pagina worden de ingangssignalen (inputs) vastgelegd, wat wil zeggen met welke ingang op de betreffende IO-board de terugmeldcontacten van de aangesloten randapparatuur zijn verbonden.



Parameter	Richting	Waarde	Lac
Door contact IoModule	Ingang		
Deurcontact, contact nr	Ingang		
Deurschakelaar IoModule	Ingang	IO Modul: 1	
Deur knop contact nr	Ingang	2	
Bout contact IoModule	Ingang		
Bolt contact, contact no	Ingang		
Lock ingang IoModule	Ingang		
Lock ingang contact geen	Ingang		
Sabotage contact IoModule	Ingang		
Sabotage contact, contact no	Ingang		
Lezer activering IoModule	Ingang		
Lezer activering contact nr	Ingang		
IoModule voor EMA arm klaar	Ingang		
EMA arm klaar contact no	Ingang		
IoModule de arm EMA	Ingang	IO Modul: 1	
EMA gewapend Contact nr	Ingang	3	
Key switch alarm IoModule	Ingang		
Key switch alarm contact nr	Ingang		

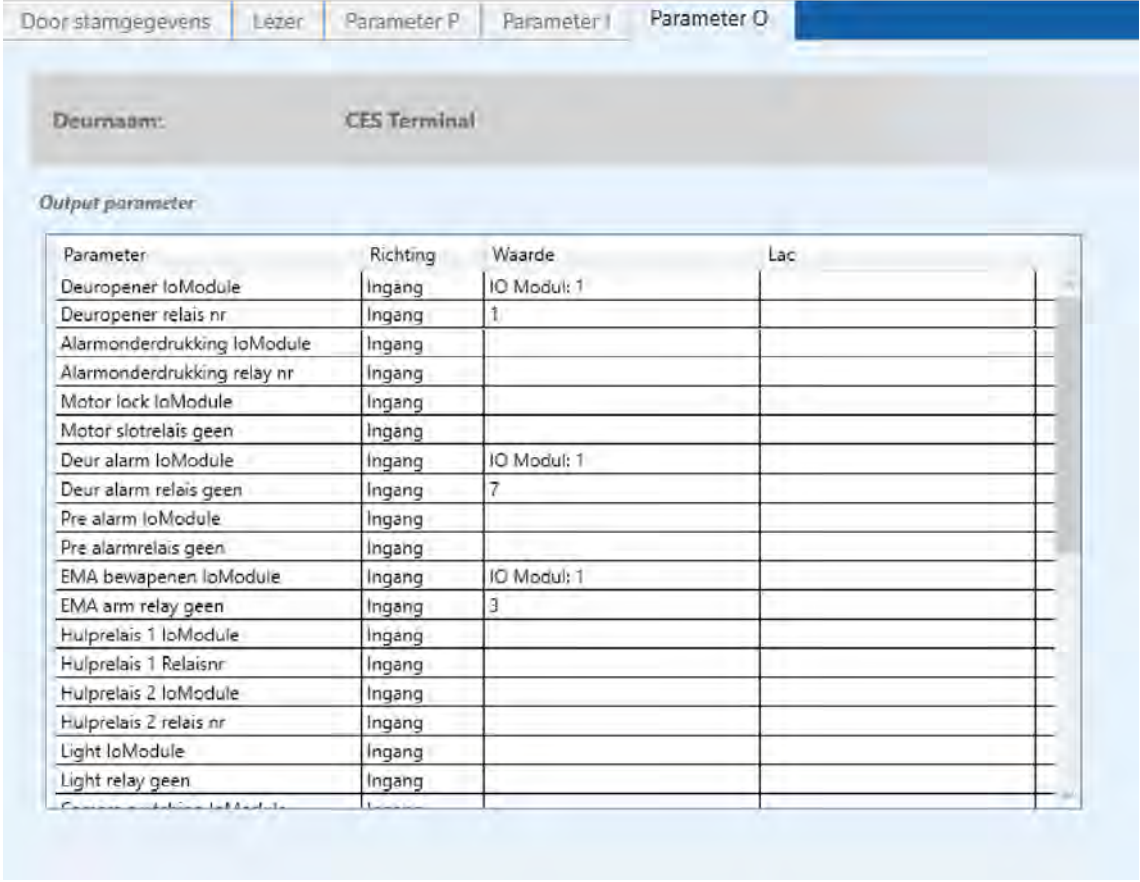
De betekenis van de individuele ingangssignalen, onafhankelijk van het deurtype:

Door contact IoModule	IO-module waarop het deurcontact is aangesloten (input).
Deurcontact, contact nr.	Nummer van het contact op deze module.
Deurschakelaar IoModule	IO-module waarop het contact Request to Exit (handmatige vrijgave) is aangesloten.
Bout contact IoModule	Een aanvullend signaal dat aangeeft of de deur niet alleen is gesloten, maar dat ook de grendel is uitgeschoven.
Lock ingang IoModule	IO-module waarop het contact is aangesloten voor het blokkeren van de doorgang.
Sabotage contact IoModule	Als dit signaal wordt herkend, wordt een sabotagemelding gegenereerd en wordt het sabotagerelais ingesteld.
Toegang in groep	Wanneer het is vereist dat er verschillende personen nodig zijn om een gebied te mogen betreden, kan dat worden ingesteld via deze parameter. Als bijvoorbeeld waarde 3 wordt ingevoerd, moeten minstens drie kaarten van verschillende geautoriseerde personen na elkaar voor de lezer worden gehouden voordat de deur wordt vrijgegeven.
Lezer activering IoModule	IO-module waarop het luscontact/lichtrelais is aangesloten.
IoModule voor EMA arm klaar	IO-module waarop het contact "Alarmsysteem gereed" is aangesloten.

IoModule de arm EMA	IO-module waarop het contact "Alarmsysteem actief" is aangesloten.
Key switch alarm IoModule	IO-module waarop het (sleutel-)contact "Alarmsysteem op actief zetten" is aangesloten.
Handle contact IoModule	Wordt in werking gesteld wanneer bij een deur vanaf de binnenzijde, die geen ID-kaartlezer heeft, de hendel (deurklink) wordt bediend. Daardoor wordt een inbraakmelding bij het openen met de hendel vermeden.
Key contact IoModule	Op dezelfde manier als bij het hendelcontact bekend een ingesteld signaal dat de deur wordt geopend met een sleutel.

8.1.4.5 Parameter O

Op deze pagina worden de uitgangssignalen (outputs) vastgelegd, wat wil zeggen met welke relaisuitgang op de betreffende IO-board de actuatoren van de aangesloten randapparatuur zijn verbonden.



Parameter	Richting	Waarde	Lac
Deuropener IoModule	Ingang	IO Modul: 1	
Deuropener relais nr	Ingang	1	
Alarmonderdrukking IoModule	Ingang		
Alarmonderdrukking relay nr	Ingang		
Motor lock IoModule	Ingang		
Motor slotrelais geen	Ingang		
Deur alarm IoModule	Ingang	IO Modul: 1	
Deur alarm relais geen	Ingang	7	
Pre alarm IoModule	Ingang		
Pre alarmrelais geen	Ingang		
EMA bewapenen IoModule	Ingang	IO Modul: 1	
EMA arm relay geen	Ingang	3	
Hulprelais 1 IoModule	Ingang		
Hulprelais 1 Relaisnr	Ingang		
Hulprelais 2 IoModule	Ingang		
Hulprelais 2 relais nr	Ingang		
Light IoModule	Ingang		
Light relay geen	Ingang		

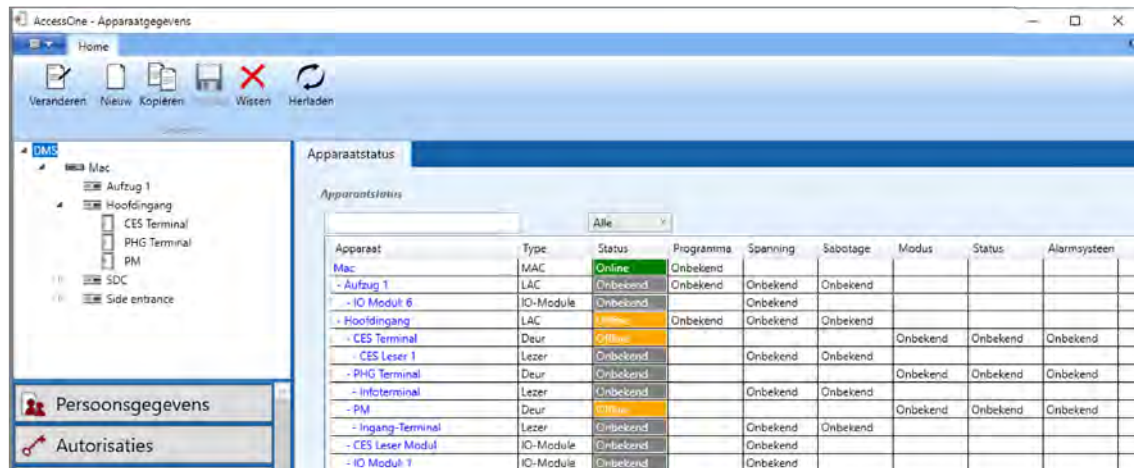
De betekenis van de individuele uitgangssignalen:

Deuropener IoModule	IO-module waarop het deuropenerrelais is aangesloten (output).
Alarmonderdrukking IoModule	IO-module waarop het relais voor de alarmonderdrukking is aangesloten (output).
Motor lock IoModule	Bij automatisch vergrendelende deuren moet naast de deuropener ook het motorslot worden aangestuurd om de grendel in te schuiven. Dit uitgangssignaal kan worden gecombineerd met een tijdmodel. Als de deur in de toestand "Permanent open" staat, wordt dit signaal permanent ingesteld.
Deur alarm IoModule	Uitgangssignaal voor de EMA. Wordt altijd ingesteld wanneer een deur onbevoegd is geopend of te lang is geopend. Het instellen van dit signaal kan worden onderdrukt via parameters.
Pre alarm IoModule	Als voor een deur een vooralarmtijd is ingevoerd, wordt na de deuropening en het verstrijken van de ingestelde tijd dit signaal ingesteld.
EMA bewapenen IoModule	IO-module waarop het relais voor het activeren van het alarmsysteem is aangesloten (output).
Hulprelais 1 IoModule	IO-module waarop het relais voor Speciale functie 1 is aangesloten (output).

Hulprelais 2 IoModule

IO-module waarop het relais voor Speciale functie 2 is aangesloten (output).

8.1.5 Apparaatstatus weergeven



Klik met de linkermuisknop op "DMS" in de structuurboom wanneer u de status van alle apparaten wilt bekijken in het overzicht. De status van een individueel apparaat (online of offline) ziet u in de detailweergave van het apparaat. U kunt deze vermelding niet wissen en ook geen tweede aanmaken.

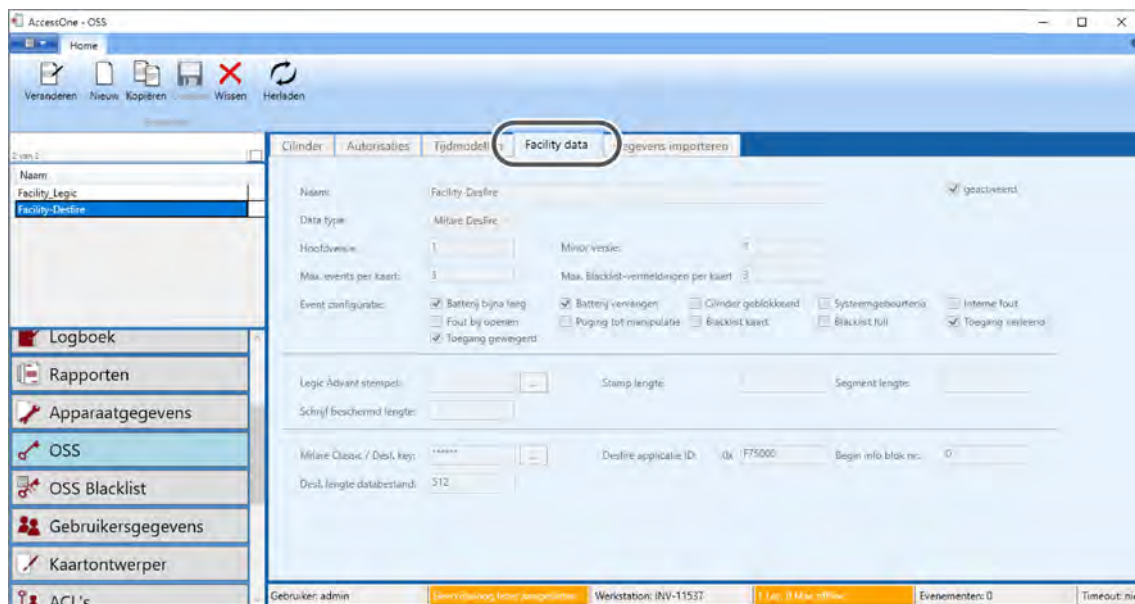
Door met de rechtermuisknop te klikken op "DMS", verschijnt er een verdere selectiemogelijkheid. Hier kan een nieuwe MAC, een nieuwe EMC of een nieuwe PS-online (sleutelkast) worden aangemaakt.

8.2 Apparaatgegevens offline-apparaten (OSS-SO)

Voor elke installatie van OSS Standard Offline moeten facility data worden aangemaakt. Hier worden de basisgegevens voor de offline-apparaten ingevoerd, zoals cilinders en beslag. Via deze gegevens wordt onder andere vastgelegd hoe groot het geheugen voor de offline-gegevens op de transponder is en hoeveel ruimte voor gebeurtenissen en meldingen op blokkeringslijsten dient te worden gereserveerd. Bij Mifare bevatten de facility data de toegangssleutel voor de offline-segmenten van de kaart en de applicatie-ID, bij LEGIC wordt hier de stempel geregistreerd.

8.2.1 Facility data

De facility data zijn meestal door CES vooraf geïnstalleerd. Deze kunnen echter ook door de gebruiker worden ingevoerd of gewijzigd. Er is één gegevensrecord per systeem. Klik in de taakbalk op Nieuw om een nieuwe melding aan te maken.



Geef deze een naam en kies het gegevenstype. Voer de hoofd- en nevenversienummers in (bijvoorbeeld de cijfers 1 en 0 voor versie 1.0). Het versienummer is noodzakelijk als onderscheidend kenmerk.

In het gebied "Gebeurtenisconfiguratie" wordt ingesteld welke gebeurtenissen door de cilinder naar de kaart dienen te worden teruggeschreven. Deze instellingen gelden voor het volledige systeem. Deze worden dus op de updater voor alle transponders op dezelfde manier geschreven.

Voor een LEGIC advant-systeem voert u de stempel en de stempellengte in. Klik voor het invoeren van de stempel op de knop achter het invoerveld. Zowel de stempel als de sleutel worden doorgaans in een hexadecimale notatie opgegeven, wat wil zeggen dat getallen van 0 tot 9 en letters van A tot F zijn toegelaten. In totaal moet de sleutelwaarde voor Mifare DESFire een lengte hebben van 32 posities (Mifare Classic 12 posities).



De toegangssleutels worden versleuteld gearchiveerd in de databank. Eenmaal ingevoerd, wordt deze waarde om veiligheidsredenen nooit (!) meer in gewone tekst weergegeven. Er kan alleen een nieuwe waarde worden opgegeven.

Klik op OPSLAAN in de taakbalk wanneer de gegevens volledig zijn.



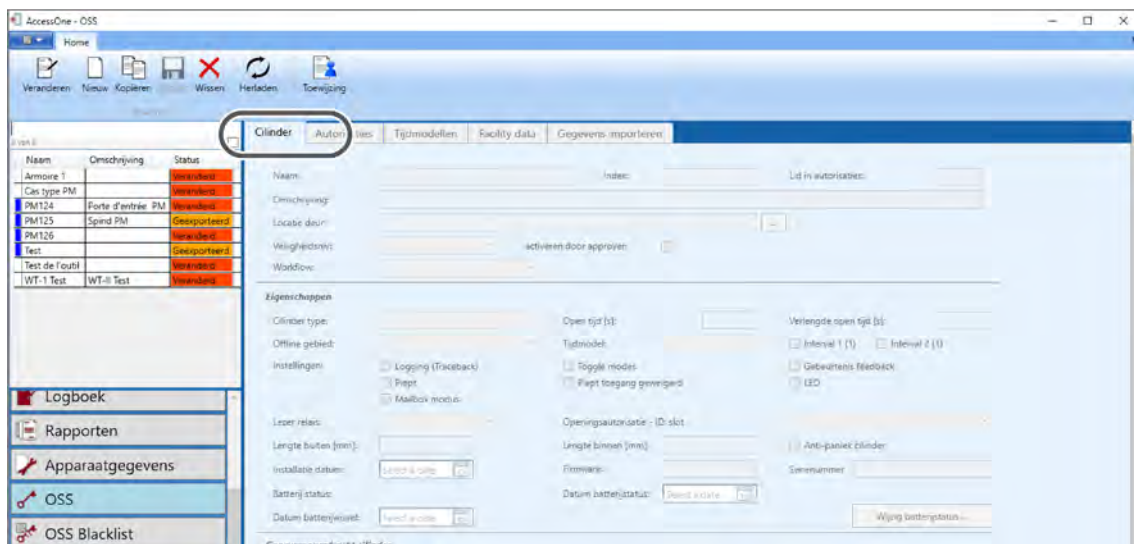
Wanneer u de sleutel wijzigt, wordt deze wijziging onmiddellijk actief. Dat kan betekenen dat vanaf dat moment geen transponder meer kan worden geactualiseerd.

8.2.2 Cilinders (en beslag)

Op dit tabblad worden de offline-componenten aangemaakt. Klik in de taakbalk op NIEUW en voer de gegevens voor de cilinder in.



Geef in het veld "Omschrijving" de precieze inbouwlocatie op. Offline-systemen die werken op batterijen en als standaard offline-componenten, zijn in staat om de batterijstatus naar de transponder terug te schrijven wanneer de batterij een bepaalde spanningswaarde niet bereikt. Voor het vervangen van een bijna lege batterij moet de inbouwlocatie bekend zijn.



