2N Access Commander

Installatiehandleiding

2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Inhoudsopgave

Gebruikte symbolen en termen 6

Algemene informatie 7

Gebruikersrechten 7

Ondersteunde apparaten en applicaties 8

Ondersteunde apparaten 8

web browsers 9

Virtualisatieplatforms 9

Poorten gebruikt 10

Licentie 10

Installatie 13

Distributie via Access Commander Box 13

Distributie via virtuele machine 13

Aanbevolen hardware 15

Technische parameters 16

Aanbevolen hardware 16

Licentie activatie 17

Het licentiebestand verkrijgen 17

Licentie uploaden 17

Verlenging van licentie 18

Elektronische sloten 19

Fortis Commander 19

De kaart updaten 22

Compatibele kaarten 22

Tijdprofielen op elektronische sloten 23

Fortis Commander 23

Instellingen voor IP-apparaatlezer 26

Vergrendelingen instellen in Access Commander 27

Onderhoudskaarten 29

Basistoegang tot de interface 30

Dashboard 31

Verandering van taal 31

verander het wachtwoord van je account 31

Verander je profielfoto 32

Logo's 33

Systeemlogboeken 33

Export van logo's 33

Levensduur van logboeken 33

Toegang tot logboeken 34

Export van logo's 35

Levensduur van logboeken 35

Kennisgeving 35

Notificatie instellingen 36

Levensduur van logboeken 36

Bedrijven 38

Het creëren van een nieuw bedrijf 38

Bedrijfsinstellingen 38

De taal van de samenleving 38

Zones 38

My2N app 38

Bezoeken 38

Werkfonds 39

Vakantie 39

E-mails verzonden naar bedrijfsleden ... 39
Bedrijfssynchronisatie (LDAP) ... 40
Gebruikers importeren in het bedrijf ... 41

Gebruikers ... 44
Maak een nieuwe gebruiker aan ... 45
Gebruikersinstellingen ... 45
De naam en foto van de gebruiker wijzigen ... 45
Authenticatie ... 45
Rekening ... 47
Persoonlijke gegevens ... 48
Benaderingen ... 48
Telefoonnummers ... 48
Toegangslogboek ... 48
Wijzig logboek ... 48
Vingerafdruk uploaden ... 49
Bluetooth-authenticatie ... 49
Gebruikersrechten ... 50
Aanwezigheidsregistratie van gebruikers ... 51

Groepen ... 53
Maak een nieuwe groep ... 53
Groepsinstellingen ... 53
Leden ... 53
Toegangsregels ... 53

Zones ... 54
Een nieuwe zone creëren ... 54
Zone-instellingen ... 54
Authenticatie met meerdere factoren ... 54
Toegang tot instellingen ... 55
Apparaat ... 55
Slotgroepen ... 55
Bedrijven ... 55
Toegangsregels ... 55

Apparaat ... 56
IP-apparaat toevoegen ... 56
Slotgroepen ... 57
Groepen bekijken ... 57
Een nieuwe slotgroep aanmaken ... 57
Vergrendelingen instellen in Access Commander ... 57
Noodvergrendeling ... 59
Apparaat instellingen ... 59
Overzicht ... 60
Telefoongesprek ... 61
Tillen ... 62
Toezicht houden ... 63
Firmware ... 63
Uitsluiting van apparaten ... 64
Incompatibele firmwareversie ... 64
Beveiliging ... 64
Hoe kunt u certificaten beheren ... 65
Instellingen voor invoer-/uitvoerapparaat ... 65

Toegangsregels ... 67
Matrixweergave ... 67
Een voorbeeld van een matrixrepresentatie ... 68
Lijst met regels ... 68

Tijdprofielen 69
Tijdprofielen op elektronische sloten 69
Een tijdprofiel aanmaken 69
Het tijdprofiel instellen 70
Aanwezigheid 71
Aanwezigheid van een specifieke gebruiker 71
Wijzig de aanwezigheid van gebruikers 71
Aanwezigheidsinstellingen 72
Instellingen voor invoer-/uitvoerapparaat 72
Bezoeken 74
Instellen van het bewaren van bezoekersgegevens 74
Een nieuw bezoek aanmaken 74
Einde bezoek 74
Bezoek instellingen 75
Benaderingen 75
Bezoek 75
Persoonlijke gegevens 75
Authenticatie 75
Toegangslogboek 75
Kaarten 75
Een beveiligde kaart beheren met een USB-lezer 76
Aanwezigheid 77
Verstrijken van de aanwezigheid van de gebruiker 77
Rapporten 78
Gebiedsbeperkingen 79
Gebiedsbeperkingen instellen 79
Input en output 79
Bezetting 79
Anti-passback 80
Een uitzondering instellen 80
Lijst met geblokkeerde gebruikers 80
Beperkingen opnieuw instellen 80
Creëer een gebied om te beperken 81
De meest voorkomende installatiefouten 81
Een voorbeeld van het instellen van beperkingen 82
Systeem instellingen 83
Linux-instellingen 83
Systeem update 84
Downgrade 84
Beta testen 85
Systeemback-up 85
Synchronisatie van gebruikers 86
Datum en tijd 88
Tijdsynchronisatie met apparaten 88
Automatisering 89
Automatiseringen creëren 89
Veilige modus (safe mode) 90
Knooppunten (nodes) Access Commander 90
Voorbeelden van stromen (flows) 92
Streams exporteren/importeren 94
Foutstatussen 95
Installatienaam 95
De e-mailfunctie (SMTP) inschakelen en instellen 95
Tweefactorauthenticatie 96

Aanwezigheidsinstellingen 96
Instellingen voor invoer-/uitvoerapparaat 97
Sta SSH-toegang toe 98
Encryptiesleutels voor My2N-applicatie 99
Compatibiliteitsmodus voor RFID-kaarten 100
PICard-sleutels 100
USB-lezers ingeschakeld 101
CAM-logboeken 101
CAM-logo's instellen 101
Elektronische sloten 102
Fortis Commander 102
De kaart updaten 105
Compatibele kaarten 105
Tijdprofielen op elektronische sloten 106
Onderhoudskaarten 106
Probleemoplossen 107
Diagnostische logboeken 107
Gebruiksstatistieken 107
Kennisgeving 107
Notificatie instellingen 107
Netwerkinstellingen 109
Detectie van wijziging van het IP-adres van het apparaat 109
Proxy-instellingen 109
NodeRed gebruiken 110
Extra informatie 111
HTTP-API 111
SignalR 111
Licenties van derden 111

Gebruikte symbolen en termen

In de handleiding worden de volgende symbolen en pictogrammen gebruikt:

GEVAAR
Altijd naleven deze instructies om het risico op letsel te voorkomen.

WAARSCHUWING
Altijd naleven deze instructies om schade aan het apparaat te voorkomen.

LET OP
Belangrijke waarschuwing. Als u de instructies niet opvolgt, kan het apparaat defect raken.

TIP
Bruikbare informatie voor eenvoudiger en sneller gebruik of installatie.

OPMERKING
Procedures en advies voor effectief gebruik van apparaatfuncties.

Algemene informatie

2N Access Commander is een softwaretool voor het beheer van bulktoegangssystemen. Koppel Access Commander is toegankelijk via een webbrowser.

Instellingen kunnen binnen één installatie worden uitgevoerd **Access Commander** verdelen in **Door de samenleving**, die afzonderlijk worden beheerd. Deze werkwijze maakt het mogelijk om de administratie te verdelen over beheerders van individuele bedrijven. Een beheerder van het ene bedrijf heeft geen toegang tot informatie over een ander bedrijf.

Toevoegen **Apparaat** naar **Commandant voor toegang** voor toegangscontrole. De apparaten zijn fysieke eenheden in een gebouw die ingangen (2N-intercoms, 2N-toegangscontrole-eenheden, 2N elektronische sloten) of communicatie mogelijk maken (2N-antwoordapparaten). De apparaten zijn gegroepeerd in **Zones**. Elk apparaat kan zich maar in één zone bevinden.

Zones of faciliteiten kunnen door bedrijven worden gedeeld, waardoor het beheer van bedrijven toegang krijgt tot gemeenschappelijke ruimtes (ingangen, restaurants, vergaderzalen...).

Gebruikers zijn individuele mensen wier beweging door het gebouw moet worden beheerd, of die kunnen worden gebeld vanaf aangesloten apparaten. Gebruikers zijn gegroepeerd in **Groepen**, waarin massabeheer van hun toegang tot zones wordt uitgevoerd. De gebruiker authenticeert zich op het apparaat en het apparaat evalueert vervolgens of de gebruiker geldige toegang tot het apparaat heeft. De geldigheid van de toegang wordt bepaald door **Toegangsrechten**. Geselecteerde gebruikers kunnen ook beheerdersrechten hebben Access Commander of delen daarvan.

Tijdprofielen zij stellen de tijden in waarop het apparaat toegang geeft of waarop gebruikers gebeld kunnen worden.

Aanwezigheidsmodule maakt het mogelijk om de aanwezigheid van gebruikers te monitoren.

Aanwezigheidsmodule Hiermee kunt u bijhouden in welke zones gebruikers zich momenteel bevinden.

Bezoeken zijn mensen van wie de toegangsrechten slechts voor een beperkte tijd geldig zijn.

Gebruikersrechten

Rapporteer binnen Access Commander kan door meerdere gebruikers worden uitgevoerd, afhankelijk van de rechten die aan hen zijn toegewezen.

Verhoogde accounts worden ingesteld via een rol in de gebruikersinstellingen. Er kunnen meerdere rollen aan één gebruiker worden toegewezen.

OPMERKING
Gebruikersmachtigingen zijn van toepassing op het beheer binnen het bedrijf van de gebruiker. De beheerder heeft toegang tot het volledige beheer van bedrijven.

Beheerder

- Instelling van het systeem en de afzonderlijke modules volgens de geldige licentie.
- Licentiewijziging

- Alle machtigingen van andere rollen zijn van toepassing op alle bedrijven.

Toegangsbeheerder

- Groepen maken en beheren.
- Beheer hun groepslidmaatschappen.
- Bezoeken aanmaken en beheren.
- Tijdprofielen aanmaken en beheren.
- Toegangsregels instellen.

Gebruikersbeheerder

- Gebruikers aanmaken en beheren.
- Bezoeken aanmaken en beheren.
- Beheer hun groepslidmaatschappen.
- Het toegangs- en systeemlogboek bekijken.

Bezoekt beheerder

- Bezoeken aanmaken en beheren.
- Beheer hun groepslidmaatschappen.
- Het toegangslogboek van bezoeken bekijken.

Deurbeheerder

- Bewaking van cameratransmissie vanaf toegewezen apparaten.
- Op afstand openen van toegewezen apparaten.
- Noodvergrendeling van toegewezen apparaten.
- Het toegangslogboek van toegewezen apparaten bekijken.
- Bewaking van statussen en beveiligingsgebeurtenissen in het systeemlogboek.

Aanwezigheidsmanager

- Het monitoren en beheren van de aanwezigheid van toegewezen groepen.
- Het toegangslogboek bekijken van gebruikers van toegewezen groepen.

Ondersteunde apparaten en applicaties

In dit hoofdstuk worden de ondersteunde apparaten, ondersteunde webbrowsers en compatibele virtualisatieplatforms vermeld waarmee Access Commander kan worden geïnstalleerd.

Ondersteunde apparaten

Hieronder vindt u een overzicht van de apparaten die door het toegangssysteem worden ondersteund Access Commander. Deze apparaten kunnen in het systeem worden beheerd.

OPMERKING
De ondersteunde firmwareversies van deze apparaten staan vermeld in het hoofdstuk Firmware (p. 63).

Intercoms 2N

- 2N IP Style – ondersteunt het lezen van QR-codes
- 2N IP Verso 2.0 – ondersteunt het lezen van QR-codes
- 2N IP Force 2.0 – ondersteunt het lezen van QR-codes

- 2N IP Verso
- 2N LTE Verso
- 2N IP One
- 2N IP Force
- 2N IP Safety
- 2N IP Vario
- 2N IP Base
- 2N IP Solo
- 2N IP Uni
- 2N IP Video Kit
- 2N IP Audio Kit
- 2N IP Audio Kit Lite

Toegangseenheden 2N

- Access Unit QR – ondersteunt het lezen van QR-codes
- 2N Access Unit 2.0
- 2N Access Unit
- 2N Access Unit M

2N elektronische sloten

- 2N Fortis Handle
- 2N Fortis Cylinder

Reactie-eenheden 2N

- 2N Indoor View (Wi-Fi)
- 2N Indoor Compact
- 2N Indoor Talk
- 2N Indoor Touch 2.0
- 2N Clip
- 2N Clip 2wire-IP

web browsers

Access Commander wordt geconfigureerd via de webinterface. Het systeem is geoptimaliseerd voor Google Chrome (versie 90 en hoger).

Andere ondersteunde browsers:

- Mozzila Firefow (versie 35 en hoger)
- Microsoft Edge (versie 84.0.522 en hoger)
- Safari (versie 14 en hoger)

Andere browsers zijn niet getest, dus de volledige functionaliteit ervan kan niet worden gegarandeerd.

Virtualisatieplatforms

- Virtual Box
- VMware Player (versie 6.5 en hoger)
- VMware vSphere (versie 6.5 en hoger)
- Hyper-V

Poorten gebruikt

Lijst met services en vereiste poorten

Dienst	Haven
HTTP//HTTPS[a.]	80/443
SMTP	225
DHCP	68
DNS	53
NTP	123
LDAP*[b.]	389
SSH	22

[a.] Het wordt zowel gebruikt voor de communicatie met de opdrachtgever als voor de communicatie met de poortwachters.
[b.] De gebruiker kan dit doen in de instellingenAccess Commanderkies een andere poort voor de LDAP-service.

Licentie

Na de eerste installatie Access Commander er is een proeflicentie beschikbaar. Met de proeflicentie kunt u alle functies testen op het beheer van 1 apparaat en 5 gebruikers. Voor volledig beheer dient u één van de vier licenties te activeren: *Basis* (vrij), *Geavanceerd*, *Voor* of *Voor onbeperkt*, zien licentieoverzichttabel (p. 10).

Licentie:	Trial	Basic	Advanced	Pro	Unlimited
Bestellingsnummer	n/a	n/a	91379031	91379032	91379033
Maximaal aantal gebruikers	5	50	300	1000	Onbeperkt[a.]
Maximaal aantal apparaten (zowel geactiveerd als gedeactiveerd)	1	5	30	100	Onbeperkt[a.]
Maximaal aantal beheerders/managers	5	1	5	1000	Onbeperkt[a.]

Licentie:	Trial	Basic	Advanced	Pro	Unlimited
Bestellingsnummer	n/a	n/a	91379031	91379032	91379033
Toegangs- en systeemlogboeken	✓	✓	✓	✓	✓
Toegangsregels	✓	✓	✓	✓	✓
API-beheer	✓	✓	✓	✓	✓
Accountactivering/-deactivering	✓	✓	✓	✓	✓
Beperking van het aantal mislukte toegangen	✓	✓	✓	✓	✓
Stil alarm	✓	✓	✓	✓	✓
Zonecode	✓	✓	✓	✓	✓
Apparaatbewaking	✓	✓	✓	✓	✓
Logboekbeheer	✓	✓	✓	✓	✓
Beheer van elektronische sloten	✓	✓	✓	✓	✓
Importeer gebruikers uit CSV of vanaf apparaten	✓	×	✓	✓	✓
Bulkbeheer van firmware	✓	×	✓	✓	✓
Meerdere authenticatie	✓	×	✓	✓	✓
Autorisatie van gebruiker	✓	×	✓	✓	✓
Kennisgeving	✓	×	✓	✓	✓
Aanwezigheid	✓	×	✓	✓	✓

Licentie:	Trial	Basic	Advanced	Pro	Unlimited
Bestellingsnummer	n/a	n/a	91379031	91379032	91379033
API-toegangssleutel	✓	×	✓	✓	✓
CAM-logboeken	✓	×	✓	✓	✓
Liftbediening	✓	×	✓	✓	✓
Dashboard	✓	×	✓	✓	✓
Noodvergrendeling	✓	×	✓	✓	✓
Ondersteuning voor mobiele inlog-gegevens	✓	×	✓	✓	✓
Bezoek beheer	✓	×	✓	✓	✓
Automatisering	✓	×	✓	✓	✓
Bezettingsbeheer	✓	×	×	✓	✓
Synchronisatie (LDAP & CSV)	✓	×	×	✓	✓
Anti-passback	✓	×	×	✓	✓
Aanwezigheid	✓	Optio-neel	Optioneel	Optioneel	Optioneel

[a] Onbeperkt binnen de maximale mogelijkheden van het softwareplatform, nl Aanbevolen hardware (p. 16)

Installatie

Access Commanderkan op twee manieren worden verdeeld:

- Een kleine desktopcomputer 2N Access Commander Box 2.0 (bestelnr. 1120120xx)
- Virtuele computer

Oplossing Access Commander Boxis beperkt tot 2000 aangesloten apparaten. Overige softwarefuncties zijn voor beide oplossingen identiek.

Distributie via Access Commander Box

Access Commander Box 2.0 (1120120xx, 03129-00) is een compacte desktop-minicomputer met voorgeïnstalleerde software. Het is een "plug and play" oplossing waarbij je alleen een voeding en een Ethernet-kabel hoeft aan te sluiten op deze minicomputer. Voor een goede en volledige werking van het systeem wordt aanbevolen om deze minicomputer op een veilige plaats te zetten en permanent te laten werken. De Access Commander Box 2.0 dient als server voor het verzamelen van gegevens, gebeurtenissen en logbestanden van het hele toegangscontrolesysteem.

Wij raden aan om het aantal van 1500 gebruikers in de groep niet te overschrijden. Als er beperkingen zijn voor gebieden, zoals anti-passback of bezettingsbeheer voor een groot aantal gebruikers, kan de applicatie vertragen.

Inloggen Access Commander **met een dynamisch IP-adres**

1. Aansluiten Access Commander Box met het netwerk via een Ethernet-kabel.
2. Met behulp van de app2N IP-netwerkscanner lokaliseren Access Commander Box in het netwerk.
3. Ga in uw webbrowser naar het IP-adres Access Commander Box en meld u aan Access Commander. Het standaardwachtwoord van de Admin-gebruiker is 2n en moet na het inloggen worden gewijzigd.

OPMERKING
Bij distributie via Access Commander Box verbinding maken met de webinterface vanaf een andere computer in het netwerk. Besturingssysteem Access Commander Box zorgt voor werking Access Commander en de standaard Linux-installatie zorgt ervoor dat de webbrowser niet kan worden uitgevoerd.

Een statisch adres instellen Access Commander **hulp** Access Commander Box

1. Aansluiten Access Commander Box met het netwerk via een Ethernet-kabel.
2. Verbinden aan Access Commander Box toetsenbord en monitor. Er verschijnt een zwart scherm.
3. Log in op het systeem als “wortel” met wachtwoord “2n”. Zodra het blauwe scherm verschijnt, wijzigt u het standaardwachtwoord.
4. Selecteer in het menu Geavanceerd “Netwerken” en vervolgens “Statisch ip”.
5. Stel een statisch IP-adres, gateway en DNS in.
6. Sla deze instelling op en gebruik uitloggen om het consolemenu te verlaten.
7. Maak via een webbrowser verbinding met het ingestelde IP-adres.

Distributie via virtuele machine

Access Commander kan worden gedistribueerd als een virtuele machine. Hieronder staan de installatieprocedures op ondersteunde virtualisatieplatforms.

Virtual Box

TIP
Het wordt aanbevolen om VT-X-virtualisatietechnologie in het BIOS in te schakelen.

1. Download de nieuwste versie van VirtualBox van https://www.virtualbox.org/wiki/Downloads.
   Het wordt aanbevolen om de versie inclusief het VirtualBox Extension Pack te downloaden.
2. Download de juiste software via de sectie Ondersteuning > Downloadcentrum > Software en firmware op 2N.com. Na het downloaden pak je het bestand uit.
3. Open VirtualBox en selecteer "Bestand - App importeren...".
4. Bewerk de titel.
5. Controleer CPU-instellingen (minimaal 2), RAM-instellingen (minimaal 2048 MB) en netwerkkaartselectie.
6. Bevestig de licentievoorwaarden.
   Na de installatie wordt de Linux-configuratieconsole geopend, waar u basissysteeminstellingen kunt uitvoeren. De volledige configuratie gebeurt in de webinterface.

VMware Player

LET OP
De ondersteunde versie van VMWare is 6.5 en hoger.

1. Download de juiste software via de sectie Ondersteuning > Downloadcentrum > Software en firmware op 2N.com. Na het downloaden pak je het bestand uit.
2. Selecteer in VMware Player "Bestand – Openen..." het pad naar het OVA-bestand.
3. Hernoem indien nodig en klik op "Importeren".
4. Controleer CPU-instellingen (minimaal 2), RAM-instellingen (minimaal 2048 MB) en netwerkkaartselectie.
   Na de installatie wordt de Linux-configuratieconsole geopend, waar u basissysteeminstellingen kunt uitvoeren. De volledige configuratie gebeurt in de webinterface.

VMware vSphere

LET OP
De ondersteunde versie van VMWare is 6.5 en hoger.

1. Download de juiste software via de sectie Ondersteuning > Downloadcentrum > Software en firmware op 2N.com. Na het downloaden pak je het bestand uit.
2. Selecteer in VMware vSphere "File – Deploy OVF Template" en volg de wizard.
3. Controleer na het importeren de instellingen "Edit Settings..."
   Bewerk de naam (op het tabblad Options).

4. Controleer CPU-instellingen (minimaal 2), RAM-instellingen (minimaal 2048 MB) en netwerkkaartselectie.
   Na de installatie wordt de Linux-configuratieconsole geopend, waar u basissysteeminstellingen kunt uitvoeren. De volledige configuratie gebeurt in de webinterface.

Hyper-V

1. Download de juiste software via de sectie Ondersteuning > Downloadcentrum > Software en firmware op 2N.com. Na het downloaden pak je het bestand uit.
2. Start Hyper-V Manager en selecteer de optie voor de gewenste host Import Virtual Machine.
3. Controleer in de installatiehandleiding de weergegeven informatie en bevestig het lezen ervan met de knop Next.
4. Selecteer het mappad uit stap 1.
5. Bevestig de selectie van de virtuele machine.
6. Selecteer het importtype.
7. Selecteer de virtuele NIC voor de virtuele machine.
8. Controleer het overzicht van de instellingen die in de voorgaande stappen zijn geselecteerd en bevestig met de knop Finish.
   Na de installatie wordt de Linux-configuratieconsole geopend, waar u basissysteeminstellingen kunt uitvoeren. De volledige configuratie gebeurt in de webinterface.

Aanbevolen hardware

Het aantal aangesloten apparaten is van invloed**Access Commander**. Stel daarom de grootte van de hardware-elementen in op basis van de werkelijke toestand. De onderstaande tabel toont het aanbevolen minimumaantal CPU-kernen en RAM-groottes voor verschillende aantallen beheerde apparaten en gebruikersAccess Commander.

LET OP
Het wordt aanbevolen om een continue verbinding tussen te onderhouden Access Commander en apparaten. Als de verbinding wordt verbroken, slaan apparaten gebeurtenislogboeken offline op, en als ze opnieuw worden verbonden, worden de loggegevens gesynchroniseerd Access Commander. Tijdens het synchronisatieproces blijft de applicatie draaien, maar bij een groter aantal apparaten kan het hele proces langer duren.

Hardware voor virtuele machines

Aantal apparaten	aantal gebruikers	Minimumaantal CPU-kernen	Minimale RAM-grootte	Minimale toewijzing van harde schijven
1 000	10 000	2	2 GB	120 GB
2 000	100 000	2	4GB	120 GB
2 000	200 000	4	8 GB	120 GB

Aantal apparaten	aantal gebruikers	Minimumaantal CPU-kernen	Minimale RAM-grootte	Minimale toewijzing van harde schijven
7 000	200 000	4	16 GB	120 GB

Technische parameters

Opties voor Access Commander Box 2.0

Aantal aangesloten apparaten	Aantal gebruikers	Aantal gebruikers in de groep
7 000	200 000	1 500

Technische parameters van Access Commander Box

1e generatie

Onderdeel. Nr. 91379030

- afmetingen: 56,1 x 107,6 x 114,4 mm (2,21" x 4,24" x 4,50")
- Intel-processor® Celeron® J3160 (2M cache; max. 2,24 GHz)
- 2,5" SSD SATA III harde schijf (120 GB)
- DDR3 SODIMM-geheugen (4 GB) – 1,35 V, 1600 MHz
- Ondersteuning voor twee schermen via VGA- en HDMI-poort
- Gigabit LAN-poort voor Ethernet-verbinding
- VESA-montageframe (75 x 75 mm + 100 x 100 mm)
- Opslagtemperatuur: -20 °C tot +60 °C
- Omgevingstemperatuur tijdens bedrijf: 0 °C tot +35 °C

2e generatie

Onderdeel. Nr.
1120120E, 1120120GB, 1120120US

- afmetingen: 127.5 x 132 x 57.6 mm (5.02 " x 5.20" x 2.27")
- Intel® Processor N100, 6W TDP
- SSD 980 NVMe M.2 – 250 GB
- DDR4 SO-DIMM memory – 16 GB, 1,2 V, 3200 MHz
- Ondersteuning voor HDMI 2.1, DisplayPort 1.4 en VGA VGA
- 2.5G RJ45 LAN-poort voor Ethernet-aansluiting
- Opslagtemperatuur: -40 °C tot +85 °C
- Bedrijfstemperatuur: 0 °C tot +50 °C

Aanbevolen hardware

Het aantal aangesloten apparaten is van invloed**Access Commander**. Stel daarom de grootte van de hardware-elementen in op basis van de werkelijke toestand. De onderstaande tabel toont het aanbevolen minimumaantal CPU-kernen en RAM-groottes voor verschillende aantallen beheerde apparaten en gebruikersAccess Commander.

LET OP
Het wordt aanbevolen om een continue verbinding tussen te onderhouden Access Commander en apparaten. Als de verbinding wordt verbroken, slaan apparaten gebeurtenislogboeken offline op, en als ze opnieuw worden verbonden, worden de logge-gevens gesynchroniseerd Access Commander. Tijdens het synchronisatieproces blijft de applicatie draaien, maar bij een groter aantal apparaten kan het hele proces langer duren.

Hardware voor virtuele machines

Aantal appara-ten	aantal gebrui-kers	Minimumaan-tal CPU-kern-en	Minimale RAM-grootte	Minimale toewijzing van harde schijven
1 000	10 000	2	2 GB	120 GB
2 000	100 000	2	4GB	120 GB
2 000	200 000	4	8 GB	120 GB
7 000	200 000	4	16 GB	120 GB

Licentie activatie

Om te activeren moeten licenties worden verkregen *licentie bestand* en upload het naar Access Commander. De Basislicentie kan direct worden geactiveerd in Access Commander op de pagina Instellingen > tabblad Licentie.

Het licentiebestand verkrijgen

Om een licentie te verkrijgen, moet u de distributeur het serienummer geven van een van de 2N-apparaten die zijn aangesloten op de **Access Commander**. Het licentiebestand wordt gegenereerd op basis van het serienummer van dit gelicentieerde apparaat. Dit moet het serienummer zijn van de hoofdintercomeenheid, toegangseenheid of antwoordeenheid (2N Indoor Touch kan niet worden gebruikt).

Verbinding *gelicentieerd apparaat* garandeert de geldigheid van de licentie. In geval van ontkoppeling van het gelicentieerde apparaat begint een beschermingsperiode, waarna de licentie wordt opgeschort.

Licentie uploaden

LET OP

- Na het overstappen van de Proeflicentie is het niet meer mogelijk om de Proeflicentie opnieuw te activeren.
- Geavanceerde functie-instellingen die niet door de nieuwe licentie worden ondersteund, worden niet opgeslagen.

1. Ga naar **Instellingen > tabblad Licentie**.
2. Klik op Licentie uploaden en upload in het open venster het licentiebestand verkregen uit de repository.
3. Na het uploaden van het bestand klikt u op Activeer de licentie.
4. Zorg ervoor dat het gelicentieerde apparaat waarvoor de licentie is gegenereerd, is geactiveerd.

licentie apparaat	Geselecteerd 2N-apparaat waarmee verbinding is gemaakt Access Commander, die de geldigheid van de licentie garandeert. Het licentieapparaat dient als hardwaresleutel voor de licentie.
licentie bestand	Een bestand met een licentie, bij het uploaden wordt de licentie geactiveerd. Het licentiebestand wordt door de distributeur gegenereerd op basis van het serienummer van het licentieapparaat.

Verlenging van licentie

Om een geschorste licentie te herstellen, moet u het gelicentieerde apparaat verbinden en activeren of een nieuw licentiebestand laten genereren en uploaden voor een ander apparaat. Zodra een nieuwe licentie is geüpload, activeert u eerst het licentieapparaat waarvoor de licentie is gegenereerd. De andere apparaten kunnen pas worden geactiveerd als dit licentieapparaat is geactiveerd.

Een licentie wordt opgeschort wanneer de verbinding met het licentieapparaat wordt verbroken **Commandant voor toegang** gedurende een langere periode dan de beschermingsperiode. De duur van de beschermingsperiode is afhankelijk van hoe lang het licentieapparaat was aangesloten **Commandant voor toegang**. Raadpleeg de onderstaande tabel voor de waarden van de beschermingsperiode. Wanneer een licentie wordt opgeschort, worden alle verbonden apparaten automatisch uit het beheer verwijderd en gemarkeerd als onbeheerd

OPMERKING
Apparaten verwijderen uit het beheer betekent dat u geen wijzigingen kunt aanbrengen in hun configuratie via **Access Commander**. Wijzigingen in **Access Commander** worden niet doorgevoerd op het apparaat. De apparaten blijven echter werken op basis van de gegevens van de laatste configuratie die vanuit **Access Commander** is overgedragen. Dit betekent dat de toegangen en andere instellingen op de apparaten hetzelfde blijven als voordat de licentie werd opgeschort.

Je kunt de configuratie van een onbeheerd apparaat alleen wijzigen in de webconfiguratie-interface van het individuele apparaat. Wanneer het apparaat opnieuw wordt aangesloten op het beheer van **Access Commander**, wordt het apparaat gesynchroniseerd en worden wijzigingen die rechtstreeks in de webconfiguratie-interface van het apparaat zijn aangebracht, overschreven door de instellingen in **Access Commander**.

De hoeveelheid tijd waarmee het gelicentieerde apparaat verbonden is geweest Access Commander	**De beschermingsperiode waarvoor dit geldt** Access Commander **in bedrijf zonder aangesloten licentieapparaat**
minder dan 24 uur	1 dag
1 dag - 30 dagen	10 dagen

De hoeveelheid tijd waarmee het gelicentieerde apparaat verbonden is geweest Access Commander	**De beschermingsperiode waarvoor dit geldt** Access Commander **in bedrijf zonder aangesloten licentieapparaat**
31 dagen - 180 dagen	1 maand
meer dan 180 dagen	3 maanden

Elektronische sloten

Systeem **Commandant voor toegang** biedt toegangsbeheer via elektronische sloten 2N Fortisdie worden ontgrendeld met een RFID-kaart met MIFARE® DESfire®. Bij het configureren van elektronische sloten wordt aan elk slot een coderingssleutel toegewezen. De sleutels van de sloten worden vervolgens opgeslagen op de RFID-kaarten van geautoriseerde gebruikers. Als de sleutels op de kaart en in het slot overeenkomen, wordt het vergrendelingsmechanisme ontgrendeld.

Eén RFID-toegangskaart kan gebruikt worden om tot 90 deuren met sloten 2N Fortis te openen, afhankelijk van het aantal tijdsprofielen dat toegepast wordt. Als de geheugencapaciteit van de kaart overschreden wordt, zal het schrijven van gegevens naar de kaart mislukken. Het mislukte schrijven wordt geregistreerd in het toegangslogboek van het systeem. Als er Slotgroepen worden gebruikt, kunnen er meer deuren naar één kaart worden geschreven dan bij individuele toewijzing. Als er Slotgroepen worden gebruikt, kunnen er meer deuren per kaart worden geregistreerd dan bij een individuele toewijzing.

Fortis Commander

Fortis Commander is een standalone toepassing die de **Fortis** elektronische sloten verbindt met het **Access Commander** systeem. De toepassing stelt vergrendelingen in volgens het projectbestand dat is gemaakt in **Access Commander**u en dat de vergrendelingsconfiguratie bevat. Het bestand is gecodeerd en kan alleen op één specifieke installatie worden gebruikt.

Installatie

Fortis Commander is ontworpen om geïnstalleerd te worden op een Windows computer met Bluetooth Low Energy (BLE) ondersteuning.

De app is te vinden op de website 2N Download Centre.

Installatieprocedure

1. Download het installatiepakket van de opgegeven link.
2. Voer het installatieprogramma uit en voltooi de installatie door de instructies op het scherm te volgen.

Projectbestand

Het projectbestand wordt gemaakt in **Access Commander** en bevat de volledige projectconfiguratie. Het bestand is gecodeerd en beveiligd met een wachtwoord.

Vergrendelingen instellen in Access Commander

Voordat u sleutels naar afzonderlijke sloten uploadt, moet u **Access Commander** koppelen met **Fortis Commander**.

Master Encryption Key (MEK) genereren en projectvoorbereiding

1. Meld u aan bij Access Commander.
2. Ga naar de pagina **Instellingen > Elektronische sloten**.
3. Op de kaart **Eerste installatie** klik Sleutels genereren.

4. Maak een hoofdcoderingssleutel.

LET OP
De hoofdcoderingssleutel kan niet later zijn **tonen of wijzigen**.

OPMERKING
Volgens de master encryptiesleutel (MEK) genereert **2N Access Commander** een reeks encryptiesleutels. De sleutel moet dus uniek en voldoende veilig zijn. De sleutelset is gebaseerd op de master-encryptiesleutel, dus projecten met dezelfde master-encryptiesleutel genereren dezelfde sleutelsets. Als een project verloren gaat, kan een nieuw project met dezelfde mastercoderingssleutel aangemaakt worden en de codering voortzetten.

5. Nadat u de sleutels hebt gegenereerd en het wachtwoord voor het projectbestand hebt ingesteld, kunt u **het projectbestand** downloaden, dat een afbeelding is van de configuratie van het elektronische slot in het systeem **Access Commander**.
6. In het tabblad **van Fortis Commander** klikt u op Download toepassing, vanwaar het downloaden van **Fortis Commander** (toepassing voor het configureren van elektronische sloten) zal beginnen.

