An ALLIED UNIVERSAL® Company

Betjeningsvejledning

2N Access Commander

I Indhold

Indholdet af denne vejledning kan ændres uden forudgående varsel. Firmaer, navne og data anvendt i eksempler er fiktive, medmindre andet er angivet. Elektronisk, mekanisk eller anden gengivelse af indholdet af denne vejledning, eller dele deraf, er forbudt til ethvert brug uden udtrykkelig skriftlig tilladelse fra G4S Security Services A/S herefter kaldet G4S.

I samarbejde med 2N Telekomunikea a.s.
(Version 3.2)

II Indholdsfortegnelse

2N Access Commander I
Indhold II
Indholdsfortegnelse III
Generel information 1
Brugerrettigheder 1
Administrator 1
Adgangsstyring 2
Brugeradministrator 2
Besøgschef 2
Dør manager 2
Tilstedeværelseschef 2
Understøttede enheder og applikationer 3
Understøttede enheder 3
2N Intercoms (samtaleanlæg) 3
2N Access Units (adgangsenheder) 3
2N telefonsvarer 3
Webbrowsere 4
Virtualiseringsplatforme 4
Brugte porte 5
Licens oversigt 5
Installation 9
Access Commander Box Distribution 9
Adgangskommando 9
Log ind på Access Commander med dynamisk IP-adresse 9
Statisk adresseindstilling for Access Commander via Access Commander Box . 10
Tekniske data Access Commander Box 10
Distribution af virtuelle maskiner 11
Virtuel boks 11
VMware-afspiller 11
VMware vSphere 11
Hyper-V 12
Anbefalet hardware 12
Hardware til virtuel maskine 12
Aktivering af licens 13
Hentning af licensfil 13
Upload af licens 13
Suspendering af licens 14
Grundlæggende adgang til grænseflade 15
Installationsnavn 15
Dashboard (betjeningspanel) 15
Ændring af sprog 16
Ændring af kontoadgangskode 16
Ændring af profilbillede 16
Logfiler 17
System-logfiler 17
Eksport af logfiler 17
Log levetid 17

Adgangslogfiler . . . 18
Eksport af logfiler . . . 18
Log levetid . . . 18
Meddelelser . . . 19
Indstilling af meddelelsestype . . . 19
Indstillinger for notifikationer . . . 19
Leveringsmetoder . . . 19
Overvågede enheder . . . 19
Log levetid . . . 19
Virksomheder . . . 21
Oprettelse af virksomhed . . . 21
Firma indstillinger . . . 21
Virksomhedens sprog . . . 21
Zoner . . . 21
My2N app . . . 21
Besøgende . . . 22
Arbejdstid . . . 22
Ferie . . . 22
E-mails sendt til virksomhedsbrugere . . . 22
Synkronisering af virksomheder (LDAP) . . . 23
Indstillinger for LDAP-synkronisering . . . 24
Brugerimport til virksomhed . . . 24
Brugerimport fra CSV-fil . . . 24
Importer fra 2N-enhed . . . 25
Brugere . . . 27
Bruger-indstillinger . . . 28
Ændring af brugernavn og foto . . . 28
Legitimationsoplysninger . . . 28
Konto . . . 29
Forenklet grænseflade . . . 29
Personlige oplysninger . . . 29
Adgang . . . 30
Telefonnumre . . . 30
Adgangslog . . . 30
Skift log . . . 30
Registrering af fingeraftryk . . . 30
Registrering af fingeraftryk . . . 31
Bluetooth-godkendelse . . . 31
Oprettelse af parringskode via pc . . . 31
Oprettelse af parringskode ved hjælp af enhed . . . 31
My2N Mobile Application Parring . . . 32
Brugerrettigheder . . . 32
Administrator . . . 32
Adgangsstyring . . . 33
Brugeradministrator . . . 33
Besøgschef . . . 33
Dør styring . . . 33
Tilstedeværelseschef . . . 33
Brugernes deltagelse . . . 34
Grupper . . . 35

Oprettelse af gruppe . . . 35
Indstillinger for grupper . . . 35
Medlemmer . . . 35
Regler for adgang . . . 35
Zoner . . . 37
Aktivering af adgangspunkter . . . 37
Oprettelse af zone . . . 37
Zone indstillinger . . . 37
Multi-Factor Godkendelse . . . 37
Få adgang til indstillinger . . . 38
Enheder . . . 38
Virksomheder . . . 38
Regler for adgang . . . 38
Enheder . . . 39
Tilføjelse af enhed . . . 39
Nødlukning . . . 40
Konfiguration af enhed . . . 40
Overblik . . . 41
Stat . . . 41
Adgangskontrol . . . 41
Konfiguration . . . 41
Dør kontrol . . . 41
Sikkerhedskopi . . . 41
Opkald . . . 42
Telefonbog med berøringsskærm . . . 42
Tilføjelse af kontakter til enhedens skærm . . . 42
Yderligere virtuelle numre . . . 43
Knapper . . . 43
Elevator . . . 44
Indstillinger for elevatorkontrol . . . 44
Elevator etager . . . 44
Elevator kontrolmoduler . . . 44
Overvågning . . . 45
Firmware . . . 45
Udelukkelse af enhed . . . 45
Inkompatible firmwareversioner . . . 45
Understøttede firmwareversioner . . . 45
Sikkerhed . . . 46
Indstilling af enhedsadgangspunkter . . . 46
Angive adgangsregler . . . 46
Adgangsregler . . . 47
Matrix-skærm . . . 47
Eksempel på matrixvisning . . . 48
Regelliste (Rule List) . . . 48
Tidsprofiler . . . 49
Oprettelse af tidsprofil . . . 49
Indstillinger for tidsprofil . . . 49
Deltagelse . . . 51
Specifik brugerdeltagelse . . . 51
Ændring af brugerdeltagelse . . . 51

Indstillinger for fremmøde . . . 52
Indstilling af enhedsadgangspunkter . . . 53
Angive adgangsregler . . . 53
Besøgende . . . 55
Indstillinger for opbevaring af besøgsdata . . . 55
Oprettelse af besøgende . . . 55
Afslutning af besøget . . . 55
Indstillinger for besøgende . . . 56
Kort . . . 56
Tilstedeværelse . . . 57
Udløb af brugertilstedeværelse . . . 57
Rapporter . . . 59
Områdebegrænsninger . . . 61
Oprettelse af områdebegrænsninger . . . 61
Indstillinger for områdebegrænsning . . . 61
Ind- og udrejse . . . 61
Belægning . . . 61
Anti-Passback . . . 62
Indstillinger for undtagelser . . . 62
Liste over blokerede brugere . . . 62
Nulstilling af begrænsning . . . 62
De mest almindelige opsætningsfejl . . . 63
Eksempel på begrænsningsindstilling . . . 63
Systemopsætning . . . 65
Dato og klokkeslæt . . . 65
Tidssynkronisering med enheder . . . 65
Konfiguration af netværk . . . 66
E-mail (SMTP) aktivering og indstilling . . . 66
Installationsnavn . . . 66
Systemopdatering . . . 67
Installation af opdatering til Access Commander . . . 67
Beta-test . . . 67
Sikkerhedskopiering af systemet . . . 68
Engangs sikkerhedskopiering af data . . . 68
Indstillinger for automatisk sikkerhedskopiering af data . . . 68
Indstillinger for SMB-sikkerhedskopiering af data . . . 68
Gendannelse af sikkerhedskopiering af data . . . 68
Gendan fra sikkerhedskopifil . . . 69
Dataoverførsel fra en anden Access Commander . . . 69
Synkronisering af brugere . . . 69
Automatisk brugersynkronisering med FTP . . . 69
CSV-fil . . . 70
Aktiverede USB-læsere . . . 71
PICard-nøgler . . . 71
Import af PICard-krypteringsnøgle . . . 71
Krypteringsnøgler til My2N-appen . . . 71
CAM-logfiler . . . 72
Oprettelse af CAM-logtype . . . 72
Indstillinger for CAM-log . . . 72
Overvågede hændelser . . . 72

Overvågede enheder 73
To-faktor-godkendelse 73
Muligheder for anmodning om to-faktor-godkendelse 73
To-faktor-godkendelse aktiveret 73
Aktiver SSH-adgang 74
Linux-indstillinger 74
Automatisering 76
Oprettelse af automatiseringer 76
Fejlsikret tilstand 77
Adgangskommandonoder 77
Adgangslog 77
Systemlog 78
SignalR 78
Dynamisk SignalR 78
Skriv systemlog 79
Eksempler på flows 80
Få alle brugere 80
Få brugere fra én virksomhed 80
Hent systemlog 80
Vis adgang givet 81
Skriv til systemlog 81
Opret bruger med data 81
Grupper af brugere, der kommer i gang med at bygge 82
Opret virksomhed og tilføj en bruger og et virtuelt nummer med samme indeks 82
Flow-eksport/-import 82
Fejl tilstande 83
Fejlfinding 85
Logfiler til diagnosticering 85
Download af diagnosticeringslog 85
Brugsstatistik 85
Supplerende oplysninger 87
HTTP API 87
Godkendelse 87
SignalR 87
Tredjeparts licenser 87

1 Generel information

2N Access Commander er et softwareværktøj til massestyring af adgangssystemer. Adgangsstyring grænsefladen er tilgængelig via en web browser.

I én installation kan Access Commander-indstillingerne opdeles i virksomheder og administreres separat. På den måde kan du fordele administrationen mellem administratorerne i virksomhederne. Administratoren fra en virksomhed har således ikke adgang til oplysninger fra en anden virksomhed. Administratorer fra en virksomhed kan ikke se brugerne af en anden virksomhed.

Føj enheder til Access Commander for at få adgang til administration. Enheder er adgangskontrol (2N samtaleanlæg eller 2N adgangsenheder) eller kommunikationsforsynende (2N telefonsvarer) fysiske enheder i en bygning. Enheder er samlet i zoner. Hver enhed kan kun være i én zone.