De cilinders en het beslag worden via de nummers eenduidig onderscheiden. AccessOne verstrekt de nummers bij het aanmaken en opslaan van een nieuwe cilinder automatisch (weergave in het veld "Index").

Gebied "Eigenschappen"

Geef meer gegevens op over het ingebouwde apparaat.

Cilindertype

Selectie tussen cilinder, beslag en wandlezer. De apparaten kunnen verschillende batterijen nodig hebben.

Openingstijd

Geeft aan hoelang de cilinder bij een geautoriseerde toegang ontgrendeld blijft. Een waarde van 5 tot 10 seconden is over het algemeen voldoende (standaardinstelling: 5).

Verlengde openingstijd

Voor bepaalde personengroepen kan de standaardopeningstijd worden verlengd.

Offline-gebied

Het offline-gebiedsnummer (Site-ID) moet altijd worden opgegeven bij Standaard offline. Een 0 is hier niet toegelaten. Onder het gebiedsnummer kan een systeem in verschillende gebieden worden verdeeld. In dat geval bestaat de cilinder met nummer 1 verschillende keren, namelijk één keer voor elk gebied. Dat betekent dat het cilindernummer alleen eenduidig is in combinatie met het gebiedsnummer. Als er van het ene naar het andere gebied wordt overgeschakeld, wist de updater de gegevens van het vorige gebied en vervangt deze door die van het actuele gebied. Door het verdelen in verschillende gebieden kan het aantal offline-sluitapparaten in een systeem willekeurig groot worden.

Tijdmodel

Selectiemogelijkheden voor het tijdmodel. De functie is afhankelijk van het apparaattype en de fabrikant.

Intervallen 1 en 2

De functie is afhankelijk van het apparaattype en de fabrikant.

Instellingen

De instelmogelijkheden zijn afhankelijk van het apparaattype en de fabrikant.

Lezerrelais

De functie is afhankelijk van het apparaattype en de fabrikant.

Paniekcilinder

Aanduiding van het apparaattype.

Lengte

Gegevens over lengte binnenzijde en buitenzijde.

Serienummer

Opgave van het serienummer.

Batterijstatus

In het veld "Batterijstatus" wordt weergegeven of een offline-apparaat een bijna lege batterij heeft gemeld. Het veld Batterijstatusdatum geeft weer wanneer deze melding werd gegenereerd. Als de batterij wordt vervangen, genereert het offline-apparaat bij de volgende boeking een melding "Batterij vervangen" die via de key-card terugkomt in het systeem en waardoor de gegevens dienovereenkomstig worden geactualiseerd. Via het rapport "Reader batterijstatus" kan te allen tijde een lijst worden gegenereerd met apparaten met een bijna lege batterij.

Vervolgens draagt u de gegevens over via de knop **Overdragen**.

8.2.3 Offline-apparaten programmeren

De gegevens worden direct vanuit het tabblad op de offline-apparaten geprogrammeerd. Daarvoor is het volgende

nodig:

- RF-Stick
- Systeemmaster
- RF-Stick-Master

Procedure:

1. Steek de RF-Stick in de pc.
2. Klik op OVERDRAGEN.
3. Lees de A-licentie in AccessOne in (eenmalig proces bij het eerste apparaat dat wordt geprogrammeerd).
4. Houd de RF-Stick-Master vóór het apparaat.

8.2.4 Toegangsrechten

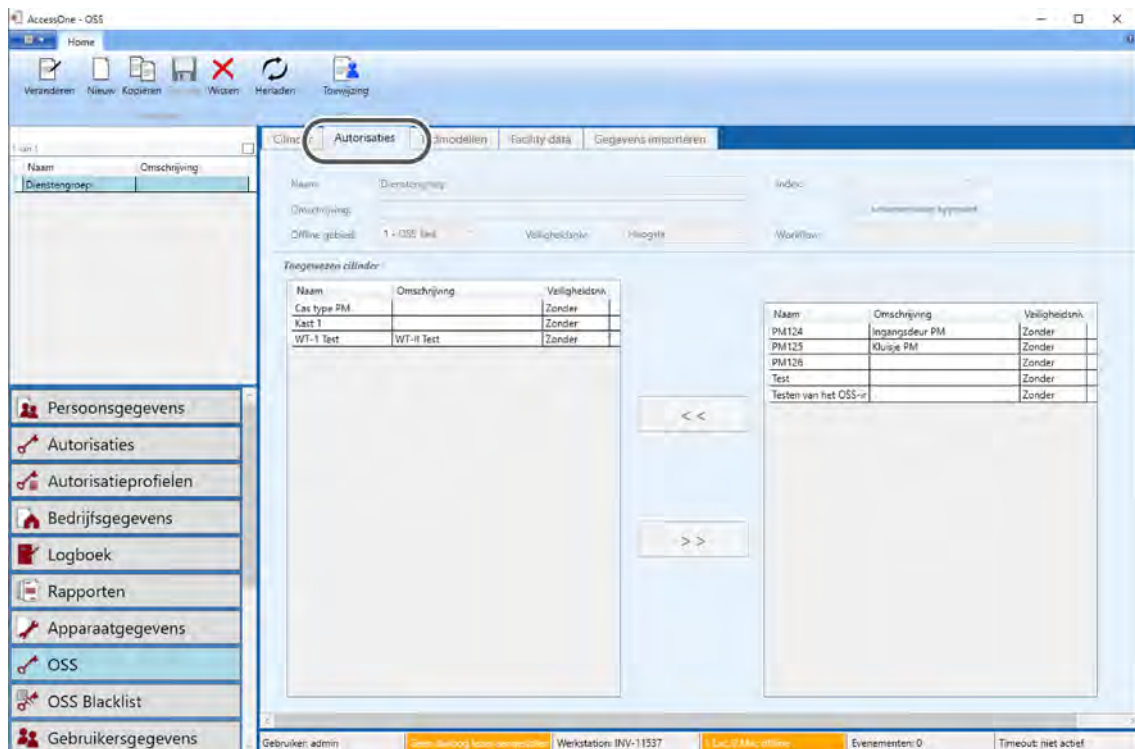
Voeg verschillende deuren samen tot één deurgroep.



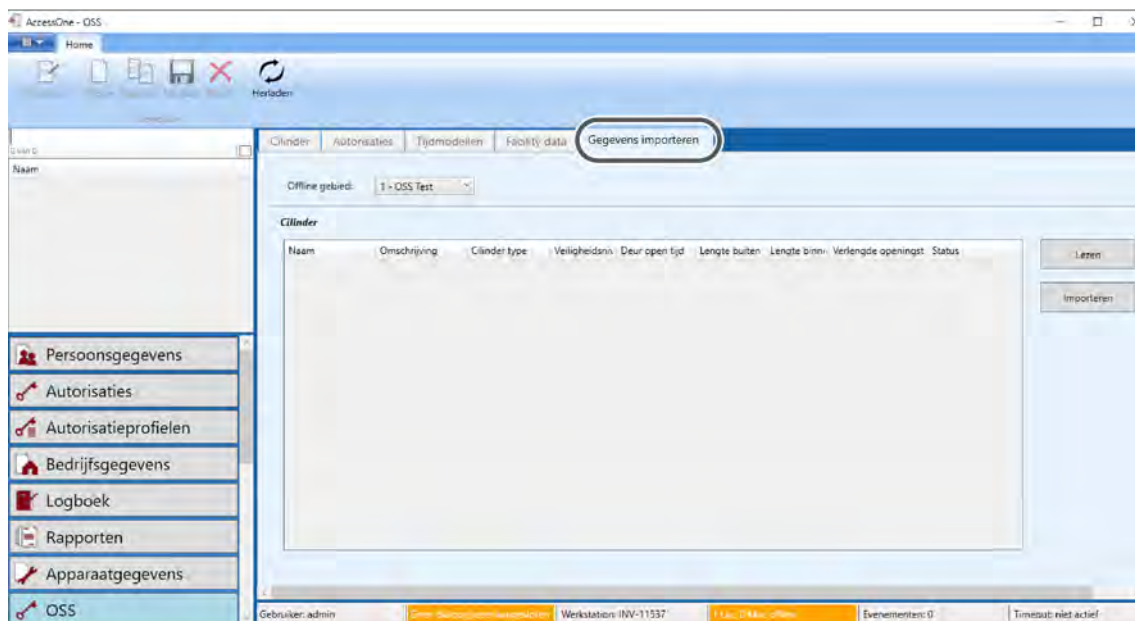
Wanneer u een nieuwe toegangsrecht aan een cilinder toewijst, moet u deze gegevens ook naar het offline-apparaat overdragen.



Toegangsrechten dienen zo te worden vormgegeven dat deze alleen ruimten met hetzelfde veiligheidsniveau samenvoegen. Wanneer er in een ruimte of gang verschillende toegangen zijn, dan dienen de overeenkomstige cilinders te worden samengevoegd in één toegangsrecht. Via de toegangsrechtprofielen voegt u dan de deurgroepen op basis van het gebruikersprofiel samen.



8.2.5 Gegevens importeren

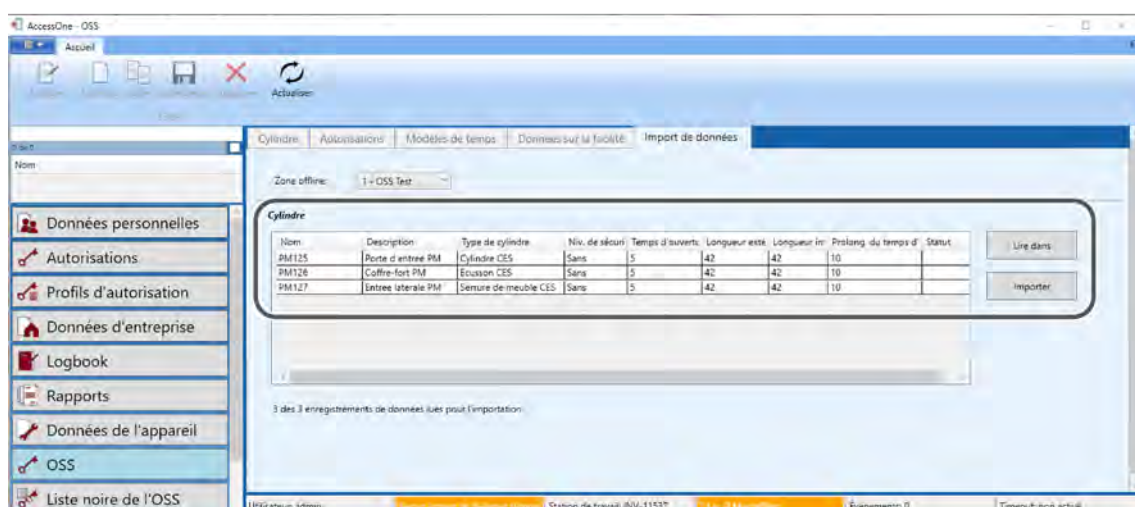


Maakt de import van een *.csv-deurenlijst mogelijk. Kies het offline-gebied en klik op **Lezen**. Kies de betreffende deurenlijst uit de directorymap.



De deurenlijst wordt doorgaans aangemaakt door CES bij het configureren van het systeem. De lijst kan ook worden bewerkt door de klant.

Nom	Description	Type de cylindre	Niv. de sécuri	Temps d'ouvert	Longueur exte	Longueur in	Prolong. du temps d'	Status
PM125	Porte d'entree PM	Cylindre CES	Sans	5	42	42	10	
PM126	Coffre-fort PM	Ecusson CES	Sans	5	42	42	10	
PM127	Entree laterale PM	Serrure de meuble CES	Sans	5	42	42	10	

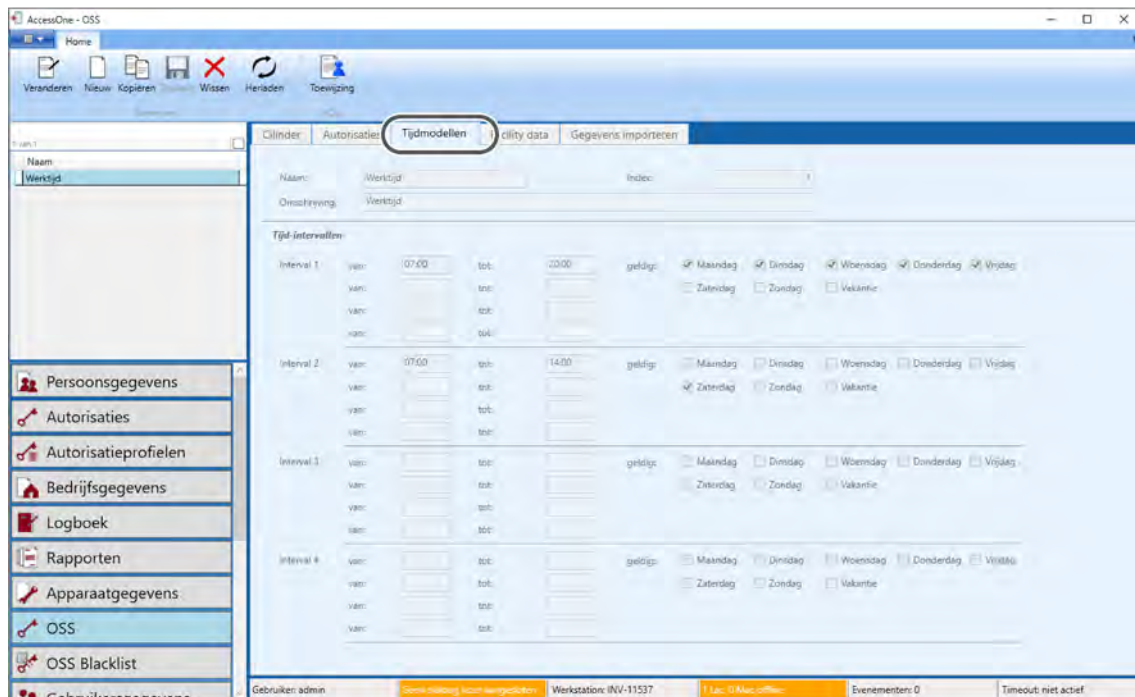


Het ingelezen bestand kan nu in de lijstweergave in het veld "Cilinder" opnieuw worden gecontroleerd. Druk op de knop Importeren om de lijst naar de databank te importeren. De bevestiging gebeurt in het tekstvak onder het veld.

8.2.6 Tijdmodellen

 OSS Standard Offline gebruikt een ander formaat voor de tijdmodellen en is niet zo flexibel voor de onlinecomponenten als AccessOne. Daarom kunnen de onlinetijdmodellen niet algemeen worden gebruikt en hebben de OSS Standard Offline-tijdmodellen een eigen tabblad.

Bij OSS Standard Offline bestaat een tijdmodel uit maximaal vier intervallen. Voor iedere intervalgroep kunnen dagen worden geselecteerd waarop dit geldig is. Als bij een toegangsrecht voor een persoon geen tijdmodel is ingevoerd, dan geldt dit voor de volledige dag.



In het voorbeeld is van maandag tot vrijdag van 7.00 tot 20.00 en op zaterdag van 7.00 tot 14.00 de toegang verleend. Op zon- en feestdagen is er geen toegang mogelijk.

9 Toegangsrechten configureren

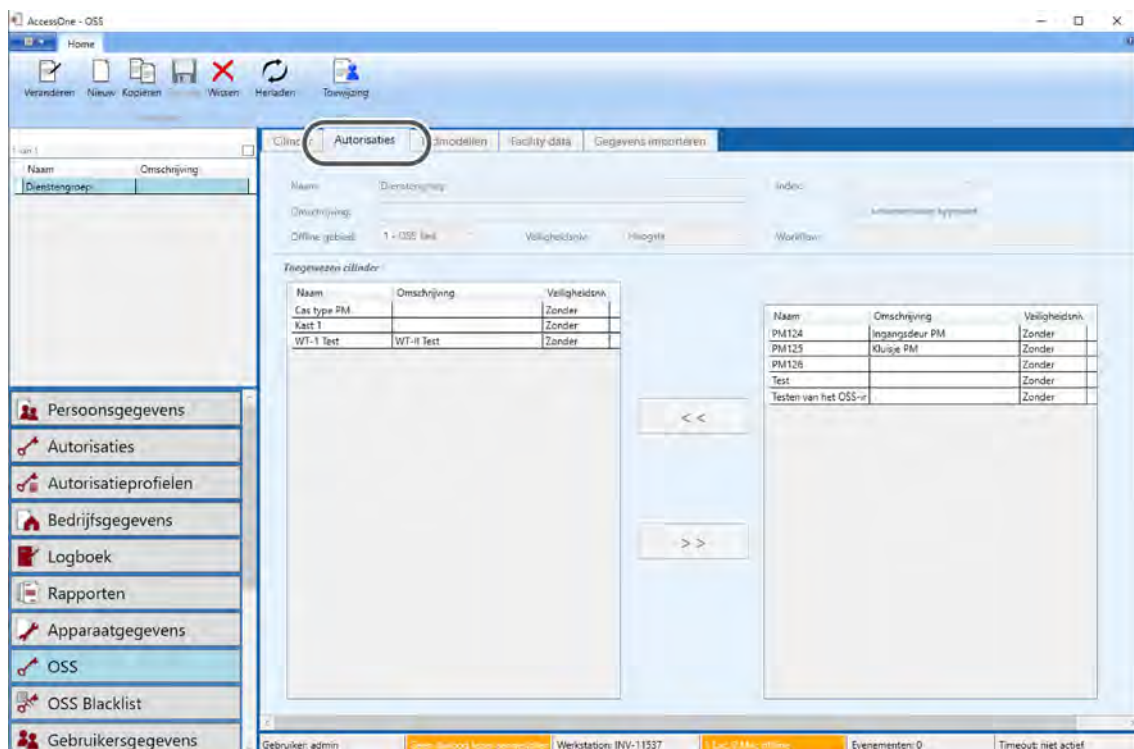
Doelgroep van dit hoofdstuk:

- Voor het product opgeleid personeel

9.1 Toegangsrechten

Configureer eerst de toegangsrechtgroepen voor online- en offline-apparaten. Daarna bepaalt u via de dag- en tijdmodellen verdere beperkingen of deurfuncties (bijvoorbeeld openingsfuncties gedurende bepaalde tijden van de dag) met inachtneming van speciale en feestdagen.