LET OP
Projectinformatie is gevoelige informatie. Bescherm het tegen misbruik.

Het elektronische slot configureren met Fortis Commander

1. Installeer **Fortis Commander** en open het.
2. Klik op Open project en open het gedownloade projectbestand in File Explorer.
3. Voer in het dialoogvenster dat verschijnt het wachtwoord voor het projectbestand in.
4. Selecteer na het openen van het projectbestand Verbinden met apparaat en bevestig de servicekaart aan het slot.
5. Klik op **Toewijzen**, waarmee de vergrendeling aan het project wordt toegewezen.
6. Koppel het apparaat los en klik op **Bestand > Project sluiten**.
7. Wanneer de configuratie voltooid is, opent u het systeem **Access Commander**. Ga naar het tabblad **Instellingen > Elektronische sloten** en klik opnieuw op Fortis Commander. Upload het projectbestand.

OPMERKING
Wanneer u het slot verplaatst tussen installaties of wanneer u een claim indient, moet u een **Fabrieksreset** uitvoeren. Deze handeling zet het slot terug naar de fabrieksinstellingen en verwijdert alle eerdere configuraties.

Procedure voor het bijwerken van de configuratie

1. Breng wijzigingen aan in **Access Commander**.
2. Download het nieuwe projectbestand.
3. Upload het bestand naar **Fortis Commander** en breng de vereiste wijzigingen in de vergrendelingen aan.

4. Als u andere wijzigingen aanbrengt in **Access Commander**u, download dan altijd een nieuw projectbestand.

LET OP
Voor elke configuratiewijziging in **Access Commander**u moet u een nieuw projectbestand downloaden - u kunt geen ouder bestand gebruiken dat al is geüpload naar **Fortis Commander**.

Permanent vergrendelen en ontgrendelen

Met de app kunt u het slot permanent vergrendelen en ontgrendelen. De functie wordt gebruikt voor serviceinterventies of noodbediening zonder het gebruik van een kaart.

Verzamelen van gebeurtenissen van elektronische sloten met RFID-kaarten/chips

Instellingen voor gebeurtenisverzameling

1. Open **Instellingen > Elektronische sloten > Tabblad gebeurtenissen**.
2. Selecteer het type gebeurtenis:
   - **Toegangs- en systeemgebeurtenissen verzamelen** - Alle toegangs- en systeemgebeurtenissen worden op de kaart/chip geregistreerd en naar het **Systeemlogboek** en **Toegangslogboek** geschreven.
   - **Alleen systeemgebeurtenissen verzamelen** - alleen systeemgebeurtenissen worden gelogd, toegangsgebeurtenissen worden niet op kaarten opgeslagen.
   - **Verzamel geen gebeurtenissen op tabbladen** - er worden geen gebeurtenissen naar het tabblad geschreven; ze zijn alleen toegankelijk via **Fortis Commander**u.

TIP
Het selecteren van de juiste event set kan de systeembelasting en het opslaggebruik verminderen. Gedetailleerd loggen is echter belangrijk voor diagnostiek en veiligheidsaudits.

Gebeurtenissen van een kaart exporteren

De kaart slaat maximaal **16 eerste voorvallen** op. Gebeurtenissen kunnen op twee manieren worden gelezen:

- Klik in **Access Commander** op het pictogram in het zoekvak in de koptekst en laad het tabblad.
- Met een apparaat met **2N OS** worden gebeurtenissen van de kaart gelezen en naar **Access Commander**u verzonden.

Gebeurtenissen uploaden naar het slot

1. Open **Instellingen > Elektronische sloten > Fortis Commander** en klik op Download bestand.
2. Open het bestand in **Fortis Commander**.
3. Maak in de app **Fortis Commander** verbinding met het elektronische slot.
4. Upload het bijgewerkte bestand terug naar **Access Commander**.
5. Zodra de gebeurtenissen zijn geüpload, worden ze weergegeven in **Toegangslogboeken** en **Systeemlogboeken**.

Servicewerkzaamheden

Deze bewerkingen zijn beschikbaar voor **Fortis Cylinder**:

- **Demontage** - demontage van sloten voor onderhoudsdoeleinden.
- **De batterij vervangen** - de batterij in het slot vervangen.

LET OP
Servicebewerkingen zijn niet relevant voor andere typen vergrendelingen.

OPMERKING
Vanuit de servicemodus keert het slot terug naar de normale modus door op de knop Lock te drukken om het slot permanent te vergrendelen.

De kaart updaten

Gebruikerstoegangskaarten moeten regelmatig worden bijgewerkt. De gebruiker werkt de kaart bij door de kaart te koppelen aan het 2N IP-apparaat waartoe hij geldige toegangsrechten heeft. De kaart moet door de apparaatlezer worden vastgehouden totdat de schakelaar voor het openen van de deur wordt ingeschakeld. De deuropeningsschakelaar wordt pas geactiveerd nadat de toegang tot de sloten is bijgewerkt

De standaardgeldigheidsduur van kaarten van 10 dagen kan worden gewijzigd in **Instellingen > Elektronische sloten > tabblad Kaartparameters**.

LET OP
Als in **Commandant voor toegang** u wijzigt de toegangsrechten tot de sloten, de wijzigingen worden pas weergegeven op de toegangskaart van de gebruiker nadat deze is bijgewerkt op de kaartlezer van het 2N-apparaat! Om veiligheidsredenen raden we u aan een kortere geldigheidsduur van de kaarten in te stellen om ervoor te zorgen dat ze regelmatig worden bijgewerkt

Lezers voor IP-apparaten waarmee u de kaart kunt bijwerken, en hun instellingen worden beschreven in het hoofdstuk Instellingen voor IP-apparaatlezer (p. 26).

Compatibele kaarten

OPMERKING
Voor de doeleinden van deze documentatie wordt de term **kaart** elke compatibele identificatiecode die gebruikmaakt van MIFARE DESFire-technologie.

Voor het openen van elektronische sloten 2N Fortis Je kunt geen willekeurige identiteitskaarten gebruiken.

Kaarten met PiCard-technologie kunnen niet worden gebruikt om elektronische sloten te openen 2N Fortis.

Tijdprofielen op elektronische sloten

Elektronische sloten ondersteunen tijdprofielen met de volgende beperkingen:

- Feestdagen zijn niet van toepassing.
- Binnen één dag kunnen maximaal 4 verschillende tijdsintervallen worden ingesteld.
- Binnen één tijdprofiel kunnen 4 dagelijkse intervalschema's worden gedefinieerd.

TIP
Dit betekent dat je verschillende instellingen kunt hebben voor bijvoorbeeld maandag, dinsdag, woensdag en donderdag, maar voor vrijdag, zaterdag en zondag moet je al een van de bestaande instellingen gebruiken.

LET OP
Als het tijdprofiel deze beperkingen overtreedt, wordt de toegangsregel genegeerd en krijgt de gebruiker geen toegang.

Fortis Commander

Fortis Commander is een standalone toepassing die de **Fortis** elektronische sloten verbindt met het **Access Commander** systeem. De toepassing stelt vergrendelingen in volgens het projectbestand dat is gemaakt in **Access Commander**u en dat de vergrendelingsconfiguratie bevat. Het bestand is gecodeerd en kan alleen op één specifieke installatie worden gebruikt.

Installatie

Fortis Commander is ontworpen om geïnstalleerd te worden op een Windows computer met Bluetooth Low Energy (BLE) ondersteuning.

De app is te vinden op de website 2N Download Centre.

Installatieprocedure

1. Download het installatiepakket van de opgegeven link.
2. Voer het installatieprogramma uit en voltooi de installatie door de instructies op het scherm te volgen.

Projectbestand

Het projectbestand wordt gemaakt in **Access Commander** en bevat de volledige projectconfiguratie. Het bestand is gecodeerd en beveiligd met een wachtwoord.

Vergrendelingen instellen in Access Commander

Voordat u sleutels naar afzonderlijke sloten uploadt, moet u **Access Commander** koppelen met **Fortis Commander**.

Master Encryption Key (MEK) genereren en projectvoorbereiding

1. Meld u aan bij Access Commander.
2. Ga naar de pagina **Instellingen > Elektronische sloten**.
3. Op de kaart **Eerste installatie** klik Sleutels genereren.

4. Maak een hoofdcoderingssleutel.

LET OP
De hoofdcoderingssleutel kan niet later zijn **tonen of wijzigen**.

OPMERKING
Volgens de master encryptiesleutel (MEK) genereert **2N Access Commander** een reeks encryptiesleutels. De sleutel moet dus uniek en voldoende veilig zijn. De sleutelset is gebaseerd op de master-encryptiesleutel, dus projecten met dezelfde master-encryptiesleutel genereren dezelfde sleutelsets. Als een project verloren gaat, kan een nieuw project met dezelfde mastercoderingssleutel aangemaakt worden en de codering voortzetten.

5. Nadat u de sleutels hebt gegenereerd en het wachtwoord voor het projectbestand hebt ingesteld, kunt u **het projectbestand** downloaden, dat een afbeelding is van de configuratie van het elektronische slot in het systeem **Access Commander**.
6. In het tabblad **van Fortis Commander** klikt u op Download toepassing, vanwaar het downloaden van **Fortis Commander** (toepassing voor het configureren van elektronische sloten) zal beginnen.

LET OP
Projectinformatie is gevoelige informatie. Bescherm het tegen misbruik.

Het elektronische slot configureren met Fortis Commander

1. Installeer **Fortis Commander** en open het.
2. Klik op Open project en open het gedownloade projectbestand in File Explorer.
3. Voer in het dialoogvenster dat verschijnt het wachtwoord voor het projectbestand in.
4. Selecteer na het openen van het projectbestand Verbinden met apparaat en bevestig de servicekaart aan het slot.
5. Klik op **Toewijzen**, waarmee de vergrendeling aan het project wordt toegewezen.
6. Koppel het apparaat los en klik op **Bestand > Project sluiten**.
7. Wanneer de configuratie voltooid is, opent u het systeem **Access Commander**. Ga naar het tabblad **Instellingen > Elektronische sloten** en klik opnieuw op Fortis Commander. Upload het projectbestand.

OPMERKING
Wanneer u het slot verplaatst tussen installaties of wanneer u een claim indient, moet u een **Fabrieksreset** uitvoeren. Deze handeling zet het slot terug naar de fabrieksinstellingen en verwijdert alle eerdere configuraties.

Procedure voor het bijwerken van de configuratie

1. Breng wijzigingen aan in **Access Commander**.
2. Download het nieuwe projectbestand.
3. Upload het bestand naar **Fortis Commander** en breng de vereiste wijzigingen in de vergrendelingen aan.

4. Als u andere wijzigingen aanbrengt in **Access Commander**u, download dan altijd een nieuw projectbestand.

LET OP
Voor elke configuratiewijziging in **Access Commander**u moet u een nieuw projectbestand downloaden - u kunt geen ouder bestand gebruiken dat al is geüpload naar **Fortis Commander**.

Permanent vergrendelen en ontgrendelen

Met de app kunt u het slot permanent vergrendelen en ontgrendelen. De functie wordt gebruikt voor serviceinterventies of noodbediening zonder het gebruik van een kaart.

Verzamelen van gebeurtenissen van elektronische sloten met RFID-kaarten/chips

Instellingen voor gebeurtenisverzameling

1. Open **Instellingen > Elektronische sloten > Tabblad gebeurtenissen**.
2. Selecteer het type gebeurtenis:
   - **Toegangs- en systeemgebeurtenissen verzamelen** - Alle toegangs- en systeemgebeurtenissen worden op de kaart/chip geregistreerd en naar het **Systeemlogboek** en **Toegangslogboek** geschreven.
   - **Alleen systeemgebeurtenissen verzamelen** - alleen systeemgebeurtenissen worden gelogd, toegangsgebeurtenissen worden niet op kaarten opgeslagen.
   - **Verzamel geen gebeurtenissen op tabbladen** - er worden geen gebeurtenissen naar het tabblad geschreven; ze zijn alleen toegankelijk via **Fortis Commander**u.

TIP
Het selecteren van de juiste event set kan de systeembelasting en het opslaggebruik verminderen. Gedetailleerd loggen is echter belangrijk voor diagnostiek en veiligheidsaudits.

Gebeurtenissen van een kaart exporteren

De kaart slaat maximaal **16 eerste voorvallen** op. Gebeurtenissen kunnen op twee manieren worden gelezen:

- Klik in **Access Commander** op het pictogram in het zoekvak in de koptekst en laad het tabblad.
- Met een apparaat met **2N OS** worden gebeurtenissen van de kaart gelezen en naar **Access Commander**u verzonden.

Gebeurtenissen uploaden naar het slot

1. Open **Instellingen > Elektronische sloten > Fortis Commander** en klik op Download bestand.
2. Open het bestand in **Fortis Commander**.
3. Maak in de app **Fortis Commander** verbinding met het elektronische slot.
4. Upload het bijgewerkte bestand terug naar **Access Commander**.
5. Zodra de gebeurtenissen zijn geüpload, worden ze weergegeven in **Toegangslogboeken** en **Systeemlogboeken**.

Servicewerkzaamheden

Deze bewerkingen zijn beschikbaar voor **Fortis Cylinder**:

- **Demontage** - demontage van sloten voor onderhoudsdoeleinden.
- **De batterij vervangen** - de batterij in het slot vervangen.

LET OP
Servicebewerkingen zijn niet relevant voor andere typen vergrendelingen.

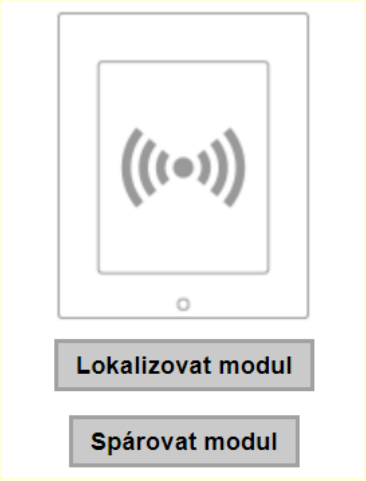
OPMERKING
Vanuit de servicemodus keert het slot terug naar de normale modus door op de knop Lock te drukken om het slot permanent te vergrendelen.

Instellingen voor IP-apparaatlezer

Voor een goede en volledige werking van elektronische sloten is het noodzakelijk om een 2N-apparaat met een speciale firmwareversie in het IP-beheer te hebben. De firmwareversie die elektronische sloten ondersteunt https://www.2n.com/cs-CZ/2nos-elocks-fw.

De firmwareversie met ondersteuning voor elektronische sloten is niet inbegrepen in het pakket op de updateserver. Firmware-updates voor IP-apparaten die elektronische sloten beheren, moeten handmatig worden uitgevoerd, onafhankelijk van automatische systeemupdates

LET OP



Instellingen voor de webinterface van het IP-apparaat

Als u een nieuwe uitbreidingsmodule voor RFID-kaartlezers via een VBUS-kabel op een 2N-apparaat aansluit, moet u deze module aan het apparaat koppelen. Koppel de kaartlezer via de webinterface van het apparaat in het menu Extending Modules van de sectie Hardware.

1. Voer de webconfiguratie van het apparaat in.

> **TIP**
>
> U kunt naar de webconfiguratie-interface gaan door op te klikken in de lijst op de pagina Apparaten.

2. Ga naar Hardware > Modules uitbreiden.
3. Ga naar de instellingen van de RFID-kaartlezermodule op de pagina.
4. Klik Module koppelen.
5. Selecteer “2N elektronische sloten” in het **Toegestane kaarttypen** menu.

> **LET OP**
> Schakel alleen de kaarttypen in die u daadwerkelijk gebruikt voor een optimale functionaliteit.

6. Sla de wijzigingen op.

Compatibele modules

Synchronisatie van de toetsen naar de 2N Fortis elektronische sloten kunnen worden uitgevoerd op alle 2N RFID-lezers die in februari 2023 of later op de markt zijn gebracht. De meeste lezers die na deze datum zijn vervaardigd, zijn ook compatibel, met uitzondering van de onderstaande modellen.

Voor een goede en volledige werking van elektronische sloten is het noodzakelijk om een 2N-apparaat met een speciale firmwareversie in het IP-beheer te hebben. De firmwareversie die elektronische sloten ondersteunt https://www.2n.com/cs-CZ/2nos-elocks-fw.

De volgende modellen **zijn niet compatibel**:

- **2N IP-basis**: alle RFID-lezers
- **2N IP Force**: 9151011, 9151012, 9151016, 9151017, 9151019
- **2N IP Vario**: alle RFID-lezers
- **2N IP Verso**: 915503x, 915504x, 915508x
- **2N Access Unit M**: 91611x
- **2N Access Unit 1.0**: 916008, 916009, 916010, 916011, 916013, 916016, 916019
- **2N Access Unit 2.0**: 916033x

Voor de volgende modules is de compatibiliteit alleen gegarandeerd voor de eenheden die in de herfst van 2023 of later zijn vervaardigd:

- **2N IP Force**: 9151031, 9151031S

Vergrendelingen instellen in Access Commander

Voordat u sleutels naar afzonderlijke sloten uploadt, moet u **Access Commander** koppelen met **Fortis Commander**.

Master Encryption Key (MEK) genereren en projectvoorbereiding

1. Meld u aan bij Access Commander.
2. Ga naar de pagina **Instellingen > Elektronische sloten**.
3. Op de kaart **Eerste installatie** klik Sleutels genereren.

4. Maak een hoofdcoderingssleutel.

LET OP
De hoofdcoderingssleutel kan niet later zijn **tonen of wijzigen**.

OPMERKING
Volgens de master encryptiesleutel (MEK) genereert **2N Access Commander** een reeks encryptiesleutels. De sleutel moet dus uniek en voldoende veilig zijn. De sleutelset is gebaseerd op de master-encryptiesleutel, dus projecten met dezelfde master-encryptiesleutel genereren dezelfde sleutelsets. Als een project verloren gaat, kan een nieuw project met dezelfde mastercoderingssleutel aangemaakt worden en de codering voortzetten.

5. Nadat u de sleutels hebt gegenereerd en het wachtwoord voor het projectbestand hebt ingesteld, kunt u **het projectbestand** downloaden, dat een afbeelding is van de configuratie van het elektronische slot in het systeem **Access Commander**.
6. In het tabblad **van Fortis Commander** klikt u op Download toepassing, vanwaar het downloaden van **Fortis Commander** (toepassing voor het configureren van elektronische sloten) zal beginnen.

LET OP
Projectinformatie is gevoelige informatie. Bescherm het tegen misbruik.

Het elektronische slot configureren met Fortis Commander

1. Installeer **Fortis Commander** en open het.
2. Klik op Open project en open het gedownloade projectbestand in File Explorer.
3. Voer in het dialoogvenster dat verschijnt het wachtwoord voor het projectbestand in.
4. Selecteer na het openen van het projectbestand Verbinden met apparaat en bevestig de servicekaart aan het slot.
5. Klik op **Toewijzen**, waarmee de vergrendeling aan het project wordt toegewezen.
6. Koppel het apparaat los en klik op **Bestand > Project sluiten**.
7. Wanneer de configuratie voltooid is, opent u het systeem **Access Commander**. Ga naar het tabblad **Instellingen > Elektronische sloten** en klik opnieuw op Fortis Commander. Upload het projectbestand.

OPMERKING
Wanneer u het slot verplaatst tussen installaties of wanneer u een claim indient, moet u een **Fabrieksreset** uitvoeren. Deze handeling zet het slot terug naar de fabrieksinstellingen en verwijdert alle eerdere configuraties.

Procedure voor het bijwerken van de configuratie

1. Breng wijzigingen aan in **Access Commander**.
2. Download het nieuwe projectbestand.
3. Upload het bestand naar **Fortis Commander** en breng de vereiste wijzigingen in de vergrendelingen aan.

4. Als u andere wijzigingen aanbrengt in **Access Commander**u, download dan altijd een nieuw projectbestand.

LET OP
Voor elke configuratiewijziging in **Access Commander**u moet u een nieuw projectbestand downloaden - u kunt geen ouder bestand gebruiken dat al is geüpload naar **Fortis Commander**.

Permanent vergrendelen en ontgrendelen

Met de app kunt u het slot permanent vergrendelen en ontgrendelen. De functie wordt gebruikt voor serviceinterventies of noodbediening zonder het gebruik van een kaart.

Onderhoudskaarten

Onderhoudskaarten bieden geautoriseerde toegang tot het slot. Hiermee kunt u het slot in gebruik nemen, de batterij vervangen en het slot verwijderen

LET OP
De onderhoudskaart kan niet tegelijkertijd als gebruikerstoegangskaart worden gebruikt.

Instellingen voor de onderhoudskaart

1. In **Commandant voor toegang** ga naar **Instellingen > Elektronische sloten**.
2. Klik Creëren in **Onderhoudskaarten**.
3. Selecteer het kaarttype dat moet worden gemaakt in het dialoogvenster dat geopend moet worden.
   - Nieuwe sloten instellen — activeer de eerder geconfigureerde nieuwe sloten in de fabrieksinstellingen in de servicemodus.
   - Service — activeer de servicemodus voor de reeds ingestelde vergrendeling.
   - Demontage — Maakt het reeds ingestelde 2N Fortis-cilinderslot vrij voor verwijdering, zie de installatiehandleiding van 2N Fortis.
   - Batterij vervangen — Maakt het reeds ingestelde 2N Fortis-cilinderslot los om de batterij te vervangen, zie de installatiehandleiding van 2N Fortis.

   TIP
   Het is mogelijk om tegelijkertijd naar één fysieke kaart te uploaden **Nieuwe sloten opzetten** en elke tweede servicekaart. We raden een combinatie **Nieuwe sloten opzetten** en **Service**.
4. Klik Ga verder.
5. Tik met de kaart op de aangesloten USB RFID-lezer. Wacht tot de gegevens op de kaart zijn geladen.

geldigheidsduur van de gegevens op de onderhoudskaart is een jaar. Na deze tijd moet u de gegevens verwijderen en het tabblad opnieuw instellen

Basistoegang tot de interface

In dit hoofdstuk worden de inbedrijfstelling en het basisgebruik beschreven Access Commander. De installatie wordt beschreven in het hoofdstuk Installatie (p. 13).

Koppel Access Commander is toegankelijk via een webbrowser. Met het programma kan het IP-adres van de webinterface worden opgezocht 2N Network Scanner.

OPMERKING
Bij distributie via Access Commander Box verbinding maken met de webinterface vanaf een andere computer in het netwerk. Besturingssysteem Access Commander Box zorgt voor werking Access Commander en de standaard Linux-installatie staat niet toe dat de webbrowser wordt uitgevoerd.

De standaardreferenties zijn:

Gebruikersnaam: **Admin**

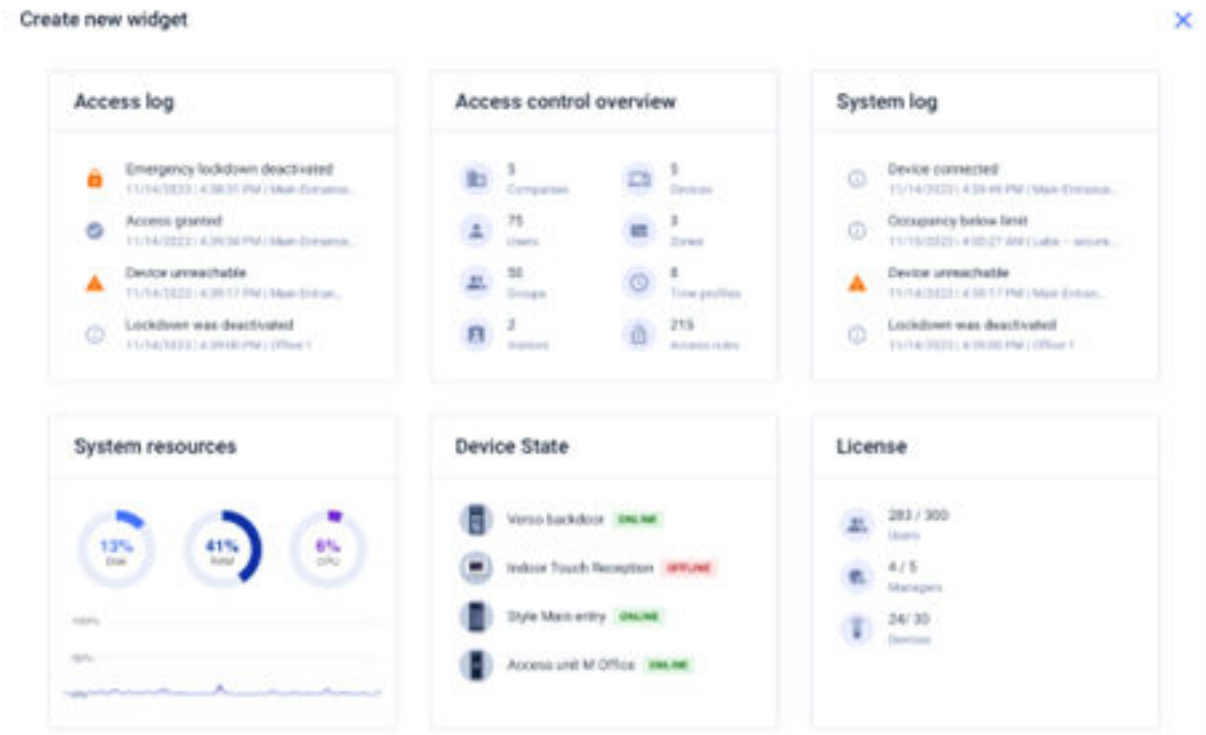
Wachtwoord: **2n**

Na de eerste keer inloggen dient u direct uw wachtwoord te wijzigen.

OPMERKING
Vink de optie **Niet uitloggen** aan als u wilt voorkomen dat u de volgende keer dat u inlogt uw inloggegevens opnieuw moet invoeren. De aanmelding is maximaal 7 dagen geldig, daarna moet u zich opnieuw aanmelden.

Mogelijk hebt u Tweefactorauthenticatie (p. 96) nodig om in te loggen.

Dashboard



Dashboard is de basisweergave van de webinterface Access Commander. Het is een configureerbaar bulletinboard dat realtime gegevens weergeeft. Access Commander biedt verschillende Widgets die met een knop aan het Dashboard worden toegevoegd . Widgets op het Dashboard kunnen worden verplaatst, hernoemd of de basisinstellingen kunnen op verschillende manieren worden uitgevoerd. Het beheren en verwijderen van Widgets gebeurt in het uitgebreide menu ⋮ in de kop van elke widget.

Elke gebruiker met een account bij Access Commander u kunt uw eigen Dashboard opzetten. De beschikbaarheid van Widgets is beperkt, afhankelijk van de rol van de gebruiker.

Verandering van taal

Na de eerste login se **Access Commander** wordt weergegeven in de taal die is ingesteld voor het bedrijf van de ingelogde gebruiker. Elke gebruiker kan de taal wijzigen. Na de volgende login wordt de interface weergegeven in de nieuw ingestelde taal.

1. Klik op het gebruikerspictogram in de rechterbovenhoek om het gebruikersmenu te openen.
2. Selecteer Taal wijzigen.
3. Selecteer de juiste taal en bevestig met Taal wijzigen.

verander het wachtwoord van je account

1. Klik op het gebruikerspictogram in de rechterbovenhoek om het gebruikersmenu te openen.
2. Selecteer Profiel bekijken.
3. Klik op ✎ bij de parameter Wachtwoord.

4. Bevestig het huidige wachtwoord en voer een nieuw wachtwoord in.

OPMERKING
Als het wachtwoord voor het 'admin'-account hetzelfde is als het root-wachtwoord van de systeemgebruiker (voor inloggen op de Linux-installatieconsole), dan zal, wanneer het wachtwoord voor het 'admin'-account wordt gewijzigd, het wachtwoord van het root-account worden gewijzigd. worden ook automatisch gewijzigd.

Verander je profielfoto

1. Klik op het gebruikerspictogram in de rechterbovenhoek om het gebruikersmenu te openen.
2. Selecteer Profiel bekijken.
3. Klik op de afbeelding in de kop van het gebruikersdetail.
4. Stel de foto in het geopende dialoogvenster in.
   De beeldresolutie wordt automatisch aangepast naar 432 × 432 px.

Logo's

Hier is een overzicht van wat u in het hoofdstuk kunt vinden:

- Systeemlogboeken (p. 33)
- Toegang tot logboeken (p. 34)
- Kennisgeving (p. 35)
- Levensduur van logboeken (p. 33)

Systeemlogboeken

OPMERKING

- De gebruiker krijgt de logboeken te zien die hij of zij mag bekijken, afhankelijk van zijn gebruikersrechten.
- Gegevens worden in het Engels naar de logs geschreven.

De pagina System Logs toont een lijst met gebeurtenissen en meldingen die het systeem heeft gegenereerd.

In de lijst met systeemlogboeken wordt voor elke gebeurtenis en melding het volgende aangegeven:

- ernst (info, waarschuwing, fout).
- het tijdstip waarop de gebeurtenis plaatsvond.
- de categorie waartoe de actie behoort (Apparaatstatus, Importeren, Gebruikerssynchronisatie, Systeem, Gebruikersacties, Gebiedsbeperkingen).
- de entiteit waarop de actie betrekking heeft (faciliteit, gebruiker, zone, bezoeker...).
- een korte beschrijving van het evenement.
- auteur van het evenement.

Als u op een regel klikt, wordt gedetailleerde informatie over het gegeven record weergegeven.

De lijst kan worden gefilterd met boven de lijst. Als alternatief kunnen filters worden ingesteld voor individuele kolommen in het uitgebreide menu dat wordt geopend door op te klikken in de kop van elke kolom. Uitgebreid menu met kolommen het maakt het ook mogelijk kolommen te verplaatsen, vast te zetten op de eerste of laatste positie of te verbergen.

De kolommen Ernst en Tijd kunnen niet worden verborgen.

Export van logo's

De records kunnen in een CSV-bestand worden gedownload door op de knop Export boven de lijst te klikken. In het geëxporteerde CSV-bestand wordt de tijd weergegeven in GMT+0.

Levensduur van logboeken

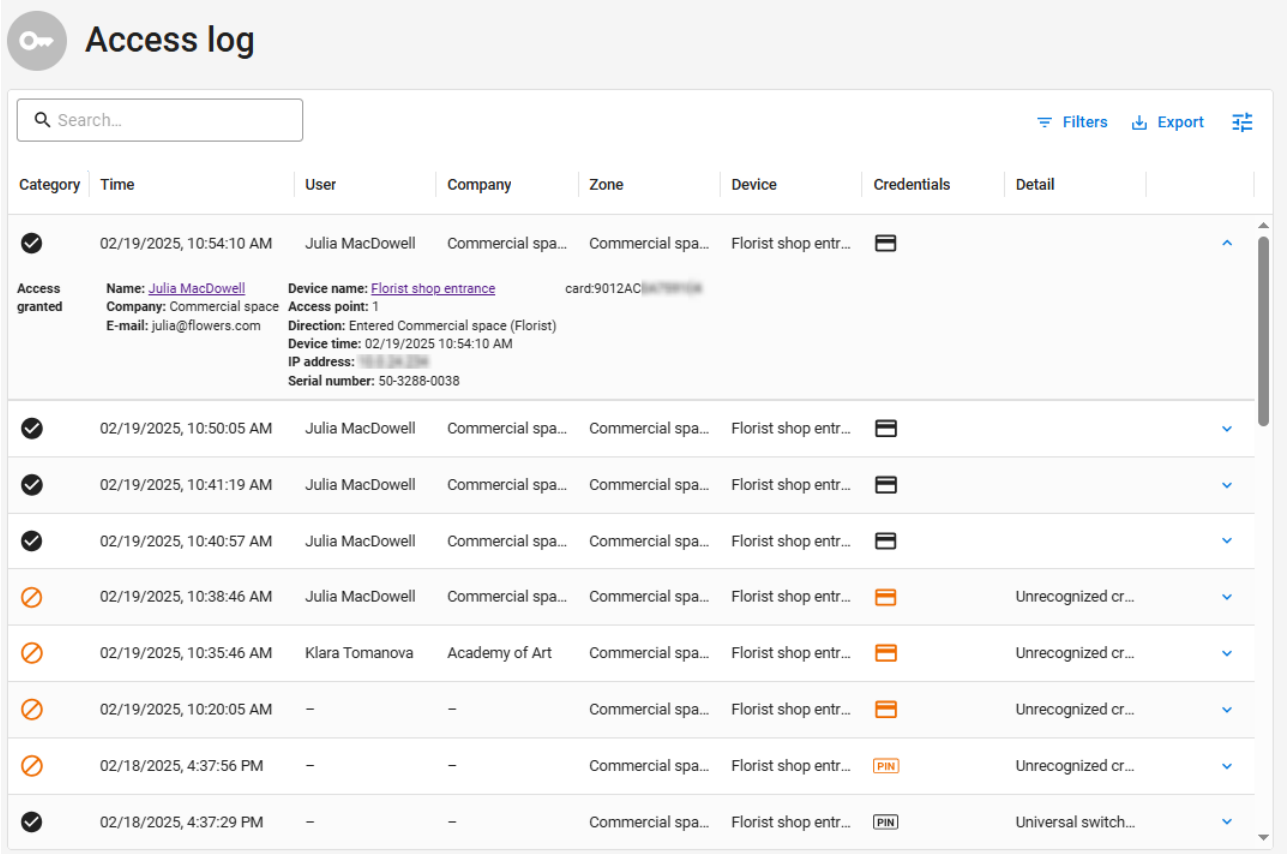
Zodra het gebruik van de schijfcapaciteit 80% bereikt, wordt het automatisch verwijderen van logbestanden gestart. De schijfcapaciteit kan worden gecontroleerd op de pagina Instellingen. Logboeken van het eerste type worden eerst in volgorde verwijderd, andere logbestanden worden geleidelijk verwijderd totdat het

schijfruimtegebruik daalt tot 75% of totdat alleen logbestanden met een onvolledige minimaal mogelijke opslagtijd van het gegeven logtype overblijven.

De opslagtijd voor een bepaald type logboek wordt ingesteld op het tabblad **Instellingen > Logboekbehoud**. Het bewaren van camera-opnamen kan niet langer duren dan het bewaren van systeem- en toegangslogboeken.

TIP
Als u voortdurend 70% van de schijfcapaciteit gebruikt, raden wij u aan de maximale logopslagtijd te verkorten.