Zoner eller enheder kan deles af alle virksomhederne, hvilket hjælper med at administrere virksomhedens adgang til fællesarealer (indgange, restauranter, konferencesale osv.).

Brugere er personer, hvis bevægelse rundt i bygningen skal styres, eller som skal tilkaldes fra de tilsluttede enheder. Brugere samles i Grupper til massestyring af deres zoneadgange. Brugeren godkender sig selv på enheden, og enheden evaluerer derefter brugeradgangen for gyldighed. Adgangens gyldighed er i overensstemmelse med adgangsreglerne. Udvalgte brugere kan også være berettiget til at administrere Access Commander eller dele heraf.

Time profiles (tidsprofiler) angiver de tidspunkter, hvor enheden giver adgang, eller brugerne kan ringes op.

Attendance module (fremmødemodulet) overvåger brugernes fremmøde.

Presence module (tilstedeværelsesmodulet) overvåger den aktuelle brugertilstedeværelse i zonerne.

Visitors (besøgende) er personer, hvis adgangsrettigheder er begrænset til en begrænset periode.

1.1 Brugerrettigheder

Flere brugere kan administrere adgange i Access Commander afhængigt af deres tildelte rettigheder eller privilegier.

Konti med udvidede rettigheder indstilles gennem rollen i brugerindstillingerne. En bruger kan tildeles flere roller.

Brugerrettigheder vedrører administrationen i brugerens virksomhed. Administratoren har adgang til den komplette administration på tværs af virksomhederne.

1.1.1 Administrator

- System- og modulindstillinger i henhold til den gyldige licens.
- Ændring af licens.
- Alle rettigheder til andre roller relateret til alle virksomhederne.

1.1.2 Adgangsstyring

- Oprettelse og administration af grupper.
- Tilføjelse af brugere til grupper.
- Oprettelse og administration af besøgende.
- Oprettelse og administration af tidsprofiler.
- Indstilling af adgangsregler.

1.1.3 Brugeradministrator

- Oprettelse og administration af brugere.
- Oprettelse og administration af besøgende.
- Tilføjelse af brugere til grupper.
- Oprettelse og administration af besøgende.

1.1.4 Besøgschef

- Oprettelse og administration af besøgende.
- Administration af besøgstildeling til grupper (ikke tilgængelig i den forenklede grænseflade).
- Visning af besøgendes adgangslog (ikke tilgængelig i den forenklede grænseflade).

1.1.5 Dør manager

- Visning af kameratransmissioner fra tildelte enheder.
- Fjernåbning af tildelte enheder.
- Nødlåsning af tildelte enheder.
- Visning af adgangslog for tildelte enheder.
- Overvågning af tilstande og sikkerhedshændelser i systemloggen.

1.1.6 Tilstedeværelseschef

- Overvågning og styring af deltagelse af tildelte grupper.
- Visning af adgangslog for brugere i tildelte grupper.

1.2 Understøttede enheder og applikationer

Dette underafsnit indeholder lister over understøttede enheder, understøttede web-browsere og kompatible virtualiseringsplatforme, hvorigennem Access Commander kan installeres.

1.2.1 Understøttede enheder

Se nedenfor for en liste over enheder, der understøttes af Access Commander adgangs-systemet. Disse enheder kan administreres i systemet.

De understøttede firmwareversioner til enhederne er inkluderet i afsnit Firmware på side 45.

1.2.1.1 2N Intercoms (samtaleanlæg)

- 2N IP-Style – understøttelse af QR-kodelæsning
- 2N IP Verso 2.0 – understøttelse af QR-kodelæsning
- 2N IP-Verso
- 2N LTE Verso
- 2N IP-Force
- 2N IP-Safety (sikkerhed)
- 2N IP Vario
- 2N IP-Base
- 2N IP Solo
- 2N IP Uni
- 2N IP-Video Kit (videosæt)
- 2N IP-Audio Kit (lydsæt)
- 2N IP-Audio Kit Lite (lydsæt)

1.2.1.2 2N Access Units (adgangsenheder)

- Access Unit QR – understøttelse af QR-kodelæsning
- 2N Access Unit 2.0
- 2N Access Unit
- 2N IP- Access Unit M

1.2.1.3 2N telefonsvarer

- 2N Indoor View
- 2N Indoor Compact
- 2N Indoor Talk
- 2N Indoor Touch 2.0
- 2N Clip

1.2.2 Webbrowsere

Access Commander konfigureres via webgrænsefladen. Systemet er optimeret til Google Chrome-browseren (version 90 og nyere).

- Andre understøttede browsere
- Mozilla Firefox (version 78 og nyere)
- Microsoft Edge (version 91 og nyere)
- Safari (version 14 og nyere)

De andre browsere er ikke blevet testet, og deres fulde funktionalitet kan derfor ikke garanteres.

1.2.3 Virtualiseringsplatforme

- Virtuel Box
- VMware Player (version 6.5 og nyere)
- VMware vSphere (version 6.5 og nyere)
- Hyper-V

1.3 Brugte porte

Tabel 0-1: Liste over tjenester og nødvendige porte

Service	Port
HTTP//HTTPS[a.]	80/443
SMTP	225
DHCP	68
DNS	53
NTP	123
LDA[b.]	389
SSH	22

[a.] Det bruges både til klientkommunikation og intercom-kommunikation.

[b.] Brugeren kan vælge en anden port til LDAP i indstillingerne for Access Commander.

1.4 Licens oversigt

En prøvelicens er tilgængelig efter den første installation af Access Commander. Prøvelicensen giver dig mulighed for at teste alle administrationsfunktioner med 1 enhed og 5 brugere. En af følgende fire licenser skal aktiveres for at få fuld administrationsfunktionalitet: *Basic Free (gratis)*, *Advanced*, *Pro eller Unlimited*.

Tabel 1: Licens oversigt

Licenses	Trail	Basic Free	Advanced	Pro	Unlimited
2N Part No.	n/a	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Maksimalt antal brugere	5	50	300	1000	Ubegrænset[a.]
Maksimalt antal enheder (både aktive og deaktiveret)	1	5	30	100	Ubegrænset
Maksimalt antal administrator/ manager	5	1	5	1000	Ubegrænset
Adgangs- og systemlogfiler	✓	✓	✓	✓	✓

Tabel 1: Licens oversigt

Licenses	Trail	Basic Free	Advanced	Pro	Unlimited
2N Part No.	n/a	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Regler for adgang	✓	✓	✓	✓	✓
API-administration	✓	✓	✓	✓	✓
Kontoaktivering/deaktivering	✓	✓	✓	✓	✓
Grænse for mislykkede adgangsforsøg	✓	✓	✓	✓	✓
Lydløs alarm	✓	✓	✓	✓	✓
Zonekode	✓	✓	✓	✓	✓
Overvågning af enheder	✓	✓	✓	✓	✓
Logstyring	✓	✓	✓	✓	✓
Brugerimport fra CSV eller enhed	✓	X	✓	✓	✓
Masseadministration af firmware	✓	X	✓	✓	✓
Multi-Factor Godkendelse	✓	X	✓	✓	✓
Bruger-rettigheder	✓	X	✓	✓	✓
Meddelelse	✓	X	✓	✓	✓
Tilstedeværelse	✓	X	✓	✓	✓
API-adgangs-nøgler	✓	X	✓	✓	✓
CAM-logfiler	✓	X	✓	✓	✓
Lift kontrol	✓	X	✓	✓	✓
Betjeningspanel	✓	X	✓	✓	✓

Tabel 1: Licens oversigt

Licenses	Trail	Basic Free	Advanced	Pro	Unlimited
2N Part No.	n/a	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Nødlukning	✓	X	✓	✓	✓
Understøttelse af mobile legitimationsoplysninger	✓	X	✓	✓	✓
Administration af besøgende	✓	X	✓	✓	✓
Automatisering	✓	X	✓	✓	
Administration af belægning	✓	X	X	✓	✓
Synkronisering (LDAP og CSV)	✓	X	X	✓	✓
Anti-Passback	✓	X	X	✓	✓
Deltagelse	✓	Valgfri	Valgfri	Valgfri	Valgfri

[a.] Ubegrænset inden for softwareplatformens maksimale kapacitet, se Anbefalet hardware (se afsnit 2.2.5 side 12).

2 Installation

Access Commander kan distribueres som:

- 2N Access Commander Box 2.0, en lille stationær computer (varenr. 1120120xx, Axis varenr. 03129-00)
- Virtuel maskine

Access Commander Box-løsningen er begrænset til 2000 tilsluttede enheder. Den anden softwarefunktion er identisk for begge løsninger.

2.1 Access Commander Box Distribution

Access Commander Box (varenr. 1120120xx, Axis varenr. 03129-00) er en lille kompakt desktop-computer med forudinstalleret software. Det er en plug & play-løsning, som kun kræver en strømforsyning og et Ethernet-kabel tilsluttet computeren. Det anbefales, at denne computer placeres sikkert og holdes kørende for en korrekt og fuld systemfunktionalitet. Access Commander Box bruges som en data-/hændelses-/logindsamlingsserver for hele adgangssystemet.

2.1.1 Adgangskommando

Antal tilsluttede enheder	Antal brugere	Antal brugere pr. gruppe
7000	200000	1500

Vi anbefaler, at 1500 brugere pr. gruppe ikke overskrides. Hvis der er nogle restriktioner i området, f.eks. som Anti-passback eller belægningskontrol på grund af et højt antal brugere, kan applikationen blive langsommere.

2.1.2 Log ind på Access Commander med dynamisk IP-adresse

1. Tilslut Access Commander Box til netværket ved hjælp af et Ethernet-kabel.
2. Lokaliser Access Commander Box i netværket ved hjælp af 2N IP-netværksscanner.
3. Gå til Access Commander Box IP-adressen i web browser og log ind på Access Commander.
   Standardadgangskoden for Admin-brugeren er **2n**, og efter login er ændring af password påkrævet.