9.1.1 Overzicht van de toegangsrechten



De dialoogselectie "Toegangsrechten" opent in het dialoogvenster verschillende tabbladen.

In het tabblad "Toegangsrechten" kunnen verschillende lezers worden samengevoegd tot een groep. De lezers worden opgeroepen uit de lijst met niet-toegewezen lezers (rechterlijst) en met de knop "<<" toegewezen aan de actuele groep.



Toegangsrechtgroepen bestaan uit samengevoegde toegangsrechten. De toegangsrechten die aan de rechterzijde van het venster zijn aangemaakt (niet toegewezen), kunnen op hun beurt enkele bevoegdheden of groepsbevoegdheden zijn.

9.1.2 Algemene informatie over tijd- en dagmodellen

Tijdmodellen worden in AccessOne op verschillende plaatsen gebruikt.

- Voor beperking van de toegang. Hier kan een tijdmodel persoonsgebonden worden opgeslagen als tijdmodel voor een medewerker. Als bij een toegangsrecht geen eigen tijdmodel is opgegeven, geldt altijd het persoonsgebonden tijdmodel.
- Tijdmodellen worden bij deuren bijvoorbeeld gebruikt om een Permanent open-functie op bepaalde tijden van de dag vast te leggen.

In AccessOne voldoet een tijdmodel aan een weekschema en bestaat uit individuele dagmodellen voor elke afzonderlijke weekdag, of uit aanvullende dagmodellen voor speciale of feestdagen.

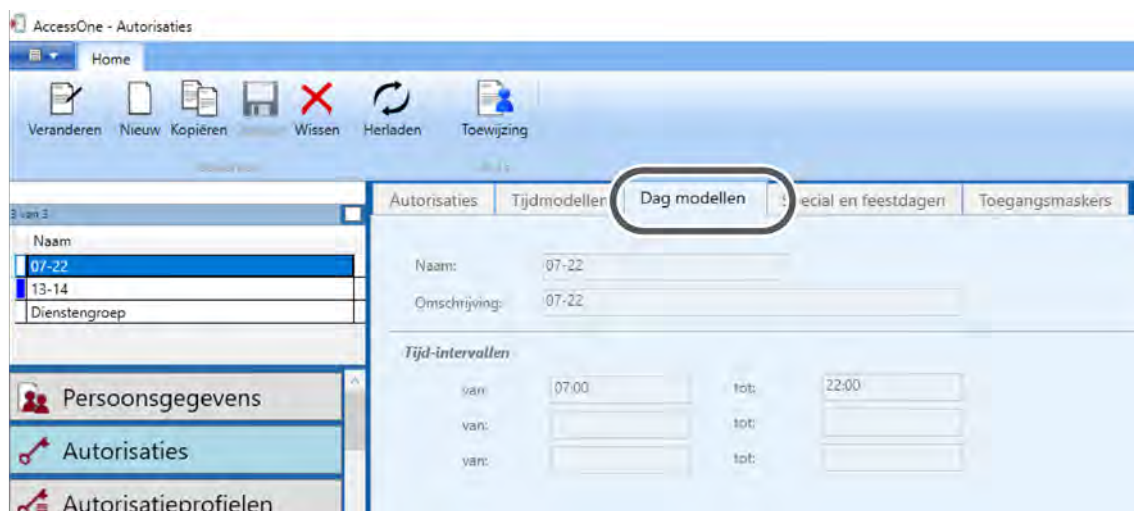


Elk dagmodel kan drie intervallen bevatten en legt de toegangstijden voor precies één dag vast.

Wij adviseren de volgende procedure wanneer u de schema's definieert:

1. Dagmodellen aanmaken
2. Speciale dagen en feestdagen in groepen samenvoegen
3. Tijdmodellen voor deuren aanmaken

9.1.3 Dagmodellen



Klik in de taakbalk op NIEUW. Geef uw dagmodel een naam. Optioneel kunt u een omschrijving toevoegen.

Bij de "Tijd-intervallen" geeft u ten minste 1 op. Deze moet u definiëren met een "van/tot-tijd".

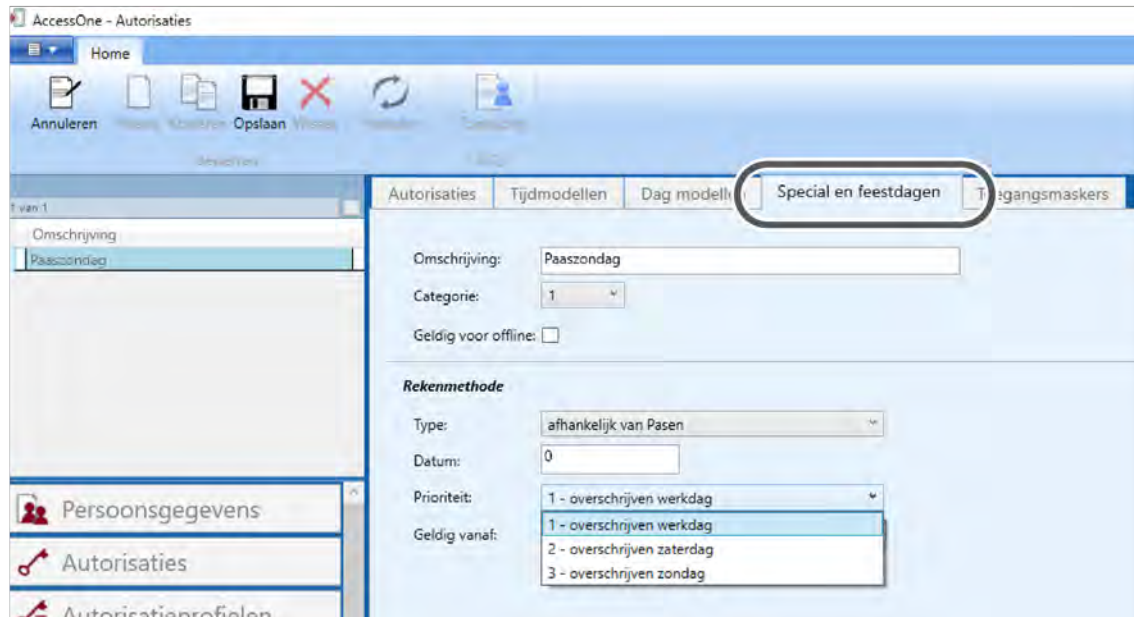
Vervolgens klikt u op OPSLAAN.

TIP Maak ook het tijdmodel "Geen toegang" aan. Het tijdmodel is bijvoorbeeld geschikt voor medewerkers die alleen op bepaalde dagen zijn geautoriseerd en op andere dagen niet. Zo kunnen ook feestdagen eenvoudig in acht worden genomen.

9.1.4 Speciale en feestdagen

Klik op NIEUW en voer een "Benaming" voor uw speciale dag in. De categorieën zijn bestemd om de speciale dagen in groepen samen te voegen en daarmee dan voor een dergelijke groep een dagmodel te kunnen vastleggen.

TIP Voeg de landelijke feestdagen samen in één categorie. Voor deze dagen geldt dan het dagmodel "Geen toegang" (optioneel: geen vermelding in deze categorie functioneert net als een dagmodel met een interval van 0.00 tot 0.00). Door de verdeling van de feestdagen in betreffende categorieën kan worden bereikt dat voor de tijdmodellen de feestdagen van de betreffende provincie in acht worden genomen en de andere worden genegeerd.



Verder omhoog wordt de rekenmethode gekozen:

De gedenk- en feestdagen die het meest veranderen, zijn afhankelijk van de datum van eerste paasdag:

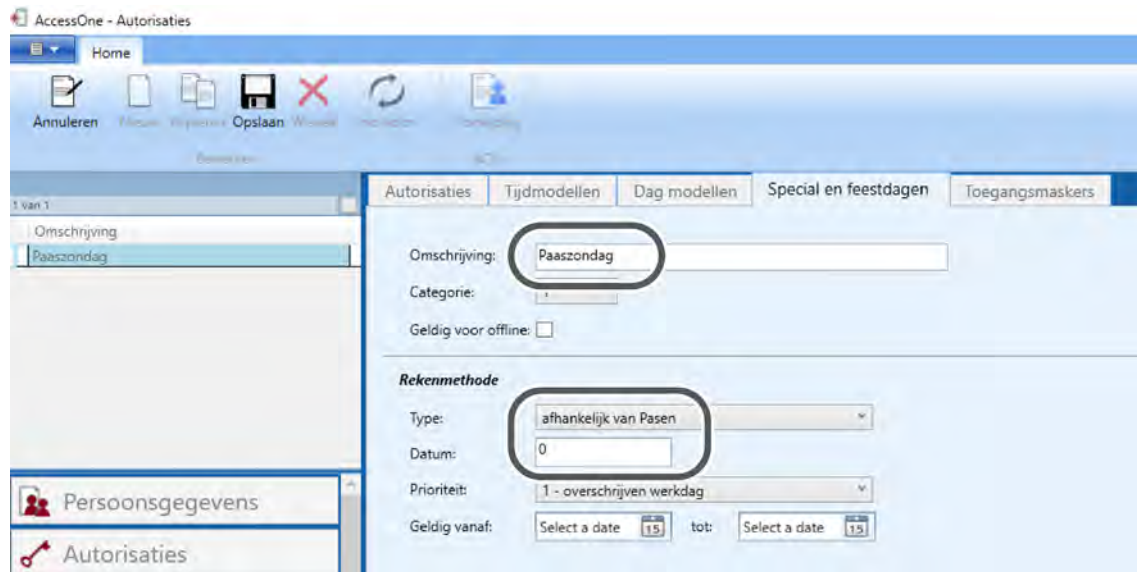
- Aswoensdag = 46 dagen voor Pasen
- Palmzondag = 7 dagen voor Pasen
- Witte Donderdag = 3 dagen voor Pasen
- Goede Vrijdag = 2 dagen voor Pasen
- Tweede paasdag = 1 dag na Pasen
- Hemelvaartsdag = 39 dagen na Pasen (de 40^e dag)
- Eerste pinksterdag = 49 dagen na Pasen (de 50^e dag)

In de katholieke kerk gelden bovendien

- Sacramentsdag = 60 dagen na Pasen
- Heilig Hart van Jezus, 68 dagen na Pasen

De deurbesturing berekent de datum van eerste paasdag automatisch en kan deze van Pasen afhankelijke feestdagen daarom bepalen wanneer deze in het systeem zijn aangemaakt. Bij dagen die afhankelijk van Pasen worden berekend, wordt in het datumveld het aantal dagen ingevoerd dat bij de berekende datum moet worden opgeteld.

In het voorbeeld wordt tweede paasdag (= 1 dag na Pasen) als volgt gedefinieerd:



Als de feestdag vóór Pasen ligt, kan ook een negatieve waarde worden aangegeven. Voorbeeld: voor Goede Vrijdag (2 dagen voor Pasen) is de vermelding "-2".

- Vaste datum

Speciale dagen die elk jaar opnieuw moeten worden aangemaakt, of eenmalige gebeurtenissen zoals bedrijfsjubilea, worden met een vaste datum aangemaakt. Deze gelden dan precies één keer.

- Jaarlijks terugkerend

Er zijn data die jaarlijks als speciale dag of feestdag terugkeren: bijvoorbeeld 1 mei of 24 december. Selecteer hiervoor een datum uit de kalender. Het jaartal wordt dan bij de controle genegeerd.

- Prioriteit/categorie

De prioriteit van een speciale dag bepaalt zijn relevantie. Een normale feestdag heeft prioriteit 1, wat wil zeggen dat wanneer deze op een werkdag valt, niet het dagmodel van deze werkdag geldt, maar het dagmodel van de speciale dag.

Voorbeeld 1: kerstavond is aan categorie 8 toegewezen en voor alle speciale dagen van categorie 8 is in uw tijdmodel een dagmodel van een halve werkdag (07.00 tot 12.00 uur) ingevoerd. Wanneer kerstavond op een maandag zou vallen, zijn de beveiligde gebieden toegankelijk van 7.00 – 12.00 uur. Als kerstavond op een zaterdag of zondag valt, dient er geen toegang te worden verleend. In dat geval dient de prioriteit van kerstavond op 1 te worden ingesteld, omdat zaterdag en zondag een hogere prioriteit hebben.

Voorbeeld 2: voor de inventarisatie in het weekeinde dient aan bepaalde medewerkers toegang te worden verleend. Voor deze speciale dag moet prioriteit 2 of zelfs 3 worden ingesteld, zodat het normale dagmodel van de zaterdag of zondag wordt overschreven.

De volgende tabel biedt een overzicht van de feestdagen in Duitsland:

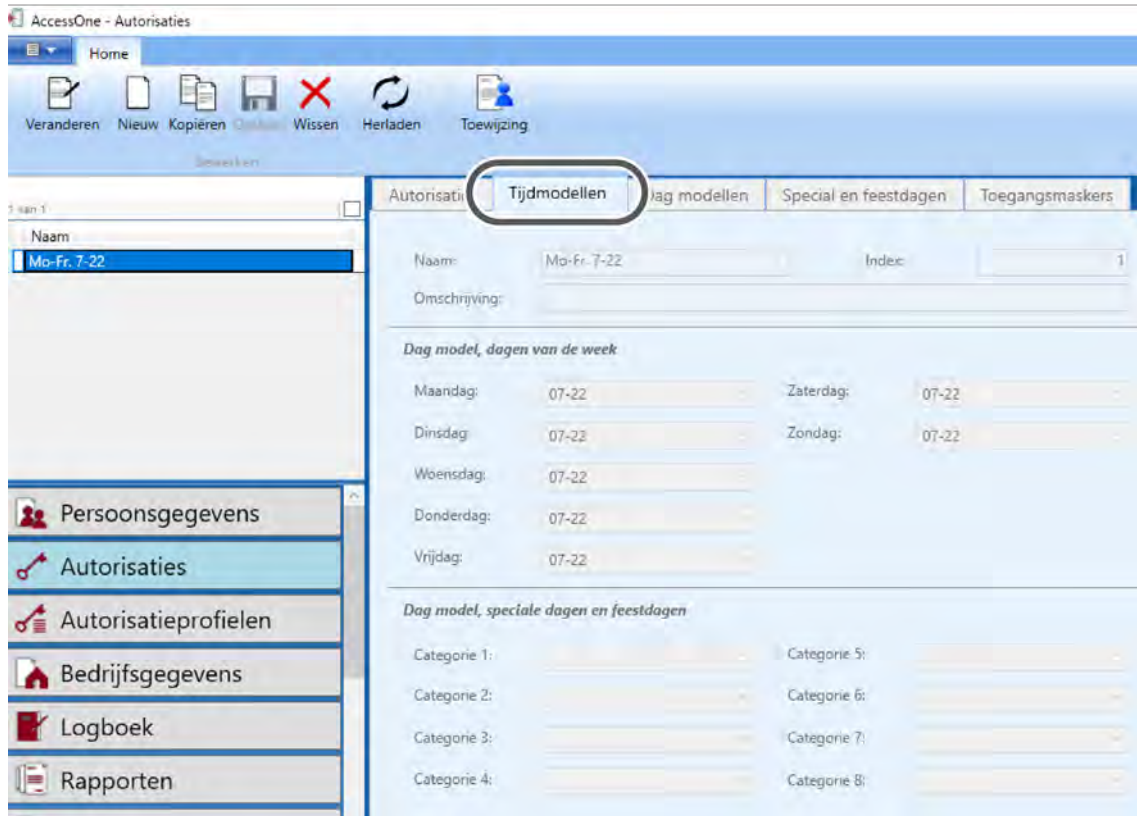
Feestdag	Toepassingsgebied
Nieuwjaar	Landelijk
Driekoningen	Baden-Württemberg, Beieren, Sachsen-Anhalt
Goede Vrijdag	Landelijk
Eerste paasdag	Landelijk
Tweede paasdag	Landelijk
Dag van de Arbeid / 1 mei	Landelijk
Hemelvaartsdag	Landelijk
Eerste pinksterdag	Landelijk
Tweede pinksterdag	Landelijk
Sacramentsdag	Baden-Württemberg, Beieren, Hessen, Noordrijn-Westfalen, Rijnland-Palts, Saarland
Maria-Tenhemelopneming	Beieren (in katholieke gebieden), Saarland
Dag van de Duitse eenheid	Landelijk
Hervormingsdag	Brandenburg, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt, Thüringen
Allerheiligen	Baden-Württemberg, Beieren, Noordrijn-Westfalen, Rijnland-Palts, Saarland
Boete- en biddag	Saksen
1. Kerstmis	Landelijk
2. Kerstmis	Landelijk

Het is raadzaam om de categorieën van de speciale dagen zo te kiezen dat feestdagen die in dezelfde provincie

geldig zijn, ook in dezelfde categorie zitten.