Toegang tot logboeken



OPMERKING

- De gebruiker krijgt de logboeken te zien die hij of zij mag bekijken, afhankelijk van zijn gebruikersrechten.
- Gegevens worden in het Engels naar de logs geschreven.

Op de pagina Toegangslogboeken worden records weergegeven van succesvolle en mislukte authenticatiepogingen en nooduitsluitingen.

In de lijst met toegangslogboeken staat:

- **Categorie:**
  - Toegang toegestaan
  - Toegang geweigerd
  - Publieke toegang toestaan
  - Apparaatvergrendeling;
- **Tijd**, wanneer de actie plaatsvond;
- **Gebruiker**, die de actie heeft uitgevoerd;
- **Bedrijf** van de gegeven gebruiker;
- **Zone**, waarin de actie plaatsvond;
- **Apparaat**, waarop de actie plaatsvond;
- **Authenticatie**, die voor het experiment werd gebruikt (pincode, QR-code, enz.).

Als u op een regel klikt, wordt gedetailleerde informatie over het gegeven record weergegeven.

De lijst kan worden gefilterd met boven de lijst. Als alternatief kunnen filters worden ingesteld voor individuele kolommen in het uitgebreide menu dat wordt geopend door op te klikken in de kop van elke kolom. Uitgebreid menu met kolommen het maakt het ook mogelijk kolommen te verplaatsen, vast te zetten op de eerste of laatste positie of te verbergen.

Export van logo's

De records kunnen in een CSV-bestand worden gedownload door op de knop Export boven de lijst te klikken. In het geëxporteerde CSV-bestand wordt de tijd weergegeven in GMT+0.

Levensduur van logboeken

Zodra het gebruik van de schijfcapaciteit 80% bereikt, wordt het automatisch verwijderen van logbestanden gestart. De schijfcapaciteit kan worden gecontroleerd op de pagina Instellingen. Logboeken van het eerste type worden eerst in volgorde verwijderd, andere logbestanden worden geleidelijk verwijderd totdat het schijfruimtegebruik daalt tot 75% of totdat alleen logbestanden met een onvolledige minimaal mogelijke opslagtijd van het gegeven logtype overblijven.

De opslagtijd voor een bepaald type logboek wordt ingesteld op het tabblad **Instellingen > Logboekbehoud**. Het bewaren van camera-opnamen kan niet langer duren dan het bewaren van systeem- en toegangslogboeken.

TIP
Als u voortdurend 70% van de schijfcapaciteit gebruikt, raden wij u aan de maximale logopslagtijd te verkorten.

Kennisgeving

Met de module Meldingen kunt u monitoring instellen van geselecteerde gebeurtenissen en systeemeigenschappen waarvan de module op de hoogte is **Access Commander** informeer per e-mail of melding in de bovenste balk naast het gebruikersmenu.

De lijst met meldingen wordt ook weergegeven op de pagina **Systeemlogboeken > Meldingen**.

De records kunnen in een CSV-bestand worden gedownload door op de knop Export boven de lijst te klikken. In het geëxporteerde CSV-bestand wordt de tijd weergegeven in GMT+0.

Een nieuw meldingstype instellen

1. Ga naar de pagina **Instellingen > Meldingen**.
2. Klik op de knop Toevoegen in de rechterbovenhoek van de pagina.
3. Voer een naam in voor het nieuwe meldingstype.
   Na het aanmaken worden de details van de melding weergegeven, waarbij het mogelijk is om de apparaten te selecteren waarvoor de melding moet worden gemonitord; gebruikers toevoegen aan wie de melding moet worden verzonden; kies de bezorgmethode voor meldingen.

Notificatie instellingen

De meldingstypes worden ingesteld in de details van het meldingstype. Om de details van het meldingstype te openen, klikt u op de geselecteerde melding in de lijst op de pagina **Instellingen > Meldingen**.

Wijze van kennisgeving

Meldingen kunnen worden weergegeven zoals in **Access Commander**, dus stuur ze per e-mail.

In **Access Commander** verschijnen meldingen onder het in de bovenste balk, naast het gebruikersmenu of in **Systeemlog > Meldingen**.

Er kunnen notificatie-e-mails worden verzonden naar gebruikers die worden beheerd in **Access Commander** en ontvangers buiten het systeem. Gebruikers kunnen uit de lijst worden geselecteerd. De e-mailadressen van de overige ontvangers moeten handmatig worden ingevoerd.

OPMERKING
Voor de juiste werking van e-mail notificaties is het noodzakelijk dat SMTP correct is ingesteld, zie De e-mailfunctie (SMTP) inschakelen en instellen (p. 95).

Bewaakte apparaten

Het opgegeven type melding kan zowel voor alle apparaten als voor slechts enkele apparaten worden gegenereerd. Als Monitor alle apparaten is ingeschakeld, kan de gebeurtenis op elk apparaat plaatsvinden en wordt er een melding gegenereerd. Als Monitoring alle apparaten is uitgeschakeld, wordt er alleen een melding gegenereerd als er een gebeurtenis plaatsvindt op een van deze geselecteerde apparaten. De selectie van het apparaat vindt plaats in het menu, dat wordt geopend met .

Levensduur van logboeken

Zodra het gebruik van de schijfcapaciteit 80% bereikt, wordt het automatisch verwijderen van logbestanden gestart. De schijfcapaciteit kan worden gecontroleerd op de pagina Instellingen. Logboeken van het eerste type worden eerst in volgorde verwijderd, andere logbestanden worden geleidelijk verwijderd totdat het schijfruimtegebruik daalt tot 75% of totdat alleen logbestanden met een onvolledige minimaal mogelijke opslagtijd van het gegeven logtype overblijven.

De opslagtijd voor een bepaald type logboek wordt ingesteld op het tabblad **Instellingen > Logboekbehoud**. Het bewaren van camera-opnamen kan niet langer duren dan het bewaren van systeem- en toegangslogboeken.

TIP
Als u voortdurend 70% van de schijfcapaciteit gebruikt, raden wij u aan de maximale logopslagtijd te verkorten.

Bedrijven

Instellingen kunnen binnen één installatie worden uitgevoerd **Access Commander** verdelen in **Door de samenleving**, die afzonderlijk worden beheerd. Deze werkwijze maakt het mogelijk om de administratie te verdelen over beheerders van individuele bedrijven. Een beheerder van het ene bedrijf heeft geen toegang tot informatie over een ander bedrijf.

Zones of faciliteiten kunnen door bedrijven worden gedeeld, waardoor het beheer van bedrijven toegang krijgt tot gemeenschappelijke ruimtes (ingangen, restaurants, vergaderzalen...).

Het creëren van een nieuw bedrijf

1. Ga naar de pagina **Bedrijven**.
2. Klik rechtsboven op de knop bedrijf toevoegen.
3. Vul de bedrijfsnaam in.
4. U kunt een bedrijf starten door op te klikken Creëren.
   Het nieuw aangemaakte bedrijf verschijnt in de lijst. In de details van het bedrijf is het noodzakelijk om de instellingen te configureren. Het toevoegen van gebruikers aan het bedrijf gebeurt in de instellingen van individuele gebruikers.

Bedrijfsinstellingen

Bedrijfsinformatie kunt u bekijken en bewerken in de bedrijfsgegevens. Een bedrijfsdetail wordt geopend door op een geselecteerd bedrijf in de lijst op de Bedrijvenpagina te klikken.

In de kop van het bedrijfsdetail staat een knop Vergrendel die Noodvergrendeling (p. 59) activeert voor alle apparaten in de zones van dit bedrijf.

Bedrijfsgegevens zijn onderverdeeld in de tabbladen Overzicht, E-mails en Gebruikerssynchronisatie.

De taal van de samenleving

Op het tabblad Algemeen kunt u de bedrijfstaal selecteren waarin de interface gebruikt zal worden Access Commander weergeven aan gebruikers in dat bedrijf. Gebruikers kunnen de interfacetaal later wijzigen. De taalkeuze van het bedrijf heeft ook invloed op de e-mailsjablonen die naar Gebruikers worden verzonden. De tekst van e-mails kan worden gewijzigd op het tabblad E-mails.

Zones

Het toewijzen van zones aan een bedrijf definieert de reeks faciliteiten waartoe bedrijfsgebruikers recht hebben op toegang (bijvoorbeeld de zone voor de gemeenschappelijke ruimtes en de zone op de 4e verdieping, die de toegangsdeur naar de receptie en alle ingangen van de vierde verdieping omvat).). Zones kunnen tegelijkertijd aan meerdere bedrijven worden toegewezen, en meerdere zones kunnen aan één bedrijf worden toegewezen.

My2N app

Binnen het bedrijf is het mogelijk om de koppelingsparameters met de applicatie in te stellen My2N app, waarmee Bluetooth-authenticatie mogelijk is. Zowel de apparaten waarop gebruikers kunnen koppelen als de geldigheidsduur van de mobiele sleutel die nodig is voor het koppelen, zijn ingesteld. De mobiele sleutel zelf wordt gegenereerd in de gebruikersinstellingen.

Bezoeken

Op dit tabblad worden groepen ingesteld waaraan de bezoekbeheerder nieuwe bezoeken kan toewijzen. Eén van de groepen kan als standaard worden opgegeven. Het nieuwe bezoek wordt automatisch toegewezen aan de standaardgroep, tenzij anders ingesteld.

LET OP
Zonder een correct ingestelde standaardgroep is het niet mogelijk om bezoekers toegang te verlenen in de vereenvoudigde interface.

Ook is het mogelijk om de authenticatiemethoden te selecteren die aan het bezoek kunnen worden toegewezen. De authenticatiemethode wordt vervolgens door de bezoekmanager aan het bezoek toegewezen.

Meer over het opzetten van bezoeken in Bezoeken (p. 74).

Werkfonds

Werkpool en Vakanties worden gebruikt om de maandelijkse werkpool van gebruikers in de aanwezigheidsmodule te berekenen. Door de dagen te selecteren, is het mogelijk om te bepalen welke dagen van de week als werkdagen worden geteld. De dag wordt geselecteerd door te klikken. Groene dagen geven aan welke dagen als werkdagen worden beschouwd.

De werktijdaanpassing bepaalt hoeveel tijd één dagelijkse dienst heeft.

Vakantie

Door vakantiedagen in te stellen, bepaalt u welke dagen niet worden meegenomen in de berekening van de maandelijkse werkpool. De uren die op een feestdag worden gewerkt, worden op dezelfde manier geteld als de uren die in het weekend worden gewerkt: de gewerkte tijd wordt naast de normale werkuren geregistreerd.

Uitgebreide aanbieding ⋮ Hiermee kunt u vakantiedagen van een ander bedrijf kopiëren. Feestdagen worden gekopieerd, inclusief datums en namen. Kopiëren kan herhaaldelijk worden gebruikt, maar als de nieuw gekopieerde vakantie al in het bedrijf is ingesteld, wordt de naam ervan overschreven.

E-mails verzonden naar bedrijfsleden

E-mailinstellingen hebben een eigen tabblad in de bedrijfsinstellingen. **Access Commander** Hiermee kunt u automatische e-mails sturen naar bedrijfsleden (inclusief bezoekers) met informatie over de toewijzing van een authenticatiemethode. Er wordt een e-mail verzonden naar de gebruiker of bezoeker met het ingestelde e-mailadres.

E-mailtypen:

- Pincode voor het bezoek
- QR-code voor bezoek
- Pincode voor de gebruiker
- QR-code voor gebruikers
- My2N app om Bluetooth-authenticatie voor de gebruiker in te stellen

In detail **bedrijven > tabblad E-mails > tabblad Sjablonen** voor e-mail is het mogelijk om het uiterlijk van deze e-mails in te stellen en de bewoording ervan te bewerken. Het bewerken van de tekst van een e-mail gebeurt in een dialoogvenster dat wordt geopend door op het geselecteerde type e-mail te klikken. In het dialoogvenster kunt u het volgende bewerken:

- onderwerp - het onderwerp van de e-mail
- header – weergegeven in het gekleurde veld van de e-mailtekst
- introductie – de tekst die wordt gegeven vóór de automatisch gegenereerde gegevens uit **Access Commander**
- volgend bericht – de tekst die volgt op de gegevens die zijn gegenereerd **Access Commander**
- handtekening - de handtekening die aan het einde van de e-mail wordt gegeven

Bedrijfssynchronisatie (LDAP)

Synchronisatie met LDAP wordt gebruikt voor het downloaden van gebruikers en hun wijzigingen van een extern LDAP-systeem. Gebruikersgegevens omvatten gebruikersnaam, ID, kaartidentificatiegegevens, PIN/QR-code, afbeelding, e-mailadres, telefoonnummer, wachtwoord en login, kentekens van voertuigen.

OPMERKING
Meer informatie over LDAP kunt u vinden op www.ldap.com.

1. Ga naar **Bedrijven > details van het geselecteerde bedrijf > tabblad Gebruikerssynchronisatie**.
2. Als er geen verbinding is ingesteld, maakt u er een.
   Vul in:

   - **De naam van de server** – als DNS correct is ingesteld, voert u gewoon de naam van de server in (“WIN-9ABEB4AUOHD”). Als DNS niet is ingesteld, wordt het IP-adres van de server waarop de LDAP-service draait, ingevoerd in de servernaam.
   - **Haven** – de standaardinstelling is LDAP-poort 389 (zonder SSL). Als u in uw bedrijf gebruik wilt maken van een gecodeerde verbinding, voert u poortnummer 636 in. SSL-ondersteuning moet ook aan de LDAP-serverzijde zijn ingeschakeld. Als de beheerder een ander poortnummer instelt, moet dit ook in v worden gewijzigd **Toegang tot commandant**.
   - **Inlog naam** – de inlognaam van de gebruiker die de bijbehorende rechten heeft voor de opgegeven root, of de gehele boom. De loginnaam moet worden ingevoerd in de vorm: "administrator@domain.com".
   - **Wachtwoord** – het wachtwoord van de opgegeven gebruiker op de LDAP-server.
   - **Communicatiebeveiliging (SSL)** – wanneer SSL is uitgeschakeld, is het niet nodig om het poortnummer te herschrijven. Bij het inschakelen van SSL moet het poortnummer worden gewijzigd in 636.
   - **Basis-DN** – het hoofdpunt van waaruit het zoeken in de directory begint. Het kan een extensie of de root van een directory zijn, zoals: CN=administrator, CN=users, DC=domain, DC=com.

   Als u TLS inschakelt, wordt Transport Layer Security (TLS) ingeschakeld voor uw FTP-verbinding. TLS versleutelt de gegevens die worden verzonden tussen de **Access Commander** en de server.

   Schakel TLS-certificaatverificatie in om TLS-verificatie van door de server geleverde certificaten in te schakelen. Als dit is ingeschakeld, controleert **Access Commander** of er wordt gecommuniceerd met een vertrouwde server, wat de beveiliging van de verbinding verhoogt.
3. Het detail van de ingestelde LDAP-verbinding wordt geopend. Verbindingsinstellingen kunnen worden getest. Met behulp van de knop Synchroniseer nu u start een eenmalige synchronisatie.
4. De **Opties** tab helpt u bij het beheren van de manier waarop gegevens worden gesynchroniseerd.

   In het uitgebreide menu kunt u de ingestelde verbinding verwijderen ⋮ kaarten **Importeren**. Op kaart **Opties** andere synchronisatieparameters zijn ingesteld.

TIP
Automatische synchronisatie wordt ingesteld op het tabblad **Importeren**. Wanneer u automatische synchronisatie inschakelt, vult u de intervallen in waarop de synchronisatie moet plaatsvinden. Kies afhankelijk van de frequentie in welke minuut of tijd de gegevens worden gesynchroniseerd.

Instellingen voor LDAP-gegevenssynchronisatie

Geïmporteerde kenmerken — wijzig het schema om de toewijzing van kenmerken van de LDAP-server naar de **Commandant voor toegang** parameters.

OPMERKING
De telefoonnummerkenmerken worden uitgebreid met een filter dat de nummers converteert naar het gewenste formaat dat compatibel is met de gebruikerslijst van het bedrijf in **Commandant voor toegang**. Er zijn twee filters beschikbaar:

- `toPhoneNumber` — overbodige tekens (spaties, koppeltekens, enz.) uit de telefoonnummers verwijderen.
- `skipExtension` — verwijder de extensie van de telefoonnummers.

Gebruiksvoorbeeld: Als u het kenmerk invoert `{telephoneNumber|toPhoneNumber|skipExtension}`, de oorspronkelijke waarde van het telefoonnummer in Active Directory “+420 123 456 789 x 2222” wordt omgezet in “+420123456789”.

Gebruikers verwijderd uit LDAP — bepaal wat u moet doen met de gebruikers die uit LDAP zijn verwijderd. U kunt de gebruikers die uit LDAP zijn verwijderd, behouden of verwijderen **Commandant voor toegang**. Als de gebruikers die uit LDAP zijn verwijderd, worden gedeactiveerd, blijven hun gegevens **Commandant voor toegang** maar wordt niet gesynchroniseerd met de apparaten. Gedeactiveerde gebruikers hebben geen toegangsrechten, zijn niet bereikbaar, enz.

Gebruikers die zijn verbannen uit Active Directory — stel in wat er gebeurt met de gebruikers die uit Active Directory zijn verbannen. **Commandant voor toegang** kan deze Active Directory-wijziging negeren of de gebruiker uitschakelen. Gedeactiveerde gebruikers hebben geen toegangsrechten, zijn niet bereikbaar, enz. Nadat ze opnieuw zijn geactiveerd in Active Directory, worden de gehandicapte gebruikers ook opnieuw **Commandant voor toegang**.

Groepssynchronisatie — groepsopdrachten uploaden van LDAP naar **Commandant voor toegang**. Door een synchronisatieschema in te stellen, kunt u een eigen basis-DN en filter instellen om te worden gebruikt voor groepssynchronisatie. In de schema-instellingen kunt u de synchronisatie van gebruikers uit geneste groepen inschakelen

Avatar-synchronisatie – stelt het downloaden van foto's door de gebruiker in vanaf het LDAP-systeem.

Link volgen – stelt in of gegevens van LDAP-koppelingen moeten worden gesynchroniseerd.

Geneste zoekopdracht — maak gebruikerssynchronisatie vanuit de hele boomstructuur mogelijk. Indien uitgeschakeld, worden alleen gegevens van de root doorzocht en gesynchroniseerd

Paging ingeschakeld – paginering maakt gebruik van de Simple Paged Results Control LDAP-extensie. Hierdoor kunnen de resultaten worden opgesplitst in meerdere pagina's, wat essentieel is voor grote directoryservices. Parameter **Pagina grootte** bepaalt hoeveel records één pagina zal bevatten.

Gebruikers importeren in het bedrijf

Uitgebreide aanbieding ⋮ in de bedrijfsdetailkop maakt het een eenmalige import van nieuwe gebruikers in het bedrijf mogelijk, hetzij vanuit een CSV-bestand of vanaf een ander 2N-apparaat.

Importeer gebruikers uit een CSV-bestand

TIP
U kunt een voorbeeld-CSV-bestand downloaden om gebruikers te importeren met behulp van deze koppeling.

Access Commander maakt het mogelijk om gebruikers in bulk te uploaden naar het bedrijf. Basisinformatie over gebruikers kan worden voorbereid in een extern bestand en vervolgens kan de gebruiker eenvoudig worden geïmporteerd. Gebruikers kunnen slechts naar één specifiek bedrijf tegelijk worden geüpload in één bestand.

Met deze functie kunnen gebruikers niet worden verwijderd.

OPMERKING
Gebruikers met de rol Beheerder kunnen uitgebreide, herhaalbare synchronisatie van de gebruikerslijst tussen bedrijven uitvoeren, namelijk Synchronisatie van gebruikers (p. 86).

Importeren vanaf 2N-apparaat

U kunt een lijst met gebruikers overbrengen van een 2N-apparaat naar **Access Commander**. U kunt alleen importeren van een apparaat dat nog niet is toegevoegd aan **Access Commande**r. Een apparaat kan geen gebruikers bevatten die al in **Access Commander** staan (d.w.z. dezelfde UUID hebben). Alle gebruikers kunnen alleen in bulk naar één specifiek bedrijf worden geïmporteerd.

1. Het is raadzaam om een back-up te maken van de configuratie voordat u importeert. Van het **Access Commander** systeem wordt een back-up gemaakt in het tabblad **Instellingen > Back-up systeem**. De back-up van de configuratie van het apparaat wordt gemaakt in de webconfiguratie-interface, onder **Systeem > Onderhoud**.
2. Voeg het apparaat waarvan u de gebruikerslijst wilt importeren toe als **Access Commander**-apparaat.

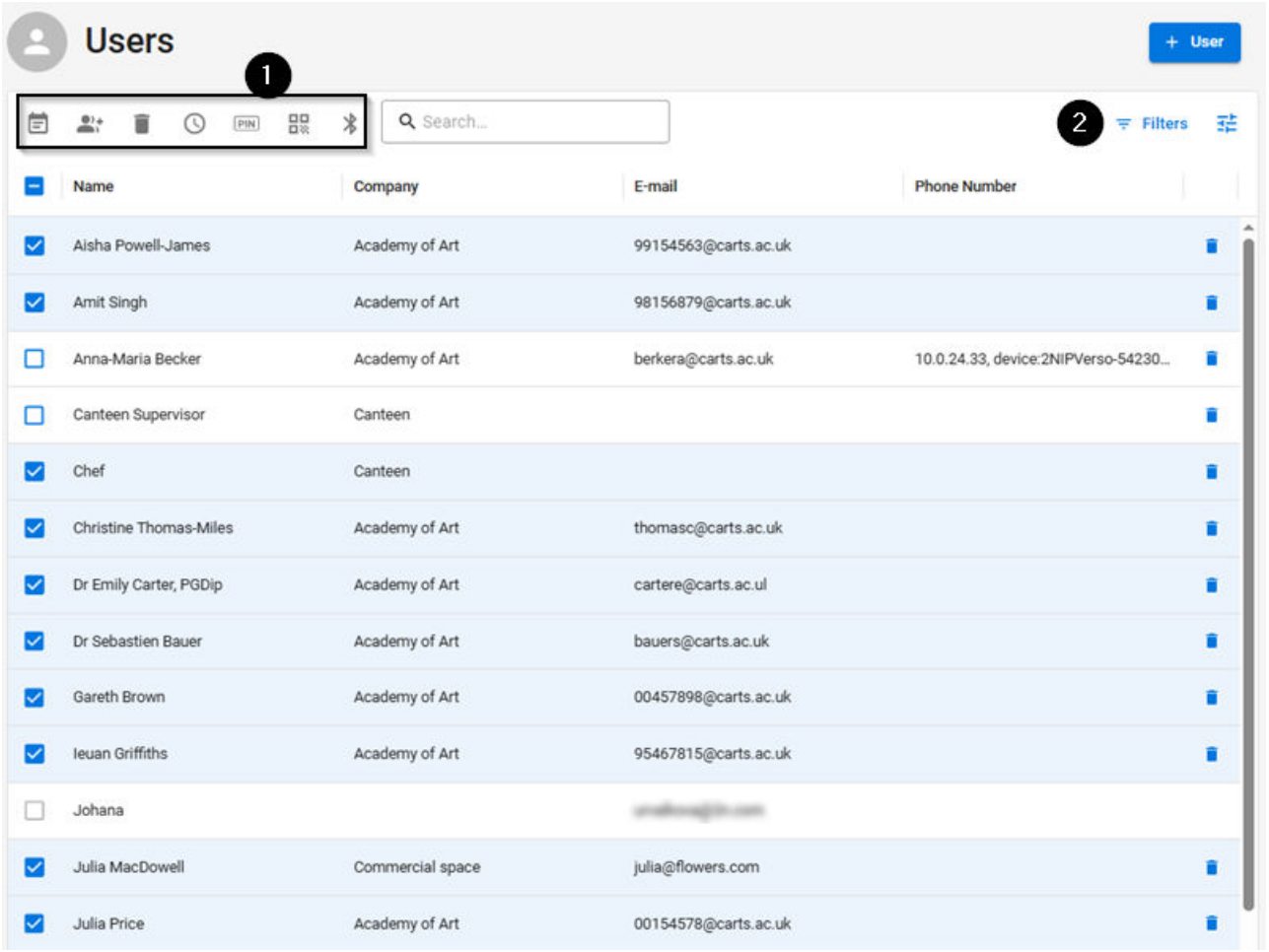
   LET OP
   Voeg nog geen apparaten toe aan zones! Het apparaat zou de toegangsregels overnemen en de gebruikerslijst op het apparaat zou worden overschreven.
3. Ga naar de detailgegevens van het bedrijf waar je de gebruiker naartoe wilt importeren. Selecteer in het geavanceerde menu (⋮) Importeren van apparaat.
4. Er wordt een dialoogvenster geopend. Selecteer in de vervolgkeuzelijst met beschikbare apparaten het apparaat waarvan u de gebruikerslijst wilt importeren.
5. Klik op Importeren om het importeren op de achtergrond te starten. De voltooiing van het proces wordt geregistreerd in het systeemlogboek.
6. Na succesvolle import kan het apparaat worden toegevoegd aan zones en worden opgenomen in toegangsregels.

LET OP
De importprocedure werkt alleen voor specifieke gebruikers (UUID) op het apparaat en importeert alle gebruikers van het apparaat in één keer in één bedrijf.

Gebruikers

Hulp **Access Commander** kan worden beheerd **Gebruikers**, hun toegang wijzigen, hun contactgegevens beheren, enz.

De gebruikerslijst toont alle gebruikers die zijn aangemaakt. Boven de lijst kunt u de gebruikers filteren (nummer 2 in de afbeelding) of naar een specifieke gebruiker zoeken op naam, e-mailadres of telefoonnummer.



Massale acties

Selecteer meerdere gebruikers waarop de volgende bulkacties moeten worden toegepast (nummer 1 in de afbeelding):

- Schakel aanwezigheidsregistratie in voor gebruikers
- Gebruiker toevoegen aan groep
- Verwijder gebruiker
- Stel het tijdsinterval voor de geldigheid van de toegang in
- Wijs een toegangspincode toe aan gebruikers aan wie nog geen pincode of QR-code is toegewezen.
- Wijs een toegangs-QR-code toe aan gebruikers aan wie nog geen pincode of QR-code is toegewezen

- Wijs mobiele toegang toe aan de gebruikers in de selectie aan wie nog geen mobiele toegang is toegewezen.

OPMERKING
Om een pincode/QR-code of mobiele toegang aan een gebruiker toe te kennen, is het noodzakelijk dat de gebruiker over een geldig e-mailadres beschikt.

Maak een nieuwe gebruiker aan

1. Ga naar de pagina **Gebruikers**.
2. Klik op de knop Gebruiker toevoegen in de rechterbovenhoek.
3. Vul de vereiste informatie in: gebruikersnaam en bedrijf waartoe hij behoort.
   De nieuw aangemaakte gebruiker verschijnt in de lijst. Het is mogelijk om aanvullende gebruikersinstellingen te maken in de gebruikersdetailbewerking.

OPMERKING
Access Commander maakt het mogelijk om gebruikers in bulk te uploaden naar het bedrijf. Basisinformatie over gebruikers kan worden voorbereid in een extern bestand en vervolgens kan de gebruiker eenvoudig worden geïmporteerd. Gebruikers kunnen slechts naar één specifiek bedrijf tegelijk worden geüpload in één bestand.

Massa-import vindt plaats in de details van het bedrijf, namelijk Gebruikers importeren in het bedrijf (p. 41).

Gebruikersinstellingen

Gebruikersinformatie kan worden bekeken en beheerd in het gebruikersdetail. Het gebruikersdetail wordt geopend door op de geselecteerde gebruiker in de lijst op de pagina Gebruikers te klikken.

Het gebruikersdetail is onderverdeeld in de tabbladen Overzicht, Aanwezigheid en Wijzigingslogboek. Het tabblad Aanwezigheid wordt alleen weergegeven voor gebruikers waarvoor tracking is ingeschakeld, zie Aanwezigheidsregistratie van gebruikers (p. 51). De aanwezigheidsmodule is beschikbaar afhankelijk van de licentie.

De naam en foto van de gebruiker wijzigen

Opties voor het hernoemen van de gebruiker en het instellen van de foto vindt u in het uitgebreide menu in de koptekst van het gebruikersdetail.

De beeldresolutie wordt automatisch aangepast naar 432 × 432 px.

Authenticatie

Dit tabblad wordt gebruikt om gebruikersauthenticatiemethoden op apparaten in te stellen. De gebruiker moet zich authenticeren op het apparaat en als hij geldige toegang heeft, krijgt hij toegang tot het apparaat.

RFID-kaart – voegt een bestaande RFID-kaart toe aan de gebruiker. Er wordt een dialoogvenster geopend waarin u de kaartidentificatie moet invoeren. De identificatie kan worden geladen door de kaart tegen een USB-lezer te houden of door de identiteitskaart in te voeren met behulp van het toetsenbord. De ID moet

een hexadecimaal getal zijn van minimaal zes tekens. Aan één gebruiker kunnen maximaal 2 toegangskaarten worden toegewezen.

Eén RFID-toegangskaart kan gebruikt worden om tot 90 deuren met sloten 2N Fortis te openen, afhankelijk van het aantal tijdsprofielen dat toegepast wordt. Als de geheugencapaciteit van de kaart overschreden wordt, zal het schrijven van gegevens naar de kaart mislukken. Het mislukte schrijven wordt geregistreerd in het toegangslogboek van het systeem. Als er Slotgroepen worden gebruikt, kunnen er meer deuren naar één kaart worden geschreven dan bij individuele toewijzing. Als er Slotgroepen worden gebruikt, kunnen er meer deuren per kaart worden geregistreerd dan bij een individuele toewijzing.

TIP
De Gebruikersmanager en Beheerder kunnen de kaartidentifier in het Toegangslogboek bekijken. Zo kan een nieuwe/niet-toegewezen kaart op een toegankelijk apparaat worden geladen en kan de identificatiecode uit het logboek worden gekopieerd. Zodra de identificatiecode tussen de RFID-kaarten is geplaatst, kan de gebruiker de kaart gaan gebruiken. De weergave van identificatoren in het Toegangslogboek moet ingeschakeld zijn onder **Instellingen > Authenticatie**.

OPMERKING
Als **Access Commander** meldt dat de gloednieuwe kaart die zojuist is toegevoegd al in gebruik is in het systeem, kan de reden zijn dat de compatibiliteitsmodus voor RFID-kaarten is ingeschakeld. Deze modus wordt door de beheerder ingeschakeld in **Instellingen > Authenticatie > tabblad Instellingen compatibiliteitsmodus**. De compatibiliteitsmodus kan voor elk apparaat afzonderlijk worden geactiveerd in de webconfiguratie-interface van het apparaat in het **menu Services > Toegangsbeheer > tabblad Geavanceerd > Overige instellingen**.

My2N app – gebruikt om verbinding te maken met de applicatie My2N authenticatie via Bluetooth inschakelen, zie hoofdstuk Bluetooth-authenticatie (p. 49).

Pincode – genereert automatisch een 5-cijferige pincode.

Er kan aan de gebruiker een pincode of QR-code worden toegewezen voor toegang, maar u kunt niet beide tegelijk hebben.

QR code – genereert automatisch een QR-code.

Er kan aan de gebruiker een pincode of QR-code worden toegewezen voor toegang, maar u kunt niet beide tegelijk hebben.

Vingerafdruk – opent een dialoogvenster voor het uploaden van een vingerafdruk, die de gebruiker kan gebruiken om zichzelf te authenticeren op apparaten die het lezen ervan ondersteunen. Elke gebruiker kan maximaal 2 vingerafdrukken uploaden. De procedure wordt beschreven in het hoofdstuk Vingerafdruk uploaden (p. 49).

Nummerplaat – stelt de kentekenplaat van het voertuig van de gebruiker in, die het apparaat kan scannen en gebruiken om de gebruiker te authenticeren.

Virtuele kaart – hiermee kunt u de virtuele toegangskaart-ID van de gebruiker instellen. Aan elke gebruiker kan precies één virtuele kaart worden toegewezen. De virtuele kaart-ID is een reeks van 6-32 tekens uit de

set 0-9, A-F. Het virtuele kaartnummer wordt gebruikt om de gebruiker te identificeren in apparaten die zijn aangesloten via de Wiegand-interface.

Schakelcode – maakt het instellen van maximaal 4 codes mogelijk voor het activeren van schakelaars (bijv. deurslot). Om het slot te openen met het toetsenbord op het apparaat wordt naast de schakelcode ook een DTMF-code gebruikt.

LET OP
Authenticatiemethoden voor meervoudige authenticatie moeten exact in de volgorde worden gebruikt waarin ze worden vermeld.

TIP
Bij het invullen van het e-mailadres is het mogelijk om de gegenereerde toegangs-PIN/QR-code naar het opgegeven adres te sturen.

Rekening

Door het instellen van een inlognaam en een eenmalig wachtwoord is het mogelijk om de gebruiker toegang te verlenen tot de interface **Access Commander**. Bij de eerste keer inloggen wordt de gebruiker gevraagd het wachtwoord te wijzigen. Eenmaal ingelogd kan de gebruiker zijn aanwezigheid volgen (indien beschikbaar), zijn e-mailadres wijzigen of zijn profielfoto wijzigen.

Op het tabblad Account is het mogelijk om beheerdersrechten te verlenen aan gebruikers met inloggegevens **Access Commander** gebruik van gebruikersrollen. De autorisaties van individuele rollen worden beschreven in het hoofdstuk Gebruikersrechten (p. 7).

Vereenvoudigde interface

Er kan een vereenvoudigde gebruikersinterface worden gelanceerd voor één bedrijfsbezoekmanager. Dankzij een vereenvoudigde interface kan de bezoekersbeheerder bezoekers toevoegen, verwijderen en beheren. Logboeken en aanwezigheid kunnen niet worden bekeken in de vereenvoudigde interface. Het doel van de vereenvoudigde interface is vooral om het voor appartementgebruikers gemakkelijker te maken om toegang te verlenen aan hun bezoekers. Alle bezoeken die in de vereenvoudigde interface zijn aangemaakt, worden altijd toegewezen aan *standaardgroep voor nieuwe bezoeken*. De bezoekmanager heeft niet de mogelijkheid om deze groep te wijzigen. De standaardgroep voor nieuwe bezoekers moet vooraf worden geselecteerd in de bedrijfsinstellingen en voor de groep moeten geldige toegangsregels voor toegang tot het appartement, inclusief het pad ernaartoe, worden ingesteld. De gebruiker van het appartement kan vervolgens de authenticatiemethoden en de duur van bezoeken beheren in een vereenvoudigde interface.