Med Access Commander Box-distributionen skal du oprette forbindelse til webgrænsefladen fra en anden LAN-computer. Access Commander Box-operativsystemet sikrer Access Commander-betjeningen og grundlæggende Linux-indstillinger, men tillader ikke, at webbrowseren startes.

2.1.3 Statisk adresseindstilling for Access Commander via Access Commander Box

1. Tilslut Access Commander Box til netværket ved hjælp af et Ethernet-kabel.
2. Tilslut et tastatur og en skærm til Access Commander Box. Der vises en sort skærm.
3. Log ind som "root" med adgangskoden "2n". Når en blå skærm vises, skal du ændre standardadgangskoden.
4. Vælg "Netværk" i menuen Avanceret og derefter "Statisk IP".
5. Indstil den statiske IP-adresse, gateway og DNS.
6. Gem indstillingerne, og klik på Log ud for at afslutte konsolmenuen.
7. Opret forbindelse til den indstillede IP-adresse via din web browser.

2.1.4 Tekniske data Access Commander Box

1. generation Part. nr. 91379030, akse del nr. 01672-001	2. generation Varenummer 1120120E, 1120120GB, 1120120US akse Varenr. 03129-00
• Dimensioner: 56,1 x 107,6 x 114,4 mm (2,21'' x • 4,24'' x 4,50'') • Intel® Celeron-processor® J3160 (2 MB cache, op til 2,24 GHz) • 2,5" SSD SATA III-harddisk (120 GB) • DDR3 SO-DIMM-hukommelse (4 GB) – 1,35 V, 1600 Mhz • Understøtter to skærme via en VGA- og HDMI-port • Gigabit LAN-port til Ethernet-forbindelse • VESA-monteringsbeslag (75 × 75 mm + 100 × • 100 mm) • Systemets opbevaringstemperatur: -20 °C til +60 °C • Systemmiljø driftstemperatur: 0°C • til +35°C	• Dimensioner: 127,5 x 132 x 57,6 mm (5,02 " x x 5,20" x 2,27") • Intel-processor® N100, 6W TDP • SSD 980 NVMe M.2 – 250 GB • DDR4 SO-DIMM-hukommelse - 16 GB, 1,2 V, 3200 MHz • HDMI-understøttelse 2.1, DisplayPort 1.4 a VGA • 2,5G RJ45 LAN-port til Ethernet-forbindelse • Systemets opbevaringstemperatur: -40 °C til +85°C • Systemmiljø driftstemperatur: 0 °C til +50 °C

2.2 Distribution af virtuelle maskiner

Access Commander kan distribueres som en virtuel maskine. Se nedenfor for installationsprocedurer på de understøttede virtualiseringsplatforme.

2.2.1 Virtuel boks

Det anbefales at aktivere VT-X-virtualiseringsteknologien i BIOS.

1. Download den seneste VirtualBox-version fra https//www.virtualbox.org/wiki/Downloads.
   Fortrinsvis inklusive VirtualBox Extension Pack.
2. Download den relevante software fra Support > Download Center > Software og firmware ved 2N.com.
   Pak den downloadede fil ud.
3. Åbn VirtualBox og vælg "File – Importer appliance...".
4. Rediger navnet.
5. Kontroller CPU-indstillingen (mindst 2), RAM-indstillingen (mindst 2048 MB) og valg af netværkskort.
6. Bekræft licensbetingelserne.
   Efter installationen åbnes Linux-konfigurationskonsollen, så du kan foretage grundlæggende systemindstillinger. Foretag den komplette konfiguration via web interface.

2.2.2 VMware-afspiller

Den understøttede VMWare-version er 6.5 og højere.

1. Download den relevante software fra Support > Download Center > Software og firmware ved 2N.com.
   Pak den downloadede fil ud.
2. I VMware Player File - Åbn... vælg stien til OVA-filen.
3. Omdøb den om nødvendigt, og klik på Importer.
4. Kontroller CPU-indstillingen (mindst 2), RAM-indstillingen (mindst 2048 MB) og valg af netværkskort.
   Efter installationen åbnes Linux-konfigurationskonsollen, så du kan foretage grundlæggende systemindstillinger. Foretag den komplette konfiguration via web interface.

2.2.3 VMware vSphere

Den understøttede VMWare-version er 6.5 og højere.

1. Download den relevante software fra Support > Download Center > Software og firmware ved 2N.com.
   Pak den downloadede fil ud.

2. I VMware vSphere skal du vælge Filer – Implementer OVF-skabelon... , og følg vejledningen i guiden.
3. Efter import skal du markere Rediger indstillinger...
   Rediger navnet (på kortet Indstillinger).
4. Kontroller CPU-indstillingen (mindst 2), RAM-indstillingen (mindst 2048 MB) og valg af netværkskort.
   Efter installationen åbnes Linux-konfigurationskonsollen, så du kan foretage grundlæggende systemindstillinger. Foretag den komplette konfiguration via web interface.

2.2.4 Hyper-V

1. Download den relevante software fra Support > Download Center > Software og firmware ved 2N.com.
   Pak den downloadede fil ud.
2. Start Hyper-V Manager, og vælg **Import Virtual Machine** (Importer virtuel maskine) for den påkrævede vært.
3. Kontroller de viste oplysninger i installationsguiden, og tryk på **Next** (Næste) for at bekræfte læsningen.
4. Vælg stien til mappen fra trin 1.
5. Bekræft valget af den virtuelle maskine.
6. Vælg importtypen.
7. Vælg det virtuelle netværkskort for den virtuelle maskine.
8. Kontroller oversigten over de indstillinger, der er valgt i de foregående trin, og tryk på **Finish** (Udfør) for at bekræfte.
   Efter installationen åbnes Linux-konfigurationskonsollen, så du kan foretage grundlæggende systemindstillinger. Foretag den komplette konfiguration via web interface.

2.2.5 Anbefalet hardware

Access Commander påvirkes af antallet af tilsluttede enheder. Indstil derfor hardwarestørrelsen i henhold til den virkelige situation. Tabellen nedenfor viser det anbefalede minimum antal CPU-kerner og RAM-størrelser for forskellige enheds- og brugerantal, der administreres af Access Commander.

Det anbefales, at du opretholder kontinuerlig forbindelse mellem Access Commander og enhederne. Når forbindelsen er afbrudt, gemmer enhederne hændelsesloggene offline, og når de er tilsluttet igen, synkroniserer de logdataene med Access Commander. Applikationen fortsætter med at køre under synkronisering, men processen kan tage ret lang tid med et stort antal enheder.

2.2.6 Hardware til virtuel maskine

Antal enheder	Antal brugere	Minimum CPU Antal kerner	Minimum RAM størrelse	Minimum harddisk allokation
1 000	10 000	2	2 GB	120 GB
2 000	100 000	2	4 GB	120 GB
2 000	200 000	4	8 GB	120 GB
7 000	200 000	4	16 GB	120 GB

2.3 Aktivering af licens

Hent licensfilen, og overfør den til Access Commander. Du kan aktivere Basic-licens direkte i Access Commander i Indstillinger > kortlicens.

2.3.1 Hentning af licensfil

For at hente licensen file skal du kommunikere serienummeret på en af de 2N-enheder, der er tilsluttet Access Commander. Licensfilen genereres på baggrund af serienummeret på denne licensenhed.

Licensenhedsforbindelsen sikrer licensens gyldighed. Når licensenheden afbrydes, begynder en beskyttelsesperiode at køre, og licensen suspenderes, når perioden udløber.

2.3.2 Upload af licens

- Når prøvelicensen er slukket, kan den ikke genaktiveres.
- De avancerede indstillinger, der ikke understøttes af den nye licens, gemmes ikke.

1. Gå til Indstillinger > kortlicens.
2. Klik på Upload licens, og upload licensfilen fra lageret i den åbne boks.
3. Klik på Aktivér licens efter upload.
4. Sørg for, at den licensenhed, som licensen er genereret til, er aktiveret.

Licensér enhed
Valgt 2N-enhed tilsluttet Access Commander for at sikre licens gyldigheden. Licensenheden bruges som hardwarenøgle til licensen.

Licens fil
Licensfil, der bruges til licensaktivering. Licensen file genereres af distributøren baseret på licensenhedens serienummer.

2.4 Suspendering af licens

En licens suspenderes, når licensenheden forbliver afbrudt fra Access Commander i en længere periode end beskyttelsesperioden. Længden af beskyttelsesperioden afhænger af, hvor længe licensenheden var tilsluttet Access Commander. Se nedenstående tabel for værdier for beskyttelsesperiode.

Når en licens suspenderes, fjernes alle de tilsluttede enheder automatisk fra administrationen og markeres som ikke-administrerede. Hvis du vil genaktivere dem, skal du tilslutte og aktivere licensenheden eller få en ny licensfil genereret og uploadet til en anden enhed.

Når en ny licens er uploadet, skal du først aktivere den licensenhed, som licensen er genereret til. De andre enheder kan ikke aktiveres, før denne licensenhed er aktiveret.

Tidsperiode, hvor licensenheden var forbundet til Access Commander	Beskyttelsesperiode, hvor Access Commander vil fortsætte med at køre uden licensenheden tilsluttet
mindre end 24 timer	1 dag
1 dag - 30 dage	10 dage
31 dage - 180 dage	1 måned
over 180 dage	3 måneder

3 Grundlæggende adgang til grænseflade

I dette underafsnit beskrives idriftsættelse og grundlæggende betjening af Access Commander. Installationen er beskrevet i Installation se afsnit 2 side 9.

Access Commander-grænsefladen er tilgængelig via en webbrowser. Find web grænsefladens IP-adresse ved hjælp af 2N netværksscanner

Med Access Commander Box-distributionen skal du oprette forbindelse til webgrænsefladen fra en anden LAN-computer. Access Commander Box-operativsystemet sikrer Access Commander driften og grundlæggende Linux-indstillinger, men tillader ikke, at webbrowseren startes.