Landelijke feestdagen	Categorie 1
Driekoningen	Categorie 2
Sacramentsdag	Categorie 3
Maria-Tenhemelopneming	Categorie 4
Hervormingsdag	Categorie 5
Allerheiligen	Categorie 6
Boete- en biddag	Categorie 7
Overige speciale dagen categorie 8	Categorie 8

9.1.5 Tijdmodellen



AccessOne - Autorisaties

Home

Veranderen Nieuw Kopiëren Wissen Herladen Toewijzing

1 van 1

Naam

Mo-Fr-7-22

Persoonsgegevens

Autorisaties

Autorisatieprofielen

Bedrijfsgegevens

Logboek

Rapporten

Autorisatie Tijdmodellen Dag modellen Special en feestdagen Toegangsmaskers

Naam: Mo-Fr-7-22 Index: 1

Omschrijving:

Dag model, dagen van de week

Maandag:	07-22	Zaterdag:	07-22
Dinsdag:	07-22	Zondag:	07-22
Woensdag:	07-22		
Donderdag:	07-22		
Vrijdag:	07-22		

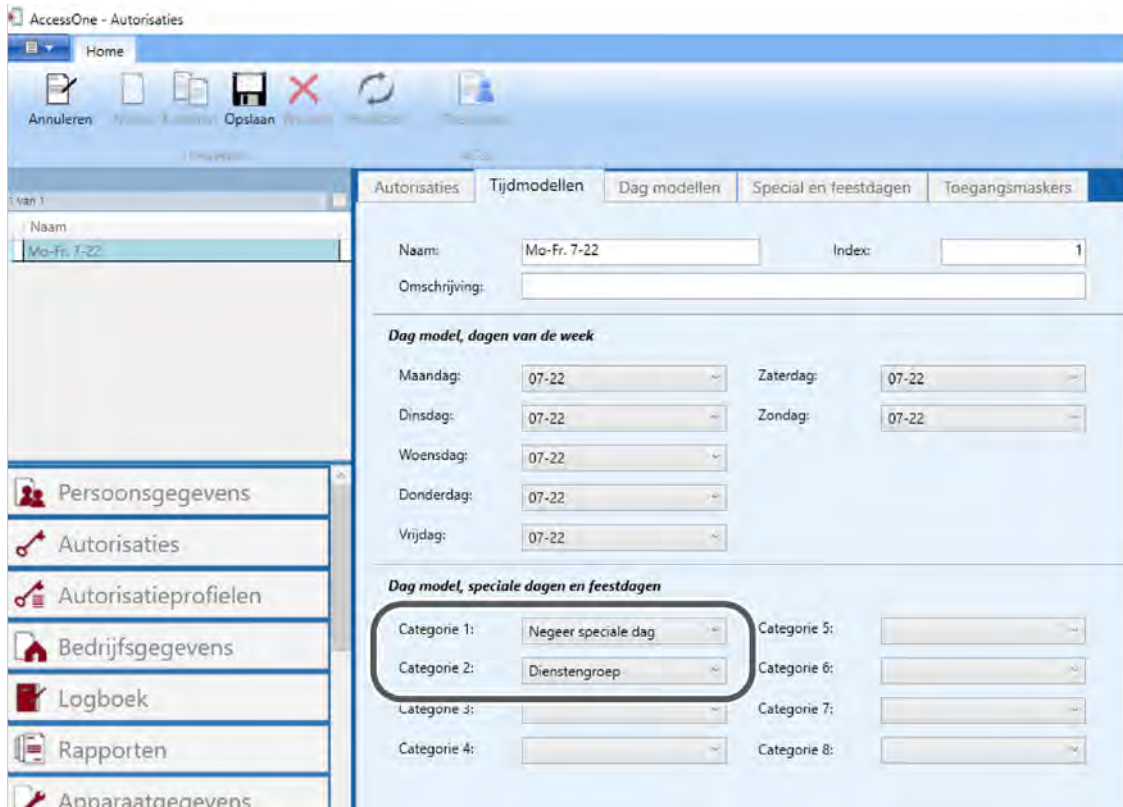
Dag model, speciale dagen en feestdagen

Categorie 1:		Categorie 5:	
Categorie 2:		Categorie 6:	
Categorie 3:		Categorie 7:	
Categorie 4:		Categorie 8:	

Als in het systeem geen speciale dag is opgeslagen, dan wordt op deze datum geen toegang verleend. Klik op NIEUW en voer de betreffende gegevens in. Sla het tijdmodel op. Als u van pagina wisselt zonder op te slaan, dan doet AccessOne dat in dit geval automatisch.

Het invoerveld "Omschrijving" is bestemd voor de toewijzing binnen het eigen bedrijf.

De opgave in het veld "Index" vermeldt een doorlopend controlenummer van in welke volgorde de tijdmodellen zijn aangemaakt.



AccessOne - Autorisaties

Home

Annuleren Nieuw Kopieeren Opslaan Wissen Herladen Toewijzing

Autorisaties Tijdsmodellen Dag modellen Special en feestdagen Toegangsmaskers

Naam: Mo-Fr. 7-22 Index: 1

Omschrijving:

Dag model, dagen van de week

Maandag: 07-22 Zaterdag: 07-22

Dinsdag: 07-22 Zondag: 07-22

Woensdag: 07-22

Donderdag: 07-22

Vrijdag: 07-22

Dag model, speciale dagen en feestdagen

Categorie 1: Negeer speciale dag Categorie 5:

Categorie 2: Dienstengroep Categorie 6:

Categorie 3: Categorie 7:

Categorie 4: Categorie 8:

Persoonsgegevens

Autorisaties

Autorisatieprofielen

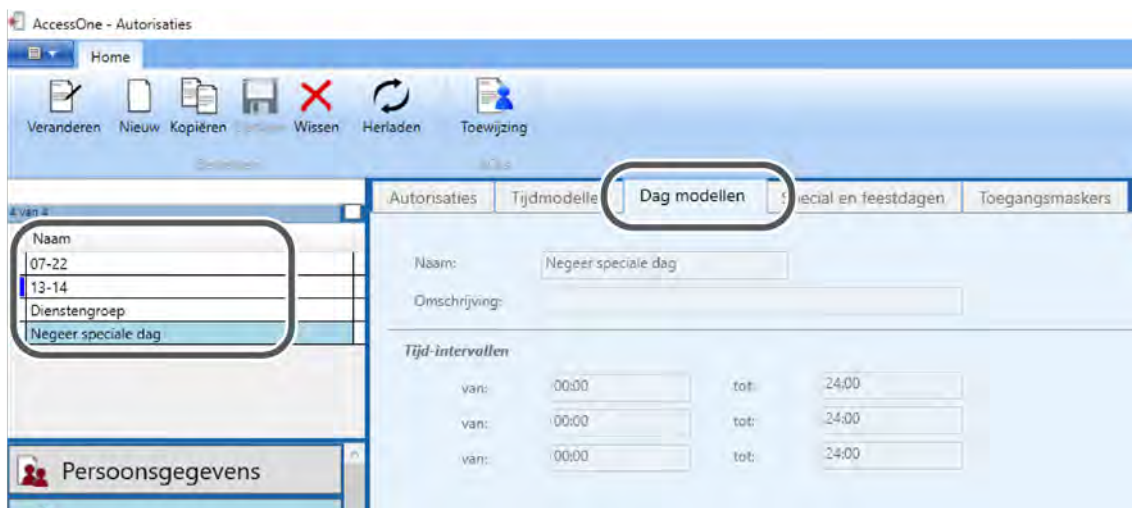
Bedrijfsgegevens

Logboek

Rapporten

Apparaatgegevens

In dit voorbeeld geldt van maandag tot vrijdag telkens hetzelfde dagmodel. De feestdagen van categorie 1 worden in dit tijdsmodel genegeerd, wat wil zeggen dat hier het betreffende dagmodel geldt van de werkdag die op deze feestdag valt. Voor de speciale dagen van categorie 2 is er een overeenkomstig dagmodel. Bij alle andere speciale dagen van de categorieën 3 tot 8 is er geen dagmodel ingevoerd en is daardoor de toegang geblokkeerd.



AccessOne - Autorisaties

Home

Veranderen Nieuw Kopieeren Opslaan Wissen Herladen Toewijzing

Autorisaties Tijdsmodellen Dag modellen Special en feestdagen Toegangsmaskers

Naam: 07-22

Omschrijving: 13-14

Dienstengroep

Negeer speciale dag

Persoonsgegevens

Dag model, speciale dagen en feestdagen

Categorie 1: Negeer speciale dag

Tijd-intervallen

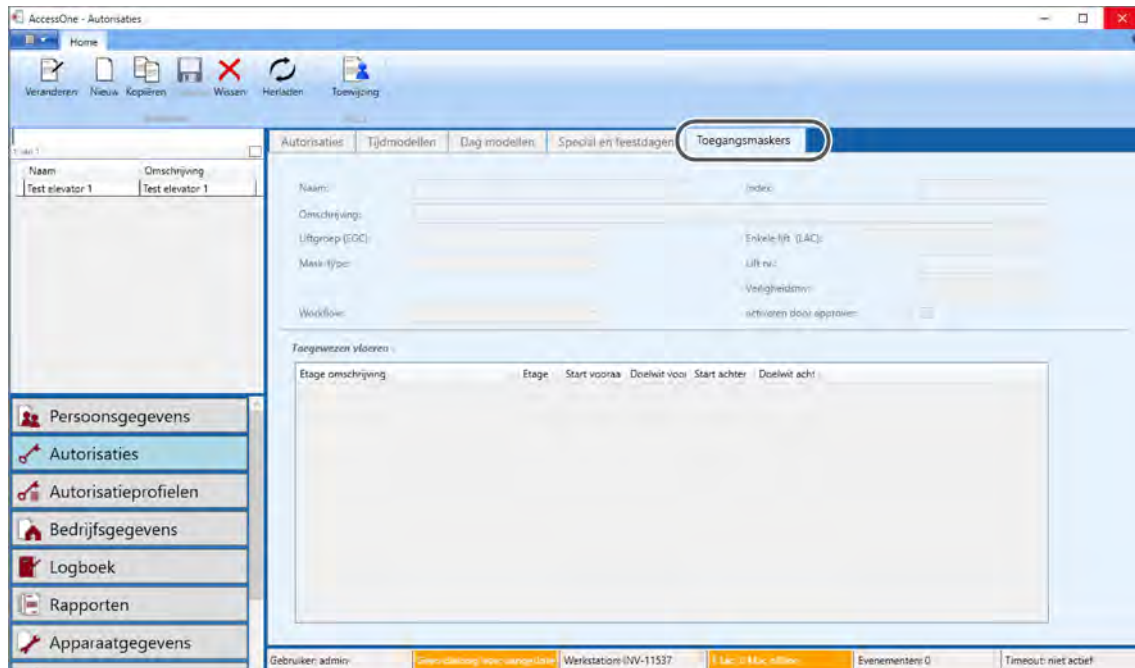
van: 00:00 tot: 24:00

van: 00:00 tot: 24:00

van: 00:00 tot: 24:00

Om te bereiken dat een speciale dag wordt genegeerd, dus dat het normale dagmodel van de betreffende werkdag geldt, moet een speciaal dagmodel worden aangemaakt, voor zover dit bij de installatie niet automatisch is aangemaakt (bijvoorbeeld "Speciale dagen negeren").

9.1.6 Toegangsmaskers

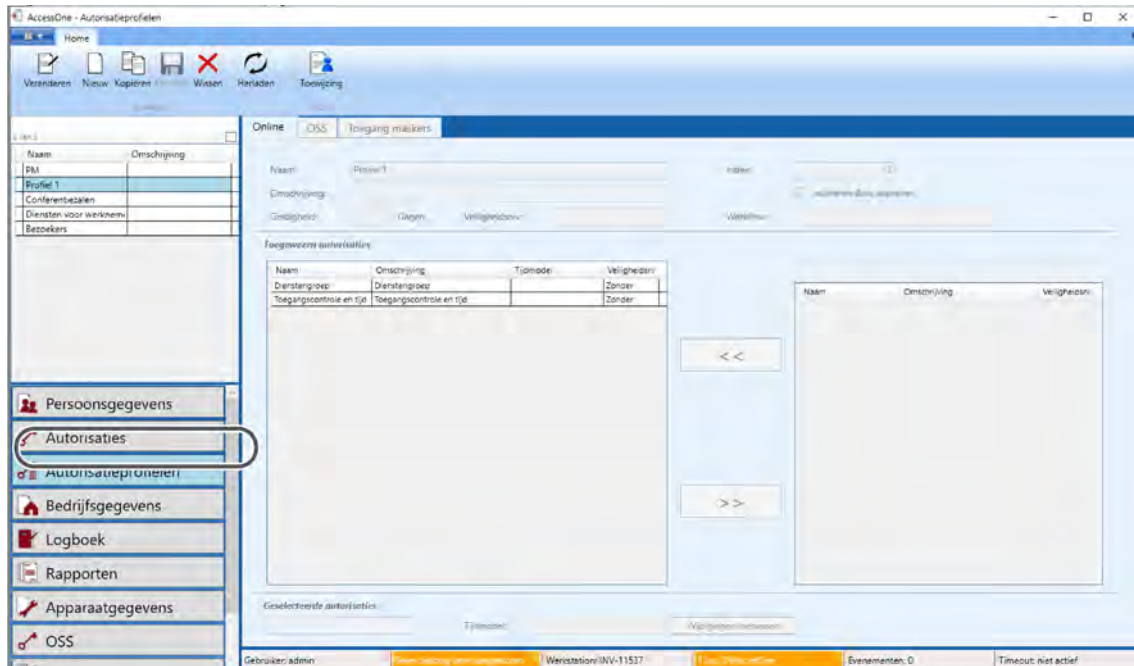


In het dialoogvenster "Toegangsmaskers" kunnen toegangsrechten op een eerder aangemaakte liftgroep worden aangemaakt. Daarvoor maakt u met NIEUW een leeg toegangsmasker aan. Voer een naam en omschrijving in en kies een liftgroep om de etages van deze groep te laten weergeven. Vervolgens bepaalt u het maskertype ("Gebruiker" of "Noodgeval"). Voor geautoriseerde toegang tot de etages schakelt of sleept u de "Start"- en "Doel"-deuren van "Nee" naar "Ja". Sla de instellingen op.

9.2 Toegangsrechtprofielen

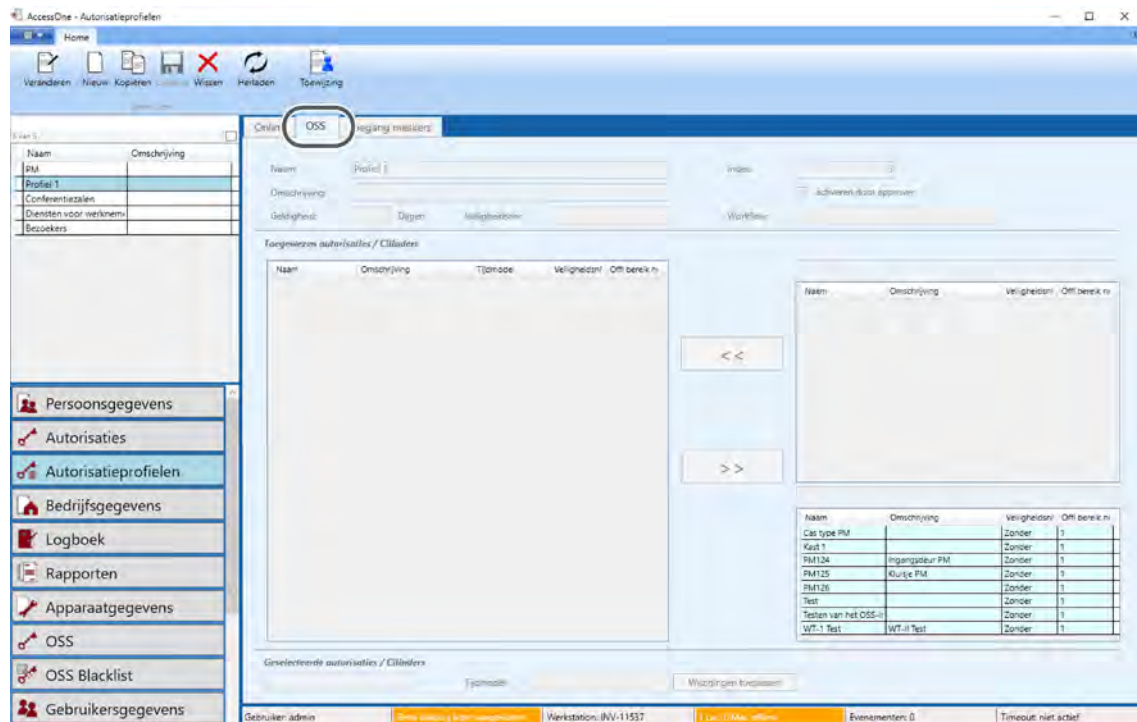
In het dialoogvenster "Toegangsrechtprofielen" heeft de gebruiker de mogelijkheid om van verschillende toegangsrechtengroepen één toegangsrechtprofiel te maken. Daarbij is het mogelijk om toegangsrechten voor online- en offline-apparaten met elkaar te combineren en in één profiel samen te voegen.

9.2.1 Overzicht van online-toegangsrechten



In het tabblad "Online" kunnen toegangsrechtgroepen voor één toegangsrechtprofiel worden samengevoegd. De groepen worden opgeroepen uit de lijst met niet-toegewezen groepen (rechterlijst) en met de knop "<<" toegewezen aan het actuele profiel (linkerlijst).

9.2.2 Overzicht van offline-toegangsrechten



In het tabblad "OSS" kunnen de offline-apparaten ook worden samengevoegd met het geselecteerde profiel. U hebt de mogelijkheid om uit de lijst aan de rechterzijde (niet toegewezen groepen en apparaten) zowel een toegangsrechtgroep als een individueel offline-apparaat via de knop "<<" toe te wijzen aan het actuele profiel.



De voorwaarde voor de koppeling van offline-apparaten is de configuratie van de offline-apparaten (zie „7.2 Apparaatgegevens offline-apparaten (OSS-SO)“ op pagina 55).

10 Persoonsgegevens aanmaken

Doelgroep van dit hoofdstuk:

- Voor het product opgeleid personeel

Het dialoogvenster "Persoonsgegevens" biedt u de mogelijkheid om toegangsrechten te verlenen en alle noodzakelijke gegevens van de persoon te registreren. Wijs de eerder geconfigureerde toegangsrechten van de online- en offline-apparaten direct toe aan de personen.

10.1 Persoonsgegevens

10.1.1 Overzicht van persoonsgegevens

Op het eerste tabblad worden alle essentiële gegevens van de persoon weergegeven. Daar is het mogelijk om een blokkering te wissen of bij personen die hun kaart zijn vergeten, een nieuwe kaart toe te wijzen (knop Kaart wisselen). De tot dusver actieve kaart wordt daardoor gedeactiveerd.



Dit overzicht is geschikt voor de snelle registratie van eigenschappen die aan een persoon zijn toegewezen (bijvoorbeeld voor objectbescherming).

Gebied "Plaats"

In het gebied "Plaats" worden de "Actuele locatie", "Laatste invoer" en "Parkeerplaats" weergegeven.

Actuele locatie

Als een persoon met een geautoriseerde kaart een deur passeert die met AccessOne is beveiligd, dan wordt de locatie geregistreerd. Voor elke deur is gedefinieerd aan welke gebieden deze grenst. Hier wordt het betreden gebied weergegeven op het tijdstip van de registratie.