LET OP
Voordat u de vereenvoudigde interface inschakelt **de systeembeheerder moet de standaardgroep voor nieuwe bezoeken instellen** in Bedrijfsinstellingen (p. 38). Dergelijke toegangsregels moeten aan de standaardgroep worden toegewezen, zodat de bezoeker toegang heeft tot de bezochte gebieden. Zonder een correct ingestelde standaardgroep is het niet mogelijk om bezoekers toegang te verlenen in de vereenvoudigde interface.

Persoonlijke gegevens

Wordt gebruikt om basisinformatie over de gebruiker toe te voegen. Hiermee kunt u het e-mailadres van de gebruiker toevoegen waarnaar informatie met betrekking tot het account van de gebruiker wordt verzonden, en een telefoonnummer toevoegen om contact op te nemen met de gebruiker.

Het is mogelijk om op de kaart te schrijven:

- **E-mail** - het adres waarnaar de gebruiker informatie met betrekking tot zijn account in **Access Commander ontvangt.**
- **Gebruikersnummer** - een specifieke identificatie die vereist is voor bulksynchronisatie met een CSV-bestand (zie Synchronisatie van gebruikers (p. 86))
- **Noot voor**

Benaderingen

Het tabblad toegangen wordt gebruikt om een gebruiker aan een groep toe te wijzen en om het tijdsinterval in te stellen waarbinnen de toegangsgegevens van de gebruiker geldig zijn. Het tijdsinterval wordt ingesteld in het geavanceerde menu van het tabblad, dat geopend wordt door te klikken op ⋮. De instelling voor de starttijd van de geldigheid geldt alleen voor toegangen tot IP-apparaten. Toegang tot elektronische sloten 2N Fortis is geldig vanaf het moment dat de toegangskaart aan de gebruiker is toegewezen.

TIP
Tijdslimieten voor apparaattoegang worden ingesteld via tijdprofielen.

Als de gebruiker lid is van een groep, wordt op het tabblad die groep weergegeven. Als de gebruiker niet aan een groep is toegewezen, kan hij op het tabblad worden toegevoegd. De groep kan worden gewijzigd of verwijderd in het geavanceerde menu ⋮.

Telefoonnummers

Deze kaart wordt gebruikt om de verbinding met de gebruiker tot stand te brengen. Het telefoonnummer is de oproepbestemming van het apparaat van deze gebruiker.

Virtueel nummer

Een virtueel telefoonnummer kan worden gebruikt om naar een gebruiker te bellen met behulp van het numerieke toetsenbord op het apparaat. Virtuele nummers zijn niet gerelateerd aan de eigen telefoonnummers van de gebruiker, waardoor gebruikers hun eigen telefoonnummers op het apparaat kunnen verbergen. Virtuele nummers kunnen bijvoorbeeld worden ingesteld op basis van appartementnummers. Virtuele nummers kunnen dus worden gebruikt in installaties waar het aantal snelkiestoetsen onvoldoende is.

Een virtueel nummer kan 1 tot 7 plaatsen bevatten. De eerste en laatste plaats kunnen een cijfer of een letter zijn, de rest mag alleen uit cijfers bestaan (bijvoorbeeld A123, 456B).

Representatief

Op het tabblad is het ook mogelijk om een snelkoppeling in te stellen waarnaar de oproep wordt doorgeschakeld in geval van onbeschikbaarheid van deze gebruiker. Het is mogelijk om een vertegenwoordiger te kiezen uit andere gebruikers in het bedrijf.

Toegangslogboek

Het toegangslogboek geeft de toegangsgeschiedenis weer.

Wijzig logboek

Alle wijzigingen in de gebruikersinstellingen kunnen worden bekeken op het tabblad Wijzigingslog. De basissortering vindt plaats op basis van het tijdstip van verandering. In het log is het mogelijk om te achterhalen

wie de wijziging heeft doorgevoerd. Nadat u op de regel heeft geklikt, kunt u de details van de aangebrachte wijziging bekijken.

Vingerafdruk uploaden

Elke gebruiker kan tot 2 vingerafdrukken uploaden. Gebruik een externe vingerafdruklezer om ze te uploaden. Controleer of u het 2N USB-stuurprogramma hebt geïnstalleerd. Het stuurprogramma kan hier worden gedownload https://www.2n.com/en-GB/download-center/?type=driver .

De geüploade vingerafdruk van een gebruiker kan voor de volgende acties worden gebruikt:

- Open de deur;
- Een stil alarm starten - kan alleen worden ingesteld als de functie Deur openen actief is;
- Automation F1 en F2: genereert de FingerEntered-gebeurtenis in Automation. F1 en F2 worden gebruikt om de aangesloten vinger in Automatisering te onderscheiden.

Vingerafdruk uploaden

1. Zorg ervoor dat de USB-vingerafdruklezer is ingeschakeld onder **Instellingen > Toegang**.
2. In gebruikersinstellingen v **Tabblad Authenticatie** kies authenticatie Vingerafdruk.
3. Selecteer de vinger waarvoor u een vingerafdruk wilt uploaden.
   Er verschijnt een venster met de titel "Vingerafdruk uploaden".
4. Plaats de geselecteerde vinger op de lezer. Herhaal deze stap 3 keer, telkens wanneer daarom wordt gevraagd.
   Na de laatste scan wordt u geïnformeerd over de succesvolle scan van de vingerafdruk.
5. Door op de knop te drukken**Creëren**het proces is voltooid.

Bluetooth-authenticatie

Gebruikersauthenticatie via Bluetooth gebeurt via My2N-applicatie, die de gebruiker op zijn mobiele telefoon moet hebben gedownload.

GET IT ON Google Play Download on the App Store

Verbinding van de applicatie op de telefoon van de gebruiker met apparaten v **Toegang tot commandant** gebeurt door het invoeren van de koppelingscode v My2N-applicatie.

De koppelingscode kan op twee manieren worden verkregen:

- via een USB Bluetooth-lezer aangesloten op een computer
- verbinding maken met het apparaat.

Een koppelingscode aanmaken via de computer

1. Download op je computer 2N IP US Driver en installeer het.
2. Controleer of de USB Bluetooth-lezer is ingeschakeld onder **Instellingen > Authenticatie > Tabblad Ingeschakelde USB-lezers**.
3. Sluit de USB Bluetooth-lezer aan op de computer.
4. In gebruikersinstellingen v **Tabblad Authenticatie** kies authenticatie My2N-applicatie.
5. Selecteer in het dialoogvenster dat wordt geopend Koppel met behulp van een lezer.
   Er verschijnt een koppelingscode in het dialoogvenster.
6. Volg de onderstaande procedure om te koppelen in de app onderstaand (p. 50).

Maak een koppelingscode op het apparaat

1. Weet zeker dat
   - het koppelingsapparaat is ingesteld voor het bedrijf van de betreffende gebruiker, zie???;
   - het koppelapparaat bevindt zich in een zone waartoe de gebruiker geldige toegang heeft, namelijk Toegangsregels (p. 67);
   - er is een geschikte tijd voor het koppelen ingesteld, nl???.
2. In gebruikersinstellingen v **Tabblad Authenticatie** kies authenticatie My2N-applicatie.
3. Selecteer in het dialoogvenster dat wordt geopend Koppel met uw apparaat.
4. De gegenereerde koppelingscode wordt samen met de resterende koppelingstijd op de kaart weergegeven. Geef de koppelingscode door aan de gebruiker. Als de gebruiker een ingevuld e-mailadres heeft, kunt u de mobiele sleutel naar de e-mail sturen door op te klikken .
5. Volg de onderstaande procedure om te koppelen in de app onderstaand (p. 50).

Koppelen in de mobiele app My2N

1. Download het My2N-applicatie naar uw mobiele telefoon. De applicatie is beschikbaar op App Store En Google Spelen.
2. Open de My2N app en voer de koppelings-PIN in.
3. Sta alle belangrijke machtigingen toe, ongeacht of de toepassing Mijn2N het werkt correct. De machtigingen verschillen niet van de applicatie Mobiele sleutel.
4. Volg de instructies op de mobiele telefoon - benader het apparaat in de koppelingsmodus en klik op Begin met koppelen. De mobiele telefoon zoekt vervolgens naar een apparaat om mee te koppelen.
5. Verleen toegang tot de geselecteerde mobiele telefoon. Vervolgens kunt u op de gehele locatie deuren openen.

WAARSCHUWING
Voor mobiele telefoons met oudere besturingssystemen (Android 9 / iOS 17 en lager) moet u een applicatie gebruiken om te koppelen Mobiele sleutel.

Koppelen in de mobiele app Mobiele sleutel

1. Download de app Mobiele sleutel naar uw mobiele telefoon. De applicatie is beschikbaar op App Store En Google Spelen.
2. Open de app en schakel de app in Mobiele sleutel toegang tot Bluetooth.
3. Afhankelijk van het type mobiele sleutel, benadert u de USB-lezer of het koppelapparaat met de mobiele telefoon.
4. In de app Mobiele sleutel klik op het aangeboden apparaat om te koppelen.
5. De applicatie vraagt u om een pincode in te voeren. Voer de koppelingscode in en bevestig de invoer ervan.

Gebruikersrechten

Rapporteer binnen Access Commander kan door meerdere gebruikers worden uitgevoerd, afhankelijk van de rechten die aan hen zijn toegewezen.

Verhoogde accounts worden ingesteld via een rol in de gebruikersinstellingen. Er kunnen meerdere rollen aan één gebruiker worden toegewezen.

OPMERKING
Gebruikersmachtigingen zijn van toepassing op het beheer binnen het bedrijf van de gebruiker. De beheerder heeft toegang tot het volledige beheer van bedrijven.

Beheerder

- Instelling van het systeem en de afzonderlijke modules volgens de geldige licentie.
- Licentiewijziging
- Alle machtigingen van andere rollen zijn van toepassing op alle bedrijven.

Toegangsbeheerder

- Groepen maken en beheren.
- Beheer hun groepslidmaatschappen.
- Bezoeken aanmaken en beheren.
- Tijdprofielen aanmaken en beheren.
- Toegangsregels instellen.

Gebruikersbeheerder

- Gebruikers aanmaken en beheren.
- Bezoeken aanmaken en beheren.
- Beheer hun groepslidmaatschappen.
- Het toegangs- en systeemlogboek bekijken.

Bezoekt beheerder

- Bezoeken aanmaken en beheren.
- Beheer hun groepslidmaatschappen.
- Het toegangslogboek van bezoeken bekijken.

Deurbeheerder

- Bewaking van cameratransmissie vanaf toegewezen apparaten.
- Op afstand openen van toegewezen apparaten.
- Noodvergrendeling van toegewezen apparaten.
- Het toegangslogboek van toegewezen apparaten bekijken.
- Bewaking van statussen en beveiligingsgebeurtenissen in het systeemlogboek.

Aanwezigheidsmanager

- Het monitoren en beheren van de aanwezigheid van toegewezen groepen.
- Het toegangslogboek bekijken van gebruikers van toegewezen groepen.

Aanwezigheidsregistratie van gebruikers

Access Commander maakt het mogelijk om de aanwezigheid van gebruikers te monitoren. In de aanwezigheidsmodus worden de in- en uitlooptijden van individuele gebruikers geregistreerd.

Registratie van gebruikersaanwezigheid moet geactiveerd zijn. Activering gebeurt in het uitgebreide menu in de koptekst van het gebruikersdetail. Het activeren van aanwezigheidsregistratie voor meerdere gebruikers tegelijk kan gedaan worden door gebruikers te selecteren in de lijst op de pagina Gebruikers en een bulkactie te gebruiken .

De aanwezigheidsmanager kan de aanwezigheidsgegevens van gebruikers bewerken. Bewerken gebeurt door op het te wijzigen tijdsinterval te klikken. Eenmaal geopend kunnen de cut-off-tijden worden bewerkt en kan een notitie aan het interval worden toegevoegd.

LET OP
Voor de juiste functie van aanwezigheid is het noodzakelijk om te hebben **Access Commander**beschikbare actieve licentie om de aanwezigheid van gebruikers bij te houden. Aanwezigheidsregistratie moet in de individuele gebruikersinstellingen worden geactiveerd.

Het monitoren en bijsturen van de aanwezigheid wordt beschreven in het hoofdstuk Aanwezigheid (p. 71).

Groepen

De groep wordt gebruikt voor het groeperen van gebruikers en voor het eenvoudiger instellen van de rechten van de leden om toegang te krijgen tot de zone. Rechten hoeven niet op het niveau van individuele gebruikers en bezoeken te worden ingesteld, maar de groep wordt aan de zone gekoppeld.

De lijst kan worden gefilterd met boven de lijst. Als alternatief kunnen filters worden ingesteld voor individuele kolommen in het uitgebreide menu dat wordt geopend door op te klikken in de kop van elke kolom. Uitgebreid menu met kolommen het maakt het ook mogelijk kolommen te verplaatsen, vast te zetten op de eerste of laatste positie of te verbergen.

Maak een nieuwe groep

1. Ga naar de pagina **Groepen**.
2. Klik op de knop om een groep toe te voegen in de rechterbovenhoek.
3. In het dialoogvenster dat wordt geopend, moet u de naam van de groep invoeren en selecteren tot welk bedrijf deze behoort.

> **LET OP**
> Zodra een groep is aangemaakt, kan het moederbedrijf niet meer worden gewijzigd.

De nieuw aangemaakte groep verschijnt in de lijst en de details ervan worden geopend. In de groepsdetails moet u leden toevoegen en hun toegangsregels instellen.

Groepsinstellingen

Groepsinformatie kan worden bekeken en bewerkt in de groepsdetails. Groepsdetails worden geopend door op de geselecteerde groep in de lijst met groepen te klikken. In detail is er een overzicht van groepsleden en een overzicht van hun toegangsregels.

Leden

Op het tabblad worden alle gebruikers weergegeven die tot de groep behoren. Alleen gebruikers of bezoekerskaarten die tot hetzelfde bedrijf als de groep behoren, kunnen aan de groep worden toegevoegd.

Toegangsregels

Het toont een overzicht van alle reeds aangemaakte toegangsregels en biedt aan om deze te wijzigen of aan te maken. Bij het aanmaken van een regel dient u een groep en een tijdprofiel in te voeren waarin de groep toegang moet hebben tot de zone.

Zones

Zones worden gebruikt voor eenvoudiger beheer van de toegang tot individuele apparaten. Zones combineren apparaten in logische eenheden. Op de pagina wordt een lijst met alle zones weergegeven.

De lijst kan worden gefilterd met boven de lijst. Als alternatief kunnen filters worden ingesteld voor individuele kolommen in het uitgebreide menu dat wordt geopend door op te klikken in de kop van elke kolom. Uitgebreid menu met kolommen het maakt het ook mogelijk kolommen te verplaatsen, vast te zetten op de eerste of laatste positie of te verbergen.

Toegangspunten inschakelen

Hulp er wordt een dialoogvenster geopend waarin de ondersteuning van toegangspunten wordt gestart, meer v Instellingen voor invoer-/uitvoerapparaat (p. 72).

Een nieuwe zone creëren

1. Ga naar de pagina **Zones**.
2. Klik op de knop om een zone toe te voegen in de rechterbovenhoek.
3. In het geopende dialoogvenster moet u de naam van de zone invoeren en selecteren tot welke bedrijven deze behoort.
   De nieuw aangemaakte zone verschijnt in de lijst. Apparaten kunnen aan een zone worden toegevoegd in het zonedetail of in het apparaatdetail. In het zonedetail kunnen aanvullende instellingen worden gemaakt.

Zone-instellingen

Zone-informatie kan worden bekeken en bewerkt in het zonedetail. Zonedetails worden geopend door op de geselecteerde zone in de lijst te klikken.

Authenticatie met meerdere factoren

Authenticatiemethoden en hun combinaties kunnen op alle apparaten in de zone worden ingesteld. Multi-factor authenticatie kan een reeks zijn van bijvoorbeeld een RFID-kaart + pincode.

1. My2N app
2. RFID-kaart
3. Vingerafdruk
4. Pincode

LET OP
Authenticatiemethoden voor meervoudige authenticatie moeten exact in de volgorde worden gebruikt waarin ze worden vermeld.

De noodzaak voor meervoudige authenticatie kan worden beperkt door een tijdsprofiel. Wanneer meerfactorauthenticatie is ingeschakeld, verschijnt er een optie **Gebruik meervoudige authenticatie**, waarin u kunt gebruiken selecteer een tijdprofiel. Wanneer u de Anytime-modus kiest, is multi-factor authenticatie altijd vereist.

Multi-factor authenticatie kan alleen vereist zijn om de zone te betreden. Deze instelling is alleen geldig bij gebruik van toegangspunten.

Toegang tot instellingen

Op de kaart is het mogelijk om een collectieve pincode in te stellen voor toegang tot de zone of deze weer te geven als er al een pincode is aangemaakt.

Bovendien kunnen de volgende functies in de toegangsinstellingen worden in- en uitgeschakeld:

Stil alarm – bij gebruik van een speciale code wordt een stille actie geactiveerd die een alarmmelding verzendt; het apparaat geeft geen alarmgeluiden tijdens een stil alarm. Het instellen van de speciale code voor het stil alarm en de exacte functie ervan gebeurt in de apparaatconfiguratie.

Toegang blokkeren – na vijf mislukte pogingen wordt pas na 30 seconden een nieuwe poging toegestaan.

Kentekenverificatie – voertuigen krijgen toegang tot de zone op basis van kentekenverificatie op alle apparaten die deze functie ondersteunen.

Apparaat

Toont een overzicht van de apparaten die aan de betreffende zone zijn toegevoegd. Op dit tabblad kunnen extra apparaten worden toegevoegd.

Als er toegangspunten worden gebruikt, worden individuele toegangspunten aan de zone toegevoegd. Het toegangspunttype van het betreffende apparaat wordt omschreven als Zone Entry.

Voor elk apparaat/toegangspunt worden de beschikbare authenticatiemethoden weergegeven.

Slotgroepen

Het tabblad toont een overzicht van de slotgroep. U kunt op dit tabblad nog een groep toevoegen.

Voor elke slotgroep kunt u de details van de groep bekijken.

Bedrijven

Op dit tabblad wordt de lijst met bedrijven beheerd die toegang kunnen hebben tot de zone. Meerdere bedrijven hebben toegang tot één zone.

Toegangsregels

Het toont een overzicht van alle reeds aangemaakte toegangsregels en biedt aan om deze te wijzigen of aan te maken. Bij het aanmaken van een regel dient u een groep en een tijdprofiel in te voeren waarin de groep toegang moet hebben tot de zone.

Het bewerken van een toegangsregel kunt u doen door op de betreffende regel te klikken.

Apparaat

Op de pagina Apparaten worden alle apparaten weergegeven die daaraan zijn toegevoegd **Access Commander**.

De lijst kan worden gefilterd met boven de lijst. Als alternatief kunnen filters worden ingesteld voor individuele kolommen in het uitgebreide menu dat wordt geopend door op te klikken in de kop van elke kolom. Uitgebreid menu met kolommen het maakt het ook mogelijk kolommen te verplaatsen, vast te zetten op de eerste of laatste positie of te verbergen.

De records kunnen in een CSV-bestand worden gedownload door op de knop Export boven de lijst te klikken. In het geëxporteerde CSV-bestand wordt de tijd weergegeven in GMT+0.

Door te taggen is het mogelijk om meerdere apparaten te selecteren en hierop de volgende bulkacties toe te passen:

- Activeer geselecteerde apparaten
- Deactiveer geselecteerde apparaten
- Maak een back-up van geselecteerde apparaten

Icoon op de apparaatregel wordt omgeleid naar de webconfiguratie-interface van het betreffende apparaat.

Apparaatstatussen

- Online
- Onbeheerd — Apparaatbeheer is door de gebruiker uitgeschakeld.
- Niet compatibel — het apparaat heeft geen ondersteunde firmwareversie.
- Niet geconfigureerd — u moet de configuratie van elektronische sloten uploaden vanuit een programma van derden.
- Offline
  - Inloggen mislukt - v **Toegang tot commandant** Er zijn verkeerde inloggegevens ingevoerd in de webconfiguratie van het apparaat.
  - Ontoegankelijk - **Toegang tot commandant** kan geen verbinding maken met het apparaat.
  - Ongeldig certificaat - SSL-certificaatvalidatie is vereist en het apparaat beschikt niet over een geldig SSL-certificaat.

IP-apparaat toevoegen

OPMERKING
Het toevoegen van 2N Fortis elektronische sloten wordt beschreven in Elektronische sloten (p. 19).

1. Ga naar de pagina **Apparaat**.
2. Klik op de knop Apparaat toevoegen in de rechterbovenhoek.

3. Om een 2N Intercom/2N access unit/2N antwoordapparaat toe te voegen, selecteert u “2N IP-apparaten”.
4. Zoek in het geopende dialoogvenster naar het apparaat in het LAN of voer het IP-adres en de poort in de volgende indeling in: “IP-adres: poort”.
   Na het invoeren van het IP-adres van het apparaat is het mogelijk om op ENTER op het toetsenbord te drukken om een ander apparaat in te voeren.
5. Nadat u alle apparaten heeft ingevoerd die u wilt toevoegen, vult u het wachtwoord in om toegang te krijgen tot de webconfiguratie van deze apparaten. Het is mogelijk om alleen die apparaten toe te voegen waarop u tegelijkertijd met hetzelfde wachtwoord inlogt.
6. Geef het apparaat een naam voordat u het maakt.
7. Nieuw toegevoegde apparaten verschijnen in de lijst. Voer verdere apparaatinstellingen uit in de apparaatdetails.

Slotgroepen

Met slotgroepen kunt u individuele sloten groeperen in logische eenheden die vervolgens kunnen worden gebruikt om toegangsregels te definiëren, apparaten te bewaken of te beheren.

Groepen bekijken

Open **Apparaten > Groepen vergrendelen**.

OPMERKING
De lijst toont alle aangemaakte slotgroepen. Gebruik het zoekvak om records op naam te filteren.

Een nieuwe slotgroep aanmaken

1. Open **Apparaten > Groepen vergrendelen**.
2. Klik op + Sloten Groep.
3. Voer een groepsnaam in en selecteer het tabblad Maak.
4. Klik in de module **Sloten** op Sloten toevoegen. Selecteer de sloten die deel moeten uitmaken van de groep.
5. Klik in de module **Zones** op Zones toevoegen. Selecteer de zones die deel moeten uitmaken van de groep.
6. Selecteer ⋮ om een slotgroep toe te voegen, een andere naam te geven of te verwijderen.

WAARSCHUWING
Als u de toewijzing van het slot aan een andere groep wilt wijzigen, moet u de configuratie opnieuw uitvoeren. Zorg ervoor dat alle systeemwijzigingen voltooid zijn voordat u het configuratiebestand exporteert.

Vergrendelingen instellen in Access Commander

Voordat u sleutels naar afzonderlijke sloten uploadt, moet u **Access Commander** koppelen met **Fortis Commander**.

Master Encryption Key (MEK) genereren en projectvoorbereiding

1. Meld u aan bij Access Commander.
2. Ga naar de pagina **Instellingen > Elektronische sloten**.
3. Op de kaart **Eerste installatie** klik Sleutels genereren.
4. Maak een hoofdcoderingssleutel.

LET OP
De hoofdcoderingssleutel kan niet later zijn **tonen of wijzigen**.

OPMERKING
Volgens de master encryptiesleutel (MEK) genereert **2N Access Commander** een reeks encryptiesleutels. De sleutel moet dus uniek en voldoende veilig zijn. De sleutelset is gebaseerd op de master-encryptiesleutel, dus projecten met dezelfde master-encryptiesleutel genereren dezelfde sleutelsets. Als een project verloren gaat, kan een nieuw project met dezelfde mastercoderingssleutel aangemaakt worden en de codering voortzetten.

5. Nadat u de sleutels hebt gegenereerd en het wachtwoord voor het projectbestand hebt ingesteld, kunt u **het projectbestand** downloaden, dat een afbeelding is van de configuratie van het elektronische slot in het systeem **Access Commander**.
6. In het tabblad **van Fortis Commander** klikt u op Download toepassing, vanwaar het downloaden van **Fortis Commander** (toepassing voor het configureren van elektronische sloten) zal beginnen.

LET OP
Projectinformatie is gevoelige informatie. Bescherm het tegen misbruik.

Het elektronische slot configureren met Fortis Commander

1. Installeer **Fortis Commander** en open het.
2. Klik op Open project en open het gedownloade projectbestand in File Explorer.
3. Voer in het dialoogvenster dat verschijnt het wachtwoord voor het projectbestand in.
4. Selecteer na het openen van het projectbestand Verbinden met apparaat en bevestig de servicekaart aan het slot.
5. Klik op **Toewijzen**, waarmee de vergrendeling aan het project wordt toegewezen.
6. Koppel het apparaat los en klik op **Bestand > Project sluiten**.
7. Wanneer de configuratie voltooid is, opent u het systeem **Access Commander**. Ga naar het tabblad **Instellingen > Elektronische sloten** en klik opnieuw op Fortis Commander. Upload het projectbestand.

OPMERKING
Wanneer u het slot verplaatst tussen installaties of wanneer u een claim indient, moet u een **Fabrieksreset** uitvoeren. Deze handeling zet het slot terug naar de fabrieksinstellingen en verwijdert alle eerdere configuraties.

Procedure voor het bijwerken van de configuratie

1. Breng wijzigingen aan in **Access Commander**.
2. Download het nieuwe projectbestand.
3. Upload het bestand naar **Fortis Commander** en breng de vereiste wijzigingen in de vergrendelingen aan.
4. Als u andere wijzigingen aanbrengt in **Access Commander**u, download dan altijd een nieuw projectbestand.

LET OP
Voor elke configuratiewijziging in **Access Commander**u moet u een nieuw projectbestand downloaden - u kunt geen ouder bestand gebruiken dat al is geüpload naar **Fortis Commander**.

Permanent vergrendelen en ontgrendelen

Met de app kunt u het slot permanent vergrendelen en ontgrendelen. De functie wordt gebruikt voor serviceinterventies of noodbediening zonder het gebruik van een kaart.

Noodvergrendeling

Noodvergrendeling wordt gebruikt om de deur die door het betreffende apparaat wordt bestuurd, volledig te vergrendelen. Tijdens de noodvergrendeling is het niet mogelijk om de deur te openen met de ingestelde gebruikerstoegangen, ook al gebruikt de gebruiker of bezoeker een geldige toegang met een geldig tijdprofiel.

Noodvergrendeling kan worden geactiveerd/gedeactiveerd vanuit:

- in apparaatdetail – vergrendelt het betreffende apparaat;
- in zonedetail - vergrendelt alle apparaten in de zone;
- in het bedrijfsdetail - vergrendelt alle apparaten in het bedrijf;
- met behulp van de globale actie in de bovenste balk door op de knop te drukken – vergrendelt alle apparaten **Access Commander**;
- in de dashboardwidget.

In de Emergency Lock-widget is het mogelijk om vooraf een specifieke groep apparaten te definiëren die in geval van nood kunnen worden vergrendeld.

LET OP
Offline apparaten, inactieve apparaten, apparaten met incompatibele firmware en apparaten met firmware ouder dan 2.32 worden niet vergrendeld na een noodvergrendelingsverzoek.

Apparaat instellingen

Apparaatinformatie kan worden bekeken en beheerd in het apparaatdetail. Apparaatgegevens worden geopend door op het geselecteerde apparaatitem in de lijst te klikken. Afhankelijk van het apparaattype kunnen de apparaatdetails worden onderverdeeld in de tabbladen Overzicht, Oproep en Lift.

Vanuit de apparaatgegevens kunt u met de knop naar de webconfiguratie van het apparaat gaan **Hardware configuratie** in de rechterbovenhoek van het apparaatdetail. De configuratie van afzonderlijke apparaten

wordt beschreven in de betreffende configuratiehandleiding. Het is mogelijk terug te keren vanuit de configuratiewebinterface door de configuratie te sluiten met een kruisje in de blauwe bovenbalk.

Overzicht

Staat

Dit tabblad toont de status van het tot stand brengen van verbindingen met apparaten. Online apparaten zijn degene waarmee het **Access Commander** verbindingen tot stand gebracht en waarop de geaccepteerde firmware wordt geüpload. Dankzij de tot stand gebrachte verbinding met het apparaat kan gegevenssynchronisatie plaatsvinden. Incompatibele firmware kan worden ingeschakeld **Apparaatpagina > Firmware**.

Na elke wijziging wordt een automatische synchronisatie geactiveerd, die in de configuratie van de eindapparaten wordt weerspiegeld. Synchronisatie vindt alleen plaats via de betrokken apparaten. Alleen verzoeken die worden geactiveerd door wijzigingen die van invloed kunnen zijn op eindapparaten, worden in de wachtrij geplaatst voor synchronisatie. Dergelijke wijzigingen zijn meestal wijzigingen in toegangsrechten, telefoonnummers, gebruikte tijdprofielen, enz. Als u bijvoorbeeld de naam wijzigt van een gebruiker die aan geen enkele groep is toegewezen, wordt er geen automatische synchronisatie geactiveerd.

Toegangscontrole

Stelt de zone in waarin het apparaat valt. Eén apparaattoegangspunt kan zich slechts in één zone bevinden.

Als er 2 toegangspunten op het apparaat zijn ingesteld en als toegangspuntdetectie is ingeschakeld (zie Instellingen voor invoer-/uitvoerapparaat (p. 72)), wordt de optie om 2 zones toe te wijzen weergegeven. Een apparaattoegangspunt kan zich slechts in één zone bevinden.

Configuratie

Het tabblad geeft de huidige firmwareversie, het MAC-adres en het IP-adres weer en biedt de mogelijkheid om het wachtwoord voor toegang tot de webconfiguratie te wijzigen.

Op het tabblad kun je het IP-adres wijzigen waar het apparaat zich bevindt, waardoor **Access Commander** kan verwijzen naar een apparaat dat is losgekoppeld en weer is aangesloten op het netwerk met een ander IP-adres.

Deurbediening

Deze kaart geeft beelden van de camera's van het apparaat weer en maakt het op afstand openen van de door het apparaat bestuurde deurschakelaar mogelijk. Het openen van de deur voor een bepaalde tijd kan worden ingesteld in het uitgebreide menu, dat wordt geopend door op te klikken ⋮ .

De huidige status van de deurschakelaar wordt naast de knop weergegeven Open.

Het wordt gebruikt om deuren te vergrendelen, zelfs voor groepen met geldige toegang Noodvergrendeling (p. 59).

Back-up

Op dit tabblad kunt u een back-up maken van de intercomconfiguratie in een xml-bestand. De back-up wordt gestart met Een back-up starten. Wanneer een back-up wordt opgeslagen op een lokale opslag, wordt deze opgeslagen in een gescheiden **Access Commander**. Wanneer u een bestand opslaat, wordt een dialoogvenster geopend waarin u het reservekopiebestand kunt versleutelen met een wachtwoord. Het bestand bevat gevoelige informatie, dus het wordt aanbevolen om het bestand te beveiligen. Back-upversleuteling is beschikbaar op apparaten met firmware 2.45 en hoger

Elke laatste back-up wordt op het tabblad weergegeven. Het is mogelijk om het apparaat automatisch te synchroniseren met de laatste back-up via het menu Resetten. In het uitklapmenu van dit menu kunt u er ook voor kiezen om te herstellen vanaf een back-up van een ander aangesloten apparaat of vanaf een extern bestand

OPMERKING
Van alle beschikbare apparaten (online apparaten en aangesloten apparaten met incompatibele firmware) kan een back-up worden gemaakt.

Oproep

telefoonkaart wordt weergegeven als er een telecommunicatieverbinding beschikbaar is en is ingeschakeld op het apparaat. Op het tabblad worden alle ingeschakelde accounts weergegeven waarmee de verbinding is beveiligd en wordt hun status weergegeven. De telecommunicatieverbinding wordt rechtstreeks in de configuratie-interface van het apparaat in kwestie ingesteld, in de sectie Oproepen. De configuratie-interface is toegankelijk via een knop Hardwareconfiguratie in de koptekst van het apparaatdetail.

Telefoongesprek

Dit tabblad wordt weergegeven in de details van het apparaat waarmee gebeld kan worden.

Contacten

Het tabblad Contacten beheert de weergave van het adresboek op apparaten met een display. Op de kaart wordt de contactstructuur weergegeven zoals deze in het adresboek op het apparaat wordt weergegeven. Door op te klikken Wijzigen er wordt een dialoogvenster geopend voor het bewerken van de contactboom. In het linkergedeelte van het geopende dialoogvenster wordt de sortering van de contactmappen weergegeven. In het rechtergedeelte worden de contacten binnen de geselecteerde map ingesteld. De hoofdmap is de eerste pagina die verschijnt wanneer u de map op uw apparaat opent. Contacten verschijnen allemaal op één adresboekpagina als ze allemaal in deze hoofdmap zijn opgeslagen. Contacten kunnen verder worden gegroepeerd in mappen en gesorteerd onder de hoofdmap.

Contacten toevoegen aan het apparaatdisplay

1. Ga naar **Toestel > Toesteldetails > tabblad Gesprekken > tabblad Contacten**.
2. Open het weergavebeheer door op te klikken Wijzigen.
3. Selecteer in het rechtergedeelte van het geopende dialoogvenster de map waaraan u contacten wilt toevoegen.
   U kunt aan de map toevoegen:

   1. **Gebruikers**
      Het is mogelijk om meerdere gebruikers tegelijk te selecteren.
   2. **Groepen**
      Gebruikers kunnen per groep massaal aan de map worden toegevoegd. Elke gebruiker uit de groep wordt onder zijn of haar naam in de directory weergegeven. Het is mogelijk om meerdere groepen tegelijk te selecteren.
   3. **Bel groepen**
      Oproepgroepen zijn groepen contacten die tegelijkertijd worden gebeld. Wanneer u een belgroep aanmaakt, is het noodzakelijk om de naam ervan in te voeren, waaronder de bellende groep in het adresboek wordt weergegeven. Gebruikerscontacten worden aan een belgroep toegevoegd, net zoals contacten aan mappen worden toegevoegd.
      U kunt de belgroep hernoemen in het uitgebreide menu naast de map, die u opent door op te klikken ⋮.