Standard login-data er:

Brugernavn: **Admin**

Adgangskode: **2n**

Det er nødvendigt at ændre adgangskoden umiddelbart efter første login.

To-faktor-godkendelse, Systemopsætning (se afsnit 17.13 side 73) kan være påkrævet for login.

3.1 Installationsnavn

Navnet på den pågældende Access Commander-installation vises i webgrænsefladens overskrift for alle de brugere, der er logget på. Du kan ændre standardnavnet på Access Commander, f.eks. til adressen på den bygning, som den pågældende installation administrerer.

Skift navnet i Indstillinger > Konfiguration > Installationsnavn. Ved at ændre navnet kan du adskille flere installationer, hvis de administreres af én person. Installationsnavnet skrives også ind i de e-mails, der sendes til virksomhederne.

3.2 Dashboard (betjeningspanel)

Dashboard er den grundlæggende visning af Access Commander-webgrænsefladen. Det er en konfigurerbar opslagstavle, der viser realtidsdata. Access Commander indeholder flere widgets, som føjes til dashboardet ved hjælp af (Dashboard-widgets) kan flyttes eller omdøbes, eller deres grundlæggende indstillinger kan foretages. Brug (Den udvidede menu) i overskriften på hver widget for at administrere og slette widgets.

Alle brugere med en konto på Access Commander kan indstille deres eget dashboard. Widgetens tilgængelighed er begrænset afhængigt af brugerrollen og den tilgængelige licens.

3.3 Ændring af sprog

Ved første login vises Access Commander på det sprog, der er indstillet for den bruger, der er logget på. Hver bruger kan ændre sproget. Til de næste logins vil grænsefladen være tilgængelig på det nyligt indstillede sprog.

5. Klik på brugerbilledet i øverste højre hjørne for at åbne brugermenuen.
6. Vælg **Change language** (Skift sprog).
7. Vælg det ønskede sprog, og tryk på **Change language** (Skift sprog) for at bekræfte valget.

3.4 Ændring af kontoadgangskode

1. Klik på brugerbilledet i øverste højre hjørne for at åbne brugermenuen.
2. Vælg **View profile** (Vis profil).
3. Klik ved parameteren Password (Adgangskode).
4. Bekræft den aktuelle adgangskode, og indtast en ny.

BEMÆRK!
Hvis adgangskoden til 'admin'-kontoen er den samme som adgangskoden til systemets root-bruger (til login til Linux-indstillingskonsollen), ændres adgangskoden til root-kontoen automatisk, når adgangskoden til 'admin'-kontoen ændres.

3.5 Ændring af profilbillede

1. Klik på brugerbilledet i øverste højre hjørne for at åbne brugermenuen.
2. Vælg **View profile** (Vis profil).
3. Klik på billedet i overskriften med brugeroplysninger.
4. Indstil billedet i den åbne dialogboks.
   Billedopløsningen justeres automatisk til 432 x 432 px.

4 Logfiler

Her er, hvad du kan finde i dette underafsnit:

System-logfiler (side 17)
Adgangslogfiler (side 18)
Meddelelser (side 19)
Log levetid (side 17)

4.1 System-logfiler

Logfiler vises, baseret på deres brugerrettigheder.
Data skrives på engelsk ind i logfilerne.

Siden System Logs (Systemlogfiler) viser en liste over hændelser og meddelelser, der er genereret af Access Commander (adgangsstyring).

Systemloglisten indeholder følgende data om hver hændelse og meddelelse:

- Alvorsgrad (info, advarsel, fejl);
- Begivenhedstid;
- Handlingskategori (Enhedstilstand, Import, Brugersynkronisering, System, Bruger-handlinger, Områdebegrænsninger);
- Relateret emne (enhed, bruger, zone, besøgende...);
- Kort beskrivelse af begivenheden;
- Forfatter af begivenheden.

Klik på rækken for at åbne detaljerede oplysninger om den valgte post.

Filtrere listeelementerne ved hjælp af over listen. Eller klik på i hver kolonneoverskrift for at åbne en udvidet menu og angive filtre for hver kolonne. Den udvidede kolonnemenu giver dig også mulighed for at flytte, fastgøre til første/sidste position eller skjule kolonnerne.

Kolonnerne Importance (Vigtighed) og Time (Tid) kan ikke skjules.

4.1.1 Eksport af logfiler

Tryk på **Export** over listen for at eksportere listen som en CSV-fil eller udskrive den. Klokkeslættet er GMT+0 i CSV-filen eksporteret fil.

4.1.2 Log levetid

Automatisk sletning udløses i det øjeblik, diskpladsforbruget når 80 %. Følg diskkapaciteten på siden Indstillinger. Logfiler af den første type i sekvensen slettes først, de andre logfiler slettes en efter en, indtil diskpladsforbruget falder til 75 %, eller indtil kun logfiler med den uafsluttede maksimale levetid for den givne logtype forbliver gemt.

Angiv opbevaringsperioden for den givne logtype i Indstillinger > Logopbevaringskort. Opbevaringstiden for kameralogfilen må ikke være længere end opbevaringstiden for systemet og adgangsloggen.

Hvis du bruger 70 % af diskkapaciteten kontinuerligt, anbefaler vi, at den maksimale loglagringsperiode forkortes.

4.2 Adgangslogfiler

- Disse logfiler vises, som brugeren kan observere baseret på deres brugerrettigheder.
- Data skrives på engelsk ind i logfilerne.

Siden Access Logs (Adgangslogfiler) viser registreringer af vellykkede/mislykkede godkendelsesforsøg og registreringer for nedlukning i nødstilfælde.

Listen over adgangslogfiler indeholder:

- **Kategori**
  Adgang aktiveret
  Adgang nægtet
  Offentlig adgang
  Låsning – låsning af enheden
- **Tidspunkt** for arrangementet
- **Bruger**, der udførte handlingen
- Givet brugerens **virksomhed**
- **Zone**, hvor handlingen fandt sted
- **Enhed**, hvor handlingen skete
- **Godkendelse** brugt til forsøget (PIN-kode, QR-kode osv.)

Klik på rækken for at åbne detaljerede oplysninger om den valgte post.

Filtrere listeelementerne ved hjælp af over listen. Eller klik på i hver kolonneoverskrift for at åbne en udvidet menu og angive filtre for hver kolonne. Den udvidede kolonnemenu giver dig også mulighed for at flytte, fastgøre til første/sidste position eller skjule kolonnerne.

4.2.1 Eksport af logfiler

Tryk på **Export** over listen for at eksportere listen som en CSV-fil eller udskrive den. Klokkeslættet er GMT+0 i CSV-filen eksporteret fil.

4.2.2 Log levetid

Automatisk sletning udløses i det øjeblik, diskpladsforbruget når 80 %. Følg diskkapaciteten på siden Indstillinger. Logfiler af den første type i sekvensen slettes først, de andre logfiler slettes en efter en, indtil diskpladsforbruget falder til 75 %, eller indtil kun logfiler med den uafsluttede maksimale levetid for den givne logtype forbliver gemt.

Angiv opbevaringsperioden for den givne logtype i Indstillinger > Logopbevaringskort. Opbevaringstiden for kameralogfilen må ikke være længere end opbevaringstiden for systemet og adgangsloggen.

Hvis du bruger 70 % af diskkapaciteten kontinuerligt, anbefaler vi, at den maksimale loglagringsperiode forkortes.

4.3 Meddelelser

Meddelelsesmodulet hjælper dig med at overvåge udvalgte systemhændelser og funktioner, som skal rapporteres af Access Commander via e-mail eller meddelelse i den øverste bjælke ved siden af brugermenuen.

Meddelelseslisten vises også i Systemlogfiler > Meddelelser.

Tryk på **Export** over listen for at eksportere listen som en CSV-fil eller udskrive den. Klokkeslættet er GMT+0 i CSV-filen eksporteret fil.

4.3.1 Indstilling af meddelelsestype

1. Gå til **Settings** (Indstillinger) > **Notifications** (Notifikationer).
2. Klik på knappen **Tilføj** i øverste højre hjørne af siden.
3. Angiv navnet på den nye meddelelsestype.
   Efter oprettelsen vil meddelelsesdetaljerne blive vist, så du kan vælge de enheder, hvis meddelelser skal overvåges, tilføje den bruger, der skal sendes meddelelser til, og vælge måden at levere meddelelser på.

4.3.2 Indstillinger for notifikationer

Indstil meddelelsestypen i detaljerne for den valgte meddelelsestype. Klik på den valgte meddelelse i vinduet Indstillinger > Notifikationer for at åbne notifikationstypedetaljerne.

4.3.3 Leveringsmetoder

Angiv leveringsmetoden for meddelelser og listen over modtagere af e-mail-meddelelser på kortet.

I Access Commander, vises meddelelser under ikonet i den øverste bjælke ved siden af brugermenuen eller i Systemlog > Meddelelser.

E-mails med meddelelser kan sendes til de brugere, der er angivet i Access Commander, samt modtagere uden for systemet. Brugerne kan vælges fra en liste. E-mail-adresser på andre modtagere skal tilføjes manuelt.

Sørg for, at SMTP er indstillet korrekt for at få e-mail-meddelelser til at fungere korrekt, se E-mail (SMTP) Aktivering og indstilling (se afsnit 17.3 side 66).

4.3.4 Overvågede enheder

Den givne notifikationstype kan genereres både for alle enheder og udvalgte enheder. Hvis Overvågning af alle enheder er aktiveret, kan hændelsen ske på enhver enhed, og der genereres en meddelelse. Hvis overvågning af alle enheder er deaktiveret, genereres der kun en meddelelse, hvis hændelsen sker på en valgt enhed. Vælg enheden i en menu, der åbnes ved hjælp af .