Laatste invoer

Elke dag wordt om middernacht het logboek van die dag gelezen en wordt de laatste invoer in de gegevensrecord van een persoon ingevoerd. Deze informatie wordt weergegeven onder "Laatste invoer". Het kan gebeuren dat een invoer van enkele weken geleden dateert. In dat geval is de actuele locatie niet bekend. De

datum van de invoer die als laatste voor de persoon is opgeslagen, blijft echter behouden.



Deze datum kan in AccessOne ook worden gebruikt om personen automatisch te blokkeren die een instelbare periode niet aanwezig waren. Dit wordt via het type vergrendeling "Afwezigheidstijd" geregeld (zie „9.1.7 Blokkeringen“ op pagina 81).

Kaarten

De lijst is een overzicht van de toegangsmedia die zijn toegewezen aan een persoon. De betreffende status en de geldigheid worden opgeslagen. Met de knop "Kaart wisselen" wijzigt u het bijbehorende toegangsmedium van de persoon. Indien de persoon zijn kaart kwijt is geraakt, moet een vervangende kaart worden geactiveerd.

Blokkeringen

Geeft weer of voor deze persoon een blokkering is ingevoerd. Blokkeringen kunnen ook voor de toekomst gelden en worden dan pas op een later tijdstip actief. Blokkeringen die op het actuele tijdstip actief zijn, hebben een oranje achtergrond.

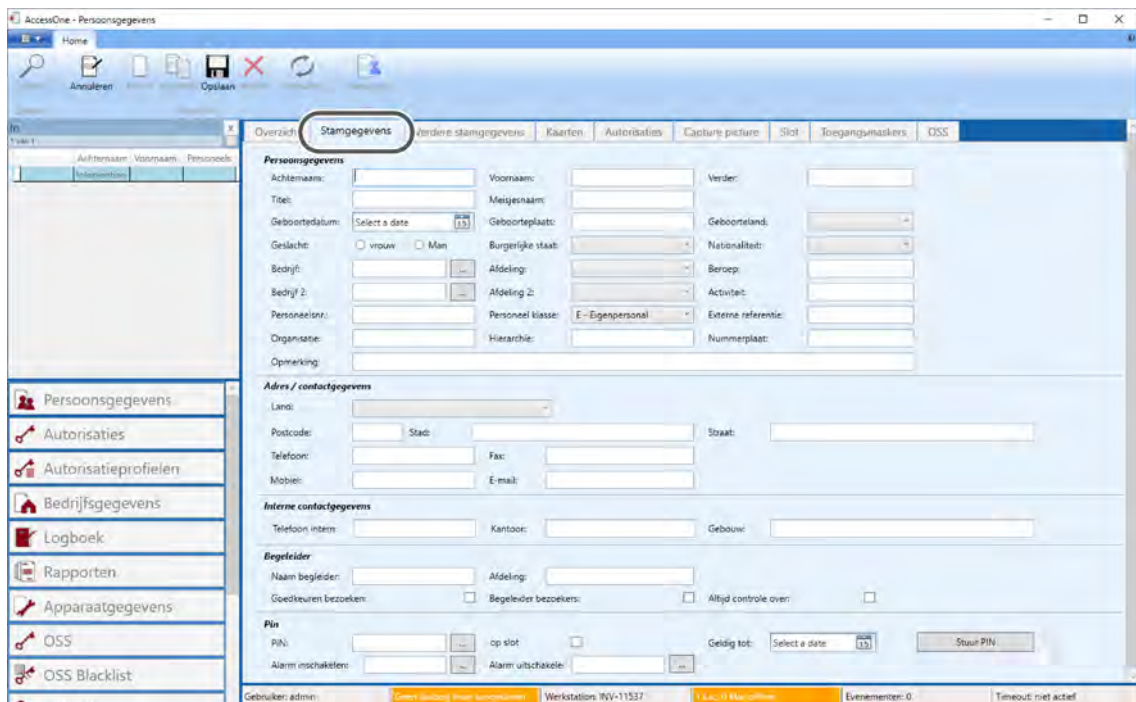
In dit dialoogvenster kunnen blokkeringen ook worden gemarkeerd en gewist. Als een verloren kaart wordt teruggevonden, kan de betreffende blokkering hier worden gewist. Selecteer daarvoor gewoon de actieve blokkering en druk op de knop Wissen.

Logboek

Door te klikken op de knop Actualiseren worden de logboekmeldingen getoond van de laatste twee dagen van die persoon. U kunt de waarde instellen tussen 2 en 7 dagen.

Voorbeeld: een persoon krijgt geen toegang meer en u informeert de objectbescherming. De bewakingsdienst kan dan bekijken bij welke deur de persoon is afgewezen en of er gegevens van de persoon zijn gewijzigd, bijvoorbeeld of er een toegangsrecht is ingetrokken of dat er een tijdmodel is gewijzigd.

10.1.2 Stamgegevens



Om nieuwe personeelsgegevens aan te maken, klikt u op de knop NIEUW. Het tabblad "Stamgegevens" wordt automatisch geopend. Als u dit tabblad wilt verlaten, moet u de twee rode, verplichte velden "Naam" en "Personeelsklasse" invullen.

Personeelsgegevens

In dit gebied bestaan verplichte velden die voor iedere persoon moeten worden ingevoerd ("Naam" en "Personeelsklasse"). AccessOne maakt in principe onderscheid tussen eigen personeel, extern personeel en bezoekers. De systeembeheerder kan in de databank aanvullende personeelsklassen aanmaken, maar deze moeten aan de drie vooraf gedefinieerde basisklassen (eigen personeel, extern personeel, bezoekers) worden toegewezen. De gebruiker kan het externe personeel bijvoorbeeld onderverdelen in "Externe bedrijven met uitzendvergunning" of "Externe bedrijven". Daarbij worden enkele blokkeringen ingesteld, afhankelijk van de personeelsklasse. Zo kan worden ingesteld dat bij eigen personeel een blokkering voor te lange afwezigheid pas na zes weken wordt ingesteld en bij extern personeel reeds na twee weken. Ook bij de toegangen wordt de personeelsklasse geanalyseerd.

Voorbeeld: voor tassencontroles kan de instelling zo worden uitgevoerd dat bezoekers altijd worden gecontroleerd, terwijl het eigen personeel alleen volgens een instelbare generator van willekeurige getallen wordt gecontroleerd.

Het personeelsnummer is een extern toewijzingscriterium dat meestal afkomstig is van een extern personeelsbeheersysteem (bijvoorbeeld SAP). Dit is bestemd voor de toewijzing van personen uit het toegangscontrolesysteem met de gegevens van de personeelsafdeling. Het personeelsnummer is ook toegelaten als zoekcriterium.

Bedrijf en afdeling definieert u in het dialoogvenster "Bedrijfsgegevens" (zie "Bedrijfsgegevens aanmaken" op pagina 1). Bij de bedrijven is gedefinieerd of het om een eigen bedrijf gaat of om een extern bedrijf. In het invoerveld "Bedrijf" kunnen alleen eigen bedrijven worden geselecteerd, in het veld "Bedrijf 2" alleen externe bedrijven. De afdelingen worden van tevoren bij de bedrijfsgegevens gedefinieerd en kunnen hier alleen worden geselecteerd. In de invoervolgorde dienen daarom eerst de bedrijven en daarna de personen te worden aangemaakt.

Adres

Voer op deze plaats alle relevante adresgegevens van de persoon in.

Contactgegevens

Voer op deze plaats alle relevante contactgegevens van de persoon in.

Begeleider

Voor medewerkers van externe bedrijven kan een begeleider worden ingevoerd. Deze moet altijd een persoon van het eigen personeel zijn. De begeleider is de verantwoordelijke contactpersoon voor de personen die deze begeleidt.

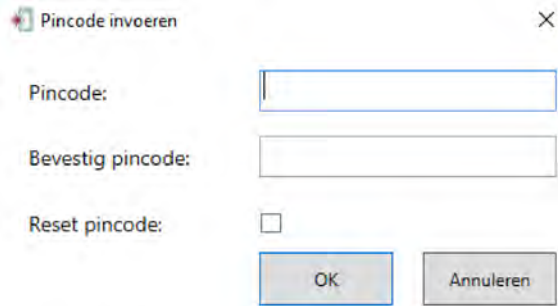
Pincodes

In AccessOne worden drie pincodes gehanteerd. Een pincode is de persoonlijke nummercontrole voor de toegangscontrole. Er zijn deuren die alleen na het invoeren van de pincode toegang verlenen. De minimale lengte van de pincode kan worden ingesteld via een systeemparemeter (standaard 4 posities, maximaal 6 posities). De pincode kan een beperkte geldigheid hebben en ook zijn geblokkeerd. Wanneer drie keer de verkeerde pincode is ingevoerd, wordt deze pincode automatisch geblokkeerd en moet deze in het systeem worden gewijzigd.

Voor de inschakeling en uitschakeling van het inbraakalarmsysteem (EMA) hanteert het systeem twee andere pincodes. De pincode mag voor de inschakeling en uitschakeling identiek zijn, maar moet wel verschillen van de pincode voor de toegangscontrole.



Het is een eis van VDS*1 dat er twee verschillende pincodes zijn. Deze pincodes hebben geen tijdelijk beperkte geldigheid. Bij een deur kan in het toegangsrecht van de persoon worden gekozen of de persoon mag inschakelen, uitschakelen of beide. Alleen wanneer dit toegangsrecht bestaat, is het invoeren van een pincode mogelijk.



Pincode invoeren

Pincode:

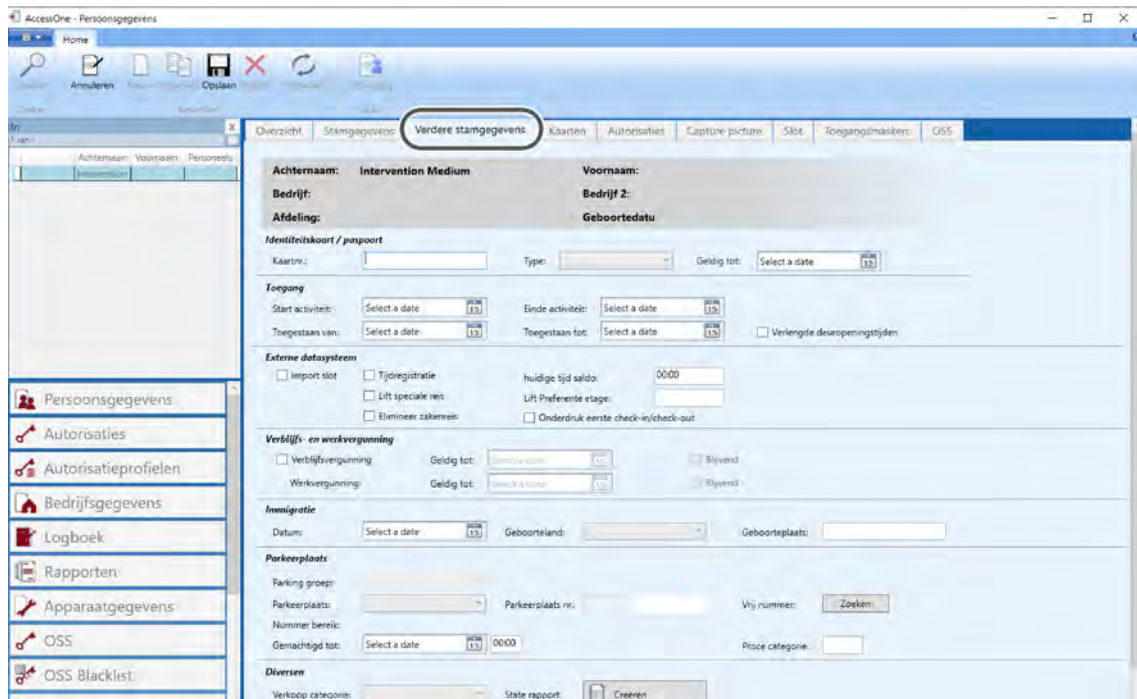
Bevestig pincode:

Reset pincode: ☐

OK Annuleren

Alle pincodes dienen afgedekt te worden ingevoerd. De pincode met vier tot zes posities moet twee keer worden ingevoerd en moet uit ten minste drie verschillende cijfers bestaan. De betreffende kaarteigenaar voert deze in via een apart numeriek toetsenbord.

10.1.3 Verdere stamgegevens



Voer alle gegevens in die u van de persoon wilt opslaan.

Identiteitskaart/paspoort

Op deze plaats hebt u de mogelijkheid om het nummer van de ID-kaart of het paspoort en de duur en geldigheid daarvan in te voeren. Deze invoer is alleen bestemd voor documentatiedoeleinden.

Toegang

Hier worden het begin en het einde van de activiteit (bijvoorbeeld bij tijdelijke contracten) ingevoerd om automatisch overeenkomstige blokkeringen in te stellen. Deze gegevens worden bijvoorbeeld bij eigen personeel gebruikt om de datum van indiensttreding bij nieuwe medewerkers of van uitdiensttreding bij ontslag vast te leggen. Vóór het begin van de activiteit en bij het bereiken van de einddatum wordt een blokkering ingesteld. Zo kunnen personen in het systeem worden aangemaakt voordat deze op de eerste werkdag verschijnen. Dat gebeurt gedeeltelijk automatisch door de interface met het personeelsbeheersysteem van de personeelsafdeling. Wanneer de ontslagdatum is bereikt, wordt de kaart automatisch geblokkeerd.

Gegevens van externe systemen

Hier kan een importblokkering worden geselecteerd, wat wil zeggen dat het systeem geen dagelijkse gegevenssynchronisatie van externe SAP-bronnen oproept. Wanneer gegevens in AccessOne zijn gewijzigd, moeten deze niet opnieuw kunnen worden overschreven.

Training

Wanneer er in het bedrijf een plicht bestaat voor verplichte trainingen voor nieuwe medewerkers, dan kunt u op deze plaats de datum van de eerste en tweede training invoeren. En ook de datum waarop de volgende training moet plaatsvinden.

Verblijfs- en werkvergunning

Een geldige verblijfs- en werkvergunning is een wettelijke voorwaarde om te mogen werken. Bij personen met een beperkte verblijfs- en/of werkvergunning bewaakt het systeem de naleving wanneer hier overeenkomstige gegevens worden ingevoerd. De invoer is bedoeld voor de opdrachtgever die zich strafbaar maakt wanneer

personen zonder deze vergunning in zijn bedrijf werken.

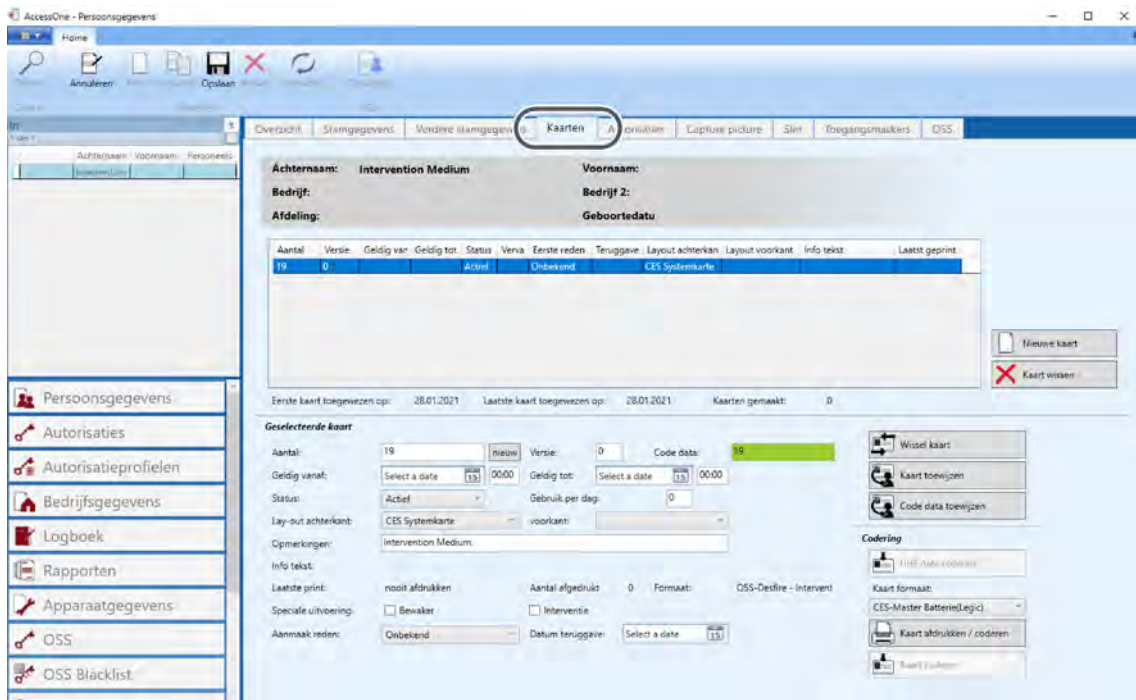
Immigratie

Deze invoer is alleen bestemd voor documentatiedoeleinden en kan optioneel worden ingevoerd.

Diversen

De "Verkoopcategorie" wordt gebruikt om een key-card voor gebruik op verkoopautomaten vrij te geven. De voorwaarde is dat de kaarten worden gecodeerd met AccessOne.

10.1.4 Kaarten (toegangsmedia)



Op dit tabblad kunt u kaarten aanmaken, wisselen, toewijzen of afdrukken. In het tabeloverzicht ziet u alle kaarten die voor deze persoon zijn gedefinieerd.



Een persoon kan verschillende kaarten bezitten. Dat is met name bij het gebruik van verschillende identificatietechnologieën noodzakelijk.

Om een nieuwe kaart aan te maken, selecteert u een persoon, drukt u in de bovenste menubalk op de knop **WIJZIGEN** en klikt u op de knop **Nieuwe kaart**.

Een kaart wordt gewist doordat deze in de lijst wordt geselecteerd en er volgens op **Kaart wissen** wordt geklikt.



OPGELET: hier volgt er geen veiligheidsvraag voordat er definitief wordt gewist! Als de knop onopzettelijk is ingedrukt, moet in de werkbalk op de knop **AFBREKEN** worden geklikt. De wijzigingen op het actuele tabblad worden dan afgewezen.

Geselecteerde kaart

Hier kunnen alle gegevens van de kaart worden ingevoerd of gewijzigd. Het kaartnummer fungeert alleen als toewijzingscriterium. In de normale situatie heeft dit niets te maken met het nummer dat in de kaart is gecodeerd. Het kan echter wel identiek zijn aan het nummer dat in de kaart is gecodeerd.