4. U kunt de map hernoemen in het geavanceerde menu van de map, dat u opent door op te klikken ⋮. In het uitgebreide menu is het mogelijk om een afbeelding aan de opgegeven map toe te voegen, die vervolgens voor deze map op het apparaat wordt weergegeven.

5. Zet de mappen of belgroepen die u wilt weergeven op de eerste plaats vast in het uitgebreide menu ⋮ voor de opgegeven map met behulp van 📌.

Andere virtuele nummers

Op een toestel met een numeriek toetsenblok is het mogelijk een uitgaand gesprek te starten door een virtueel nummer in te voeren. Op dit tabblad is het mogelijk om gebruikers toe te voegen die virtuele nummers kunnen bellen, zelfs als deze gebruikers geen toegang hebben tot het apparaat. Oproepen naar virtuele nummers van gebruikers die toegang hebben tot het apparaat worden automatisch toegestaan.

Bij het selecteren van gebruikers worden alleen de gebruikers weergegeven die een ingevuld virtueel nummer hebben.

Toetsen

Dit tabblad wordt weergegeven in de details van apparaten die knoppen hebben waarmee gebruikerstelefoonnummers kunnen worden gebeld. Op het tabblad Knoppen worden individuele gebruikers toegewezen aan individuele knoppen op het apparaat. Wanneer de gegeven knop op het apparaat wordt ingedrukt, wordt een uitgaande oproep naar de bestemming van de toegewezen gebruiker gestart.

Tillen

Door de AXIS A9188 relaismodule aan te sluiten op een 2N intercom of op een 2N toegangscontrole-eenheid, kan de toegang tot afzonderlijke liftverdiepingen in het gebouw worden geregeld. Er kunnen maximaal 8 van deze relaismodules worden aangesloten op één intercom 2N of toegangseenheid 2N. Elk van de modules kan 8 verdiepingen besturen, dus in totaal maximaal 64 verdiepingen. Om deze functie te kunnen gebruiken, moet u een actieve licentie hebben: voor IP-intercoms (bestelnr. 9137916) of voor toegangseenheden (bestelnr. 9160401).

Instellingen voor liftbediening

1. Voordat u de configuratie in **Access Commander** uitvoert, moet u ervoor zorgen dat de AXIS A9188 relaismodule is aangesloten op het 2N-apparaat dat de toegangsautorisatie voor de vloer zal leveren. Zorg er ook voor dat HTTPS is ingesteld op de module en dat het root-wachtwoord is gewijzigd.
2. Ga naar de details van het apparaat dat de toegang tot individuele verdiepingen moet controleren. In het uitgebreide menu ⋮ activeer in de header de liftbediening. Er verschijnt een tabblad in de apparaatgegevens **Tillen**.
3. Ga in de apparaatdetailkop naar ⚙ hardware configuratie van het apparaat. Schakel onder **Hardware > Liftbesturing** de modules in die de toegang vanaf de lift moeten controleren. Als de modules verificatie vereisen, voert u een gebruikersnaam en wachtwoord in. Sla de instellingen op. Sluit de hardwareconfiguratie af met het kruisje in de bovenste blauwe balk.
4. Ga naar het tabblad Lift in de apparaatdetails.
5. Selecteer op het tabblad Liftverdieping de relaisuitgang voor de verdieping waartoe u toegang wilt instellen. Het labelen van de uitgangen vindt plaats in het formaat: *io_module_relay-uitvoer*. Klik op ✎.
6. Geef in het geopende dialoogvenster de verdieping een naam en selecteer de zone die op die verdieping wordt betreden. Alleen gebruikers die geautoriseerd zijn om de betreffende zone te betreden volgens de gedefinieerde toegangsregels, mogen deze verdieping betreden. Als de toegang tot de verdieping niet onderworpen is aan de regels van de zone, vink dan het vakje aan **publieke toegang toegestaan**. Door een tijdprofiel te selecteren, beperkt u de publieke toegang alleen tot de tijd die is gedefinieerd door het geselecteerde tijdprofiel. Buiten dit tijdsprofiel is toegang weer alleen toegestaan voor gebruikers met een geldige toegang op basis van de toegangsregels.

> **LET OP**
> Als de toegang is ingesteld volgens de toegangsregels van de zone, neemt het liftapparaat geen andere instellingen van deze zone over (PIN-code, meervoudige authenticatie, stil alarm, ...).

Vloer
Eenmaal ingeschakeld, toont dit tabblad een lijst met alle configureerbare verdiepingen. Elke verdieping heeft zijn eigen aanduiding in de volgorde van module- en relaisuitgang. Elke verdieping kan vervolgens een eigen naam krijgen.

Modules
Dit tabblad toont alle aangesloten AXIS A9188-modules en hun huidige status. De afzonderlijke modules worden ingeschakeld in de apparaatconfiguratie, onder **Hardware > Liftbesturing**.

Toezicht houden
De pagina wordt gebruikt om informatie te vinden over aangesloten IP-apparaten (intercoms, toegangseenheden, antwoordapparaten). De tabel kan door elke beheerder naar eigen behoeften worden ingesteld met behulp van . De instellingen zijn uniek voor elk account. De instellingen worden gemaakt door de weergegeven kolommen te selecteren.

Klik op de regel om naar de details van het betreffende apparaat te gaan.

Firmware
De Firmware-pagina zorgt voor een massale upgrade van de firmware van individuele soorten aangesloten apparaten en helpt zo deze in optimale staat te houden. Bulkapparaatbeheer kan worden opgeschort. Optioneel kunnen sommige apparaten worden uitgesloten van bulkfirmwarebeheer.

TIP
De nieuwe firmwareversie kan eerst in de testmodus op een of meer geselecteerde apparaten worden geïmplementeerd en pas daarna de upgrade van andere apparaten mogelijk maken.

De huidige firmwareversie is online beschikbaar via de 2N Update Server, optioneel is het ook mogelijk om het upgradebestand handmatig te uploaden. Het implementeren van een nieuwe versie is altijd onderworpen aan goedkeuring door de beheerder, die daarmee de volledige controle heeft over het upgradeproces.

Het verkrijgen van firmwareversies van een 2N-updateserver kan enkele minuten duren.

De versie voor massabeheer toont een lijst met aangesloten 2N-intercomtypen, 2N-antwoordeenheden en 2N-toegangseenheden.

OPMERKING
De firmwareversie met ondersteuning voor elektronische sloten is niet inbegrepen in het pakket op de updateserver. Firmware-updates voor IP-apparaten die elektronische sloten beheren, moeten handmatig worden uitgevoerd, onafhankelijk van automatische systeemupdates

Voor een goede en volledige werking van elektronische sloten is het noodzakelijk om een 2N-apparaat met een speciale firmwareversie in het IP-beheer te hebben. De firmwareversie die elektronische sloten ondersteunt https://www.2n.com/cs-CZ/2nos-elocks-fw.

Uitsluiting van apparaten

Apparaten kunnen worden uitgesloten van bulkfirmwarebeheer door ze toe te voegen aan de v **Apparaten > Firmware > tabblad Uitgesloten apparaten**.

Incompatibele firmwareversie

Wanneer u een apparaat toevoegt of upgradet dat geen compatibele firmware heeft, zal dat apparaat een incompatibele status krijgen. Een incompatibele status betekent dat er geen nieuwe gebruikers op het apparaat worden opgeslagen. Bovendien worden gebeurtenissen van het apparaat gedownload en is het mogelijk om de configuratie of back-up van het apparaat te gebruiken. Er wordt een nieuw item in de tabel aangemaakt en de beheerder heeft de mogelijkheid om het gebruik van incompatibele firmware toe te staan.

Access Commander schakelt automatisch apparaten uit met firmware die niet wordt ondersteund door de huidige versie. Op het tabblad worden deze niet-ondersteunde firmwareversies op aangesloten apparaten weergegeven. De lijst met ondersteunde firmwareversies vindt u hieronder.

Access Commander kan alle apparaten besturen die een niet-ondersteunde firmwareversie gebruiken als die versie is goedgekeurd. Goedkeuring vindt plaats onder het tabblad **Apparaten > Firmware > Incompatibele firmwareversies** met behulp van het pictogram .

LET OP
Het goedkeuren van een niet-ondersteunde versie kan leiden tot problemen zoals gegevensverlies of kan anderszins de juiste werking verhinderen.

Ondersteunde firmwareversies

- 3.50
- 3.0
- 2.50
- 2.49
- 2.48
- 2.47
- 2.46
- 2.45

Beveiliging

Hoe de communicatie tussen Access Commander en apparaten wordt beveiligd, is ingesteld in **Apparaten > Beveiliging > Tabblad voor validatie van apparaatcertificaten**.

Access Commander biedt drie beveiligingsniveaus voor communicatie met apparaten:

1. **Gecodeerde communicatie zonder certificaatverificatie** - **Access Commander** gebruikt een zelfondertekend certificaat voor HTTPS-communicatie. Dit certificaat wordt door webbrowsers als niet-vertrouwd beschouwd.
2. **Certificaat vingerafdruk authenticatie** - communicatie wordt beveiligd door het controleren van het certificaat dat is geüpload naar het apparaat. De vingerafdruk van dit certificaat wordt geverifieerd tijdens de communicatie.
   Wanneer vingerafdrukverificatie is ingeschakeld, moet de apparaatbeheerder de geldigheid van de certificaatafdruk bevestigen bij het toevoegen van een nieuw apparaat. De apparaatbeheerder wordt gevraagd de vingerafdruk te verifiëren, zelfs als het certificaat van een reeds toegevoegd apparaat wordt gewijzigd

3. **Validatie van het certificaat voltooien** — de communicatie wordt verzekerd door een certificaat dat is ondertekend door de zogenaamde certificeringsautoriteit. Tijdens de communicatie wordt de volledige certificeringsketen geverifieerd volgens de vereisten van PKI

LET OP
Het is niet mogelijk om uw eigen SSL-certificaten te uploaden naar het 2N Indoor Touch; zodra certificaatverificatie is ingeschakeld, gaat de verbinding met de certificaten verloren.

Hoe kunt u certificaten beheren

Hoe de communicatie tussen Access Commander en apparaten wordt beveiligd, is ingesteld in **Apparaten > Beveiliging > Tabblad voor validatie van apparaatcertificaten**.

Wanneer SSL-certificaatverificatie is ingeschakeld, vindt synchronisatie alleen plaats op apparaten met een SSL-certificaat met een ondertekende vertrouwde autoriteit. De synchronisatie van apparaten zonder dergelijke SSL-certificaten wordt uitgeschakeld. Apparaten schakelen over naar de offlinestatus

Het certificaat van ondertekeningsautoriteit moet vertrouwd zijn op de server waarop het draait**Commandant voor toegang**.

TIP
Het proces van het uploaden van certificaten naar de server wordt beschreven in de FAQ.

Voor een succesvolle authenticatie moeten apparaatcertificaten worden ondertekend door de certificeringsinstantie en het IP-adres of de domeinnaam van het apparaat bevatten.

Een apparaatcertificaat uploaden

1. Voer de webconfiguratie van het apparaat in.
2. Ga naar **sectie Systeem > menu Certificaten > tabblad Persoonlijke certificaten**.
3. Upload het voorbereide certificaat.
4. Ga naar **Sectie Services > Menu Webserver**.
5. In het blok **Geavanceerde instellingen**, selecteer voor **HTTPS-servercertificaat** dit geüploade certificaat.
6. Sla de wijzigingen op.

Instellingen voor invoer-/uitvoerapparaat

Apparaten (2N intercoms of 2N toegangseenheden) kunnen maximaal twee toegangspunten hebben. Elk toegangspunt laat doorgang in één richting toe. De toegangspunten onderscheiden de doorgangsrichting door het apparaat. Aan elk toegangspunt kunnen een of meer lezers worden toegewezen die op het apparaat zijn aangesloten en in de richting van het punt werken. Toegangspunten worden gebruikt om het binnenkomen of verlaten van een zone te registreren. Het gebruik ervan is nodig wanneer het apparaat zich op de interface tussen twee zones bevindt.

Toegangspunten worden ook gebruikt om gebruikers in de module te volgen Aanwezigheid (p. 77). Toegangspunten worden ook gebruikt om het in- en uitgaand verkeer te monitoren Gebiedsbeperkingen (p. 79).

OPMERKING
Individuele toegangspunten instellen **Toegang tot commandant** wordt voorgeschreven in de webinterface van het apparaat in de sectie Services > Toegangscontrole:

- Toegangspunt 1 = Aankomstregels
- Toegangspunt 2 = Uitgangsregels

Toegangspunten instellen

1. Voer de webconfiguratie van het apparaat in.

   TIP
   U kunt naar de webconfiguratie-interface gaan door op te klikken in de lijst op de pagina Apparaten.

2. Ga naar het menu **Hardware > Uitbreidingsmodules**.
3. Zoek de toegangsmodule die moet worden gebruikt als Toegangspunt 1 (Aankomst) of Toegangspunt 2 (Uitgaand).
4. Stel in de parameter Deur de gewenste richting in en sla de instellingen op.
5. Ga naar de Zones v-pagina **Toegang tot commandant**.
6. Druk in de rechterbovenhoek op en het gebruik van toegangspunten mogelijk maken.

Toegangsregels

Toegangsregels zijn een hulpmiddel om de toegang van gebruikersgroepen tot zones duidelijk te beheren. Toegang kan worden verleend op basis van tijdprofielen.

Toegangsregels bepalen WIE toegang heeft, WAAR en WANNEER.

- **WHO** wordt bepaald door de groep en de gebruikers die eraan zijn toegewezen (een gebruiker kan zich tegelijkertijd in meerdere groepen van één bedrijf bevinden).
- **WAAR** wordt bepaald door de zone of apparaten (één apparaat kan zich slechts in één zone tegelijk bevinden).
- **WANNEER**wordt bepaald door het toegewezen tijdprofiel. Dit artikel is optioneel. Een leeg tijdprofiel betekent onbeperkte toegang (24/7).

OPMERKING
Eén groep kan toegang hebben tot meerdere zones, maar ook meerdere groepen kunnen toegang hebben tot één zone.

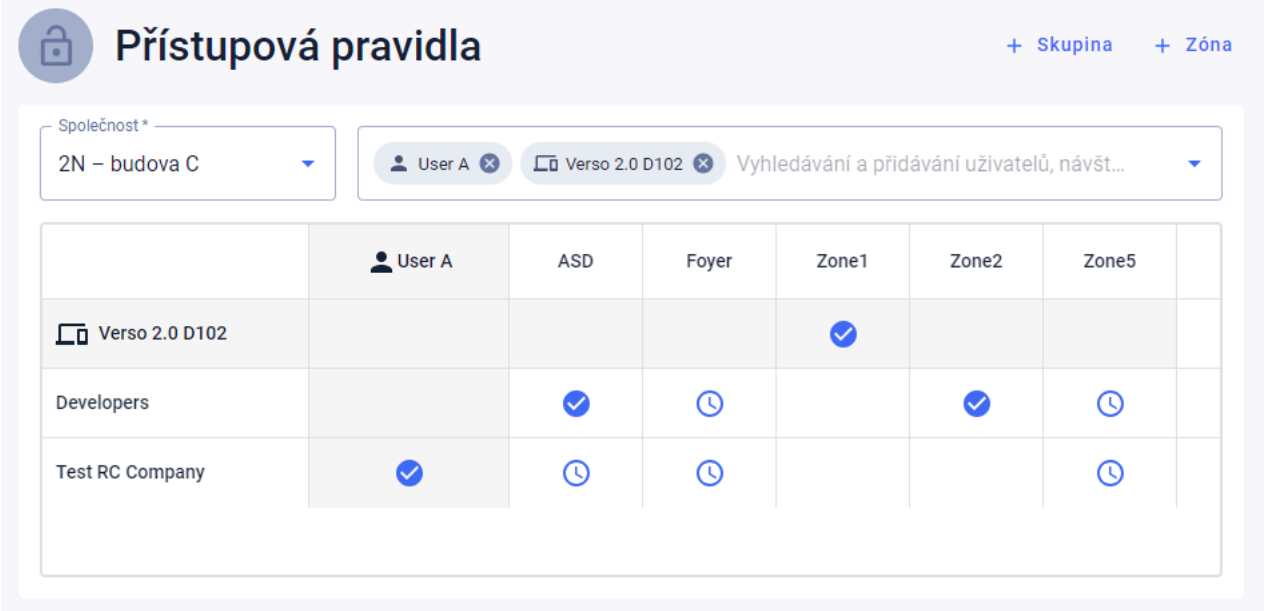
Matrixweergave

De matrixweergave van de regels op de pagina met toegangsregels geeft een overzicht van de toegangen weer en maakt het mogelijk deze in te stellen. De matrix is beschikbaar voor elk bestaand bedrijf en toont alle groepen en zones die eraan zijn toegewezen. De beheerder kan in het menu boven de matrix van bedrijf wisselen.

Door op de cel te klikken die overeenkomt met de geselecteerde zone en groep, wordt de toegang van de groep tot de zone ingesteld. Er verschijnt een menu waarin u kunt kiezen voor onbeperkte toegang of toegang beperkt door een tijdprofiel. Tijdprofielen moeten vooraf op de pagina worden ingesteld Tijdprofielen (p. 69).

In het zoekveld boven de matrix is het mogelijk om gebruikers of apparaten aan de matrix toe te voegen. Gebruikers kunnen aan een groep worden toegevoegd via de kruising van gebruiker en groep. Door een apparaat en een zone te kruisen, worden apparaten aan de zone toegevoegd.

Een voorbeeld van een matrixrepresentatie



De afbeelding geeft een overzicht van de matrix voor het bedrijf 2N Telekomunikace as. Uit het overzicht blijkt duidelijk dat:

- Het gefilterde apparaat Verso 2.0 D102 is onderdeel van Zone1.
- De gefilterde gebruiker Gebruiker A maakt deel uit van de groep Test RC Bedrijf.
- Gebruikers uit de groep Developers hebben onbeperkt toegang tot de zones ASD en Zone2, beperkte toegang tot de zones Foyer en Zone5 (volgens het ingestelde tijdprofiel) en hebben geen toegang tot de zone Zone1.
- Gebruikers uit de groep Test RC Company hebben beperkte toegang tot de zones ASD, Foyer en Zone5 (volgens het ingestelde tijdprofiel) en hebben geen toegang tot de zones Zone1 en Zone2.

Lijst met regels

Op de pagina Regellijst wordt een lijst weergegeven met alle momenteel geldige toegangsregels. Klik op de regel om deze te bewerken. Een nieuwe toegangsregel kan worden toegevoegd door op de knop Toevoegen rechtsboven te klikken. Voordat u een regel maakt, moet u de parameters van de regel instellen.

Zowel de regelslijst als de matrix geven dezelfde toegangsregels weer. Een wijziging in de ene weergave wordt automatisch gekopieerd naar de andere weergave. Ook in zone-instellingen en groepsinstellingen worden de toegangsregels aangepast.

Tijdprofielen

Geselecteerde intercomfuncties kunnen in de tijd beperkt zijn. Aan de genoemde functies kan een zogenaamd tijdprofiel worden toegewezen, dat bepaalt wanneer de betreffende functie beschikbaar is.

Tijdprofielen kunnen aan de volgende vereisten voldoen:

- blokkeer oproepen naar de geselecteerde gebruiker volledig buiten de gereserveerde tijd
- blokkeer oproepen naar geselecteerde telefoonnummers van de gebruiker buiten de gereserveerde tijd
- blokkeer gebruikerstoegang buiten de toegewezen tijd

Elk tijdprofiel definieert de beschikbaarheid van de functie waaraan het is gekoppeld met behulp van een weekkalender. U kunt eenvoudig de tijd instellen van-tot en evt dagen van de week waarop de functie beschikbaar zou moeten zijn. Toegangsbepaling met behulp van tijdprofiel wordt ingesteld door toegangsregels. De beperking van de beschikbaarheid van de gebruiker buiten het tijdprofiel wordt samen met het telefoonnummer van de gebruiker ingesteld.

Optioneel kunnen maximaal 20 algemene tijdprofielen worden aangemaakt, die naast de toegangscontrole ook voor speciale gevallen van lokale configuratie kunnen worden gebruikt. Deze tijdprofielen worden geüpload naar alle gesynchroniseerde apparaten.

Tijdprofielen op elektronische sloten

Elektronische sloten ondersteunen tijdprofielen met de volgende beperkingen:

- Feestdagen zijn niet van toepassing.
- Binnen één dag kunnen maximaal 4 verschillende tijdsintervallen worden ingesteld.
- Binnen één tijdprofiel kunnen 4 dagelijkse intervalschema's worden gedefinieerd.

TIP
Dit betekent dat je verschillende instellingen kunt hebben voor bijvoorbeeld maandag, dinsdag, woensdag en donderdag, maar voor vrijdag, zaterdag en zondag moet je al een van de bestaande instellingen gebruiken.

LET OP
Als het tijdprofiel deze beperkingen overtreedt, wordt de toegangsregel genegeerd en krijgt de gebruiker geen toegang.

Een tijdprofiel aanmaken

1. Ga naar **Tijdsprofielen**.
2. Klik op `+ Time Profile` in de rechterbovenhoek.
3. Stel in het geopende dialoogvenster de naam van het tijdprofiel in.

4. Selecteer Tijdsloten toevoegen om een tijdsbeperking te selecteren. Blauw gemarkeerde dagen geven dagen aan die binnen het tijdsprofiel vallen. Om een dag te selecteren, klikt u erop. U kunt binnen de dagen een tijdsinterval instellen om de geldigheid van het tijdsprofiel te bepalen.

   OPMERKING
   U kunt een tijdsinterval binnen dagen instellen om de geldigheid van het tijdsprofiel te bepalen.

   LET OP
   Verschillende tijden voor elke dag kunnen worden ingesteld nadat het tijdsprofiel is aangemaakt.

5. Het nieuw aangemaakte tijdprofiel wordt aan de lijst toegevoegd en de details ervan worden geopend, waarin verdere instellingen kunnen worden gemaakt. In de detaillering van het tijdprofiel is het mogelijk om de positie van het profiel op de apparaten in te stellen.

OPMERKING
Wereldwijde profielen kunnen de toegang in alle bedrijven beïnvloeden. Alleen de beheerder kan ze bewerken.

Een toegangsbeheerder kan alleen de tijdsprofielen van zijn bedrijf corrigeren.

Het tijdprofiel instellen

De uitsplitsing van dagen en tijden wordt weergegeven in de details van het tijdprofiel. De blauwe intervallen geven aan wanneer het profiel actief is. Binnen één dag kan een willekeurig aantal intervallen worden ingesteld.

Het interval wordt toegevoegd door op het uurslot te klikken en het exacte tijdstip in te stellen waarop het profiel actief moet zijn. De tijd van een individueel interval kan worden gewijzigd door op het interval te klikken. Als het profiel de hele dag actief moet zijn, moet er één interval voor de hele dag worden aangemaakt, d.w.z. 00:00-23:59.

In het uitgebreide menu dat wordt geopend door op te klikken ⋮ de positie op het apparaat kan worden ingesteld. De positie op het apparaat definieert de positie in de lijst met tijdprofielen die wordt geüpload naar alle apparaten waaraan het tijdprofiel is toegewezen.

Het beperken van de beschikbaarheid van de gebruiker buiten het tijdprofiel wordt samen met het telefoonnummer ingesteld in de instellingen van de gebruiker.

Aanwezigheid

Access Commander maakt het mogelijk om de aanwezigheid van gebruikers te monitoren. In de aanwezigheidsmodus worden de in- en uitlooptijden van individuele gebruikers geregistreerd.

Aanwezigheid en aanwezigheidsmodi worden ingesteld in **Instellingen > Configuratie > Tabblad Aanwezigheid**, zie Aanwezigheidsinstellingen (p. 72).

LET OP
Voor de juiste functie van aanwezigheid is het noodzakelijk om te hebben **Access Commander**beschikbare actieve licentie om de aanwezigheid van gebruikers bij te houden. Aanwezigheidsregistratie moet in de individuele gebruikersinstellingen worden geactiveerd.

De aanwezigheidspagina biedt een lijst met gebruikers met bijgehouden aanwezigheid. Er staat een pictogram in de rechterbovenhoek , waarmee het mogelijk is om een CSV-bestand te downloaden met samenvattende gegevens over de aanwezigheid van alle gebruikers. Bij het downloaden van de gegevens moet u de periode invoeren waarvoor de aanwezigheid moet worden gegenereerd.

Aanwezigheid van een specifieke gebruiker

U kunt een specifieke gebruiker selecteren uit de lijst met gebruikers op de pagina Aanwezigheid en alleen meer gedetailleerde informatie over hun aanwezigheid weergeven.

In het bovenste deel van het overzicht kunt u de maand selecteren waarvoor u de aanwezigheid wilt weergeven. Naast de maandselectie worden het ingestelde werkfonds voor de betreffende maand, het saldo en de gewerkte uren weergegeven.

Er is een uitbreidingsmenu naast de gebruikersnaam waardoor de aanwezigheidsgegevens van de weergegeven gebruiker kunnen worden gedownload in een CSV- of PDF-bestand. Beide bestanden bevatten gegevens van afzonderlijke dagen.

TIP
Het is ook mogelijk om de aanwezigheid van de gebruiker te bekijken in de details van de gebruiker, die toegankelijk is door deze te selecteren in de lijst met gebruikers op de pagina **Gebruikers**.

Wijzig de aanwezigheid van gebruikers

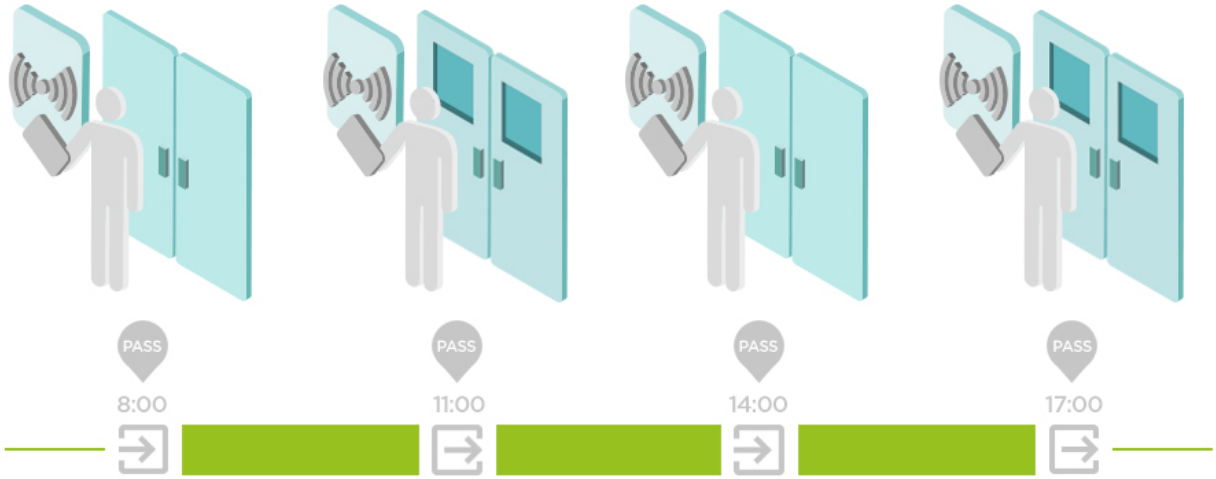
De aanwezigheidsmanager kan de aanwezigheidsgegevens van gebruikers bewerken. Bewerken gebeurt door op het te wijzigen tijdsinterval te klikken. Eenmaal geopend kunnen de cut-off-tijden worden bewerkt en kan een notitie aan het interval worden toegevoegd.

Aanwezigheidsinstellingen

Access Commander maakt het mogelijk om de aanwezigheid van gebruikers te monitoren. In de aanwezigheidsmodus worden de in- en uitlooptijden van individuele gebruikers geregistreerd.

Aanwezigheidsmodi

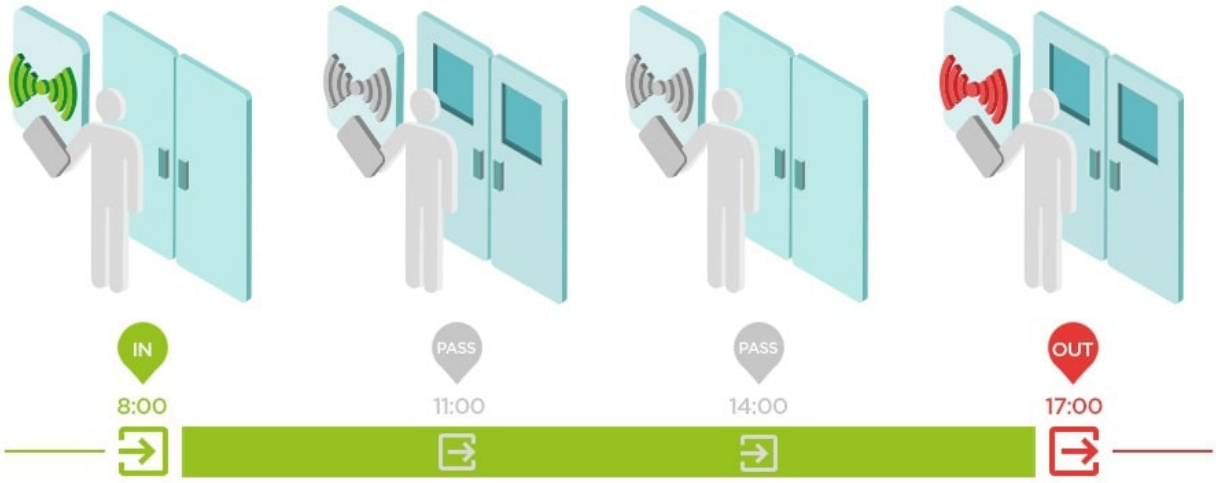
- **FREE**



Aankomst en vertrek worden geteld vanaf de eerste en laatste gebruikersauthenticatie op elk apparaat op één dag. In deze modus werkt de aanwezigheidsmodule niet.

- **IN-OUT**

Inkomende en uitgaande apparaten moeten op een goede werking worden ingesteld.



- **IN-OUT voor alle apparaten**
  Deze modus maakt aanwezigheidsbewaking mogelijk. Aankomsten worden geregistreerd op inkomende apparaten, vertrekken worden geregistreerd op uitgaande apparaten. Bewegingen tussen zones worden niet als aankomst/vertrek geregistreerd.
- **IN-OUT voor geselecteerde apparaten**
  Deze modus maakt aanwezigheidsbewaking mogelijk. Aankomst en vertrek worden geregistreerd op geselecteerde apparaten die zijn ingesteld als aankomst of vertrek. Aankomst en vertrek worden alleen op deze geselecteerde apparaten geregistreerd. Zo kan de registratie van aankomst/vertrek bijvoorbeeld alleen bij de hoofdingang van het gebouw worden ingesteld.

Instellingen voor invoer-/uitvoerapparaat

Apparaten (2N intercoms of 2N toegangseenheden) kunnen maximaal twee toegangspunten hebben. Elk toegangspunt laat doorgang in één richting toe. De toegangspunten onderscheiden de doorgangsrichting

door het apparaat. Aan elk toegangspunt kunnen een of meer lezers worden toegewezen die op het apparaat zijn aangesloten en in de richting van het punt werken. Toegangspunten worden gebruikt om het binnenkomen of verlaten van een zone te registreren. Het gebruik ervan is nodig wanneer het apparaat zich op de interface tussen twee zones bevindt.

Toegangspunten worden ook gebruikt om gebruikers in de module te volgen Aanwezigheid (p. 77). Toegangspunten worden ook gebruikt om het in- en uitgaand verkeer te monitoren Gebiedsbeperkingen (p. 79).

OPMERKING
Individuele toegangspunten instellen **Toegang tot commandant** wordt voorgeschreven in de webinterface van het apparaat in de sectie Services > Toegangscontrole:

- Toegangspunt 1 = Aankomstregels
- Toegangspunt 2 = Uitgangsregels

Toegangspunten instellen

1. Voer de webconfiguratie van het apparaat in.

   TIP
   U kunt naar de webconfiguratie-interface gaan door op te klikken in de lijst op de pagina Apparaten.

2. Ga naar het menu **Hardware > Uitbreidingsmodules**.
3. Zoek de toegangsmodule die moet worden gebruikt als Toegangspunt 1 (Aankomst) of Toegangspunt 2 (Uitgaand).
4. Stel in de parameter Deur de gewenste richting in en sla de instellingen op.
5. Ga naar de Zones v-pagina **Toegang tot commandant**.
6. Druk in de rechterbovenhoek op en het gebruik van toegangspunten mogelijk maken.

Bezoeken

In **Access Commander**het is mogelijk om bezoekersprofielen aan te maken die voor een beperkte tijd toegangsrechten hebben. Tijdens het bezoek is het mogelijk om een toegangskaart, toegangscode toe te voegen en het kenteken van het voertuig in te vullen. Bij het bezoek wordt de aanwezigheid niet meegeteld. Het aantal bezoeken is door geen enkele licentie beperkt.

Instellen van het bewaren van bezoekersgegevens

De beheerder kan de bewaartermijn van bezoekersgegevens instellen. De bewaartermijn van bezoekersgegevens stelt u in dagen in door op het icoontje te klikken naast de knop om een nieuw bezoek aan te maken.

Nadat het bezoektijdsinterval is verstreken en de ingestelde bewaartermijn voor gegevens is verstreken, worden bezoeken elke middernacht automatisch verwijderd. Bezoeken waaraan nog bezoekerskaarten zijn toegewezen, worden niet verwijderd.

OPMERKING
Instellingen kunnen worden gebruikt om te voldoen aan de lokale regelgeving inzake gegevensbescherming. De bezoeknaam en notitie worden bewaard in het toegangslogboek volgens de levenslange instellingen in logbeheer.

Een nieuw bezoek aanmaken

1. Ga naar de pagina **Bezoeken**.
2. Klik op de knop Bezoek toevoegen in de rechterbovenhoek.
3. In het dialoogvenster dat wordt geopend, vult u de naam van het bezoek in, selecteert u de bezochte groep en stelt u het begin en einde van het bezoek in. Als u het begin en einde van het bezoek niet instelt, begint het tijdsinterval voor toegang tot het bezoek onmiddellijk en eindigt het aan het einde van de dag.

   LET OP
   Het tijdsinterval voor bezoektoegang mag niet langer zijn dan één maand.

4. Voordat u een bezoek aanmaakt, kunt u de authenticatiemethoden instellen die het bezoek zal gebruiken voor toegang.
   Het nieuw aangemaakte bezoek verschijnt in de lijst. In de details van het bezoek is het mogelijk om authenticatiemethoden aan het bezoek toe te voegen en de toegang ervan te beheren,

Einde bezoek

Na het tijdsinterval vervalt de toegang voor het bezoek.