4.4 Log levetid

Automatisk sletning udløses i det øjeblik, diskpladsforbruget når 80 %. Følg diskkapaciteten på siden Indstillinger. Logfiler af den første type i sekvensen slettes først, de andre log-

filer slettes en efter en, indtil diskpladsforbruget falder til 75 %, eller indtil kun logfiler med den uafsluttede maksimale levetid for den givne logtype forbliver gemt.

Angiv opbevaringsperioden for den givne logtype i Indstillinger > Logopbevaringskort. Opbevaringstiden for kameralogfilen må ikke være længere end opbevaringstiden for systemet og adgangsloggen.

Hvis du bruger 70 % af diskkapaciteten kontinuerligt, anbefaler vi, at den maksimale loglagringsperiode forkortes.

5 Virksomheder

Inden for en installation kan Access Commander-indstillingerne opdeles i virksomheder og administreres separat. På den måde kan du fordele administrationen mellem administratorerne i virksomhederne. Administratoren fra en virksomhed har således ikke adgang til oplysninger fra en anden virksomhed. Administratorer fra en virksomhed kan ikke se brugerne af en anden virksomhed.

Zoner eller enheder kan deles af alle virksomhederne, hvilket hjælper med at administrere virksomhedens adgang til fællesarealer (indgange, restauranter, konferencesale osv.).

5.1 Oprettelse af virksomhed

1. Gå til siden **Companies** (Virksomheder).
2. Klik på knappen **adding** (Tilføjelse) af virksomhed i øverste højre hjørne.
3. Udfyld firmanavnet.
4. Klik på **Create** (Opret) for at oprette en virksomhed.
   Det nye selskab vises på listen. Indstil virksomheden i firmaoplysningerne. Tilføj brugere til virksomheden i brugerindstillingerne.

5.2 Firma indstillinger

Få vist og rediger virksomhedsoplysningerne i virksomhedsoplysningerne. Klik på det valgte firmalisteelement på knappen

Firmaer for at åbne firmaoplysningerne.

Der er en **Lock** (låse) knap i virksomhedens detaljeoverskrift, som aktiverer Emergency Lockdown (se afsnit 9.2 side 40) for alle enheder i denne virksomheds zoner.

Virksomhedsdetaljerne er opdelt i kortene Overview (Oversigt), E-mails og Brugersynkronisering.

5.2.1 Virksomhedens sprog

Vælg sproget på kortet Generelt for Access Commander-grænsefladen for at kommunikere med brugerne af den givne virksomhed. Brugerne kan ændre grænsefladesproget når som helst senere. Valget af virksomhedssprog påvirker også skabelonerne til de e-mails, der skal sendes til brugerne. E-mail-teksterne kan ændres i e-mail-mappen.

5.2.2 Zoner

Tildeling af zoner til en virksomhed betyder at definere et sæt faciliteter, som kan tilgås af virksomhedens brugere (f.eks. fællesrummet og zoner på 4. sal, som omfatter indgangsdøren til receptionen og alle indgange på 4. sal). En zone kan tildeles flere virksomheder, og en virksomhed kan tildeles flere zoner.

5.2.3 My2N app

I Company kan du også indstille parringsparametrene for My2N-appen, som giver mulighed for Bluetooth-godkendelse. Indstil både de enheder, der kan bruges til parring, og gyldigheden af den mobiladgang, der er nødvendig for parring. Selve mobiladgangen genereres i brugerindstillingerne.

5.2.4 Besøgende

Her skal du angive de grupper, som besøgsadministratoren kan tildele nye besøgende. En af grupperne kan bestemmes som standard. En ny besøgende vil automatisk blive tildelt standardgruppen, medmindre andet er defineret.

Uden en korrekt indstillet standardgruppe er det ikke muligt at give adgang til besøgende i den forenklede brugergrænseflade

Det er muligt at vælge de godkendelsesmetoder, der kan tildeles besøget. Godkendelsesmetoden tildeles derefter et besøg af besøgsadministratoren.

Se Besøgende (se afsnit 13 side 55) for flere detaljer.

5.2.5 Arbejdstid

Arbejdstid og Helligdage bruges til beregning af den månedlige brugerarbejdstid i fremmødemodulet. Du kan vælge de dage i en uge, der skal beregnes som arbejdsdage. Klik på en dag for at vælge den. Grønne dage identificerer de dage, der betragtes som arbejdsdage.

Ændring af arbejdstid definerer tidspunktet for et dagskift.

5.2.6 Ferie

Indstil helligdagene for at definere, hvilke dage der ikke er inkluderet i beregningen af den månedlige arbejdstid. De timer, der arbejdes på helligdage, tælles som arbejdstimer i weekenden – den arbejdede tid registreres ud over den almindelige arbejdstid.

Den udvidede menu ⋮ hjælper dig med at kopiere helligdage fra et andet firma. Helligdage kopieres inklusive deres datoer og navne. Kopiering kan bruges gentagne gange, men hvis ferien, der skal kopieres, allerede findes i virksomheden, vil den blive omdøbt.

5.2.7 E-mails sendt til virksomhedsbrugere

Find e-mail-indstillingerne i en dedikeret mappe i virksomhedsoplysningerne. Access Commander gør det muligt at sende automatiske e-mails, der informerer om godkendelsesmetodens tildeling til virksomhedens brugere (herunder besøgende). E-mailen sendes til brugerens eller den besøgendes e-mailadresse.

Access Commander gør det muligt at sende e-mails med følgende oplysninger:

- PIN-kode til besøgende
- QR-kode til besøgende
- PIN-kode til bruger
- QR-kode til bruger
- My2N-app til Bluetooth-brugergodkendelsesindstillinger

Angiv udseendet, og rediger teksten for disse e-mails i skabelonerne Virksomhedsoplysninger > E-mails > E-mails. Klik på den valgte e-mail-type for at åbne en dialogboks, hvor du kan redigere e-mail-teksten. Du kan redigere følgende i dialogboksen:

- Emne – e-mail-emne
- Overskrift – i e-mailens brødtekstfarvefelt
- Introduktion – tekst, der går forud for de automatisk genererede data fra Access Commander
- Yderligere meddelelse – tekst efter de data, der er genereret fra Access Commander

- Underskrift – underskrift i e-mail-enden

5.2.8 Synkronisering af virksomheder (LDAP)

LDAP-synkronisering bruges til at hente bruger- og brugerændringer fra et eksternt LDAP-system. Brugerdataene omfatter brugernavn, bruger-id, kortidentifikatorer, PIN-kode/QR-kode, foto, e-mailadresse, telefonnummer, adgangskode og login, køretøjets nummerplader.

Se www.ldap.com for flere LDAP-detaljer

1. Gå til Firmaer > Firmaoplysninger > Brugersynkronisering.
2. Hvis der ikke er oprettet en forbindelse, skal du oprette en.
   Komplet:
   • **Servernavn** – hvis DNS er indstillet korrekt, skal du blot indtaste servernavnet ("WIN-9ABEB4AUOHD"). Hvis DNS ikke er indstillet, skal du indtaste IP-adressen på den server, hvor LDAP kører.
   • **Port** – standard LDAP-porten er 389 (uden SSL). Hvis du vil bruge krypteret forbindelse i din virksomhed, skal du indtaste portnummer 636. Sørg for, at SSL-understøttelse også er aktiveret på LDAP-serversiden. Hvis administratoren angiver et andet portnummer, skal du sørge for, at det også er ændret i Access Commander.
   • **Login-navn** – login-navn for brugeren med rod-/trærettighederne. Indtast login-navnet som "administra- tor@domain.com".
   • **Adgangskode** – LDAP-serverbrugeradgangskode.
   • **Kommunikationssikkerhed (SSL)** – det er unødvendigt at omskrive portnummeret, hvis SSL er deaktiveret. Det er nødvendigt at ændre porten til 636, hvis SSL er aktiveret.
   • **Base DN** – rodpunktet, hvorfra mappesøgningen starter. Det kan være en udvidelse eller en mapperod, for eksempel: CN=administrator, CN=brugere, DC=domæne, DC=com.

   Ved at aktivere TLS aktiverer du TLS (Transport Layer Security) for din FTP-forbindelse. TLS krypterer de data, der overføres mellem Access Commander og serveren. Ved at aktivere TLS-certifikatgodkendelse aktiverer du godkendelse af de TLS-certifikater, der leveres af serveren. Når denne indstilling er aktiveret, kontrollerer Access Commander, at den kommunikerer med en server, der er tillid til, hvilket øger forbindelsessikkerheden.
3. Den indstillede LDAP-forbindelsesdetalje åbnes. Nu kan du teste forbindelsesindstillingerne. Presse Synchronize Now (Synkroniser nu) for at starte engangssynkronisering.
4. Du kan tildele brugerdata til LDAP-serverattributterne på Options (Indstillinger) kort.

   Du kan slette den indstillede forbindelse i den udvidede menu ⋮ på Import kort. Indstil flere synkroniseringsparametre på **Options** (Indstillinger) kort.

Angiv Automatisk synkronisering på kortet **Import**. Aktivering af Automatisk synkronisering, fuldfør synkroniseringsintervallerne. Vælg det minut/klokkeslæt, hvor dataene skal synkroniseres i henhold til den ønskede frekvens

5.2.8.1 Indstillinger for LDAP-synkronisering

Importerede attributter – rediger skemaet for at tildele Access Commander-data-ene til LDAP-serverattributterne.

Brugere fjernet fra LDAP – definer, hvad der skal gøres med de brugere, der er slettet fra LDAP. Du kan beholde eller slette de brugere, der er slettet fra LDAP, i Access Commander. Hvis de brugere, der fjernes fra LDAP, deaktiveres, forbliver deres data i Access Commander, men synkroniseres ikke med enhederne.