De opgave van de versie heeft één positie en gaat van 0 tot 9 of A tot Z. Als een kaart defect is, dan kan weer een identieke kaart met hetzelfde kaart- en codenummer worden geproduceerd, waarbij het versienummer dan met één wordt verhoogd en samen met het in de kaart gecodeerde nummer wordt opgeslagen. Daarom is altijd slechts de kaart met het actuele versienummer geldig. Dit nummer wordt gecontroleerd aan de deur. Als dit niet overeenkomt, wordt een betreffende melding gegenereerd en wordt de toegang geweigerd.

Geldig vanaf/tot

Kaarten kunnen een beperkte geldigheid hebben. Deze geldigheidsperiode wordt bewaakt door het systeem. Buiten de geldigheid wordt de kaart geweigerd. Als er geen waarde is ingesteld, dan betekent dat een onbeperkte geldigheid.

Status

Alleen actieve kaarten worden op de deurbesturingen geladen. Een inactieve kaart zal dus niet functioneren. Het systeem meldt dan: "Onbekende kaart". Voor een kaart die ook geldig dient te zijn, kiest u hier "Actief".

Layout achterkant/voorkant

In het dialoogvenster "Kaartontwerper" wordt beschreven hoe u kaarten bedrukt. Daar heeft u ook de mogelijkheid om verschillende layouts te selecteren die eerder zijn gedefinieerd. Wanneer u een kaart nieuw aanmaakt, stelt u hier in welke layout er dient te worden gebruikt. Layouts kunnen voor elke kaart apart worden vastgelegd.



De layouts kunnen vooraf via de personeelsklasse van de persoon worden ingesteld, doordat bij de personeelsklasse de betreffende lay-outs door de systeembeheerder worden opgeslagen (zie „9.1.2 Stamgegevens“ op pagina 73).

Codegegevens bestaan

Wanneer de kaart is aangemaakt, moet de bijbehorende in de kaart opgeslagen informatie worden opgeslagen. Indien vooraf gecodeerde kaarten worden gebruikt, gebeurt dat via de knop **Kaart toewijzen**. Dan wordt de opdracht gegeven om een kaart tegen de dialooglezer te houden, waardoor de kaartinformatie wordt uitgelezen en in de gegevensrecord wordt opgeslagen. De weergave wordt groen "Codegegevens bestaan".

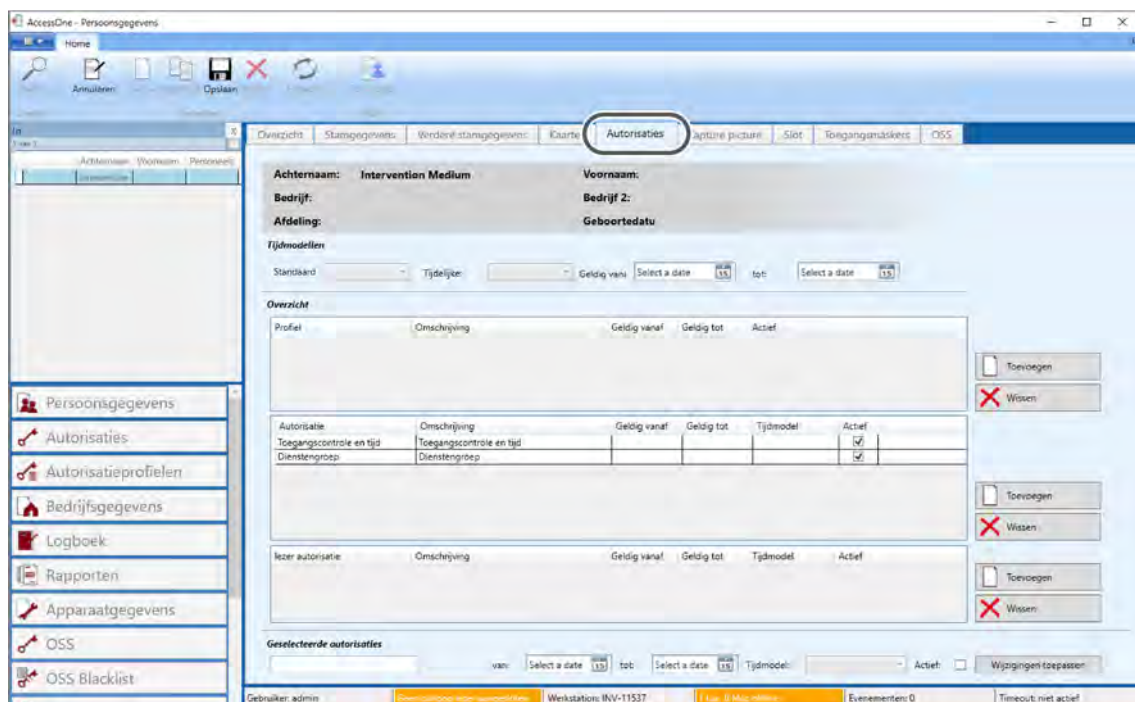
Als de kaarten door AccessOne worden gecodeerd, is optioneel de knop **Codenummer toewijzen** actief. In dat geval gebruikt AccessOne een voorschrift van de klant voor het betreffende kaartformaat en bepaalt deze een uniform, vrij codenummer. Dat wordt toegewezen aan de kaart. Via de knop **UHF-kaart coderen** wordt de kaart via de dialooglezer geprogrammeerd. Optioneel kan via de knop **Kaart dubbelzijdig printen** in één handeling worden gecodeerd en geprint. De voorwaarde daarvoor is dat in de printer een codeereenheid is geïnstalleerd.

Kaart dubbelzijdig printen

Geef de kaart in een voorbereide layout weer in een afdrukvoorbeeld. Na de bevestiging wordt de kaart geprint en, indien dat voor de printer mogelijk is, in dezelfde werkstap ook gecodeerd.

- "Laatst geprint" geeft de datum en de tijd weer wanneer deze kaart als laatste is geprint.
- "Aantal afgedrukt" geeft het aantal geprinte kaarten weer van de gekozen persoon.
- "Aanmaakreden" biedt de mogelijkheid om een reden voor het (opnieuw) aanmaken te selecteren.
- "Datum teruggave" legt de dag van de teruggave vast. Wanneer deze dag is verstreken, is de kaart geblokkeerd.

10.1.5 Toegangsrechten



The screenshot shows the 'AccessOne - Persoonsgegevens' application window. The 'Autorisaties' tab is active. The form contains the following fields:

- Achternaam:** Intervention Medium
- Voornaam:**
- Bedrijf:**
- Bedrijf 2:**
- Afdeling:**
- Geboortedatum:**
- Tijdmodellen:** A section with a dropdown menu set to 'Standaard' and a 'Tijdelijk' checkbox. Below this is a table with columns: 'Profiel', 'Omschrijving', 'Geldig vanaf', 'Geldig tot', and 'Actief'.

The table contains two rows of data:

Profiel	Omschrijving	Geldig vanaf	Geldig tot	Tijdmodel	Actief
Autorisatie	Toegangscontrole en tijd				☒
	Dienstengroep				☒

Below the table, there are buttons for 'Toevoegen' (Add) and 'Wissen' (Delete) for each row. At the bottom, there is a 'Geselecteerde autorisaties' section with a 'van' dropdown, date pickers, and an 'Actief' checkbox.

In dit menu worden gedefinieerde tijdmodellen aan de persoon toegewezen. Deze moeten in het dialoogvenster "Toegangsrechten" zijn aangemaakt (zie „9.1.5 Toegangsrechten“ op pagina 78).

Hier is alle informatie samengevoegd die relevant is voor de toegangsrechten:

Tijdmodellen

Voor elke persoon kan een standaard tijdmodel worden vastgelegd. Dat geldt wanneer er voor een toegangsrecht geen eigen tijdmodel bestaat. Zo kunt u bijvoorbeeld vastleggen dat een persoon in de normale situatie dagelijks van 09 tot 17 uur toegang dient te hebben, maar dat deze na het verstrijken van deze tijd de ondergrondse parkeergarage ook nog mag gebruiken. Optioneel kan de toegang tot bepaalde gebieden ook nog strikter worden beperkt.



Als er geen tijdmodel is opgegeven, dan is de toegang in tijd niet beperkt.

Bovendien kan een tijdelijk tijdmodel worden opgegeven dat het standaard tijdmodel voor een vastgelegde periode overschrijft. Het tijdmodel kan een kleiner tijdvenster hebben (bijvoorbeeld bij deeltijdwerk) of een groter tijdvenster (bijvoorbeeld bij weekendwerk).

Daaronder bevinden zich beide lijsten met de profielen of toegangsrechten die voor de persoon zijn gekozen.

Profielen

Een profiel omvat een groep toegangsrechten. Onder één profiel kunnen verschillende toegangsrechten worden samengevoegd. Met de profielen is het mogelijk om de toegangsrechten volgens de functie van de persoon samen te stellen. Zo kan bijvoorbeeld een profiel worden aangemaakt voor schoonmaakpersoneel en een voor monteurs. Deze procedure vergemakkelijkt de selectie van de toegangsrechten die de betreffende medewerker nodig heeft om zijn taken uit te voeren.

Voorbeeld: gebouwingangen worden in één toegangsrecht samengevoegd en een profiel voor gebouwingangen omvat dan de toegangsrechten per gebouw.



Wijzigingen in de toegangsrechten die in profielen zijn opgenomen, zijn meteen van invloed op de profielen. AccessOne draagt de profielen rechtstreeks over aan de deurbesturingen, zodat de wijziging in een toegangsrecht of in een profiel voor alle personen van kracht is, aan wie dit profiel is toegewezen of die dit hebben gekregen zonder dat daarvoor extra gegevensrecords hoeven te worden overgedragen.

Voor elk profiel kan een beperkte geldigheid en een tijdmodel worden opgegeven. Als er geen tijdmodel is opgegeven, dan geldt het tijdmodel dat voor de persoon is opgeslagen. Als er geen geldigheid is ingevoerd, dan is dit profiel onbeperkt geldig. Als er alleen een begindatum maar geen einddatum beschikbaar is, dan geldt het profiel onbeperkt vanaf de begindatum. Een ingevoerde einddatum beëindigt de geldigheid.

Een profiel wordt uit de lijst verwijderd, doordat het wordt geselecteerd en er daarna op de knop Wissen naast de selectielijst wordt geklikt. Een nieuw profiel wordt aangemaakt, doordat via de knop Toevoegen een selectievakje wordt opgeroepen, waaruit het gewenste profiel kan worden geselecteerd. Meervoudige selectie is mogelijk door te klikken met een ingedrukte Ctrl-toets.

Toegangsrechten

Toegangsrechten vatten lezers tot een gezamenlijke groep samen. Zie daarvoor ook het dialoogvenster "Toegangsrechten" (zie „9.1.5 Toegangsrechten“ op pagina 78). Voor toegangsrechten gelden dezelfde regels als voor profielen.

Geselecteerde toegangsrechten

Als een of meerdere toegangsrechten of profielen door te klikken worden geselecteerd, worden in deze velden de details weergegeven en kunnen deze daar ook worden gewijzigd. Door te klikken op de knop

Wijzigingen toepassen worden de gewijzigde velden dan naar het toegangsrecht of het profiel gekopieerd.



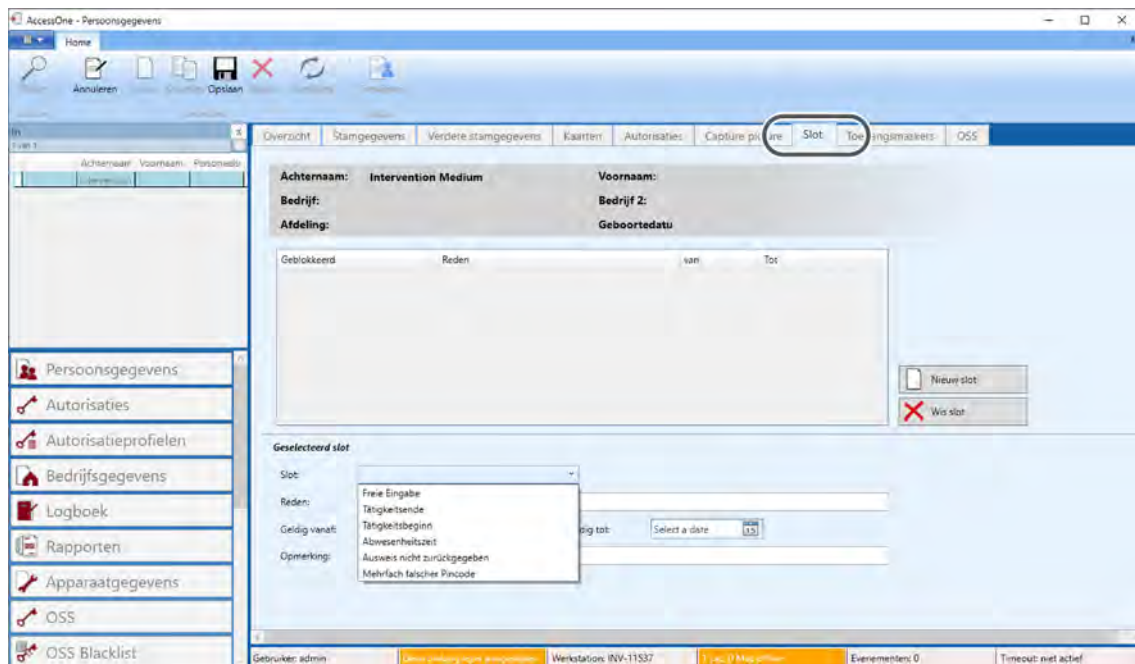
Voor het toepassen van de wijziging moet op de knop **Wijzigingen toepassen** worden gedrukt, omdat anders de wijzigingen niet worden opgeslagen.

Aan één persoon kunnen maximaal 64 toegangsrechten en/of profielen worden toegewezen (bijvoorbeeld 10 profielen en 22 toegangsrechten). Als bij veel personen telkens dezelfde toegangsrechten zijn vermeld, raden wij aan om deze toegangsrechten in een eigen toegangsrechtprofiel samen te voegen.



Wanneer een toegangsrecht wordt toegewezen aan een persoon die reeds in een toegangsrechtprofiel is opgenomen dat is toegewezen aan de persoon, wordt dit redundante toegangsrecht in het kader van het geautomatiseerde onderhoudsproces bij de wisseling van de dag gewist.

10.1.6 Capture picture



Op het tabblad "Capture picture" kunt u een foto aan de persoon toewijzen door deze foto te importeren of direct een foto te maken.

Als u voor de persoon een foto wilt importeren, roept u de persoon in het linker selectievenster op en klikt u in de bovenstaande taakbalk op de knop VERANDEREN. Druk nu op de knop **Beeld importeren**.

U kunt bestanden kiezen in de formaten *.bmp, *.png of *.jpg. Om een foto te maken, moet er een camera zijn aangesloten op uw pc/laptop.

Selecteer het betreffende apparaat in de vervolgkeuzelijst "Camera". Een andere resolutie en overige camera-instellingen kunnen afhankelijk van het aangesloten apparaattype worden uitgevoerd.

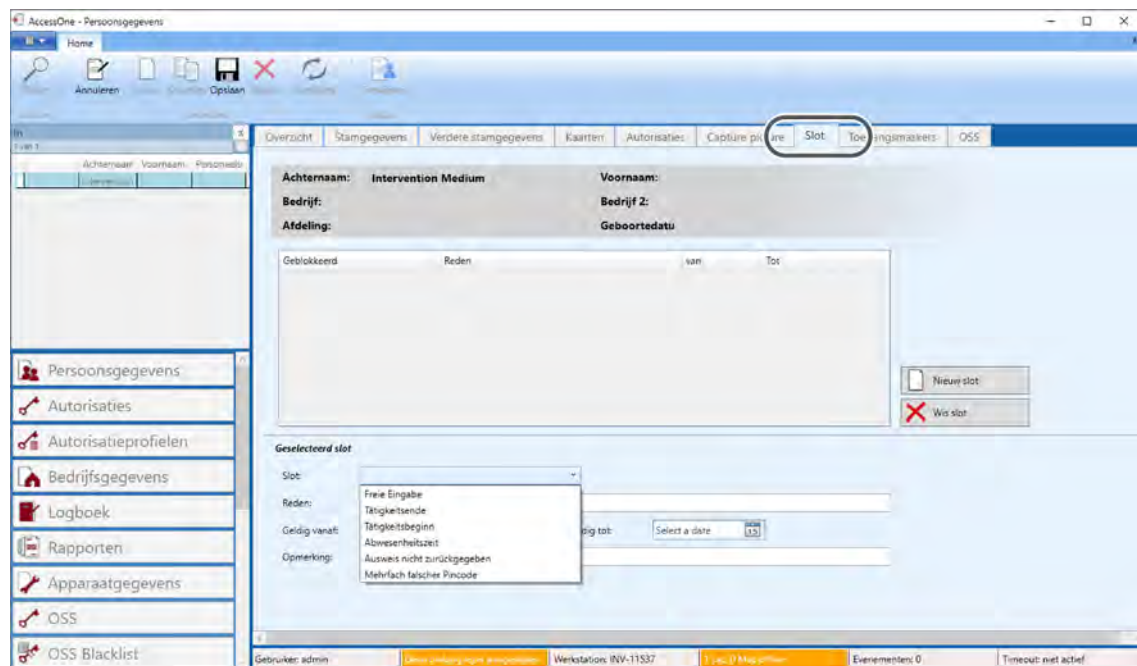
Met de knop **Start camera** maakt u een foto van de persoon.

Nadat de juiste beeldduitsnede (groen kader) is gekozen, wordt deze via de knop **Foto opslaan** in het voorbeeld bovenaan rechts weergegeven.



Als er naar een ander tabblad wordt omgeschakeld zonder dat er is opgeslagen, is de opname niet meer beschikbaar voor verdere bewerking.

10.1.7 Blokkeringen



Op dit tabblad kunt u personen blokkeren, wanneer een medewerker bijvoorbeeld zijn kaart kwijt is. Dubbelklik daarvoor in het selectievenster links op de persoon die u wilt blokkeren om naar de bewerkingsmodus te gaan. Nu is de knop **Nieuwe blokkering** geactiveerd en kunt u een blokkering aan een persoon toewijzen.