Als de beheerder of beheerder het bezoek beëindigt via de knop Einde op het tabblad Toegangen in de bezoekinstellingen wordt de toegang van dit bezoek tot de toegangspunten van het apparaat onmiddellijk geblokkeerd en kan het bezoek via geen enkel apparaat passeren. Voor een bezoeker wiens bezoek automatisch is beëindigd, is er een Stop-knop beschikbaar omdat de tijdzone op de apparaten kan verschillen.

Als aan een bezoek een bezoekerskaart is toegewezen, wordt de kaart losgemaakt en kan deze voor een ander bezoek worden gebruikt.

Bezoek instellingen

Informatie over het bezoek kunt u bekijken en bewerken bij de details van het bezoek. Bezoekdetails worden geopend door op het geselecteerde bezoek in de lijst te klikken.

Benaderingen

Op het tabblad Toegangen worden de toegangsgroep en het tijdsinterval weergegeven waarin het bezoek geldige toegang heeft. Het tijdsinterval voor bezoektoegang kan opnieuw worden ingesteld door in het uitgebreide menu Reset bezoek te kiezen .

In dit tabblad is het mogelijk om het bezoek te beëindigen.

Bezoek

Op de kaart staat de persoon van wie het bezoek afkomstig is. Het is mogelijk om de bezochte persoon te wijzigen.

Op dit tabblad is het mogelijk om een notitie aan het bezoek toe te voegen.

Persoonlijke gegevens

Op de kaart worden de contactgegevens van het bezoek weergegeven en kunnen deze worden gewijzigd. De ingestelde e-mail maakt het verzenden van Authenticatiecodes mogelijk.

Authenticatie

Tijdens het bezoek is het mogelijk om een toegangskaart, toegangspin of QR-code toe te voegen en het kenteken van het voertuig in te vullen. Per bezoek kunt u slechts één kenteken invullen.

Bij het invullen van het e-mailadres is het mogelijk om de gegenereerde toegangs-PIN/QR-code naar het opgegeven adres te sturen.

Hier kunt u de toegewezen RFID-kaart inleveren.

Toegangslogboek

Het toegangslogboek geeft de toegangsgeschiedenis weer.

Kaarten

De Kaarten-pagina wordt gebruikt om de toegangskaarten voor bezoekers te beheren die beschikbaar zijn voor het toevoegen van een bezoek. Een nieuwe kaart wordt toegevoegd met de knop Toevoegen in de rechterbovenhoek.

Kaarten moeten altijd aan een bedrijf worden toegewezen. De kaart kan alleen worden gebruikt voor bezoeken waarbij dit bedrijf wordt bezocht.

Een bestaande kaart kan worden overschreven of verwijderd door deze in het uitgebreide menu te selecteren .

LET OP
Een kaart die aan een actief bezoek is toegewezen, kan niet worden verwijderd.

OPMERKING
Als **Access Commander** meldt dat de gloednieuwe kaart die zojuist is toegevoegd al in gebruik is in het systeem, kan de reden zijn dat de compatibiliteitsmodus voor RFID-kaarten is ingeschakeld. Deze modus wordt door de beheerder ingeschakeld in **Instellingen > Authenticatie > tabblad Instellingen compatibiliteitsmodus**. De compatibiliteitsmodus kan voor elk apparaat afzonderlijk worden geactiveerd in de webconfiguratie-interface van het apparaat in het **menu Services > Toegangsbeheer > tabblad Geavanceerd > Overige instellingen**.

Een beveiligde kaart beheren met een USB-lezer

De USB-lezer kan worden gebruikt voor diagnose en beheer van de beveiligde kaart in het zoekveld in de koptekst.

TIP
Voordat u de USB-lezer kunt gebruiken, moet deze zijn ingeschakeld in **Access Commander**. Zie USB-lezers ingeschakeld (p. 101) voor meer informatie.

1. Sluit de USB-lezer aan op uw computer.
2. Klik op het pictogram in het zoekvak in de kopregel.
3. Bevestig aan de lezer.

Beschikbare bewerkingen

- Gegevens van de kaart ophalen
- Een gebruiker zoeken op kaart
- Om de gebeurtenissen te bekijken die op het tabblad zijn opgeslagen
- Toegangsgegevens bijwerken
- Een toepassing verwijderen of formatteren
- Service kaart uitbreiding

Aanwezigheid

Met de module **Aanwezigheid** kunt u gebruikersactiviteiten in realtime controleren. Deze module werkt onafhankelijk van de module **Aanwezigheidsregistratie**, waarvoor een aparte licentie nodig is. Aanwezigheid kan zelfs gemonitord worden zonder een actieve Attendance-licentie.

De twee functies worden samen weergegeven op de tabbladen **Aanwezigheidsregistratie en Aanwezigheid** in de interface van Access Commander, maar ze hebben elk hun eigen doel en werken onafhankelijk van elkaar.

Om de module te laten werken, moet u de aanwezigheidsmodus IN-OUT instellen in **Instellingen > Configuratie > Tabblad Aanwezigheid**, zie Aanwezigheidsinstellingen (p. 72).

- Als de laatste gebeurtenis van de gebruiker op een bepaalde dag een aankomst is (**IN** gebeurtenis), wordt als aanwezig beschouwd.
- Als een gebruiker een lezer passeert die is ingesteld op een niet-gespecificeerde richting, zal de zone van de gebruiker veranderen. Hetzelfde gebeurt als hij een lezer in de modus **IN** passeert.
- Als de laatste gebeurtenis van de gebruiker op een bepaalde dag een afmelding is (gebeurtenis**OUT**), wordt hij als afwezig behandeld.

LET OP
De aanwezigheidsmodule werkt niet als de FREE modus wordt gebruikt binnen het aanwezigheidsregistratiesysteem. Aanwezigheidsbewaking is alleen mogelijk in de IN-OUT-modus.

Verstrijken van de aanwezigheid van de gebruiker

Klik op het pictogram rechtsboven is Vervaldatum gebruikersaanwezigheid ingesteld. Als de aanwezigheid van de gebruiker vervalt, wordt de aanwezigheidsrecord van de gebruiker automatisch verwijderd als de gebruiker vergeet zijn vertrek te markeren. Deze tijdslimiet wordt uitgedrukt in uren en bepaalt hoe lang na de laatste passage van de huidige gebruiker zijn aanwezigheidsrecord automatisch wordt verwijderd. Door deze tijdslimiet in te stellen, kunt u definiëren hoe lang een aanwezigheidsregistratie in het systeem mag blijven als de gebruiker niet als afwezig is gemarkeerd. Dit zorgt ervoor dat de lijst met huidige gebruikers actueel blijft en geen gegevens bevat van gebruikers die het gebouw al hebben verlaten en zijn vergeten uit te loggen.

Rapporten

Het is mogelijk om samenvattende gegevens over toegevoegde gebruikers te downloaden vanaf de pagina Rapporten. De gedownloade bestanden zijn in CSV-formaat (Comma-Separated Values). De bestandsnaam geeft altijd de datum en tijd aan waarop het rapport is gegenereerd.

OPMERKING
Sommige spreadsheetprogramma's gebruiken andere scheidingstekens en het CSV-bestand wordt mogelijk niet correct weergegeven wanneer het daarin wordt geopend. In dergelijke gevallen wordt aanbevolen om de gegevens uit het CSV-bestand in een geopende werkmap te importeren.

- **My2N app** – Gekoppelde en niet-gekoppelde gebruikers met resterende koppelingstijd
  Het rapport bevat gegevens over de status van de gebruikerskoppeling via de applicatie My2N, of gegevens over de geldigheidsduur van de actieve koppelingscode.
- **Gebruikers** – Toegangsregels met groepen, zones, apparaten en tijdprofielen
  Het rapport vermeldt gegevens over de toewijzing van gebruikers aan groepen, hun toegang tot zones en apparaten in de zones, en de tijdprofielen waarin gebruikers toegang krijgen. Elke combinatie wordt op precies één rij van de tabel vermeld.
- **Gebruikers** – Gedetailleerde export
  Het rapport vermeldt alle informatie over gebruikers die in hun profiel is ingevuld, inclusief hun persoonlijke en toegangsgegevens.

  LET OP
  Het bestand bevat gevoelige gegevens!
- **Gebruikers** – Globale synchronisatie-export
  Het rapport vermeldt gegevens over de toewijzing van gebruikers aan groepen, hun toegang tot zones en apparaten in de zones, en de tijdprofielen waarin gebruikers toegang krijgen. Elke combinatie wordt op precies één rij van de tabel vermeld.
  Dit rapport kan dienen als CSV-bestand voor gebruikerssynchronisatie, zie Synchronisatie van gebruikers (p. 86).

  LET OP
  Het bestand bevat gevoelige gegevens!

Gebiedsbeperkingen

Gebruik gebiedsbeperkingen om gebieden te definiëren waarin de functies Bezetting en Anti-Passback kunnen worden gebruikt.

OPMERKING
De module Gebiedsbeperkingen en de Aanwezigheidsmodule (inclusief Aanwezigheid) zijn onafhankelijk van elkaar. Bezetting en antipassback kunnen niet worden gebruikt voor de modules Aanwezigheid en Aanwezigheid. Bezetting en antipassback werken alleen in het Area Restrictions-model

Gebiedsbeperkingen instellen

Een nieuw apparaat wordt aan het gebied toegevoegd met behulp van de knop in de gebiedsdetailkop.

Input en output

Deze kaarten geven aan welke apparaten als in- of uitgang in een bepaalde zone worden gerouteerd. Via het uitgebreide menu onder ⋮ apparaten kunnen tussen tabbladen worden verplaatst of uit het gebied worden verwijderd.

Door de gebruiker te authenticeren bij het toegangsapparaat wordt de toegang tot het gebied geregistreerd. Door de gebruiker te authenticeren bij het uitgangsapparaat verlaat de gebruiker het gebied. Hiermee kan worden gecontroleerd of de gebruiker zich nog in het gebied bevindt en of hij het gebied opnieuw wil betreden.

Als op het toegevoegde apparaat twee toegangspunten zijn ingesteld, kan elk punt voor een andere richting worden gebruikt (Invoer/Uitvoer). De toegangspuntinstellingen worden beschreven in het hoofdstuk Instellingen voor invoer-/uitvoerapparaat (p. 72). De eigenschappen van het toegangspunt worden uitgebreid door op de pijl te klikken.

Bezetting

Inkomende en uitgaande apparaten moeten op een goede werking worden ingesteld.

Het tabblad Bezettingsgraad geeft een overzicht van het aantal personen in het gebied en biedt u de mogelijkheid om bezettingslimieten in te stellen. Als de bezettingsgrens is bereikt, is het mogelijk om extra ingangen te weigeren of deze ingangen alleen op te nemen in het systeemlogboek. De bezettingsfunctie houdt niet bij welke mensen zich in de buurt bevinden. Een aparte Presence-module is ontworpen om de aanwezigheid van individuele personen te controleren

LET OP
Bij het opnieuw autoriseren van een enkele gebruiker telt elke autorisatie als één invoer. Dit betekent dat als een gebruiker zich drie keer achter elkaar registreert op het inkomende apparaat, deze wordt beoordeeld als drie personen in de buurt. Als de fysieke installatie van het apparaat het mogelijk maakt om de kaart van één gebruiker herhaaldelijk opnieuw te laden, is het daarom raadzaam om de bezettingsfunctie te combineren met de anti-passback-functie

Anti-passback

Inkomende en uitgaande apparaten moeten op een goede werking worden ingesteld.

het gebied is het mogelijk om de anti-passback-functie te activeren, die zorgt voor een uitbreiding van de toegangscontrole door monitoring en misbruik van rechten voor terugkeer naar de gereserveerde gebieden. De bewaakte gebieden worden afgebakend door grensapparatuur die hen naar het gebouw leidt of hen de mogelijkheid geeft deze te verlaten. Op deze apparaten worden bij binnenkomst de machtigingen gecontroleerd volgens de regels die voor het gebied zijn gedefinieerd. Nadat de gebruiker het gebied via het grensapparaat heeft verlaten, kan de gebruiker pas terugkeren naar het gebied nadat de time-out is verstreken, als de time-out is ingesteld. Als de gebruiker eerder probeert terug te keren naar het gebied, zal het systeem hem de toegang weigeren of de gebeurtenis alleen in het logboek registreren

WAARSCHUWING

- Een anti-passbackgebied verliest zijn betekenis en kan potentieel gevaarlijk zijn als er zich in het gebied een apparaat bevindt waaraan een actieve REX-knop is bevestigd die ongeautoriseerde toegang mogelijk maakt.

Een uitzondering instellen

Soms kan het wenselijk zijn dat anti-passback voorwaarden niet van toepassing zijn op geselecteerde gebruikers. Meestal zijn dit gebruikers zoals de gebouwbeheerder, CEO, VIP-gebruikers, enz. Gebruikers of hele groepen die niet onder de anti-passback voorwaarden moeten vallen, worden ingesteld in **Instellingen > Anti-passback > Uitzonderingen**.

OPMERKING
Het gedeelte Instellingen is alleen beschikbaar voor gebruikers met de beheerdersrol.

Lijst met geblokkeerde gebruikers

Geblokkeerde gebruikers zijn gebruikers die hebben geprobeerd toegang te krijgen tot het antipassback-gebied voordat de time-out was verstreken. ✕ gebruikers kunnen van de lijst worden uitgesloten, waardoor ze weer toegang krijgen tot het gebied.

TIP
Wanneer een gebruiker de toegang wordt geweigerd vanwege een actieve anti-passback, kan er een automatische informatieve e-mail naar de gebruiker worden gestuurd. Ga naar **Instellingen > Anti-passback > tabblad Kennisgeving geblokkeerde** gebruiker e-mail om het verzenden van de e-mail in te schakelen.

Beperkingen opnieuw instellen

Het tabblad **Instellingen > Anti-passback > Gebiedsbeperkingen resetten** stelt de dagen en tijden in waarop het gebiedsrecord wordt gewist, d.w.z. alle gebruikers kunnen weer passeren, ongeacht eerdere regelovertredingen.

Deze maatregelen verbeteren het beschermingsniveau en voorkomen potentiële veiligheidsbedreigingen. Meer specifiek helpen ze ongeautoriseerde toegang tot geselecteerde locaties te voorkomen, maken ze het volgen van de bewegingen van mensen binnen een bepaalde ruimte mogelijk en registreren ze in- en uitgangen, wat handig kan zijn voor het monitoren en analyseren van beveiligingsgebeurtenissen.

De lijst toont de aangemaakte gebieden in het systeem. Op dit tabblad kunnen gebieden worden aangemaakt, verwijderd en toegankelijk gemaakt voor de details ervan. Tegelijkertijd kunt u het gebied deactiveren en de status ervan weergeven.

Creëer een gebied om te beperken

1. Ga naar de pagina **Gebiedsbeperkingen**.
2. Klik op de knop om een regio toe te voegen in de rechterbovenhoek.
3. Geef het gebied een naam in het geopende dialoogvenster.
4. Voeg in het open gebieddetail een apparaat toe aan het gebied. Apparaten worden toegevoegd met behulp van de knop in de gebiedsdetailkop.
   Het nieuw aangemaakte gebied verschijnt in de lijst. In de details is het mogelijk om de invoer- en uitvoerapparaten in te stellen, de toegestane bezetting in te stellen, de anti-passback-functie in te schakelen en de toegang tot het gebied voor geselecteerde gebruikers te blokkeren.

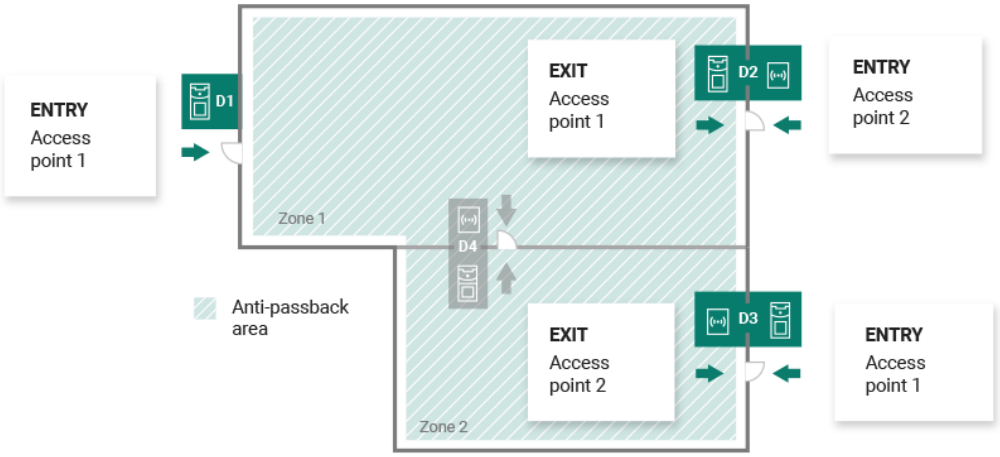
De meest voorkomende installatiefouten

LET OP
Als er in een gebied een fout optreedt, wordt het gehele gebied uitgeschakeld. Het wordt opnieuw geactiveerd nadat de fouten zijn verwijderd.

In de volgende gevallen kunnen regiobeperkingen niet goed werken

- Er is geen apparaat aan het gebied toegevoegd. Er moet minimaal één apparaat worden toegewezen.
- Sommige invoer-/uitvoerapparaten zijn niet correct geconfigureerd of bevatten geen lezer.
- Een invoerapparaat voor dit gebied wordt al gebruikt als invoer voor een ander gebied. De toewijzing moet worden gewijzigd voor een correcte werking.
- Sommige apparatuur is niet voorzien van de benodigde licentie.
- Sommige apparaten zijn uitgeschakeld.
- Er is een apparaat losgekoppeld.
- Sommige apparaten hebben geen compatibele firmwareversie.
  Sommige apparaten zijn uitgerust met een REX-knop waarmee u het APB-gebied kunt verlaten zonder toestemming van de gebruiker. Voor een correcte werking moet de REX-knop gedeactiveerd zijn.

Een voorbeeld van het instellen van beperkingen



De afbeelding toont één anti-passbackgebied met drie grensapparaten D1, D2 en D3. Er worden alleen grensapparaten gebruikt om de anti-passbackfunctie in te stellen. Het D4-apparaat in het anti-passbackgebied wordt niet gebruikt om het binnenkomen/uitgaan van het gebied te controleren. Apparaten D2 en D3 hebben ingestelde toegangspunten.

Apparaat D1 het wordt alleen gebruikt om het anti-passbackgebied te betreden. Op het apparaat is Toegangspunt 1 ingesteld om het gebied binnen te gaan.

Apparaat D2 dient voor zowel input als output. Het apparaat is ingesteld op Toegangspunt 2 om het gebied binnen te gaan, en Toegangspunt 1 om het gebied te verlaten.

Apparaat D3 dient voor zowel input als output. Het apparaat is ingesteld op Toegangspunt 1 om het gebied binnen te gaan, en Toegangspunt 2 om het gebied te verlaten.

Systeem instellingen

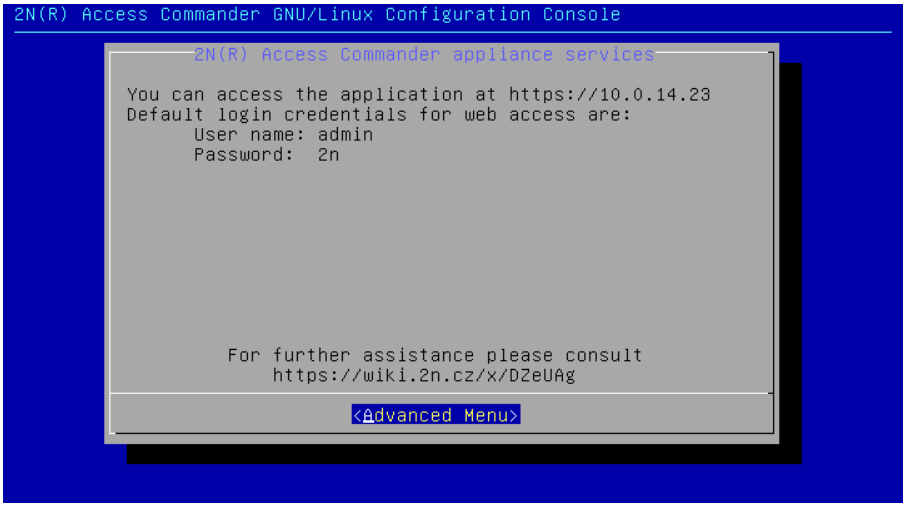
- Datum en tijd (p. 88)
- Netwerkinstellingen (p. 109)
- De e-mailfunctie (SMTP) inschakelen en instellen (p. 95)
- Systeem update (p. 84)
- Synchronisatie van gebruikers (p. 86)
- USB-lezers ingeschakeld (p. 101)
- PICard-sleutels (p. 100)
- Encryptiesleutels voor My2N-applicatie (p. 99)
- CAM-logboeken (p. 101)
- Linux-instellingen (p. 83)

Linux-instellingen

Basissysteeminstellingen kunnen worden gemaakt in de Linux-configuratieconsole.

OPMERKING
als het isAccess Commandergedistribueerd via een virtuele machine, is het mogelijk om op afstand verbinding te maken met de Linux-versie via een SSH-verbinding.

De configuratieconsole wordt geopend door in te loggen **Access Commander** met behulp van het root-account. De startpagina geeft basisinformatie weer over beheerderstoegang tot de webinterface en verwijst door naar het menu Geavanceerd.



In het Geavanceerd Menu is het mogelijk om het volgende in te stellen:

- **Netwerken**
  Proxyserverinstellingen, netwerkeigenschappen, synchronisatieopties met DHCP-server.
- **Tim**
  Handmatige tijdinstelling, NTP-server en tijdzone-instellingen

- **SSH**
  Stelt een externe verbinding in **Access Commander** via SSH. Om SSH in te schakelen, moet een ander wachtwoord dan het standaardwachtwoord worden ingesteld dat voldoet aan de vereisten voor de moeilijkheidsgraad.
- **MKB**
  Start de wizard voor het opzetten van verbindingen met gedeelde mappen. Stelt het IP-adres of de domeinnaam en het mappad in. Bijvoorbeeld "192.168.1.1/aandeel". Voor de instellingen is het noodzakelijk om de gebruikersnaam op te geven van de gebruiker die toegang krijgt tot de gegeven map en schrijfrecht. Het is noodzakelijk om het wachtwoord van de gebruiker in te vullen en de versie van het Samba-protocol te selecteren. Nadat alle verplichte stappen zijn voltooid, wordt de verbinding met de server geverifieerd en wordt informatie weergegeven of de installatie succesvol of mislukt is.
- **Wachtwoord**
  Hiermee kunt u het wachtwoord van de systeemrootgebruiker wijzigen om in te loggen op de console of om toegang te krijgen via SSH.

  OPMERKING
  Het rootwachtwoord wordt gewijzigd in de configuratieconsole, niet in Access Commander.
- **Backup en herstellen**
  Wordt gebruikt om gegevens en configuratie te importeren, herhaalde back-ups in te stellen en eerdere back-ups te herstellen.

Systeem update

Systeem **Access Commander** controleert regelmatig de updateserver en informeert over beschikbare updates en beschikbare nieuwe firmwareversies van aangesloten apparaten. IN **Instellingen > tabblad Systeemupdate** de automatische updatecontrole kan worden uitgeschakeld.

Installeer de update Access Commander

WAARSCHUWING
Het wordt aanbevolen om dit te doen voordat u de update installeert systeem back-up (p. 85). Voer de backup buiten kantooruren uit om tijdelijke onbeschikbaarheid van het systeem voor gebruikers te voorkomen.

1. Ga naar **Instellingen > tabblad Systeemupdate**.
2. Als de automatische updatecontrole is uitgeschakeld, klikt u op Controleer op updates.
3. Klik op Downloaden in het beschikbare update-informatiebericht en bevestig de download.
   Het tabblad geeft aan dat de update gereed is om te installeren.
4. Klik op Installeren Bevestig de installatie in het informatiebericht en in het geopende dialoogvenster.
   Na het starten van de installatie wordt u doorgestuurd naar de onderhoudspagina. De onderhoudspagina informeert de beheerder die de installatie heeft gestart over de huidige status van de installatie. Geeft informatie aan andere gebruikers weer dat er een update gaande is. Tijdens de installatie is dit niet mogelijk**Access Commander**aanmelden.
5. Nadat de installatie is voltooid, klikt u op Ga naar inloggen, die u doorverwijst naar de inlogpagina.

Downgrade

Terugkeren naar de vorige firmwareversie is niet mogelijk.

Beta testen

Gebruikers kunnen ervoor kiezen om deel te nemen aan bètatests van software-updates **Access Commander** vóór de officiële release van updates. De autorisatie wordt uitgevoerd in **Instellingen > tabblad Systeemupdate > parameter Updateserver**.

WAARSCHUWING
De proefversie is niet gegarandeerd en het bedrijf biedt deze niet aan 2N TELEKOMUNIKACE als is niet verantwoordelijk voor functionele beperkingen en mogelijke schade die ontstaat als gevolg van functionele beperkingen van de bètaversie. Bètaversies zijn uitsluitend bedoeld voor testdoeleinden. De bètaversie is niet bedoeld voor het werken met belangrijke gegevens.

Eenmaal ingeschakeld, verschijnen bètaversies in de beschikbare updates op het tabblad Systeemupdates.

WAARSCHUWING
Na de update **Access Commander** de nieuwste bètaversie kan niet worden gedowngraded naar een eerdere versie.

Systeemback-up

In het tabblad **Instellingen > Systeemback-up** kunt u de back-up en het herstel van **Access Commander**-gegevens uitvoeren, instellen en beheren. Gegevens kunnen worden opgeslagen op lokale opslag of op een Server Message Block (SMB). SMB is geschikt voor langdurige back-upopslag.

Er kan eenmalig of automatisch een back-up van gegevens worden gemaakt met regelmatige, vooraf ingestelde intervallen.

Elke back-up kan worden hersteld, gedownload of verwijderd in het menu dat wordt uitgevouwen nadat u op hebt geklikt ⋮ voor een item in de back-uplijst.

Eenmalige gegevensback-up

1. Ga naar **Instellingen > tabblad Systeemback-up**.
2. Klik onderaan het tabblad op Nu backuppen.
3. Selecteer of u de bestandsgegevens wilt coderen. Vul dan het wachtwoord in dat nodig is om de back-up te herstellen.

Instellingen voor automatische gegevensback-up

1. Ga naar **Instellingen > tabblad Systeemback-up**.
2. Klik op ✎ bij de parameter Regelmatige back-up.
3. Stel de vereiste back-upparameters in:
   - frequentie – het interval dat specificeert hoe vaak de back-up wordt uitgevoerd
   - tijdstip – de back-up wordt op dit tijdstip op de betreffende dag gemaakt
   - dag – dag van de week of maand waarin de back-up wordt uitgevoerd
4. Selecteer of u de bestandsgegevens wilt coderen. Vul dan het wachtwoord in dat nodig is om de back-up te herstellen.

5. Door op te slaan worden de back-ups automatisch uitgevoerd volgens de geselecteerde instellingen.

Instellingen voor gegevensback-up op SMB

1. Ga naar **Instellingen > tabblad Systeemback-up**.
2. Klik op bij de parameter Opslag.
3. Selecteer opslagtype: SMB.
4. Vul het serveradres, de inloggegevens en de protocolversie in.
5. Door op te slaan worden alle back-ups naar het ingestelde Server Message Block verzonden.

Herstellen vanaf back-upgegevens

1. Ga naar **Instellingen > tabblad Systeemback-up**.
2. Open het uitgebreide menu bij de geselecteerde back-up en selecteer Herstellen.

Herstellen vanaf een back-upbestand

1. Ga naar **Instellingen > tabblad Systeemback-up**.
2. Klik onderaan het tabblad op Herstellen vanuit bestand.
3. Selecteer het back-upbestand uit uw opslag en klik op Herstellen.

Gegevens van een ander overbrengen Access Commander

1. Ga naar **Instellingen > tabblad Systeemback-up**.
2. Klik onderaan het tabblad op Migreren.
3. Voer het IP-adres in van de Access Commander waarvan u de gegevens wilt overbrengen.
4. Vul de gegevens in van het Access Commander-beheerdersaccount waarvan u de gegevens wilt overbrengen.

LET OP
Om gegevens van een andere Access Commander te importeren, moet de SSH-service zijn ingeschakeld op de server waarvan de gegevens worden gedownload.

Synchronisatie van gebruikers

De lijst met gebruikers en hun basisinstellingen, inclusief toewijzingen aan bedrijven en groepen, kan worden gesynchroniseerd met behulp van een extern onderhouden CSV-bestand.

Synchronisatie gebeurt in **Instellingen > tabblad Gebruikerssynchronisatie**. Je kunt een voorbeeld CSV-bestand downloaden van het tabblad (in het uitgebreide menu)

TIP
De lijst met huidige gebruikers, die overeenkomt met de structuur van het voorbeeld-CSV-bestand, kan van de pagina worden gedownload Rapporten (p. 78).

Het voorbereide CSV-bestand kan direct op de kaart worden geïmporteerd. Gegevens uit het bestand met s **Access Commander** ze zullen automatisch beginnen met synchroniseren.

Gedetailleerde informatie over het resultaat van elke synchronisatie wordt opgeslagen in het systeemlogboek. Het logboek zelf bevat basisinformatie over het slagen of mislukken van de synchronisatie. Gedetailleerde informatie wordt opgeslagen in een bestand dat kan worden gedownload via het pictogram aan het einde van de regel.

Automatische synchronisatie van gebruikers met FTP

Op het tabblad Gebruikerssynchronisatie in Instellingen kunt u koppelen **Access Commander** met de FTP-opslag waar het CSV-bestand met de lijst met gebruikers zich bevindt. Op het tabblad wordt vervolgens informatie over deze FTP-opslag weergegeven.

1. Ga naar **Instellingen > Gebruikerssynchronisatie**.
2. Klik op in de parameter Opslag.
3. Stel in het geopende dialoogvenster het adres in van de FTP-server waarop het CSV-bestand is opgeslagen.
4. Als u TLS inschakelt, wordt Transport Layer Security (TLS) ingeschakeld voor uw FTP-verbinding. TLS versleutelt de gegevens die worden verzonden tussen de **Access Commander** en de server.
   Schakel TLS-certificaatverificatie in om TLS-verificatie van door de server geleverde certificaten in te schakelen. Als dit is ingeschakeld, controleert **Access Commander** of er wordt gecommuniceerd met een vertrouwde server, wat de beveiliging van de verbinding verhoogt.

   LET OP
   Proxy voor FTP met TLS-authenticatie wordt niet ondersteund.
5. Voer de inloggegevens in voor toegang tot de FTP-server.

CSV-bestand

OPMERKING
Sommige spreadsheetprogramma's gebruiken andere scheidingstekens en het CSV-bestand wordt mogelijk niet correct weergegeven wanneer het daarin wordt geopend. In dergelijke gevallen wordt aanbevolen om de gegevens uit het CSV-bestand in een geopende werkmap te importeren.

Een CSV-bestand heeft een bepaalde structuur die moet worden gevolgd. Alle waarden worden gescheiden door een komma, alleen de lijst met groepen wordt gescheiden door een puntkomma. Het CSV-bestand heeft de volgende structuur:

- WerknemerID – primaire sleutel die moet worden ingevuld. Dit is een unieke gebruikersidentificatie.
- Gebruikersnaam – de naam van de gebruiker die is aangemaakt in Access Commander.
- Bedrijf – de naam van het bedrijf waaronder de gebruiker zal worden opgericht. Het bedrijf moet zijn aangemaakt in Access Commander. Kleine letters en hoofdletters die in bedrijfs- of groepsnamen worden gebruikt, zijn niet uitwisselbaar.
- Gebruikersmail – het e-mailadres van de gebruiker.
- Kaartnummers – het kaartnummer van de gebruiker. Er kunnen maximaal twee kaarten voor één gebruiker worden ingesteld. De nummers van individuele kaarten moeten worden gescheiden door een puntkomma (;).
- Schakelcode - een schakelcode, er wordt altijd een code aangemaakt onder de eerste schakelaar.
- Telefoonnummer 1 – telefoonnummer op de eerste positie.

- Groepsoproep – groepsoproep naar het hierboven ingestelde telefoonnummer. Neemt de waarden True/ False aan. Indien ingesteld op True, worden groepsoproepen geactiveerd. Indien ingesteld op False, zijn groepsoproepen uitgeschakeld.
- Telefoonnummer 2 – telefoonnummer op de tweede positie.
- Groepsoproep – groepsoproep naar het hierboven ingestelde telefoonnummer. Neemt de waarden True/ False aan. Indien ingesteld op True, worden groepsoproepen geactiveerd. Indien ingesteld op False, zijn groepsoproepen uitgeschakeld.
- Telefoonnummer 3 – telefoonnummer op de derde positie.
- Virtueel nummer – het virtuele nummer van de gebruiker.
- Groepen - lijst met groepen waaraan de gebruiker moet worden toegevoegd. Alle groepen moeten zijn opgericht inAccess Commander. De lijst met groepen wordt gescheiden door een puntkomma. Kleine letters en hoofdletters die in bedrijfs- of groepsnamen worden gebruikt, zijn niet uitwisselbaar.
- Is verwijderd – markeer of de gebruiker moet worden verwijderd. Wanneer ingesteld op FALSE, wordt de gebruiker aangemaakt en worden alleen zijn gegevens bijgewerkt tijdens de volgende synchronisatie. Indien ingesteld op TRUE, wordt de gebruiker verwijderd bij de volgende synchronisatie. Indien ingesteld op FALSE, wordt de gebruiker opnieuw aangemaakt.
- Kentekenplaten - registratietekens. Het is mogelijk om meerdere kentekenplaten in te stellen, deze moeten gescheiden worden door een puntkomma.

Datum en tijd

De wijziging in de manier van tijdwinst wordt doorgevoerd in **Instellingen > Configuratie > tabblad Datum en tijd**.

Datum en tijd in **Toegangscommandant** kan worden gesynchroniseerd met het internet of handmatig worden ingesteld. In het geval dat dit niet het geval is **Toegangscommandant** verbonden met het internet, moet u de datum, tijd en tijdzone handmatig instellen. Anders is het mogelijk om over te schakelen naar NTP en tijd van de NTP-server te krijgen. In dit geval hoeft u alleen de tijdzone in te stellen. De NTP-server werkt de datum en tijd automatisch

LET OP
Na het opslaan van de tijd verandert u se **Access Commander** wordt automatisch opnieuw opgestart.