Brugere deaktiveret i Active Directory – definer, hvad der skal gøres med de brugere, der er deaktiveret i Active Directory. Access Commander kan ignorere deaktivering eller sletning (deaktivering) af brugere, der er deaktiveret i Active Directory. Når de er gendannet i Active Directory, genindlæses de tidligere slettede brugere i Access Commander.

Gruppesynkronisering – upload gruppetildelinger fra LDAP til Access Commander. Ved at angive et synkroniseringsskema kan du angive et basis-DN og et eget filter, der skal bruges til gruppesynkronisering. Skemaet muliggør synkronisering for indlejrede grupper.

Avatarsynkronisering – indstil upload af brugerfoto fra LDAP-systemet.

Referenceovervågning – indstil, om data fra LDAP-referencerne skal synkroniseres eller ej.

Indlejret søgning – aktiver søgning i hele træet eller, hvis parameteren er deaktiveret, kun roden.

Aktivering af sideinddeling – LDAP bruger sideinddeling til udvidelse af kontrolelementet Enkle sideinddelte resultater. Dette gør det muligt at opdele resultaterne i flere sider, hvilket er nødvendigt for omfattende bibliotekstjenester. Parameteren Page Size (Sidestørrelse) definerer antallet af poster pr. side.

5.2.9 Brugerimport til virksomhed

Den udvidede menu ⋮ i virksomhedsdetaljeoverskriften gør det muligt at importere nye brugere til virksomheden på engangsbasis, enten fra en CSV-fil eller fra en anden 2N-enhed.

5.2.9.1 Brugerimport fra CSV-fil

ⓘ Du kan downloade en CSV-skabelon til import af brugere ved hjælp af dette link.

Access Commander giver brugerne mulighed for at blive uploadet til virksomheden i bulk. Derfor er det muligt at forberede grundlæggende brugeroplysninger på forhånd i en ekstern fil og derefter blot importere brugeren. Brugere i én fil kan kun uploades til én bestemt virksomhed ad gangen.

Denne funktion tillader ikke, at brugerne slettes.

ⓘ Brugere med rollen Administrator kan udføre kompleks, gentagelig synkronisering af brugerlister på tværs af firmaer, se Brugersynkronisering (se afsnit 17.7 side 69).

5.2.9.2 Importer fra 2N-enhed

Du kan overføre brugerlisten fra en 2N-enhed til Access Commander. Import kan kun udføres fra en enhed, der endnu ikke er føjet til Access Commander. Enheden kan ikke indeholde de brugere, der allerede er i Access Commander (dvs. har det samme UUID). Det er muligt kun at importere alle brugere i bulk til en bestemt virksomhed.

1. Det anbefales at sikkerhedskopiere konfigurationen før import. Den Access Commander systemet sikkerhedskopieres i Indstillinger > Sikkerhedskopiering af system. Sikkerhedskopien af enhedskonfigurationen foretages i enhedens webkonfigurationsgrænseflade, i System > Maintenance.
2. Tilføj den enhed, hvorfra du vil importere brugerlisten, til listen over Access Commander Enheder.

ⓘ Tilføj ikke enheder til zoner endnu! Enheden ville tilsidesætte adgangsreglerne, og listen over brugere ville blive omskrevet på enheden.

3. Gå til detaljerne for det firma, som du vil importere brugeren til. Vælg **Import from Device** (Importer fra enhed) fra den ⋮ Avanceret menu.
4. Der åbnes en dialogboks. Vælg den enhed, hvorfra du vil importere brugerlisten, fra rullelisten over tilgængelige enheder.
5. Klik på **Import** for at begynde at importere i baggrunden. Afslutningen af processen er skrevet i Systemlog.
6. Efter vellykket import er det muligt at tilføje enheden til zonerne og inkludere den i adgangsreglerne.

ⓘ Importproceduren fungerer kun for specifikke enhedsbrugere (UUID'er) og importerer alle brugere fra enheden til én virksomhed på én gang.

6 Brugere

Access Commander hjælper dig med at administrere brugere, ændre deres adgange, administrere deres kontaktdata osv.

Brugerlisten indeholder alle de oprettede brugere. Du kan filtrere brugerne over listen eller blot finde en bruger ved navn, e-mail eller telefonnummer.

FLERE-HANDLINGER

Vælg flere brugere, der skal anvendes følgende handlinger på:

- Aktiver overvågning af brugerdeltagelse
- Føj bruger til gruppe
- Fjern bruger
- Indstil tidsinterval for adgangsgyldighed
- Tildel adgangskode til de brugere, der ikke har fået tildelt PIN/QR-kode
- Tildel adgang QR-kode til de brugere, der ikke har fået tildelt PIN/QR-kode
- Tildel mobilnøgle til de udvalgte brugere, der ikke har fået tildelt nogen mobilnøgle

Sørg for, at der er udfyldt en gyldig e-mail-adresse, så brugeren kan tildeles PIN/QR-kode eller mobilnøgle.

1. Gå til **Users** (Brugere) side.
2. Klik på knappen til tilføjelse af bruger i øverste højre hjørne.
3. Udfyld de obligatoriske data: brugernavn og den virksomhed, som brugeren er tilknyttet.
   Den nyoprettede bruger vises på listen, og brugeroplysningerne åbnes. Du kan indstille sådanne andre brugerparametre i detaljerne som brugertelefonnummertildeling, valg af godkendelsesmetode, gruppetildeling osv.

Access Commander giver brugerne mulighed for at blive uploadet til virksomheden i flere. Derfor er det muligt at forberede grundlæggende brugeroplysninger på forhånd i en ekstern fil og derefter blot importere brugeren. Brugere i én fil kan kun uploades til én bestemt virksomhed ad gangen.

Masseimport udføres i virksomhedsdetaljer, se Brugerimport til virksomhed (se afsnit 5.2.9 side 24.

6.1 Bruger-indstillinger

Du kan se og administrere brugeroplysninger i brugeroplysningerne. Klik på det valgte brugerlisteelement på siden Brugere for at åbne brugeroplysningerne.

Brugeroplysningerne er opdelt i fanerne Oversigt, Fremmøde og Ændringslog. Fremmøde vises kun for de brugere, hvis fremmødeovervågning er aktiveret, se Brugerfremmøde (se afsnit 6.2 side 34). Tilstedeværelsesmodulet er tilgængeligt afhængigt af licensen.

6.1.1 Ændring af brugernavn og foto

Find indstillingerne for brugeromdøbning og fotoindstilling i en avanceret menu i ⋮ brugerdetaljeoverskriften. Billedopløsningen justeres automatisk til 432 x 432 px.

6.1.2 Legitimationsoplysninger

Dette kort hjælper dig med at indstille brugergodkendelsesmetoderne på enheder. Brugeren skal godkende sig selv på en enhed, og hvis der gives adgang, får han adgang til enheden.

RFID-kort – tilføj et eksisterende RFID-kort til brugeren. Der åbnes en dialogboks, hvor du kan angive kort-id'et. Det gør du ved at trykke på et kort på USB-læseren eller indtaste kort-id'et via et tastatur. Identifikatoren skal være et hexadecimalt tal med mindst 6 tegn. En bruger kan tildeles op til 2 adgangskort.

ⓘ Brugeradministratoren og administratoren kan se kort-id'et i adgangsloggen. Det nye/ikke-tildelte kort kan således indlæses på en tilgængelig enhed, og derefter kan dets identifikator kopieres fra loggen. Efter at have tilføjet identifikatoren til RFID-kortene, kan brugeren begynde at bruge kortet. Visningen af id'er i adgangsloggen skal være aktiveret i Indstillinger > godkendelse

My2N-app – bruges til sammenkobling med My2N-app-appen, som giver godkendelse via Bluetooth, se Bluetooth-godkendelse (se afsnit 6.1.12 side 31).

PIN-kode – automatisk generering af en 5-cifret PIN-kode.

En bruger kan tildeles en PIN-kode eller en QR-kode, aldrig begge dele på samme tid.

QR-kode – automatisk generering af QR-kode. De enheder, der gør det muligt at læse QR-koder, er inkluderet i Understøttede enheder og applikationer (se afsnit 1.2 side 3.

En bruger kan tildeles en PIN-kode eller en QR-kode, aldrig begge dele på samme tid.

Fingeraftryk – en dialogboks hjælper dig med at registrere fingeraftryk til godkendelse på de enheder, der understøtter fingeraftrykslæsning. Hver bruger kan tilmelde op til 2 fingeraftryk. Se Udskiftninger. Fingeraftryksregistrering (se afsnit 6.1.11 side 31) for detaljer.

Nummerplade – indstil køretøjets nummerplade, der skal scannes af enheden og bruges til brugergodkendelse.

Virtuelt kort – indstil brugerens virtuelle adgangskort-id. Hver bruger kan kun tildeles ét virtuelt kort. Det virtuelle kort-ID er en sekvens på 6-32 tegn: 0-9, A-F. Det virtuelle kort-ID bruges til brugeridentifikation i de enheder, der er tilsluttet via Wiegand-grænsefladen.

Kontaktkode – indstil op til 4 kontaktaktiveringskoder (f.eks. til dørlåsen). Kontaktkoden bruges til døroplåsning via enhedens tastatur selv som en DTMF-kode.

Husk at holde rækkefølgen af autentificeringsmetoder, mens du bruger multifaktorgodkendelse

Det er muligt at sende den genererede adgangskode/QR-kode til en e-mailadresse, hvis den er tilgængelig.

6.1.3 Konto

En bruger kan tildeles adgang til Access Commander-grænsefladen ved at angive et logonnavn og en engangsadgangskode. Ved login kan brugeren følge sin deltagelse (hvis den er tilgængelig) og ændre sin e-mail eller profilbillede. Brugeren vil blive bedt om at ændre adgangskoden ved første login. Hvis der anmodes om tofaktorgodkendelse for en bruger, bliver brugeren bedt om at oprette forbindelse til deres egen godkendelsesapplikation, se Tofaktorgodkendelse (se afsnit 17.13 side 73). Forbindelsen med godkendelsesapplikationen kan også fjernes på dette kort.