In het gebied "Geselecteerde blokkering" voert u extra instellingen in.

Als de blokkering in tijd is beperkt, bijvoorbeeld vóór "Activiteit beginnen", roept u een "Geldig vanaf/tot-datum" op.

Voeg de gegevens over de blokkering toe in het invoerveld "Opmerking". Met de knop OPSLAAN in de taakbalk slaat u de blokkering op. U kunt een blokkering wissen door deze in de lijst te selecteren en op de knop **Blokkering wissen** te drukken.

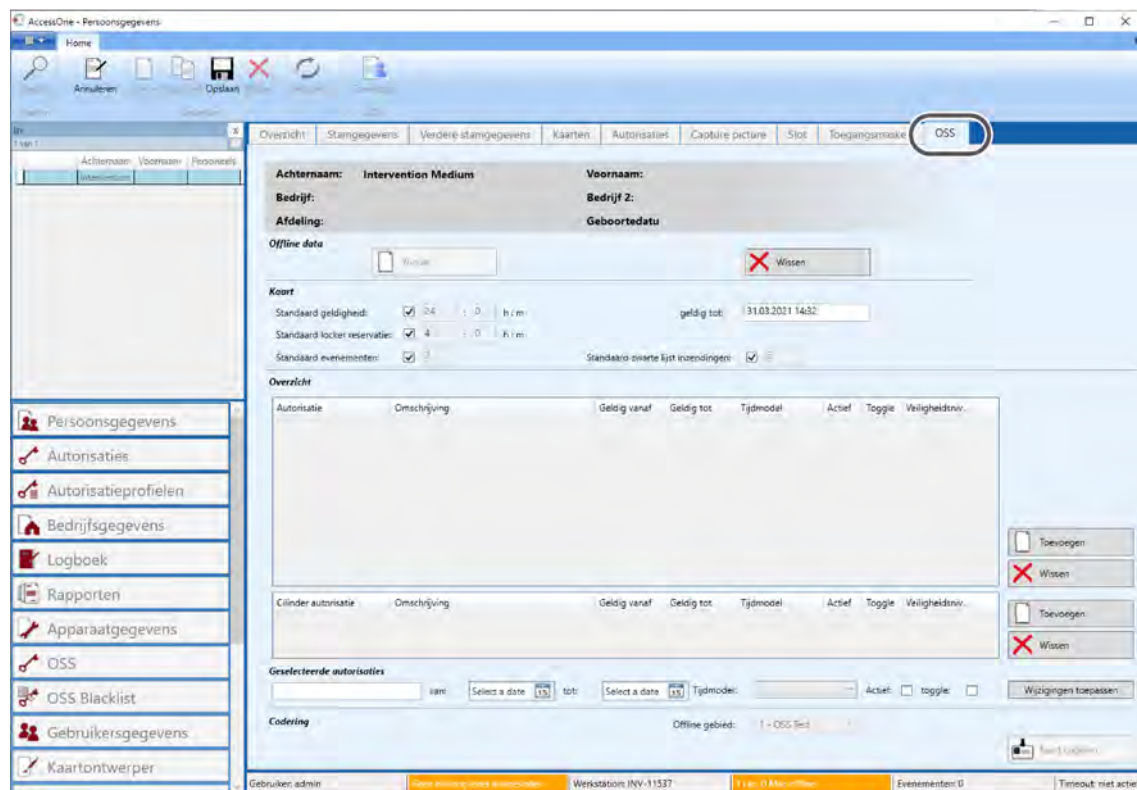
AccessOne maakt een onderscheid tussen automatische en handmatige blokkeringen. Indien gewenst kunnen in het systeem aanvullende blokkeringen worden voorgedefinieerd.

Voorbeeld: blokkering vanaf Activiteit beginnen en na Activiteit beëindigen

Deze blokkering kan ook handmatig worden ingesteld en deze is onmiddellijk effectief! In dat geval dient erop te worden gelet dat het systeem tijdens de nachtelijke uren de blokkering actualiseert op basis van de gegevens die bij de persoon zijn ingevoerd. Wanneer een persoon bijvoorbeeld is geblokkeerd vanwege het einde van de activiteit, maar de volgende dag opnieuw naar het kantoor moet gaan, dan kan deze blokkering weliswaar handmatig worden gewist, maar wordt deze na middernacht automatisch weer ingesteld.

10.1.8 OSS-SO

Dankzij OSS Standard Offline kunnen cilinders en beslag van verschillende merken dezelfde toegangsrechten van de kaart lezen en deze op dezelfde manier interpreteren.



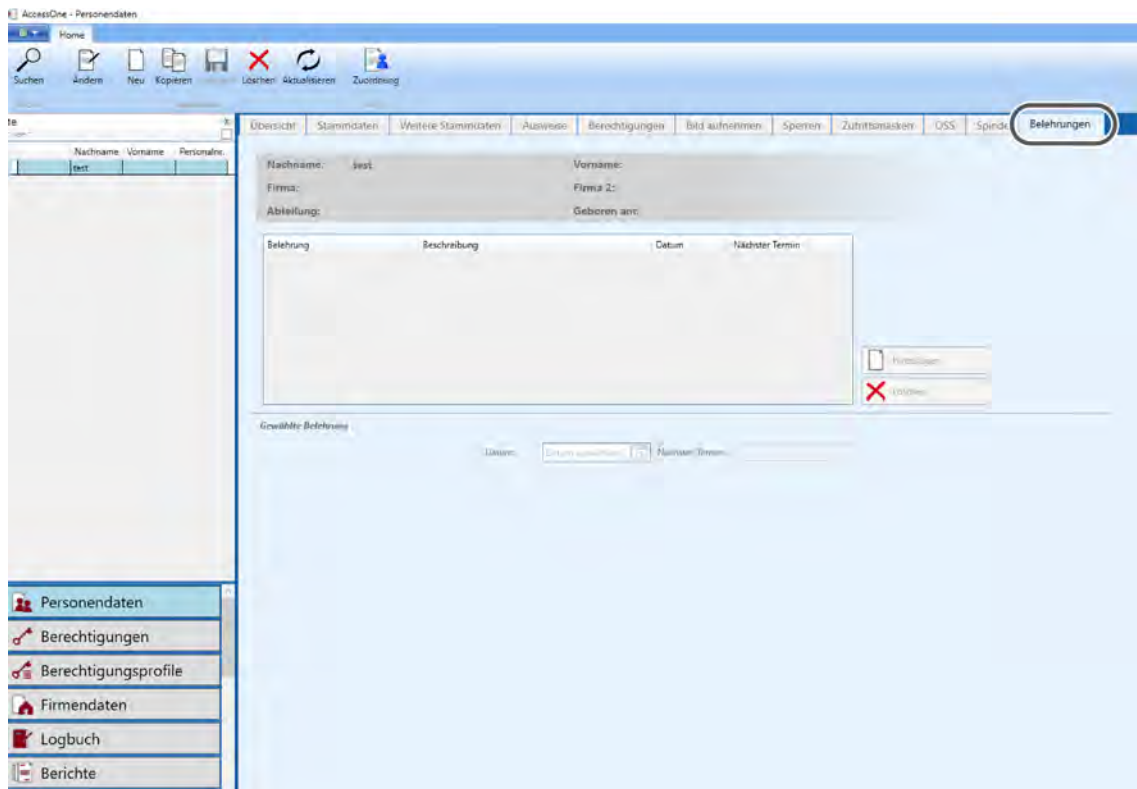
De configuratie en het beheer van elektronische cilinders en beslag die compatibel zijn met OSS Standard, is volledig geïntegreerd in AccessOne. Voor de configuratie heeft u bovendien het door de betreffende fabrikant geleverde configuratiehulpmiddel nodig waarmee de configuratiegegevens in de cilinder worden geprogrammeerd.

Alle configuratiegegevens worden geregistreerd in AccessOne. Uit de gebruikersinterface kunt u dan een XML-bestand genereren dat door het betreffende configuratiehulpmiddel wordt ingelezen. In dit bestand zijn alle gegevens opgenomen voor de initialisatie van de cilinder.

Na installatie van de betreffende licentie is in de functieselectie een knop voor OSS beschikbaar. Via deze knop komt u terecht bij de dialoogvensters voor het onderhoud van de gegevens van de offline-componenten. Daar bepaalt u de geldigheid van de kaarten van de personen en voegt u profielen, toegangsrechten en cilinderbevoegdheden toe.

Tot slot codeert u de kaart.

10.1.9 Instructions



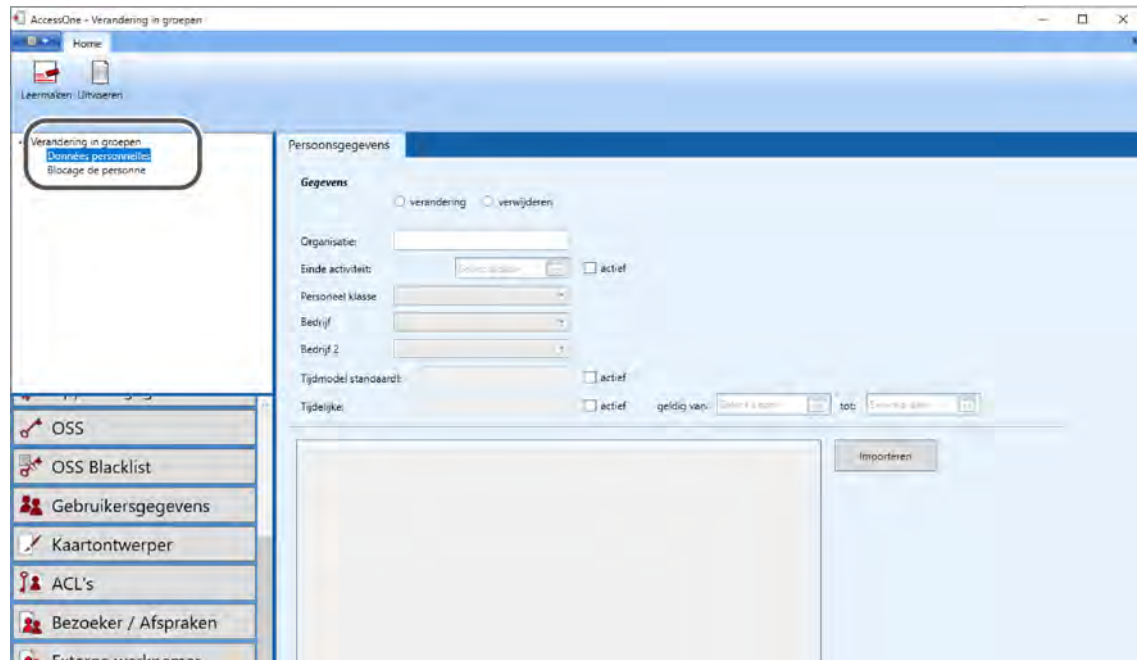
The screenshot shows the 'AccessOne - Persoonendaten' application window. The 'Bevelingen' tab is active, displaying a form for entering instructions. The form includes fields for 'Nachname' (Last Name), 'Voorname' (First Name), 'Firma' (Company), 'Afdeling' (Department), 'Geboren aan' (Born on), and 'Datum' (Date). Below these fields is a table with columns for 'Beveling' (Instruction), 'Beschrijving' (Description), 'Datum' (Date), and 'Nächster Termin' (Next Date). The table is currently empty. To the right of the table are buttons for 'Nieuw' (New), 'Verwijderen' (Delete), and 'Opslaan' (Save). At the bottom of the form, there are fields for 'Gewijzigde Bevelingen' (Changed Instructions), 'Lokalen' (Local), and 'Nieuwste Datum' (Newest Date). The left sidebar contains a navigation menu with options: 'Persoonendaten', 'Berechtigungen', 'Berechtigingsprofiel', 'Firmendaten', 'Logboek', and 'Berichte'.

Hier kunnen instructies die in een bepaalde periode moeten worden gegeven, worden gearchiveerd (bijvoorbeeld ongevallenpreventie, AVG enz.). Via de knop Toevoegen kunt u deze selecteren en met een datum invoeren.

10.2 Verandering in groepen

In het dialoogvenster "Verandering in groepen" kunnen wijzigingen in persoonsgegevens, persoonsblokkeringen en toegangsrechten voor volledige groepen worden toegepast door deze te importeren.

10.2.1 Persoonsgegevens



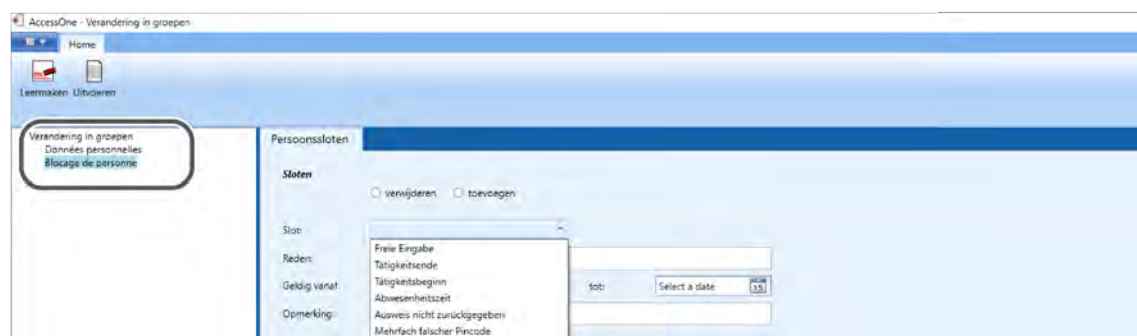
In het tabblad "Persoonsgegevens" kunnen eerder ingestelde gegevens voor personengroepen die door te klikken op de knop **Importeren** zijn geladen, worden gewijzigd of gewist.

De gegevens die moeten worden geïmporteerd, moeten beschikbaar zijn als *.csv-bestand. Dit bestand kan worden gegenereerd via de dialoogpagina "Rapporten > Personen > Persoonsgroepen export". Op deze dialoogpagina zijn veel filters beschikbaar voor het configureren van personengroepen. Als er een rapport wordt aangemaakt, kan de gegenereerde personengroep als MS Excel-bestand worden opgeslagen op de vaste schijf en verder worden bewerkt.



Het uit dit programma opgeslagen *.csv-bestand is bestemd als importbestand voor alle andere dialoogvensters voor het wijzen van groepen.

10.2.2 Personenblokkeringen toevoegen of wissen

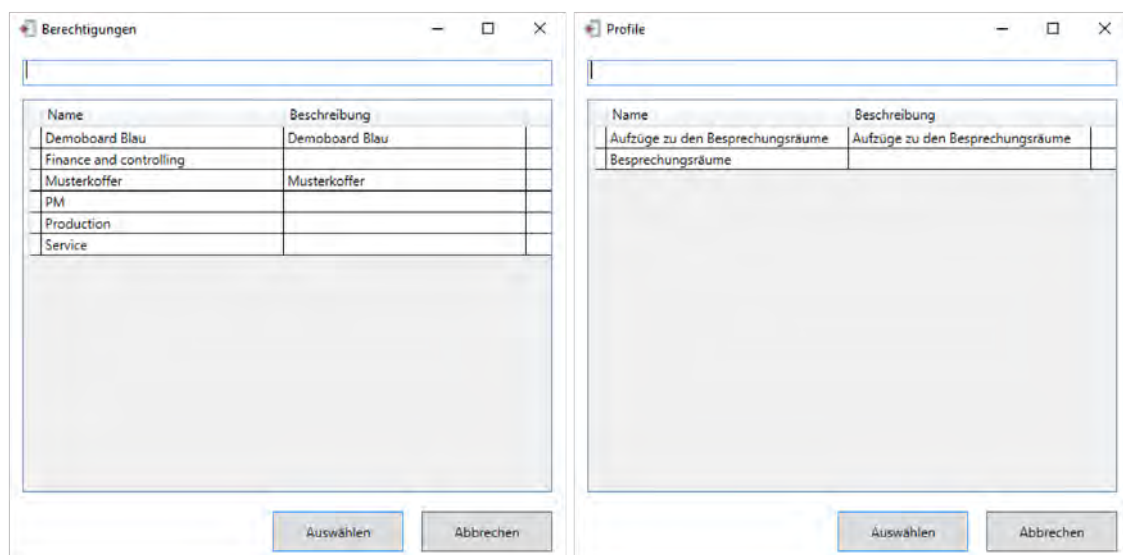
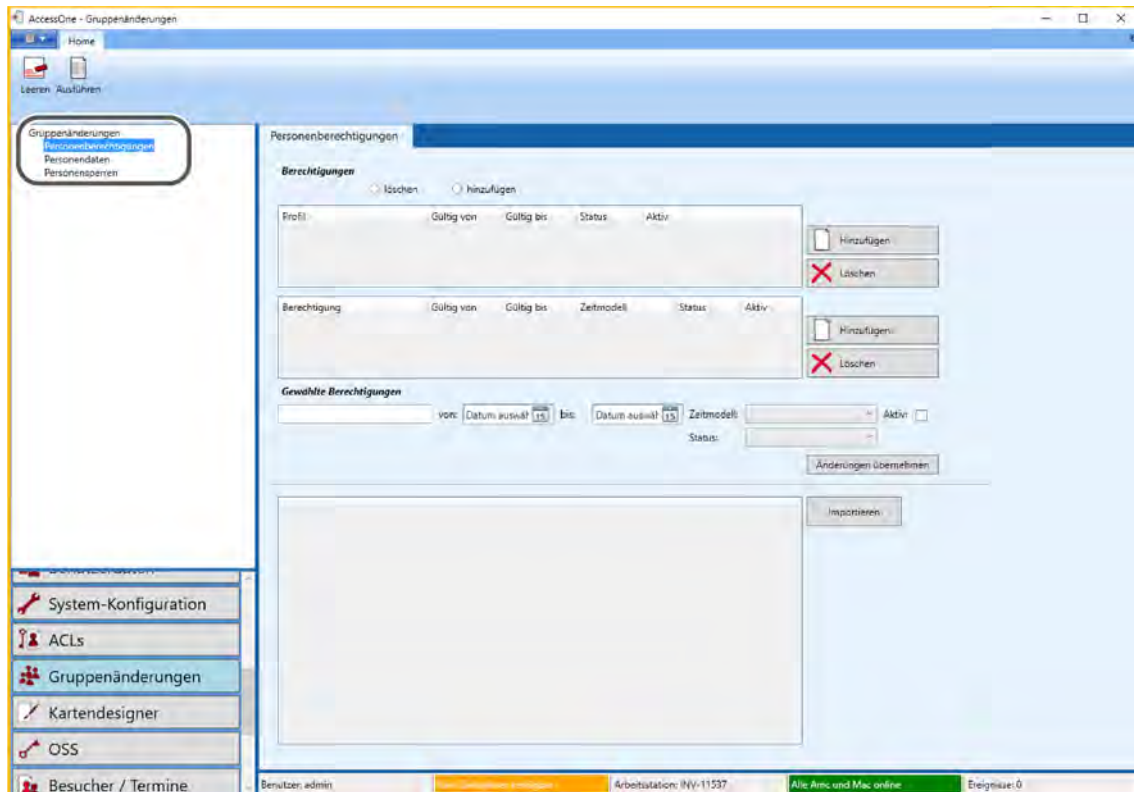


In het tabblad "Personenblokkeringen" kunnen voor de betreffende personengroepen blokkeringsgegevens

worden toegevoegd of gewist door bestanden te importeren.