Tijdsynchronisatie met apparaten

De tijd op de aangesloten apparaten kan worden gesynchroniseerd met de tijd op de **Access Commander**. Tijd delen met apparaten wordt geactiveerd door de parameter Apparaat synchronisatie aan te zetten in **Instellingen > Configuratie > Tabblad Datum & Tijd**.

Als tijdsynchronisatie met het apparaat is ingeschakeld, is het mogelijk om uit de volgende synchronisatie-methoden te kiezen:

- **De apparaten gebruiken dezelfde NTP-server** – de tijd op de apparaten wordt bepaald door de ingestelde NTP-server **Access Commander**.

TIP
De tijd van de NTP-server zorgt voor de beste tijdnauwkeurigheid op het apparaat.

- **De apparaten gebruiken Access Commander als NTP-server** – regelt de tijd op de apparaten volgens de ingestelde tijd**Access Commander**.

Automatisering

De automatiseringsfunctie is beschikbaar in **2N Access Commander** vanaf firmwareversie 3.2 onder de licenties Advanced, Pro en Unlimited. Deze toevoeging is gebouwd op het Node-RED platform en biedt **Access Commander** direct uitgebreide flow-gebaseerde programmeermogelijkheden. Hiermee kunnen gebruikers **Access Commander** verbinden met verschillende systemen van derden en aangepaste workflows automatiseren op basis van gebeurtenissen binnen het platform.

LET OP

Om deze veelzijdige automatiseringstool optimaal te benutten, moet u rekening houden met het volgende:

- **Klantverantwoordelijkheid voor beveiliging**: Gebruikers zijn verantwoordelijk voor het verzekeren dat hun Automation-configuraties en workflows veilig zijn en in lijn met de best practices voor cybersecurity. Dit omvat het beveiligen van de Node-RED-omgeving, het op de juiste manier beheren van machtigingen en het beschermen van gevoelige gegevens binnen hun automations.
- **Gebruik van het REST API-knooppunt**: Als dit knooppunt niet goed wordt gebruikt, kan dit leiden tot gegevensverlies of onbedoelde wijzigingen. Het is de verantwoordelijkheid van de gebruiker om ervoor te zorgen dat het knooppunt correct is geconfigureerd en geïmplementeerd. Wees voorzichtig en controleer uw instellingen nogmaals om mogelijke risico's voor uw gegevens te voorkomen.
- **Nodes en add-ons van derden**: 2N Telekomunikace is niet verantwoordelijk voor het gebruik of de integratie van externe nodes, add-ons of aangepaste wijzigingen aan Node-RED binnen de Automation-functie. Klanten moeten de beveiliging en stabiliteit van alle extra componenten die ze installeren zorgvuldig evalueren en garanderen. Problemen die voortvloeien uit externe extensies moeten worden opgelost door de klant of de betreffende externe provider.
- **Beperkingen van technische ondersteuning**: Hoewel ons supportteam u zal helpen met problemen met betrekking tot de basisfunctionaliteit van de Automation-functie binnen 2N Access Commander, inclusief onze aangepaste Access Commander-knooppunten, kunnen ze geen assistentie verlenen bij het ontwerp, de ontwikkeling of debugging van aangepaste Node-RED-stromen. Gebruikers die complexe automatiseringen willen maken, moeten mogelijk aanvullende ondersteuning zoeken bij gekwalificeerde Node-RED-experts of beschikbare bronnen raadplegen.

Om aan de slag te gaan met Node-RED is het raadzaam om de beschikbare online bronnen, zoals gedetailleerde handleidingen en talloze YouTube-tutorials over Node-RED, die begeleiding bieden bij het maken en beheren van de stromen.

Raadpleeg deze handleiding voor meer informatie over aangepaste **Access Commander**-knooppunten en het gebruik van de automatiseringsfunctie binnen **Access Commander**.

Deze functie vergroot de mogelijkheden van **Access Commander**. Het wordt aanbevolen om de mogelijkheden te verkennen en tegelijkertijd de veiligheid van configuraties te waarborgen.

Automatiseringen creëren

Geautomatiseerde taken worden aangemaakt in een externe editor. De editor is toegankelijk via een tabblad op de pagina **Instellingen > Configuratie > tabblad Automatisering**. Wijzigingen die in de editor worden aangebracht, worden pas van kracht nadat ze op de server zijn geïmplementeerd, wat met een knop gebeurt Deploy in de rechterbovenhoek van de editor.

Het creëren van geautomatiseerde taken is gebaseerd op het samenstellen van stromen. Stromen worden getrokken uit individuele knooppunten die met elkaar zijn verbonden. In het linkerpaneel wordt een menu

met knooppunten weergegeven. In het linkerpaneel is het mogelijk om knooppunten op naam te zoeken. Een nieuw knooppunt kan ook worden toegevoegd na het maken van een nieuwe verbinding vanuit een bestaand knooppunt.

De gegevens die tussen knooppunten worden doorgegeven, worden berichten genoemd. Hun beschrijving en het werken met hen is gedetailleerd hier. Deze stand beschrijft ook de basisknooppunten (nodes) die het formaat van individuele berichten of hun reeksen verwerken, zoals de knooppunten Change, Split, Join,... Automatisering kan niet alleen werken met de gegevens verkregen in deze unieke taak (msg.), maar kan ook werken met dynamische waarden in de context van de gehele stroomgeschiedenis (flow.) of zelfs alle stromen in de installatie (global.).

LET OP
Knop Deploy stuurt de ingestelde streams naar de server. Alleen door verzending naar de server worden de nieuwe streams van kracht!

Veilige modus (safe mode)

Veilige modus is een belangrijk hulpmiddel voor het oplossen van automatiseringsproblemen. Als u de editor in de veilige modus uitvoert, kunt u wijzigingen aanbrengen in streams zonder dat deze streams op de achtergrond worden uitgevoerd. Dit betekent dat u naar de editor kunt gaan, kunt bewerken wat u nodig hebt en de wijzigingen vervolgens opnieuw kunt implementeren met een knop Deploy. Deze modus is vooral handig als een van de stromen ervoor zorgt dat Node-RED niet goed functioneert of crasht, bijvoorbeeld als gevolg van een fout in de stroom of een knooppunt van een derde partij, of als de stroom onmiddellijk moet worden gestopt.

Knooppunten (nodes) Access Commander

REST API

De REST API-node stuurt een gedefinieerd HTTP API-verzoek. De invoergegevens in de **body**-eigenschap worden gebruikt als de verzoekpunten van deze toepassing. De uitvoer van het knooppunt zijn de respons-gegevens op het verzoek. De selectie en volgorde van de uitvoergegevens kan worden gespecificeerd in de parameter **Query**.

Knooppuntparameters

- **Method** – biedt een keuze aan API-aanvraagmethoden
- **Endpoint** – wordt gebruikt om het volledige eindpunt te specificeren waarnaar het verzoek zal worden geleid. Het pad van het eindpunt kan worden aangevuld met de parameter points.
  Het werken met HTTP-verzoeken wordt beschreven in HTTP-API (p. 111).
- **Query** – wordt gebruikt om te specificeren welke gegevensparameters moeten worden geadresseerd in het eindpunt en hoe ze moeten worden geretourneerd in de uitvoer. Deze parameter kan worden gespecificeerd door een invoerwaarde, de **query** eigenschap. Een beschrijving van hoe **query** opgebouwd moet worden staat beschreven in het Data Query Customization document (alleen in het Engels).
- **Only send non-2xx responses to Catch node** – Deze optie beïnvloedt welke HTTP-responsen worden vastgelegd in het Catch knooppunt.
- **Name** – Hiermee kun je de naam van het knooppunt wijzigen voor betere oriëntatie bij het werken met de stroom.

Access log

Het knooppunt laadt de vermeldingen in het toegangslogboek en maakt verdere verwerking van deze vermeldingen mogelijk.

De beheerder kan automatische taken instellen die worden uitgevoerd wanneer **Access Commander** een gedefinieerde logboekvermelding ziet. De actie wordt gedefinieerd in de knooppuntinstellingen. De uitvoer zijn

specifieke gegevens over de gelogde gebeurtenis. Een SignalR-gebaseerde functie draait op de achtergrond van deze functie.

Knooppuntparameters

- **Filter** – wordt gebruikt om aan te geven welke records het knooppunt moet verwerken. Records die niet overeenkomen met dit filter worden genegeerd door de flow. Het formaat van het filter is JSON object. Deze parameter kan worden overschreven door de invoerwaarde.
- **Name** – Hiermee kun je de naam van het knooppunt wijzigen voor betere oriëntatie bij het werken met de stroom.

System Log

Het knooppunt laadt de records in het systeemlogboek en zorgt ervoor dat deze records verder kunnen worden verwerkt.

De beheerder kan automatische taken instellen die worden uitgevoerd wanneer **Access Commander** een gedefinieerde logboekvermelding ziet. De actie wordt gedefinieerd in de knooppuntinstellingen. De uitvoer zijn specifieke gegevens over de gelogde gebeurtenis. Een SignalR-gebaseerde functie draait op de achtergrond van deze functie.

Knooppuntparameters

- **Filter** – wordt gebruikt om aan te geven welke records het knooppunt moet verwerken. Records die niet overeenkomen met dit filter worden genegeerd door de flow. Het formaat van het filter is JSON object. Deze parameter kan worden overschreven door de invoerwaarde.
- **Name** – Hiermee kun je de naam van het knooppunt wijzigen voor betere oriëntatie bij het werken met de stroom.

SignalR

Het SignalR-knooppunt leest de gegevens in het geabonneerde onderwerp. Het knooppunt haalt gegevens in realtime op, dus het is geschikt voor scenario's waarin het een geautomatiseerde taak heeft om informatie op te halen uit Access Commander zonder de noodzaak van constante polling.

Knooppuntparameters

- **Topic** – biedt beschikbare onderwerpen voor inschrijving.
- **Filter** – wordt gebruikt om aan te geven welke records het knooppunt moet verwerken. Records die niet overeenkomen met dit filter worden genegeerd door de flow. Het formaat van het filter is JSON object. Deze parameter kan worden overschreven door de invoerwaarde.
- **Name** – Hiermee kun je de naam van het knooppunt wijzigen voor betere oriëntatie bij het werken met de stroom.

Meer informatie over de SignalR-functionaliteit vindt u in het hoofdstukSignalR (p. 111).

Dynamic SignalR

Het knooppunt Dynamic SignalR versus het knooppunt Signal* maakt dynamische wijzigingen in de gegevensbemonstering mogelijk. Dit kan inhouden dat het onderwerp of de samplingmethode wordt gewijzigd op basis van de invoerwaarden. De outputwaarden van het knooppunt zijn zowel de gegevens die worden opgehaald uit het onderwerp (Data) als informatie over het succes of falen van de actie van het knooppunt.

Knooppuntparameters

- **Topic** – definieert het onderwerp waarvoor de wijziging voor het ophalen van gegevens moet plaatsvinden.
- **Filter** – wordt gebruikt om aan te geven welke records het knooppunt moet verwerken. Records die niet overeenkomen met dit filter worden genegeerd door de flow. Het formaat van het filter is JSON object. Deze parameter kan worden overschreven door de invoerwaarde.
- **Records** – Bepaalt het aantal records dat moet worden gelezen als het type fetch read wordt gebruikt.

- **Fetch When Ready** – stelt in of de waarden moeten worden teruggelezen wanneer het fetch-commando wordt geactiveerd.
- **Name** – Hiermee kun je de naam van het knooppunt wijzigen voor betere oriëntatie bij het werken met de stroom.

Geldige invoerwaarden

Het knooppunt accepteert de volgende eigenschappen als invoerwaarden. Geldige invoerwaarden overschrijven tijdelijk de parameters die zijn ingesteld in de knooppuntconfiguratie.

- **topic** – een tekenreeks die het te selecteren onderwerp specificeert.
- **filter** – in JSON-formaat, die de op te halen records specificeert.
- **fetchWhenReady** – bootlean die de parameter van het knooppunt Fetch When Ready specificeert.
- **action** – een tekenreeks die de uit te voeren actie specificeert. Dit kan inschrijven, uitschrijven zijn...
- **update** – kan een tijdstempel (string) en een timeWindow (object) bevatten die aangeeft wanneer de uit te voeren actie is gewijzigd.

Meer informatie over de functionaliteit van SignalR vindt u in het hoofdstukSignalR (p. 111).

Write system log

Het knooppunt *Write system log maakt een Access Commander systeemlogboekvermelding. Het logboekitem bevat de opgegeven ernst, een beschrijving van de gebeurtenis en andere details. Als er tijdens het proces een fout optreedt, wordt deze gelogd en wordt de status van het knooppunt overeenkomstig bijgewerkt. Het knooppunt heeft geen uitvoerwaarden.

Knooppuntparameters

- **Severity** – bepaalt de ernst van het record. Deze parameter kan worden gespecificeerd door de query invoerwaarde.
- **Filter** – wordt gebruikt om aan te geven welke records het knooppunt moet verwerken. Records die niet overeenkomen met dit filter worden genegeerd door de flow. Het formaat van het filter is JSON object. Deze parameter kan worden overschreven door de invoerwaarde.
- **Detail** – wordt gebruikt voor een meer gedetailleerde beschrijving van het record, die wordt weergegeven in het systeemlogboek. Deze parameter kan overschreven worden door een invoerwaarde.
- **Name** – Hiermee kun je de naam van het knooppunt wijzigen voor betere oriëntatie bij het werken met de stroom.

Geldige invoerwaarden

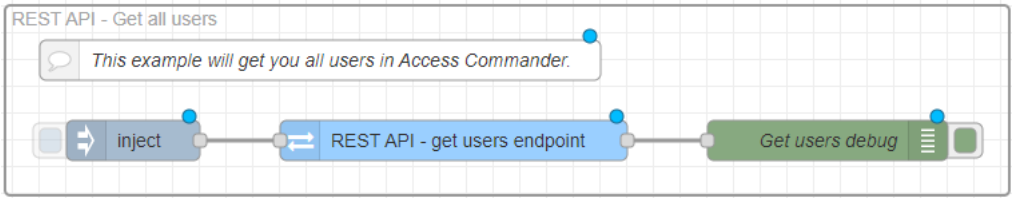
Het knooppunt accepteert de volgende eigenschappen als invoerwaarden. Geldige invoerwaarden overschrijven tijdelijk de parameters die zijn ingesteld in de knooppuntconfiguratie.

- **severity** – een tekenreeks die de ernst van de record aangeeft.
- **event** – een korte beschrijving van de opgenomen actie.
- **detail** – tekenreeks die de gedetailleerde beschrijving van het record invult die zal worden weergegeven in het systeemlogboek.

Voorbeelden van stromen (flows)

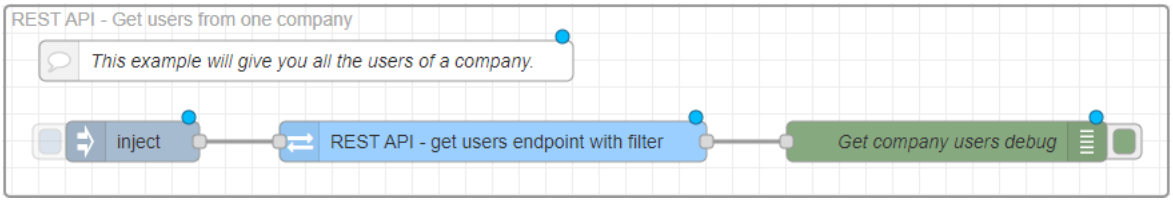
Access Commander biedt verschillende geautomatiseerde basistaken die de mogelijkheden van automatisering weergeven. De flows van deze taken kunnen worden geïnstalleerd wanneer je de automatiseringsfunctie voor het eerst start in **Access Commander**, maar kunnen ook later worden geïmporteerd, zie Streams exporteren/importeren (p. 94). Deze voorgedefinieerde flows kunnen eenvoudig worden aangepast voor uw eigen doeleinden.

Get all users



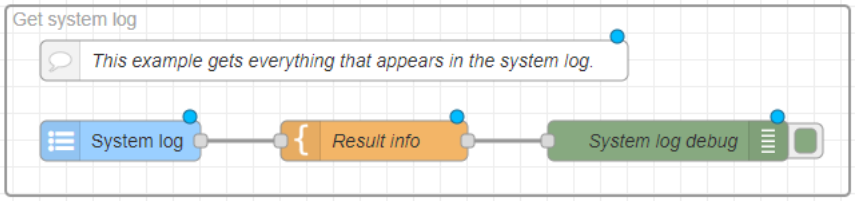
Deze flow genereert een lijst van alle gebruikers, inclusief hun informatie. De taak wordt gestart door het knooppunt Inject te activeren. Er kan een filter worden toegepast op het **REST API - get users endpoint** knooppunt om aan te geven welke gebruikers het proces moet retourneren. Op deze manier kan de uitvoer van het proces worden aangepast aan de behoeften van de beheerder.

Get users from one company



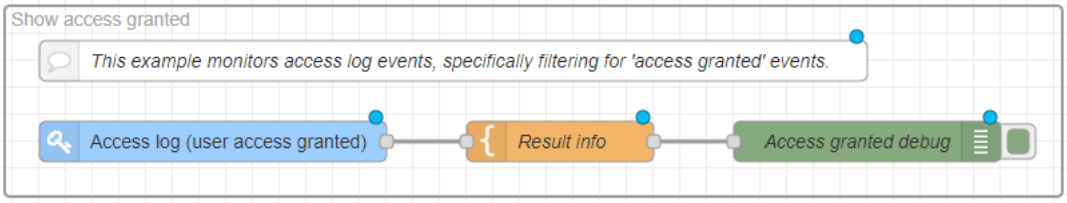
Deze flow genereert een lijst van alle gebruikers binnen één bedrijf, inclusief informatie over hen. De taak wordt gestart door het knooppunt Inject te activeren. De bedrijfsselectie wordt ingesteld in het **REST API – get users endpoint with fillter** met fillter door zijn id op te geven.

Get system log



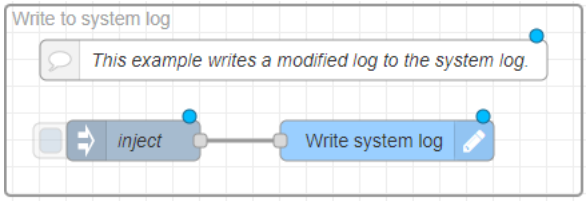
Deze stroom leest alle nieuwe items in het systeemlogboek. Je kunt de selectie van gebeurtenissen verfijnen door een filter op te geven in het knooppunt **System log**.

Show access granted



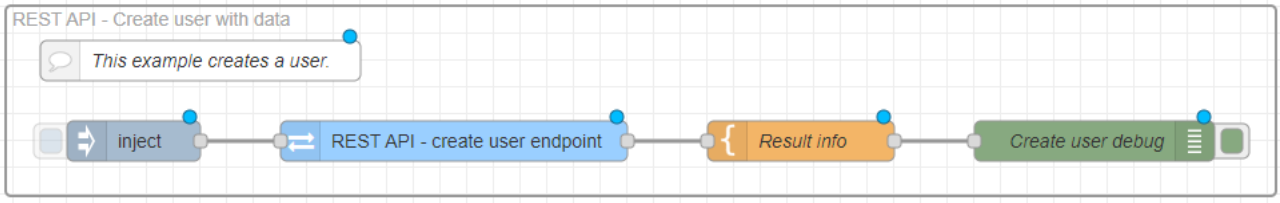
Met deze stroom worden alle nieuwe vermeldingen in het toegangslogboek opgehaald. De stream is zo ingesteld dat alleen toegang wordt geladen als deze is verleend. In het knooppunt **Access Log** Het is mogelijk om deze beperking te wijzigen.

Write to system log



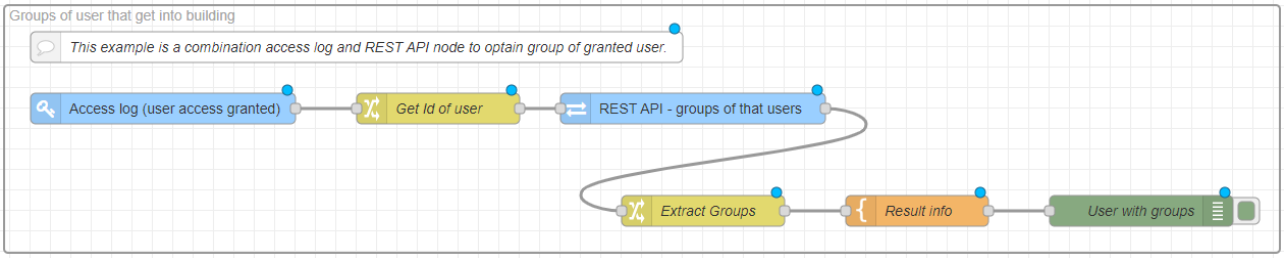
Deze stroom creëert een entry in het systeemlogboek. Het knooppunt **Write system log** kan gebruikt worden om de ernst, naam en gedetailleerde beschrijving van de entry in te stellen.

Create user with data



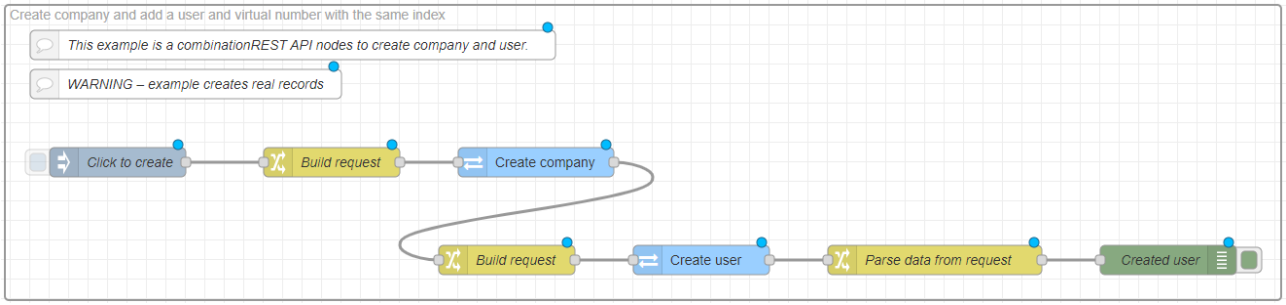
Deze flow wordt gebruikt om een nieuwe gebruiker aan te maken. De taak wordt gestart door het knooppunt **Inject** te activeren. Het **Inject** knooppunt bevat een message body die de naam van de gebruiker Joe Doe specificeert en zijn toewijzing aan het bedrijf met ID 1. Deze body wordt toegepast in het **Rest API - create user endpoint** knooppunt en de gebruiker wordt op basis hiervan aangemaakt. Het knooppunt **Result info** stelt de berichttekst in die wordt weergegeven in Debug-berichten.

Groups of users that get into building



Deze flow haalt de gebruikersgroepen op die toegang hebben gekregen. Toegestane toegangen worden opgehaald uit het toegangslogboek. De flow haalt dan het ID op van de gebruiker aan wie toegang is verleend en gebruikt het **REST API - groups of that users** knooppunt om informatie over die gebruiker op te halen. Het **Extrack Groups** knooppunt haalt de groepsnamen van die gebruiker op en het **Result info**knooppunt stelt de tekst van het uiteindelijke bericht samen.

Create company and add a user and virtual number with the same index



Deze stroom creëert een nieuw bedrijf, de eerste gebruiker in dat bedrijf en zijn virtuele nummer. De taak wordt gestart door het knooppunt **Inject** te activeren. Bij de initialisatie wordt een willekeurig geheel getal gegenereerd dat wordt gebruikt in de bedrijfsnaam, de naam van de gebruiker en dat zal dienen als het virtuele nummer van de gebruiker. Het knooppunt **Create company** creëert een bedrijf met de gedefinieerde naam. Het antwoord van dit knooppunt levert het bedrijfs-ID op, op basis waarvan het volgende knooppunt **Create user** een nieuwe gebruiker in dit bedrijf aanmaakt en er tegelijkertijd een virtueel nummer aan toekent. Het knooppunt **Parse data from request** haalt dan de bedrijfsnaam, de gebruikersnaam en het virtuele nummer van de gebruiker op.

Streams exporteren/importeren

Flows kunnen worden geëxporteerd naar .json-bestanden en later opnieuw worden geïmporteerd in de automatiseringsinterface. Zowel exporteren als importeren gaat via het uitgebreide menu in de rechterboven-

hoek. Flows die van de ene **Access Commander**-installatie naar de andere worden verplaatst, moeten mogelijk worden bewerkt.

In de importopties staan vooraf geladen voorbeeldflows voor **Access Commander**. Deze staan op het tabblad Voorbeelden, in de map Access-Commander-nodes.

LET OP
Geavanceerde functie-instellingen die niet door de nieuwe licentie worden ondersteund, worden niet opgeslagen.

Vergeet daarom niet om uw geconfigureerde flows te exporteren wanneer u uw proeflicentie beëindigt.

Foutstatussen

Bij het werken met automatiseringen kunnen soms fouten optreden die de stabiliteit en functionaliteit beïnvloeden. Als er zich een foutconditie voordoet, zal het tabblad Automatisering in **Access Commander** u waarschuwen voor de conditie en aanbieden om het Node-RED platform opnieuw op te starten in veilige modus. In de veilige modus worden de flows tijdelijk gestopt en kunnen de flows die de fout veroorzaken veilig worden hersteld. Het herstarten van de flows wordt geactiveerd met de knop Deploy.

Er zijn twee fundamentele foutcondities:

- **Node-RED reageert niet**
  Deze toestand treedt op wanneer Node-RED niet meer reageert. Er zijn geen vaste automatiseringen actief. Dit probleem kan worden veroorzaakt door verschillende factoren, zoals overbelasting van het systeem, fouten in de stroominstellingen of conflicten tussen geïmporteerde modules van derden.
- **Knooppunt-RED is onstabiel**
  De instabiliteit van Node-RED manifesteert zich door het platform herhaaldelijk opnieuw op te starten, wat de werking van de automatisering kan verstoren en gegevensverlies kan veroorzaken. Een herhaalde herstart vindt meestal plaats als een van de stromen verkeerd is geconfigureerd en een herstart veroorzaakt. Alle streams worden opgeschort voor de duur van de herstart.

Installatienaam

De naam van de specifieke **Access Commander**-installatie wordt weergegeven in de kop van de webinterface en de naam wordt getoond aan alle aangemelde gebruikers. De standaardnaam van **Access Commander** kan worden gewijzigd, bijvoorbeeld in het adres van het gebouw dat een bepaalde installatie beheert.

Ga naar **Instellingen > Configuratie > tabblad Installatienaam** om de naam te wijzigen. Je kunt de naamsverandering gebruiken om individuele installaties te onderscheiden als één persoon meerdere installaties beheert. De installatienaam wordt ook geschreven in e-mails die naar bedrijven worden gestuurd.

De e-mailfunctie (SMTP) inschakelen en instellen

De e-mailfunctie zorgt voor het verzenden van meldingen of het verzenden van inlogwachtwoorden naar gebruikers. E-mails worden verzonden via het SMTP-protocol.

1. De instellingen worden gemaakt in **Instellingen > Configuratie > E-mail**.

2. Na het inschakelen van de e-mailfunctie wordt een dialoogvenster geopend waarin u de volgende parameters kunt instellen:
   - **SMTP-serveradres**, waarnaar e-mails worden verzonden.
   - **Server poort**, vooraf ingesteld op 25.
   - **Gebruikersnaam** En **wachtwoord** naar het account op de SMTP-server als de SMTP-server autorisatie vereist.
   - **Standaard afzenderadres**, van waaruit e-mails worden verzonden.
3. Schakel indien nodig in:
   - **SSL** voor e-mailversleuteling,
   - **SSL-servercertificaatverificatie**,
   - **Compatibiliteitsmodus** in geval van verbinding met oudere SMTP-servers die geen nieuwe functies ondersteunen (GSSAPI).
4. Na het opslaan kunt u dit instellen op het tabblad E-mail **Basisadres voor e-maillinks**, dat deel zal uitmaken van verzonden e-mailberichten en e-mailontvangers kan verwijzen naar het geselecteerde deel van de interface **Access Commander**.
5. U kunt de gemaakte instellingen controleren door een testmail te sturen.

Tweefactorauthenticatie

Tweefactorauthenticatie biedt een hoger niveau van beveiliging van gebruikersaccounts **Toegang tot commandant**. Om in te loggen voert de gebruiker logingegevens in en moet vervolgens zijn login bevestigen met behulp van de authenticatietoepassing. Zodra de beheerder de noodzaak van tweefactorauthenticatie inschakelt, wordt de gebruiker bij de volgende login gevraagd zijn account te koppelen aan zijn eigen authenticatietoepassing.

Schakel tweestapsverificatie in

Als de beheerder optionele tweestapsverificatie instelt, schakelt de gebruiker zelf tweestapsverificatie als volgt in:

1. Twee-factor-authenticatie wordt ingesteld door de beheerder op de pagina **Instellingen > Configuratie > Tabblad Twee-factor-authenticatie**.
2. De beheerder kan selecteren welke gebruikers tweefactorauthenticatie nodig hebben.

   ### Opties om tweestapsverificatie te vereisen

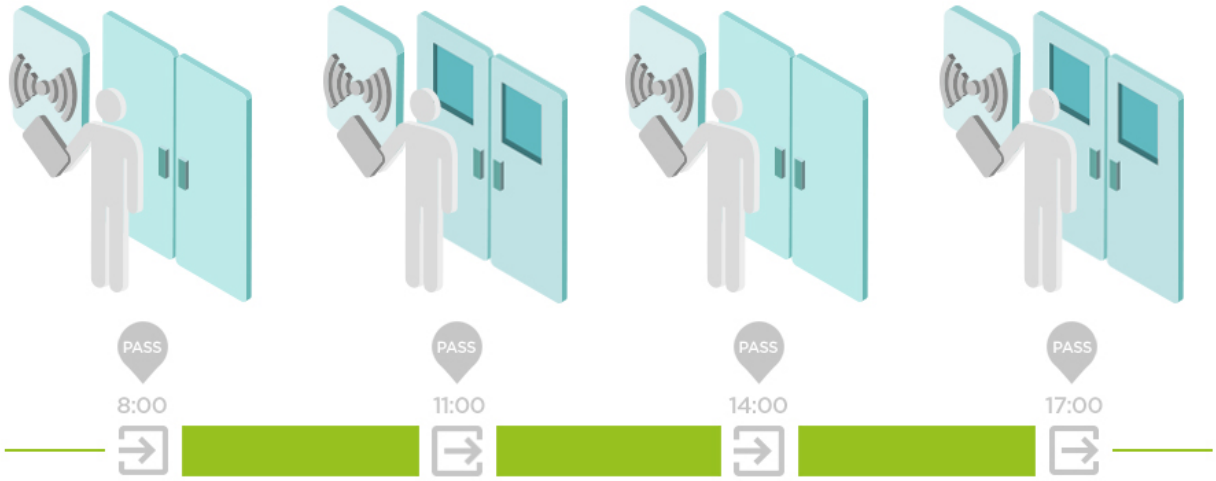
   - **Optioneel**
     Tweefactorauthenticatie is optioneel. Gebruikers kunnen het zelf inschakelen op hun profiel, zie ???.
   - **Vereist voor gebruikers met rollen**
     Elke gebruiker aan wie een rol is toegewezen, moet zijn aanmelding bevestigen met behulp van een verificatietoepassing.
   - **Verplicht**
     Alle gebruikers moeten hun aanmelding bevestigen met een verificatie-app.
3. Klik op het gebruikerspictogram in de rechterbovenhoek om het gebruikersmenu te openen.
4. Selecteer Profiel bekijken.
5. Op het tabblad Authenticatie-apps koppelt u het account aan de geselecteerde authenticatie-app. Volg de instructies **Commandant voor toegang**.

Aanwezigheidsinstellingen

Access Commander maakt het mogelijk om de aanwezigheid van gebruikers te monitoren. In de aanwezigheidsmodus worden de in- en uitlooptijden van individuele gebruikers geregistreerd.

Aanwezigheidsmodi

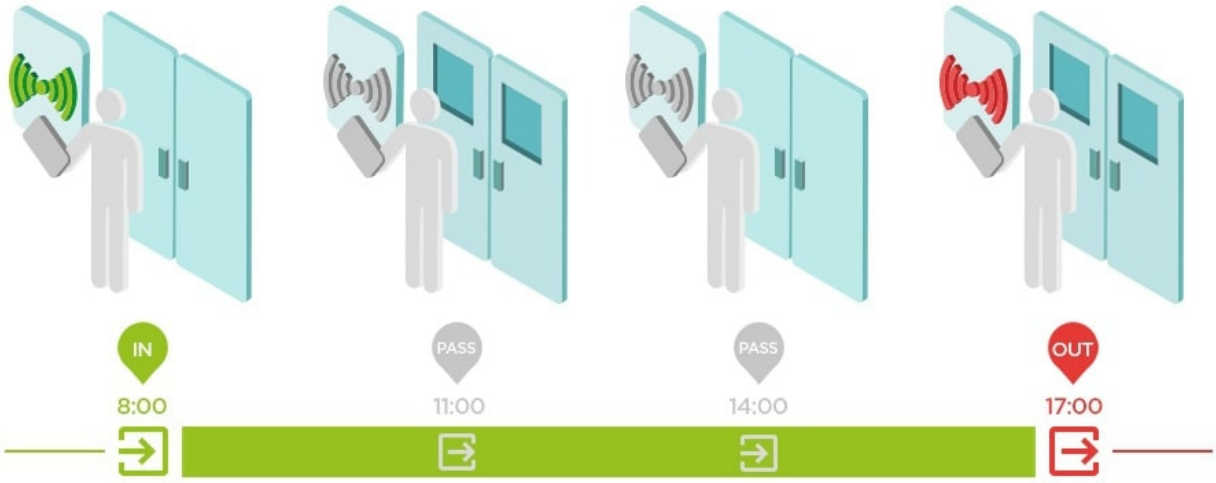
- **FREE**



Aankomst en vertrek worden geteld vanaf de eerste en laatste gebruikersauthenticatie op elk apparaat op één dag. In deze modus werkt de aanwezigheidsmodule niet.