På kontokortet kan brugere med logindata tildeles rettigheder til at administrere Access Commander gennem brugerroller. Se Brugerrettigheder (se afsnit 1.1 side 1) for en beskrivelse af rollerettigheder.

6.1.4 Forenklet grænseflade

Det er muligt at køre en forenklet brugergrænseflade for besøgslederen i en virksomhed. Den forenklede grænseflade giver besøgslederen mulighed for at tilføje, fjerne og administrere besøgende. Logfiler og tilstedeværelse kan ikke ses i den forenklede grænseflade. Det primære formål med den forenklede grænseflade er at lette besøgendes adgang til brugernes lejligheder. Alle de besøgende, der oprettes i den forenklede grænseflade, tildeles altid standardgruppen for nye besøgende. Besøgslederen kan ikke ændre denne gruppe. Det er nødvendigt at vælge standardgruppen for nye besøgende i firmaindstillingerne og indstille gyldige regler for adgang til lejligheden for gruppen, herunder stien til lejligheden. Således kan lejlighedsbrugeren administrere godkendelsesmetoderne og besøgets varighed i den forenklede grænseflade.

Før den forenklede grænseflade aktiveres, **skal systemadministratoren indstille standardgruppen for nye besøgende** i Virksomhedsindstillinger (se afsnit 5.1 side 21). Standardgruppen skal tildeles sådanne adgangsregler, der giver besøgende adgang til de påkrævede rum. Ingen besøgende kan garanteres adgang i den forenklede grænseflade uden en korrekt indstillet standardgruppe.

6.1.5 Personlige oplysninger

Bruges til at tilføje grundlæggende oplysninger om brugeren. Brugerens e-mail-adresse, som kontooplysninger skal sendes til, og et brugerkontakttelefonnummer kan tilføjes.

Følgende kan skrives på kortet:

- **E-mail** – adresse, hvortil oplysninger relateret til brugerens konto i Access Commander vil blive sendt;
- **Brugernummer (bruger-id)** – specifik identifikator, der er nødvendig for massesynkronisering med CSV-filen (se Brugersynkronisering (se afsnit 17.7 side 69));
- **Bemærk**.

6.1.6 Adgang

Adgangskortet hjælper med at tildele en bruger til en gruppe og indstille det tidsinterval, hvor brugerens adgangsdata skal være gyldige. Klik ⋮ for at åbne en avanceret menu for at indstille tidsintervallet.

ⓘ Tidsbegrænsninger for adgang fra enhederne indstilles ved hjælp af tidsprofiler

Kortet viser den gruppe, som brugeren er tildelt. Hvis der ikke er tildelt en gruppe, kan der tilføjes en bruger på dette kort. En gruppe kan ændres eller slettes i en avanceret menu ⋮.

6.1.7 Telefonnumre

Dette kort hjælper dig med at oprette forbindelse til en bruger. Telefonnummeret er opkaldsdestinationen for den enhed, der er tildelt brugeren.

Et virtuelt telefonnummer kan bruges til brugeropkald via det numeriske tastatur på enheden. Et virtuelt tal kan indeholde to til fire cifre. Virtuelle numre er ikke relateret til brugernes personlige telefonnumre og hjælper dermed med at skjule brugernes personlige telefonnumre på enheden. En stedfortræder kan også defineres på det kort, som et opkald viderestilles til, hvis brugeren ikke er tilgængelig. Stedfortræderen kan vælges blandt de øvrige brugere i virksomheden.

6.1.8 Adgangslog

Adgangsloggen viser adgangshistorikken.

6.1.9 Skift log

Alle ændringer af brugerindstillinger kan vises i mappen Ændringslog. Grundarrangementet er baseret på ændringstidspunktet. Det er muligt at finde ud af, hvem der har foretaget ændringen i loggen. Klik på rækken for at finde oplysninger om den gennemførte ændring.

6.1.10 Registrering af fingeraftryk

Hver bruger kan tilmelde op til 2 fingeraftryk. Brug en ekstern fingeraftrykslæser til tilmelding. Sørg for, at 2N USB-driver er blevet installeret. Download driveren her.

Det tilmeldte brugerfingeraftryk kan bruges til følgende handlinger:

- Åbn døren;
- Udløs lydløs alarm – kan kun indstilles, hvis funktionen Åbn dør er aktiv;
- F1- og F2-automatisering – genererer FingerEntered-hændelsen i Automation. F1 og F2 hjælper med at skelne mellem den scannede finger i Automatisering.

6.1.11 Registrering af fingeraftryk

1. Sørg for, at USB-fingeraftrykslæseren er aktiveret i Indstillinger > legitimationsoplysninger.
2. Vælg Fingeraftryksgodkendelse i brugerindstillingerne på **Credentials card** (kort) med legitimationsoplysninger.
3. Vælg den finger, der skal scannes og tilmeldes.
   Feltet Fingeraftrykstilmelding vises.
4. Sæt den valgte finger på læseren. Gentag dette trin 3 gange, altid efter invitation.
   Du vil blive informeret om, at dit fingeraftryk er blevet scannet med succes efter den sidste scanning.
5. Klik **Create** for at fuldføre processen.

6.1.12 Bluetooth-godkendelse

Sørg for, at My2N-appen er installeret på din mobiltelefon for at foretage vellykket godkendelse via Bluetooth.

GET IT ON Google Play Download on the App Store

Indtast My2N-appens parringskode for at forbinde applikationen på din telefon med enhederne i Adgangsstyring.

Få parringskoden som følger:

- via en USB Bluetooth-læser, der er tilsluttet din pc
- gennem sammenkobling med enheden

6.1.12.1 Oprettelse af parringskode via pc

1. Download og installer 2N IP USB-driver på din pc.
2. Sørg for, at USB Bluetooth-læseren er aktiveret på kortet Indstillinger > Legitimationsoplysninger > Aktiverede USB-læsere.
3. Tilslut USB Bluetooth-læseren til pc'en.
4. Vælg My2N-appgodkendelse i brugerindstillingerne på Kort med legitimationsoplysninger.
5. Vælg **Pair using reader** (Par ved hjælp af læser) i den åbne dialogboks.
   Parringskoden vises i dialogboksen.
6. Følg nedenstående trin for parring i applikationen.

6.1.12.2 Oprettelse af parringskode ved hjælp af enhed

1. Sørg for, at
   - parringsenheden er indstillet til den givne brugers virksomhed, se Virksomhedsindstillinger (se afsnit 5.1 side 21);
   - parringsenheden er placeret i den zone, som brugeren har adgang til, se Adgangsregler (se afsnit 10 side 47);
   - En passende parringstidsværdi er indstillet, se Virksomhedsindstillinger (se afsnit 5.1 side 21).

2. Vælg My2N-appgodkendelse i brugerindstillingerne på Kort med legitimationsoplysninger.
3. Markere **Pair using reader** (Par ved hjælp af enheder) i åben dialogboks.
4. Den genererede parringskode vises på kortet sammen med den resterende parringstid. Overfør parringskoden til brugeren. Hvis brugerens e-mailadresse er udfyldt, kan du sende mobilnøglen ved at klikke .
5. Følg nedenstående trin for parring i applikationen.

6.1.12.3 My2N Mobile Application Parring

1. Download My2N-applikationen til din mobiltelefon. Appen er tilgængelig på App Store og Google Play.
2. Åbn appen, og indtast parrings-PIN-koden.
3. Tillad alle de vigtige tilladelser for at få My2N til at fungere korrekt. Autorisationerne adskiller sig ikke fra dem for Mobile Key.
4. Følg instruktionerne på din mobiltelefon – bring telefonen tæt på enheden i parringstilstand, og klik på **Start parring**. Efterfølgende begynder mobiltelefonen at søge efter en enhed til parring.
5. Giv adgang til den valgte mobiltelefon. Nu kan du åbne døre på hele stedet.

Brug Mobile Key-applikationen til parring af mobiltelefoner med ældre operativsystemer (Android 9 / iOS 17 og lavere).

Parring af mobilnøgle

1. Download Mobile Key-applikationen til din mobiltelefon. Appen er tilgængelig på App Store og Google Play.

2. Åbn applikationen, og aktiver Bluetooth-adgang for Mobile Key.

3. Afhængigt af mobilnøgletypen skal du trække din mobiltelefon i nærheden af USB-læseren eller parringsenheden.

4. Klik på den enhed, der tilbydes til parring i Mobile Key.

5. Applikationen beder dig om at indtaste PIN-koden. Indtast parringskoden og bekræft.

6.1.13 Brugerrettigheder

Flere brugere kan administrere adgange i Access Commander afhængigt af deres tildelte rettigheder eller privilegier.

Konti med udvidede rettigheder indstilles gennem rollen i brugerindstillingerne. En bruger kan tildeles flere roller.

Brugerrettigheder vedrører administrationen i brugerens virksomhed. Administratoren har adgang til den komplette administration på tværs af virksomhederne.

6.1.13.1 Administrator

- System- og modulindstillinger i henhold til den gyldige licens.
- Ændring af licens.
- Alle rettigheder til andre roller relateret til alle virksomhederne.

6.1.13.2 Adgangsstyring

- Oprettelse og administration af grupper.
- Tilføjelse af brugere til grupper.
- Oprettelse og administration af besøgende.
- Oprettelse og administration af tidsprofiler.
- Indstilling af adgangsregler.

6.1.13.3 Brugeradministrator

- Oprettelse og administration af brugere.
- Oprettelse og administration af besøgende.
- Tilføjelse af brugere til grupper.
- Oprettelse og administration af besøgende.

6.1.13.4 Besøgschef

- Oprettelse og administration af besøgende.
- Administration af besøgstildeling til grupper (ikke tilgængelig i den forenklede grænseflade).
- Visning af besøgendes adgangslog (ikke tilgængelig i den forenklede grænseflade).