In het invoerveld "Geblokkeerd" kunt u meerdere redenen voor blokkering selecteren die kunnen worden ingevoerd met een geldigheid.

10.2.3 Persoonstoegangsrechten aanpassen



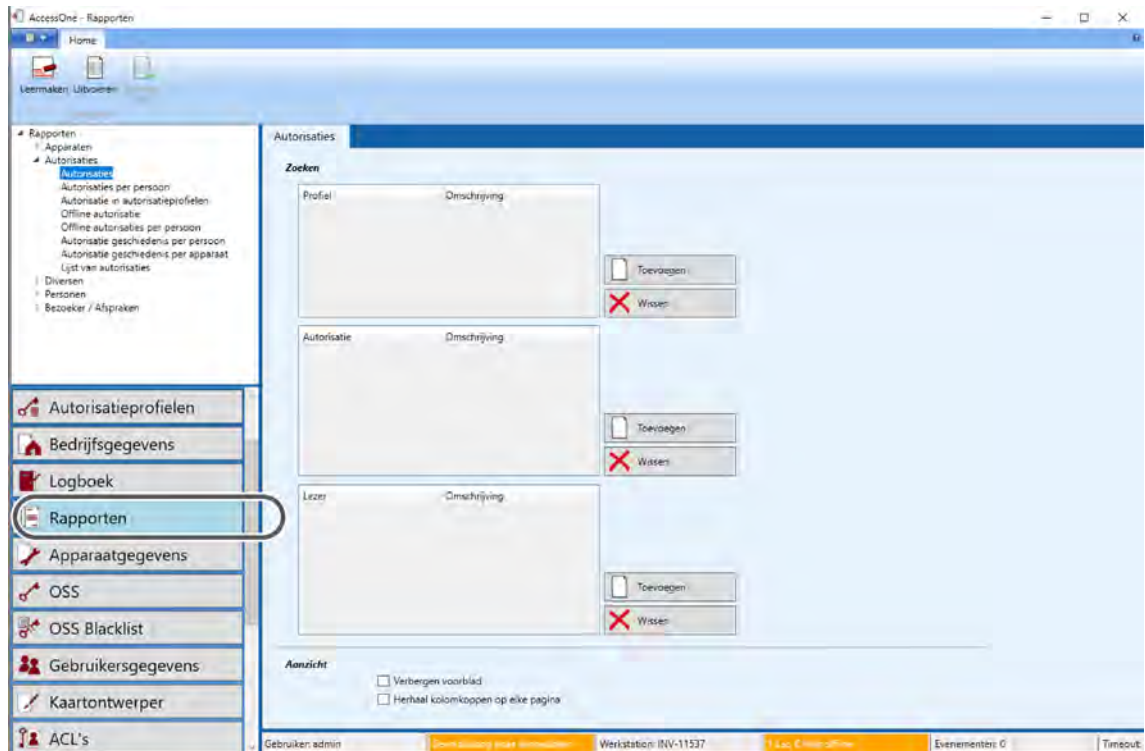
In het tabblad "Persoonstoegangsrechten" kunnen voor de betreffende personengroep toegangsrechten worden toegevoegd en gewist door bestanden te importeren of een profiel en een toegangsrecht in te voeren. Bevestig wijzigingen altijd met **Wijzigingen toepassen**.

11 Systeemdocumentatie

Voor de documentatie van het systeem op een bepaald tijdstip kunnen rapporten worden gegenereerd en logboekvermeldingen worden bekeken en geëxporteerd.

11.1 Rapporten

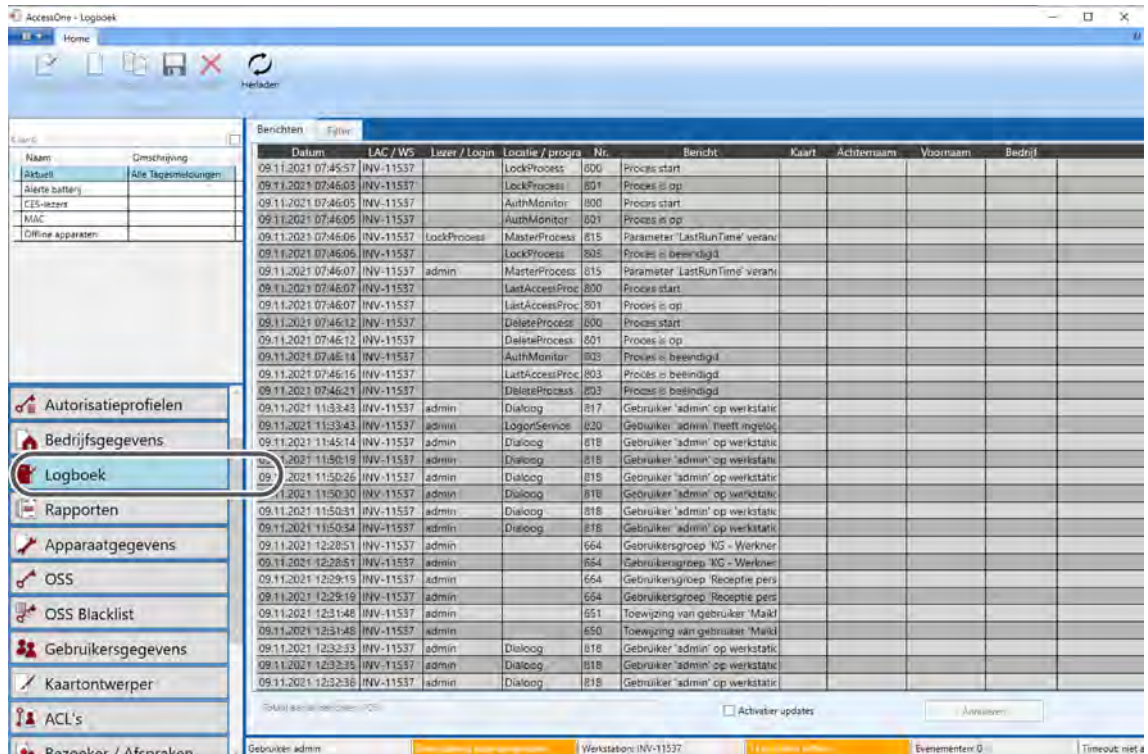
Via de dialoogselectie "Rapporten" kunnen alle vermeldingen worden bekeken en gepubliceerd. AccessOne kan te allen tijde een volledige systeemdokumentatie publiceren.



11.2 Logboek

Het dialoogvenster "Logboek" maakt het oproepen van alle actuele dagmeldingen en het aanmaken van individuele filters mogelijk.

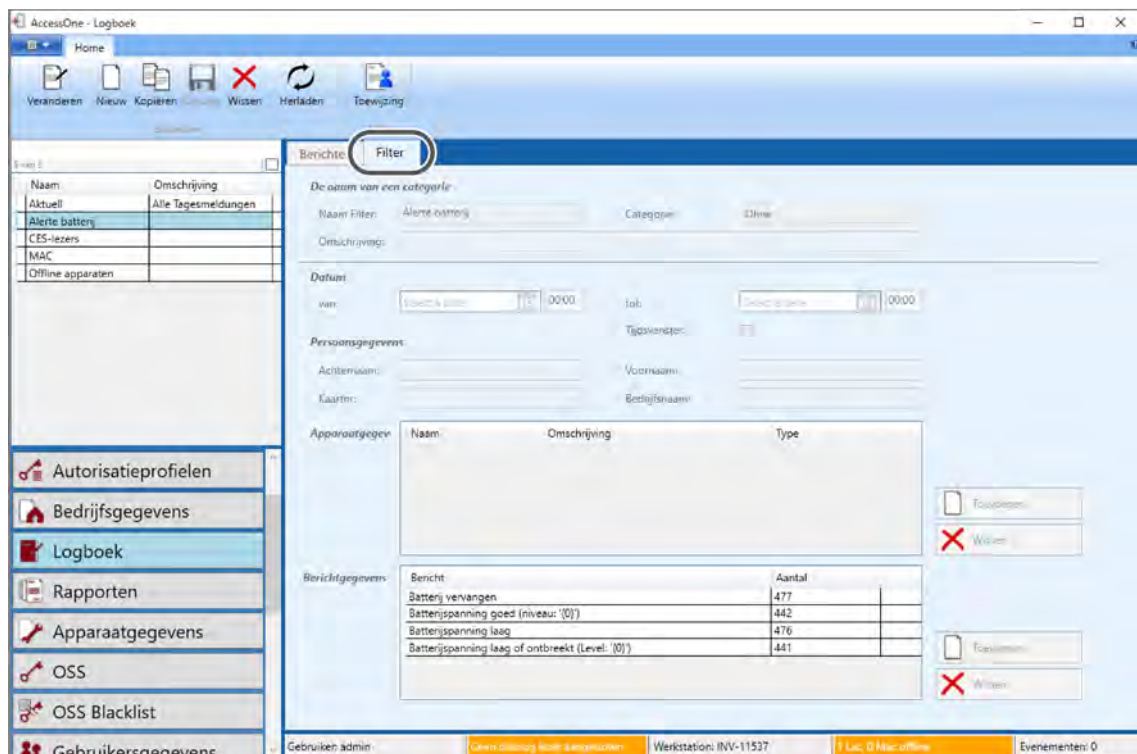
11.2.1 Berichten



Naam	Omschrijving	Datum	LAC / WS	Luser / Login	Locatie / progra	Nr.	Bericht	Kaart	Achternnaam	Voornaam	Bedrijf
Aktueel	Alle Tagesmeldungen	09.11.2021 07:45:57	INV-11537		LockProcess	600	Process start				
Alerte battery		09.11.2021 07:46:03	INV-11537		LockProcess	601	Process is op				
CES-lezers		09.11.2021 07:46:05	INV-11537		AuthMonitor	600	Process start				
MAC		09.11.2021 07:46:05	INV-11537		AuthMonitor	601	Process is op				
Offline apparaten		09.11.2021 07:46:06	INV-11537		LockProcess	615	Parameter 'LastRunTime' veranderd				
		09.11.2021 07:46:06	INV-11537		LockProcess	605	Process is beëindigd				
		09.11.2021 07:46:07	INV-11537	admin	MasterProcess	615	Parameter 'LastRunTime' veranderd				
		09.11.2021 07:46:07	INV-11537		LastAccessProc	600	Process start				
		09.11.2021 07:46:07	INV-11537		LastAccessProc	601	Process is op				
		09.11.2021 07:46:12	INV-11537		DeleteProcess	600	Process start				
		09.11.2021 07:46:12	INV-11537		DeleteProcess	601	Process is op				
		09.11.2021 07:46:14	INV-11537		AuthMonitor	603	Process is beëindigd				
		09.11.2021 07:46:16	INV-11537		LastAccessProc	603	Process is beëindigd				
		09.11.2021 07:46:21	INV-11537		DeleteProcess	603	Process is beëindigd				
		09.11.2021 11:33:43	INV-11537	admin	Dialoog	617	Gebruiker 'admin' op werksite				
		09.11.2021 11:33:43	INV-11537	admin	LogonService	620	Gebruiker 'admin' heeft ingelogd				
		09.11.2021 11:45:14	INV-11537	admin	Dialoog	618	Gebruiker 'admin' op werksite				
		09.11.2021 11:50:19	INV-11537	admin	Dialoog	618	Gebruiker 'admin' op werksite				
		09.11.2021 11:50:26	INV-11537	admin	Dialoog	618	Gebruiker 'admin' op werksite				
		09.11.2021 11:50:30	INV-11537	admin	Dialoog	618	Gebruiker 'admin' op werksite				
		09.11.2021 11:50:31	INV-11537	admin	Dialoog	618	Gebruiker 'admin' op werksite				
		09.11.2021 11:50:34	INV-11537	admin	Dialoog	618	Gebruiker 'admin' op werksite				
		09.11.2021 12:28:51	INV-11537	admin		664	Gebruikersgroep IG - Werker				
		09.11.2021 12:28:51	INV-11537	admin		664	Gebruikersgroep IG - Werker				
		09.11.2021 12:29:19	INV-11537	admin		664	Gebruikersgroep Receptie pers				
		09.11.2021 12:29:19	INV-11537	admin		664	Gebruikersgroep Receptie pers				
		09.11.2021 12:31:48	INV-11537	admin		651	Toewijzing van gebruiker 'Maid'				
		09.11.2021 12:31:48	INV-11537	admin		650	Toewijzing van gebruiker 'Maid'				
		09.11.2021 12:32:33	INV-11537	admin	Dialoog	618	Gebruiker 'admin' op werksite				
		09.11.2021 12:32:35	INV-11537	admin	Dialoog	618	Gebruiker 'admin' op werksite				
		09.11.2021 12:32:38	INV-11537	admin	Dialoog	618	Gebruiker 'admin' op werksite				

11.2.2 Filter

Bepaal uw specifieke filters. AccessOne biedt talloze invoermogelijkheden.



Filter

De naam van een categorie:

Naam Filter: Categorie:

Omschrijving:

Datum:

van: tot:

Tijdsperiode:

Persoonsgegevens:

Achternnaam: Voornaam:

Kaart: Bedrijfsnaam:

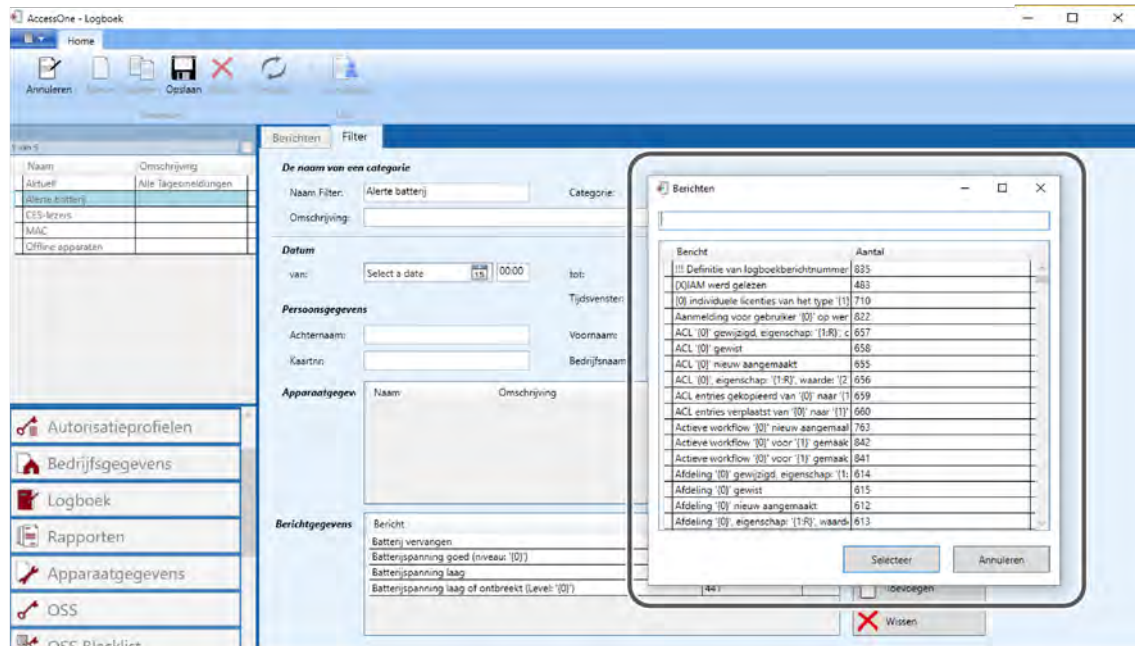
Apparaatgegevens:

Naam	Omschrijving	Type

Berichtgegevens:

Bericht	Aantal
Batterij vervangen	477
Batterijspanning goed (niveau: '0')	442
Batterijspanning laag	476
Batterijspanning laag of ontbreekt (Level: '0')	441

Via de knop **Toevoegen** wordt een venster opgeroepen dat alle apparaat- en berichtgegevens opsomt waarop kan worden gefilterd.



12 Probleemoplossing

Verbinding van de clients met AccessOneServer werkt niet	In de installatiemap	Controleer de vermeldingen in het bestand ClientConfig.xml in Installationsverzeichnis\AccessOne\config. Komen de vermeldingen voor "MasterHost" en "MasterPort" overeen?
	Op de server	- Zijn de SQL-server en de SQL-browserservice opgestart en zijn de protocollen TCP/IP en Named Pipes geactiveerd? - Controleer de regels voor de firewall. SQL-serverpoort (Standaard: TCP 1433), SQL-browserpoort (standaard: UDP 1434) en zijn de geconfigureerde AccessOnePorts (bijv. TCP 50000-500xx) toegankelijk?
	Samenwerking Serverclient	Is de tijd op de client en de AccessOneServer synchroon? Een tijdsverschil van minder dan 5 minuten is toegelaten.



C. Ed. Schulte GmbH
Zylinderschlossfabrik

Friedrichstraße 243

D-42551 Velbert

☎ +49 2051 204 0

☎ +49 2051 204 229

✉ info@ces.eu