- **IN-OUT**

Inkomende en uitgaande apparaten moeten op een goede werking worden ingesteld.



- **IN-OUT voor alle apparaten**
  Deze modus maakt aanwezigheidsbewaking mogelijk. Aankomsten worden geregistreerd op inkomende apparaten, vertrekken worden geregistreerd op uitgaande apparaten. Bewegingen tussen zones worden niet als aankomst/vertrek geregistreerd.
- **IN-OUT voor geselecteerde apparaten**
  Deze modus maakt aanwezigheidsbewaking mogelijk. Aankomst en vertrek worden geregistreerd op geselecteerde apparaten die zijn ingesteld als aankomst of vertrek. Aankomst en vertrek worden alleen op deze geselecteerde apparaten geregistreerd. Zo kan de registratie van aankomst/vertrek bijvoorbeeld alleen bij de hoofdingang van het gebouw worden ingesteld.

Instellingen voor invoer-/uitvoerapparaat

Apparaten (2N intercoms of 2N toegangseenheden) kunnen maximaal twee toegangspunten hebben. Elk toegangspunt laat doorgang in één richting toe. De toegangspunten onderscheiden de doorgangsrichting door het apparaat. Aan elk toegangspunt kunnen een of meer lezers worden toegewezen die op het apparaat zijn aangesloten en in de richting van het punt werken. Toegangspunten worden gebruikt om het binnenkomen of verlaten van een zone te registreren. Het gebruik ervan is nodig wanneer het apparaat zich op de interface tussen twee zones bevindt.

Toegangspunten worden ook gebruikt om gebruikers in de module te volgen Aanwezigheid (p. 77). Toegangspunten worden ook gebruikt om het in- en uitgaand verkeer te monitoren Gebiedsbeperkingen (p. 79).

OPMERKING

Individuele toegangspunten instellen **Toegang tot commandant** wordt voorgeschreven in de webinterface van het apparaat in de sectie Services > Toegangscontrole:

- Toegangspunt 1 = Aankomstregels
- Toegangspunt 2 = Uitgangsregels

Toegangspunten instellen

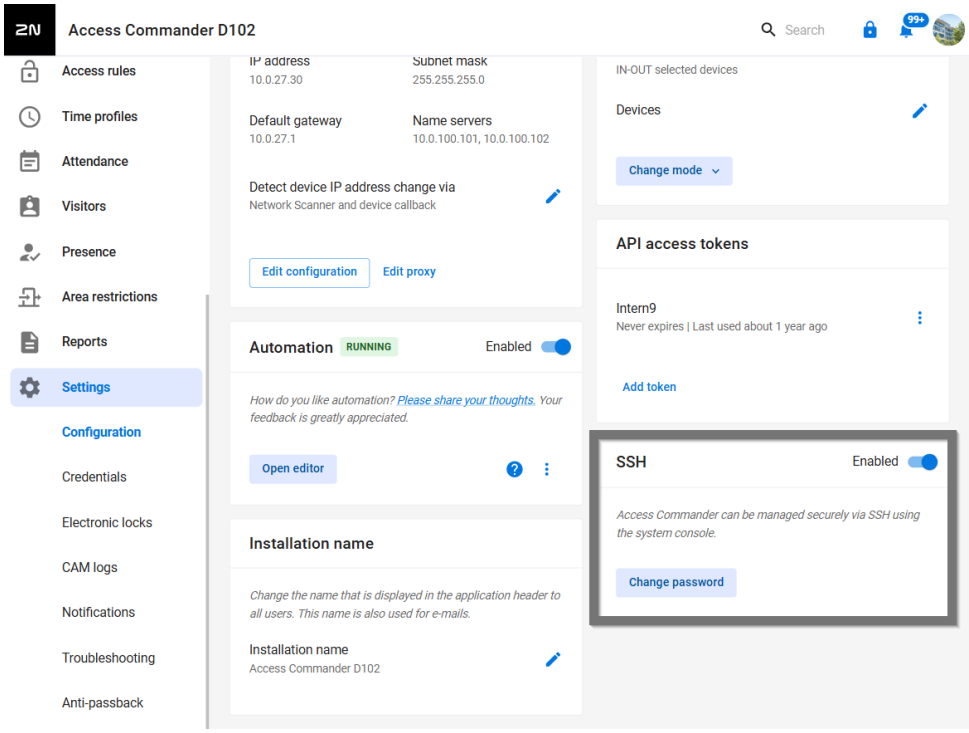
1. Voer de webconfiguratie van het apparaat in.

   TIP

   U kunt naar de webconfiguratie-interface gaan door op te klikken in de lijst op de pagina Apparaten.

2. Ga naar het menu **Hardware > Uitbreidingsmodules**.
3. Zoek de toegangsmodule die moet worden gebruikt als Toegangspunt 1 (Aankomst) of Toegangspunt 2 (Uitgaand).
4. Stel in de parameter Deur de gewenste richting in en sla de instellingen op.
5. Ga naar de Zones v-pagina **Toegang tot commandant**.
6. Druk in de rechterbovenhoek op en het gebruik van toegangspunten mogelijk maken.

Sta SSH-toegang toe



WAARSCHUWING
Het inschakelen van SSH-toegang wordt alleen aanbevolen voor gevorderde gebruikers. Onjuist gebruik is een gevaar voor de veiligheid.

Gebruik het tabblad **Instellingen > Configuratie > SSH** om Secure Shell in te schakelen, dat veilige communicatie op afstand met de systeemconsole biedt. Als u SSH inschakelt, kunt u een back-up van uw systeem maken en herstellen of **Access Commander** volledig opnieuw opstarten.

Om verbinding te maken met een Access Commander box of virtuele machine, moet de SSH-client het IP-adres van **Access Commander** en het system root-wachtwoord weten. Het systeemwachtwoord kan worden ingesteld in **Instellingen > Configuratie > tabblad SSH**.

OPMERKING
Het rootwachtwoord wordt gewijzigd in de configuratieconsole, niet in Access Commander.

SSH-toegang kan ook rechtstreeks in de Linux-configuratieconsole worden ingeschakeld en beheerd, zie Linux-instellingen (p. 83).

Encryptiesleutels voor My2N-applicatie

Gebruikers kunnen 2N gebruiken om verbinding te maken met apparaten My2N-applicatie. Communicatie tussen My2N-applicatiesen wordt altijd gecodeerd door het apparaat. Zonder kennis van de coderingssleutel kan dit niet My2N-applicatieauthenticeer de gebruiker. De primaire coderingssleutel wordt automatisch gegenereerd wanneer de intercom voor het eerst wordt gestart en kan op elk gewenst moment later handmatig opnieuw worden gegenereerd. De primaire coderingssleutel wordt tijdens het koppelen samen met de verificatie-ID naar het mobiele apparaat overgedragen.

Nieuwe sleutels aanmaken

1. Ga naar **Instellingen > Authenticatie > Coderingssleutels voor My2N**.
   kunnen maximaal 4 coderingssleutels worden gegenereerd. Wanneer u probeert de vijfde sleutel te genereren, **Toegangscommandant** zal u waarschuwen dat de oudste sleutel wordt verwijderd. De kaart toont de generatietijd voor elke sleutel.
2. Klik Genereer een nieuwe sleutel.
3. De gegenereerde sleutel wordt automatisch geüpload naar Mijn 2N bij het eerste gebruik van de mobiele telefoon met het eerder gekoppelde apparaat.

De gegenereerde sleutel kan worden verwijderd door te klikken op .

OPMERKING

- Als hij dat niet heeft My2N-applicatie toegang heeft tot een van de geldige encryptiesleutels, zal het niet mogelijk zijn deze te gebruiken om de gebruiker te authenticeren. Om de functionaliteit van de applicatie te herstellen, is het noodzakelijk om de applicatie opnieuw te koppelen met het apparaat waarmee verbinding is gemaakt **Toegang tot commandant**, waarmee geldige encryptiesleutels worden geüpload My2N-applicatie.
- Het verlenen van toegang tot het apparaat is afhankelijk van de door de gebruiker ingestelde toegangsrechten.

Compatibiliteitsmodus voor RFID-kaarten

Als **Access Commander** meldt dat de gloednieuwe kaart die zojuist is toegevoegd al in gebruik is in het systeem, kan de reden zijn dat de compatibiliteitsmodus voor RFID-kaarten is ingeschakeld. Deze modus wordt door de beheerder ingeschakeld in **Instellingen > Authenticatie > tabblad Instellingen compatibiliteitsmodus**. De compatibiliteitsmodus kan voor elk apparaat afzonderlijk worden geactiveerd in de webconfiguratie-interface van het apparaat in het **menu Services > Toegangsbeheer > tabblad Geavanceerd > Overige instellingen**.

LET OP

- Compatibiliteitsmodus mag alleen worden geactiveerd als er problemen zijn met het laden van eerder geregistreerde kaarten. Het gebruik van de compatibiliteitsmodus kan invloed hebben op authenticatiemechanismen
- De compatibiliteitsmodus is niet aan te raden om te combineren met het gebruik van kaarten die zijn beveiligd met PiCard-technologieën.

PICard-sleutels

In **Instellingen > Toegang > tabblad PICard-sleutels** worden de coderingssleutels van de 2N PICard Commander toepassing opgeslagen. Als de coderingssleutels in **Access Commander** zijn geladen, geeft het tabblad de naam van het PICard Commander project en de numerieke sleutel export identificatiecode weer. Op het tabblad kunt u de geüploade sleutels uit **Access Commander** verwijderen.

LET OP

Als u de PICard-sleutels verwijdert, werken alle kaarten die met deze sleutels zijn gecodeerd niet meer.

Importeer PICard-coderingssleutels

1. Ga naar **Instellingen > Toegang > PiCard-toetsen**.
2. Na het klikken op Importeren upload het coderingssleutelbestand vanuit uw repository.
3. Voer een wachtwoord in om het bestand te beschermen als u er een instelt bij het exporteren vanuit de applicatie PICard Commander.

2N PICard Commander is een softwareapplicatie voor het coderen van inloggegevens op toegangskaarten. De applicatie maakt projecten die een set coderings- en leessleutels genereren. Projectlezersleutels kunnen worden geïmporteerd in 2N-apparaten of in Access Commander, die vervolgens zorgt voor de distributie van leessleutels naar de aangesloten 2N-apparaten.

USB-lezers ingeschakeld

Om de registratie van sommige gebruikersverificatiemethoden te vergemakkelijken, kunt u USB-lezers gebruiken die zijn aangesloten op de computer waarop **Access Commander** wordt geopend. Lezers moeten zijn ingeschakeld in **Access Commander** onder **Instellingen > Toegang > Tabblad Toegestane USB-lezers**.

1. Ga naar **Instellingen > Toegang > Ingeschakelde USB-lezers.**
2. Klik Lezers inschakelen om een dialoogvenster te openen.
3. Activeer/deactiveer het gebruik van een extern USB-apparaat in het dialoogvenster dat wordt geopend.
4. Klik vervolgens op Verandering om de lezer aan te passen en in te schakelen.

Access Commander maakt het gebruik van de volgende USB-apparaten mogelijk:

- 125 kHz RFID-kaartlezer – Bestelnr. 9137420E
- 13,56 MHz en 125 kHz RFID-kaartlezer – Bestelnr. 9137421E
- Vingerafdruklezer - Bestelnr. 9137423E
- Externe USB Bluetooth-lezer (dongle) – Bestelnr. 9137422E

CAM-logboeken

CAM-logboeken worden gebruikt om automatisch meerdere beelden op te nemen voorafgaand aan en na de geselecteerde gebeurtenis. In **Instellingen > CAM-logboeken** kunt u verschillende soorten gebeurtenissen beheren waarvoor CAM-logboeken moeten worden gegenereerd.

Bij elke kaartinvoer kunnen bijvoorbeeld CAM-logboeken worden gegenereerd. Als iemand de kaart doorhaalt, worden 5 beelden vóór de uithaal en 3 beelden na de uithaal vastgelegd in de toegangslogboeken. Frames worden na 1 seconde opgenomen. Voor de afbeeldingen wordt een opslagruimte van 1, 3 of 5 GB gecreëerd. Als de opslag vol is, worden de oudste afbeeldingen verwijderd. De toegangslogboeken zelf worden niet verwijderd.

Een CAM-logboektype maken

1. Ga naar de pagina **Instellingen > CAM-logboeken**.
2. Klik op de knop Toevoegen in de rechterbovenhoek van de pagina.
3. Voer een naam in voor het type CAM-loggebeurtenis.
   Het nieuw gemaakte CAM-loggebeurtenistype wordt weergegeven in de lijst en de details in het CAM-logboek worden geopend. In de details van het CAM-logboek is het noodzakelijk om in te stellen voor welke gebeurtenissen en op welke apparaten de beelden van de camera's worden gegenereerd.

CAM-logo's instellen

Informatie over het CAM-logboektype kan worden beheerd in het CAM-logdetail. De details van het CAM-logboek worden geopend door op het geselecteerde CAM-logboek in de lijst te klikken of na het aanmaken van een nieuw CAM-logboek.

Evenementen bekeken

Op het tabblad kunt u een lijst met gebeurtenissen selecteren waarbij beelden van de camera's worden vastgelegd.

Bijgehouden gebeurtenissen kunnen de volgende zijn:

- **Benaderingen**
  - Gebruiker geaccepteerd
  - Kenteken van auto herkend
  - Gebruiker afgewezen
  - Druk op de REX-knop
- **Veiligheid**
  - Beveiligingsschakelaar geactiveerd
  - Ongeoorloofd openen van de deur
  - Deuropening op afstand
  - Toegang geweigerd - herhaalde onjuiste invoer
  - Stil alarm geactiveerd

Bewaakte apparaten

Het geselecteerde type CAM-log kan alleen voor bepaalde apparaten worden verkregen. Als Monitoring van alle apparaten is uitgeschakeld, moet u de apparaten selecteren waarvoor CAM-logboeken moeten worden gemaakt. De selectie wordt gemaakt met behulp van .

Elektronische sloten

Systeem **Commandant voor toegang** biedt toegangsbeheer via elektronische sloten 2N Fortisdie worden ontgrendeld met een RFID-kaart met MIFARE® DESfire®. Bij het configureren van elektronische sloten wordt aan elk slot een coderingssleutel toegewezen. De sleutels van de sloten worden vervolgens opgeslagen op de RFID-kaarten van geautoriseerde gebruikers. Als de sleutels op de kaart en in het slot overeenkomen, wordt het vergrendelingsmechanisme ontgrendeld.

Eén RFID-toegangskaart kan gebruikt worden om tot 90 deuren met sloten 2N Fortis te openen, afhankelijk van het aantal tijdsprofielen dat toegepast wordt. Als de geheugencapaciteit van de kaart overschreden wordt, zal het schrijven van gegevens naar de kaart mislukken. Het mislukte schrijven wordt geregistreerd in het toegangslogboek van het systeem. Als er Slotgroepen worden gebruikt, kunnen er meer deuren naar één kaart worden geschreven dan bij individuele toewijzing. Als er Slotgroepen worden gebruikt, kunnen er meer deuren per kaart worden geregistreerd dan bij een individuele toewijzing.

Fortis Commander

Fortis Commander is een standalone toepassing die de **Fortis** elektronische sloten verbindt met het **Access Commander** systeem. De toepassing stelt vergrendelingen in volgens het projectbestand dat is gemaakt in **Access Commander**u en dat de vergrendelingsconfiguratie bevat. Het bestand is gecodeerd en kan alleen op één specifieke installatie worden gebruikt.

Installatie

Fortis Commander is ontworpen om geïnstalleerd te worden op een Windows computer met Bluetooth Low Energy (BLE) ondersteuning.

De app is te vinden op de website 2N Download Centre.

Installatieprocedure

1. Download het installatiepakket van de opgegeven link.
2. Voer het installatieprogramma uit en voltooi de installatie door de instructies op het scherm te volgen.

Projectbestand

Het projectbestand wordt gemaakt in **Access Commander** en bevat de volledige projectconfiguratie. Het bestand is gecodeerd en beveiligd met een wachtwoord.

Vergrendelingen instellen in Access Commander

Voordat u sleutels naar afzonderlijke sloten uploadt, moet u **Access Commander** koppelen met **Fortis Commander**.

Master Encryption Key (MEK) genereren en projectvoorbereiding

1. Meld u aan bij Access Commander.
2. Ga naar de pagina **Instellingen > Elektronische sloten**.
3. Op de kaart **Eerste installatie** klik Sleutels genereren.
4. Maak een hoofdcoderingssleutel.

LET OP
De hoofdcoderingssleutel kan niet later zijn **tonen of wijzigen**.

OPMERKING
Volgens de master encryptiesleutel (MEK) genereert **2N Access Commander** een reeks encryptiesleutels. De sleutel moet dus uniek en voldoende veilig zijn. De sleutelset is gebaseerd op de master-encryptiesleutel, dus projecten met dezelfde master-encryptiesleutel genereren dezelfde sleutelsets. Als een project verloren gaat, kan een nieuw project met dezelfde mastercoderingssleutel aangemaakt worden en de codering voortzetten.

5. Nadat u de sleutels hebt gegenereerd en het wachtwoord voor het projectbestand hebt ingesteld, kunt u **het projectbestand** downloaden, dat een afbeelding is van de configuratie van het elektronische slot in het systeem **Access Commander**.
6. In het tabblad **van Fortis Commander** klikt u op Download toepassing, vanwaar het downloaden van **Fortis Commander** (toepassing voor het configureren van elektronische sloten) zal beginnen.

LET OP
Projectinformatie is gevoelige informatie. Bescherm het tegen misbruik.

Het elektronische slot configureren met Fortis Commander

1. Installeer **Fortis Commander** en open het.
2. Klik op Open project en open het gedownloade projectbestand in File Explorer.
3. Voer in het dialoogvenster dat verschijnt het wachtwoord voor het projectbestand in.
4. Selecteer na het openen van het projectbestand Verbinden met apparaat en bevestig de servicekaart aan het slot.
5. Klik op **Toewijzen**, waarmee de vergrendeling aan het project wordt toegewezen.
6. Koppel het apparaat los en klik op **Bestand > Project sluiten**.
7. Wanneer de configuratie voltooid is, opent u het systeem **Access Commander**. Ga naar het tabblad **Instellingen > Elektronische sloten** en klik opnieuw op Fortis Commander. Upload het projectbestand.

OPMERKING
Wanneer u het slot verplaatst tussen installaties of wanneer u een claim indient, moet u een **Fabrieksreset** uitvoeren. Deze handeling zet het slot terug naar de fabrieksinstellingen en verwijdert alle eerdere configuraties.

Procedure voor het bijwerken van de configuratie

1. Breng wijzigingen aan in **Access Commander**.
2. Download het nieuwe projectbestand.
3. Upload het bestand naar **Fortis Commander** en breng de vereiste wijzigingen in de vergrendelingen aan.
4. Als u andere wijzigingen aanbrengt in **Access Commander**u, download dan altijd een nieuw projectbestand.

LET OP
Voor elke configuratiewijziging in **Access Commander**u moet u een nieuw projectbestand downloaden - u kunt geen ouder bestand gebruiken dat al is geüpload naar **Fortis Commander**.

Permanent vergrendelen en ontgrendelen

Met de app kunt u het slot permanent vergrendelen en ontgrendelen. De functie wordt gebruikt voor serviceinterventies of noodbediening zonder het gebruik van een kaart.

Verzamelen van gebeurtenissen van elektronische sloten met RFID-kaarten/chips

Instellingen voor gebeurtenisverzameling

1. Open **Instellingen > Elektronische sloten > Tabblad gebeurtenissen**.
2. Selecteer het type gebeurtenis:
   - **Toegangs- en systeemgebeurtenissen verzamelen** - Alle toegangs- en systeemgebeurtenissen worden op de kaart/chip geregistreerd en naar het **Systeemlogboek** en **Toegangslogboek** geschreven.
   - **Alleen systeemgebeurtenissen verzamelen** - alleen systeemgebeurtenissen worden gelogd, toegangsgebeurtenissen worden niet op kaarten opgeslagen.
   - **Verzamel geen gebeurtenissen op tabbladen** - er worden geen gebeurtenissen naar het tabblad geschreven; ze zijn alleen toegankelijk via **Fortis Commander**u.

TIP
Het selecteren van de juiste event set kan de systeembelasting en het opslaggebruik verminderen. Gedetailleerd loggen is echter belangrijk voor diagnostiek en veiligheidsaudits.

Gebeurtenissen van een kaart exporteren

De kaart slaat maximaal **16 eerste voorvallen** op. Gebeurtenissen kunnen op twee manieren worden gelezen:

- Klik in **Access Commander** op het pictogram in het zoekvak in de koptekst en laad het tabblad.
- Met een apparaat met **2N OS** worden gebeurtenissen van de kaart gelezen en naar **Access Commander**u verzonden.

Gebeurtenissen uploaden naar het slot

1. Open **Instellingen > Elektronische sloten > Fortis Commander** en klik op Download bestand.
2. Open het bestand in **Fortis Commander**.

3. Maak in de app **Fortis Commander** verbinding met het elektronische slot.
4. Upload het bijgewerkte bestand terug naar **Access Commander**.
5. Zodra de gebeurtenissen zijn geüpload, worden ze weergegeven in **Toegangslogboeken** en **Systeemlogboeken**.

Servicewerkzaamheden

Deze bewerkingen zijn beschikbaar voor **Fortis Cylinder**:

- **Demontage** - demontage van sloten voor onderhoudsdoeleinden.
- **De batterij vervangen** - de batterij in het slot vervangen.

LET OP
Servicebewerkingen zijn niet relevant voor andere typen vergrendelingen.

OPMERKING
Vanuit de servicemodus keert het slot terug naar de normale modus door op de knop Lock te drukken om het slot permanent te vergrendelen.

De kaart updaten

Gebruikerstoegangskaarten moeten regelmatig worden bijgewerkt. De gebruiker werkt de kaart bij door de kaart te koppelen aan het 2N IP-apparaat waartoe hij geldige toegangsrechten heeft. De kaart moet door de apparaatlezer worden vastgehouden totdat de schakelaar voor het openen van de deur wordt ingeschakeld. De deuropeningsschakelaar wordt pas geactiveerd nadat de toegang tot de sloten is bijgewerkt

De standaardgeldigheidsduur van kaarten van 10 dagen kan worden gewijzigd in **Instellingen > Elektronische sloten > tabblad Kaartparameters**.

LET OP
Als in **Commandant voor toegang** u wijzigt de toegangsrechten tot de sloten, de wijzigingen worden pas weergegeven op de toegangskaart van de gebruiker nadat deze is bijgewerkt op de kaartlezer van het 2N-apparaat! Om veiligheidsredenen raden we u aan een kortere geldigheidsduur van de kaarten in te stellen om ervoor te zorgen dat ze regelmatig worden bijgewerkt

Lezers voor IP-apparaten waarmee u de kaart kunt bijwerken, en hun instellingen worden beschreven in het hoofdstuk Instellingen voor IP-apparaatlezer (p. 26).

Compatibele kaarten

OPMERKING
Voor de doeleinden van deze documentatie wordt de term **kaart** elke compatibele identificatiecode die gebruikmaakt van MIFARE DESFire-technologie.

Voor het openen van elektronische sloten 2N Fortis Je kunt geen willekeurige identiteitskaarten gebruiken.

Kaarten met PiCard-technologie kunnen niet worden gebruikt om elektronische sloten te openen 2N Fortis.

Tijdprofielen op elektronische sloten

Elektronische sloten ondersteunen tijdprofielen met de volgende beperkingen:

- Feestdagen zijn niet van toepassing.
- Binnen één dag kunnen maximaal 4 verschillende tijdsintervallen worden ingesteld.
- Binnen één tijdprofiel kunnen 4 dagelijkse intervalschema's worden gedefinieerd.

TIP
Dit betekent dat je verschillende instellingen kunt hebben voor bijvoorbeeld maandag, dinsdag, woensdag en donderdag, maar voor vrijdag, zaterdag en zondag moet je al een van de bestaande instellingen gebruiken.

LET OP
Als het tijdprofiel deze beperkingen overtreedt, wordt de toegangsregel genegeerd en krijgt de gebruiker geen toegang.

Onderhoudskaarten

Onderhoudskaarten bieden geautoriseerde toegang tot het slot. Hiermee kunt u het slot in gebruik nemen, de batterij vervangen en het slot verwijderen

LET OP
De onderhoudskaart kan niet tegelijkertijd als gebruikerstoegangskaart worden gebruikt.

Instellingen voor de onderhoudskaart

1. In **Commandant voor toegang** ga naar **Instellingen > Elektronische sloten**.
2. Klik Creëren in **Onderhoudskaarten**.
3. Selecteer het kaarttype dat moet worden gemaakt in het dialoogvenster dat geopend moet worden.
   - Nieuwe sloten instellen — activeer de eerder geconfigureerde nieuwe sloten in de fabrieksinstellingen in de servicemodus.
   - Service — activeer de servicemodus voor de reeds ingestelde vergrendeling.
   - Demontage — Maakt het reeds ingestelde 2N Fortis-cilinderslot vrij voor verwijdering, zie de installatiehandleiding van 2N Fortis.
   - Batterij vervangen — Maakt het reeds ingestelde 2N Fortis-cilinderslot los om de batterij te vervangen, zie de installatiehandleiding van 2N Fortis.

TIP
Het is mogelijk om tegelijkertijd naar één fysieke kaart te uploaden **Nieuwe sloten opzetten** en elke tweede servicekaart. We raden een combinatie **Nieuwe sloten opzetten** en **Service**.

4. Klik Ga verder.
5. Tik met de kaart op de aangesloten USB RFID-lezer. Wacht tot de gegevens op de kaart zijn geladen.

geldigheidsduur van de gegevens op de onderhoudskaart is een jaar. Na deze tijd moet u de gegevens verwijderen en het tabblad opnieuw instellen

Probleemoplossen

Diagnostische logboeken

Diagnostische logboeken worden door de technische ondersteuning gebruikt om gemelde problemen te identificeren en op te lossen. Logboeken bevatten informatie over uitgevoerde acties, fouten, statuswijzigingen en andere relevante gebeurtenissen.

Diagnostische logboeken downloaden

1. Ga naar **Instellingen > Probleemoplossing > tabblad Diagnostische logboeken**.
2. Klik op Genereer logboeken.
   Het duurt een paar minuten om het logpakket te genereren.
3. Zodra het kaartspel klaar is, verschijnt het op de kaart en is het beschikbaar Downloaden.

Gebruiksstatistieken

Als de functie is ingeschakeld, wordt er verzonden **Access Commander** één keer per dag anonieme gegevens over de gebruikte functies naar een beveiligde 2N-server. Elke zending wordt gemaakt onder een unieke identificatiecode, die bij elke nieuwe zending automatisch opnieuw wordt gegenereerd. Hierdoor wordt voorkomen dat de 2N-partij de betreffende installatie identificeert **Access Commander**. De verkregen informatie wordt gebruikt om de productontwikkeling te verbeteren, functionaliteiten te ontwikkelen en de gebruikerservaring te verbeteren.

Kennisgeving

Met de module Meldingen kunt u monitoring instellen van geselecteerde gebeurtenissen en systeemeigenschappen waarvan de module op de hoogte is **Access Commander** informeer per e-mail of melding in de bovenste balk naast het gebruikersmenu.

De lijst met meldingen wordt ook weergegeven op de pagina **Systeemlogboeken > Meldingen**.

De records kunnen in een CSV-bestand worden gedownload door op de knop Export boven de lijst te klikken. In het geëxporteerde CSV-bestand wordt de tijd weergegeven in GMT+0.

Een nieuw meldingstype instellen

1. Ga naar de pagina **Instellingen > Meldingen**.
2. Klik op de knop Toevoegen in de rechterbovenhoek van de pagina.
3. Voer een naam in voor het nieuwe meldingstype.
   Na het aanmaken worden de details van de melding weergegeven, waarbij het mogelijk is om de apparaten te selecteren waarvoor de melding moet worden gemonitord; gebruikers toevoegen aan wie de melding moet worden verzonden; kies de bezorgmethode voor meldingen.

Notificatie instellingen

De meldingstypes worden ingesteld in de details van het meldingstype. Om de details van het meldingstype te openen, klikt u op de geselecteerde melding in de lijst op de pagina **Instellingen > Meldingen**.

Wijze van kennisgeving

Meldingen kunnen worden weergegeven zoals in **Access Commander**, dus stuur ze per e-mail.

In **Access Commander** verschijnen meldingen onder het in de bovenste balk, naast het gebruikersmenu of in **Systeemlog > Meldingen**.

Er kunnen notificatie-e-mails worden verzonden naar gebruikers die worden beheerd in **Access Commander** en ontvangers buiten het systeem. Gebruikers kunnen uit de lijst worden geselecteerd. De e-mailadressen van de overige ontvangers moeten handmatig worden ingevoerd.

OPMERKING
Voor de juiste werking van e-mail notificaties is het noodzakelijk dat SMTP correct is ingesteld, zie De e-mailfunctie (SMTP) inschakelen en instellen (p. 95).

Bewaakte apparaten

Het opgegeven type melding kan zowel voor alle apparaten als voor slechts enkele apparaten worden gegenereerd. Als Monitor alle apparaten is ingeschakeld, kan de gebeurtenis op elk apparaat plaatsvinden en wordt er een melding gegenereerd. Als Monitoring alle apparaten is uitgeschakeld, wordt er alleen een melding gegenereerd als er een gebeurtenis plaatsvindt op een van deze geselecteerde apparaten. De selectie van het apparaat vindt plaats in het menu, dat wordt geopend met .

Netwerkinstellingen

Om een netwerkverbinding in te stellen, gaat u naar **Instellingen > Configuratie > tabblad Netwerk**. Op het tabblad worden de huidige netwerkparameters van de **Access Commander** weergegeven en kunt u deze instellen. Individuele parameters kunnen worden ingesteld nadat de handmatige configuratiemethode is ingeschakeld.

Met de configuratiemethode kunt u de netwerkinstellingsparameters automatisch vanaf de DHCP-server of handmatig instellen. Wanneer u het automatisch ingestelde IP-adres van de DHCP-server wijzigt naar een handmatig ingevoerd adres, wordt de webbrowser doorgestuurd naar het ingevulde IP-adres. Na de omleiding vindt een herstart plaats**Access Commander** en moet opnieuw inloggen op het systeem.

LET OP

- Als u de configuratiemethode wijzigt in DHCP, wijzigt u het IP-adres van de server, waardoor de verbinding mogelijk wordt verbroken.
- Als u de HTTP-proxyserver wijzigt,**Access Commander**wordt automatisch opnieuw opgestart.

Detectie van wijziging van het IP-adres van het apparaat

Access Commander maakt verbindingen met apparaten via hun IP-adressen. Om te voorkomen dat de verbinding met een apparaat met een dynamisch IP-adres verloren gaat, zijn er twee methoden beschikbaar om IP-adressen van apparaten te detecteren.

- **Network Scanner**
  Access Commander scant periodiek het lokale netwerksegment met behulp van de geïntegreerde 2N Network Scanner om aangesloten apparaten en hun huidige IP-adressen te identificeren.
- **Device callback**
  Deze methode detecteert IP-adressen van apparaten buiten het lokale netwerksegment. Apparaten worden gerapporteerd bij het opstarten, wanneer het IP-adres verandert en met regelmatige tussenpozen (eenmaal per uur). Voor een goede werking moet je de bestemming specificeren waarnaar de apparaten moeten rapporteren (meestal het IP-adres van de **Access Commander**).

Proxy-instellingen

De proxy wordt gebruikt voor diensten zoals: HTTP-aanvragen, FTP-synchronisatie, upgrades, enz.

OPMERKING
Proxy voor FTP met TLS-authenticatie wordt niet ondersteund.

1. Ga naar **Instellingen > Configuratie > Netwerk**.
2. Selecteer Proxy bewerken.
3. Typ de adressen van de proxyserver voor de vereiste protocollen in het dialoogvenster dat wordt geopend.

4. In het laatste veld kunt u adressen invullen waarvoor de proxyserver niet moet worden gebruikt. Verbindingen met localhost en IP-adressen in het bereik van 127.0.0.1/8 worden nooit via een proxyserver gerouteerd.
5. Nadat de instellingen zijn gewijzigd, **2N Access Commander** wordt automatisch opnieuw opgestart.

NodeRed gebruiken

De NodeRed applicatie negeert de instellingen van de proxyserver. Voor de juiste functionaliteit moet de proxyserver expliciet worden geconfigureerd in elk NodeRed knooppunt dat het gebruik ervan vereist

Extra informatie

MIFARE and DESFire are registered trademarks of NXP B.V.

HTTP-API

De URL voor de **Access Commanderu** API is: https://acom_ip_address/api/v3/.

De lijst met API-eindpunten is gepubliceerd op http(s)://acom_ip_address/support/api . Buiten de **Access Commander**-interface is een lijst met eindpunten beschikbaar om te bekijken.

Je kunt antwoorden op verzoeken filteren met Query. In het document Data Query Customization wordt beschreven hoe je een **query** maakt.

Authenticatie

HTTP API-commando's worden verzonden onder de aanmeldingsgegevens van de gebruiker of met tokenauthenticatie. Het authenticatietoken wordt door de beheerder aangemaakt in **Instellingen > Configuratie > tabblad API Toegangstokens**. Dit is het Bearer Token. Bij het aanmaken van een nieuw API toegangstoken kan de beheerder het beperken tot alleen-lezen, zodat het token alleen GET-commando's authenticeert. Het token kan worden beperkt tot: 1 maand, 6 maanden, 1 jaar.

LET OP
Nadat u de toegangssleutel hebt gemaakt, kopieert u de sleutel naar het klembord en gebruikt u deze. Later zal de sleutel niet meer zichtbaar zijn.

SignalR

SignalR is een tool die realtime communicatie tussen de server en de client mogelijk maakt. Dit betekent dat de server aangesloten clients inhoud kan sturen zodra de inhoud beschikbaar komt, en niet hoeft te wachten op een verzoek van de client. De basisprincipes van SignalR worden beschreven in het document SignalR integration manual (alleen in het Engels). Lijst met beschikbare SignalR-onderwerpen waarmee u kunt gebruiken **Access Commander** worden beschreven in het document SignalR topics reference manual (alleen in het Engels).

Licenties van derden

Een volledige lijst met gebruikte bibliotheeklicenties van derden kunt u vinden in het gebruikersmenu aan de rechterkant van de bovenste balk, in het gedeelte Over.

2N Access Commander – Installatiehandleiding

2N.com