6.1.13.5 Dør styring

- Visning af kameratransmissioner fra tildelte enheder.
- Fjernåbning af tildelte enheder.
- Nødlåsning af tildelte enheder.
- Visning af adgangslog for tildelte enheder.
- Overvågning af tilstande og sikkerhedshændelser i systemloggen.

6.1.13.6 Tilstedeværelseschef

- Overvågning og styring af deltagelse af tildelte grupper.
- Visning af adgangslog for brugere i tildelte grupper.

6.2 Brugernes deltagelse

Access Commander hjælper dig med at overvåge brugernes deltagelse. Brugerens ind- og udrejsetider registreres i Fremmødetilstand.

Overvågning af brugerdeltagelse skal aktiveres. Det gør du ved at bruge den udvidede menu ⋮ i brugerdetaljeoverskriften. Hvis du vil aktivere overvågning af fremmøde for flere brugere på samme tid, skal du vælge de brugere, der er angivet på siden Brugere og bruge handling .

Tilstedeværelsesadministratoren kan redigere brugerens tilstedeværelsesdata. Det gør du ved at klikke på det tidsinterval, der skal ændres. Du kan også redigere kanttiderne og tilføje en note til et interval.

Sørg for, at licensen til overvågning af brugerdeltagelse er aktiv i Access Commander for at overvåge fremmøde korrekt. Husk at aktivere tilstedeværelsesovervågning for hver bruger i brugerindstillingerne

Overvågning og redigering af fremmøde er beskrevet i kapitlet Fremmøde (se afsnit 12 side 51).

7 Grupper

En gruppe bruges til at samle brugere og nemmere indstille adgangsrettigheder til gruppemedlemszonen. Rettighederne behøver ikke at være indstillet på bruger-/besøgsniveau, men gruppen kan tilknyttes en zone.

Filtrere listeelementerne ved hjælp af over listen. Eller klik på i hver kolonneoverskrift for at åbne en udvidet menu og angive filtre for hver kolonne. Den udvidede kolonnemenu giver dig også mulighed for at flytte, fastgøre til første/sidste position eller skjule kolonnerne.

7.1 Oprettelse af gruppe

1. Gå til **Groups** side.
2. Klik på knappen til tilføjelse af gruppe i øverste højre hjørne.
3. Angiv gruppenavnet, og tildel gruppen til en virksomhed i den åbne dialogboks.

Når en gruppe er oprettet, kan den overordnede virksomhed ikke ændres.

Den nye gruppe vises på listen, og dens detaljer åbnes. Tilføj gruppemedlemmerne, og indstil deres adgangsregler i gruppeoplysningerne.

7.2 Indstillinger for grupper

Få vist og rediger gruppeoplysningerne i gruppeoplysningerne. Klik på det markerede gruppelisteelement for at åbne gruppeoplysningerne. Detaljerne viser en liste over gruppemedlemmerne og deres adgangsregler.

7.2.1 Medlemmer

Kortet viser alle de brugere, der er tildelt en gruppe. Du kan kun tilføje de brugere/besøgende til gruppen, der er tildelt den samme virksomhed som gruppen.

7.2.2 Regler for adgang

Dette er en oversigt over alle de adgangsregler, du kan redigere eller oprette. Når du opretter en adgangsregel, giver du zoneadgang til en bestemt gruppe. Hvis du vil oprette en regel, skal du angive gruppen og en tidsprofil for at begrænse gruppens zoneadgang.

8 Zoner

Zoner gør det nemmere at administrere adgange til enheder. Zoner kombinerer enheder i logiske sæt. Siden viser en liste over alle zoner.

Filtrere listeelementerne ved hjælp af over listen. Eller klik på i hver kolonneoverskrift for at åbne en udvidet menu og angive filtre for hver kolonne. Den udvidede kolonnemenu giver dig også mulighed for at flytte, fastgøre til første/sidste position eller skjule kolonnerne.

8.1 Aktivering af adgangspunkter

Med åbnes en dialogboks, hvor adgangspunktunderstøttelse kan aktiveres, se Indstilling af enhedsadgangpunkter (se afsnit 12.2.1 side 53).

8.2 Oprettelse af zone

1. Gå til **Zones** side.
2. Klik på knappen til tilføjelse af zone i øverste højre hjørne.
3. Angiv zonenavnet, og tildel zonen til et firma (firmaer) i den åbne dialogboks.
   Den nye zone vises på listen. Føj en enhed til zonen i zonedetaljen eller enhedsdetaljen. Der kan foretages flere indstillinger i zonedetaljerne.

8.3 Zone indstillinger

Se og rediger zoneoplysningerne i zonedetaljerne. Klik på det valgte zonelisteelement for at åbne zonedetaljerne.

8.3.1 Multi-Factor Godkendelse

Du kan indstille multifaktorgodkendelse for alle enheder i en zone. Du kan kun vælge nogle af godkendelsesmetoderne, men altid beholde følgende rækkefølge:

1. My2N app
2. RFID-kort
3. Fingeraftryk
4. PIN-kode

Husk at holde rækkefølgen af autentificeringsmetoder, mens du bruger multifaktorgodkendelse.

Nødvendigheden af multifaktorgodkendelse kan begrænses af en tidsprofil. Med multifaktorgodkendelse slået til vil **Use Multi-Factor Authentivation** (Brug multifaktorgodkendelse) vises, så du kan vælge en tidsprofil ved hjælp af . Hvis *Når som helst* er valgt, vil multifaktorgodkendelse altid være påkrævet.

Multifaktorgodkendelse kan kun kræves for zoneadgang. Denne indstilling gælder kun, hvis der bruges adgangspunkter.

8.3.2 Få adgang til indstillinger

Du kan indstille en masse-PIN-kode til zoneadgang på kortet eller vise PIN-koden, hvis den allerede er oprettet. Desuden kan du aktivere/deaktivere følgende funktioner i Adgangsindstillinger:

Lydløs alarm – når en speciel kode er brugt, aktiveres Lydløs alarm, som sender en alarmrapport. Enheden signalerer ingen alarmlyde i denne tilstand. Indstil den specielle lydløse alarmkode og funktion i enhedskonfigurationen.

Adgangsspærring – efter fem mislykkede forsøg vil det næste forsøg ikke blive tilladt, før der er gået 30 sekunder.

Nummerpladegodkendelse – køretøjer får zoneadgang baseret på deres nummerpladeverifikationer af alle de enheder, der understøtter denne funktion.

8.3.3 Enheder

Kortet viser en liste over alle de enheder, der er tilføjet til den givne zone. Flere enheder kan tilføjes på kortet.

Hvis det bruges, tildeles adgangspunkter til en zone. Adgangspunkttypen for den givne enhed er beskrevet som adgang til zone.

Tilgængelige godkendelsesmetoder vises for hver enhed/adgangspunkt.

8.3.4 Virksomheder

Dette kort viser en liste over de virksomheder, der har fået adgang til zonen. Flere virksomheder kan have adgang til én zone.

8.3.5 Regler for adgang

Dette er en oversigt over alle de adgangsregler, du kan redigere eller oprette. Når du opretter en adgangsregel, giver du zoneadgang til en bestemt gruppe. Hvis du vil oprette en regel, skal du angive gruppen og en tidsprofil for at begrænse gruppens zoneadgang.

Klik på den valgte adgangsregel for at redigere den.

9 Enheder

Siden Enheder viser alle de enheder, der er føjet til Access Commander.

Filtrere listeelementerne ved hjælp af over listen. Eller klik på i hver kolonneoverskrift for at åbne en udvidet menu og angive filtre for hver kolonne. Den udvidede kolonnemenu giver dig også mulighed for at flytte, fastgøre til første/sidste position eller skjule kolonnerne.

Presse **Eksport** over listen for at eksportere listen som en CSV-fil eller udskrive den. Klokkeslættet er GMT+0 i CSV-filen eksporteret fil.

Vælg flere enheder, der skal anvendes følgende massehandlinger på:

- Administrer udvalgte enheder
- Fjern valgte enheder fra administrationen
- Sikkerhedskopier udvalgte enheder

ikonet på enhedsrækken omdirigerer til enhedens web konfigurationsgrænseflade.

ENHEDER TILSTANDE

- Online
- Unmanaged
- Uforenelig
- Offline
  - Login mislykkedes – forkerte logindata er blevet indtastet i enhedens webkonfiguration i Adgangsstyring.
  - Utilgængelig – Access Commander kan ikke oprette forbindelse til enheden.
  - Ugyldigt certifikat – SSL-certifikatbekræftelse er påkrævet, og enheden har ikke noget gyldigt SSL-certifikat.

9.1 Tilføjelse af enhed

1. Gå til **Enheder** side.
2. Klik på knappen til tilføjelse af enhed i øverste højre hjørne.
3. I den åbne dialogboks skal du finde enheden i LAN eller indtaste dens IP-adresse og port i følgende format: "IPaddress:port" .
   Når du har indtastet IP-adressen, kan du trykke på ENTER på tastaturet og tilføje en anden enhed.
4. Når du har tilføjet alle de valgte enheder, skal du udfylde webkonfigurationsadgangskoden til disse enheder. Du kan kun tilføje de enheder på samme tid, som du logger ind på med en og samme adgangskode.
5. Navngiv enheden før oprettelse.
6. De nye enheder vises på listen. Foretag andre indstillinger i enhedsoplysningerne.

9.2 Nødlukning

Nødlåsning bruges til fuldstændig låsning af de døre, der styres af den givne enhed. Under nødnedlukningen er det umuligt at åbne døre ved hjælp af foruddefinerede brugeradgange, selv hvis brugeren/den besøgende bruger en gyldig adgang med en gyldig tidsprofil.

Du kan aktivere/deaktivere nødafspærringen:

- i enhedsdetaljen – lås den givne enhed;
- i zonedetaljen – lås alle enheder i en zone;
- i virksomhedsdetaljen – lås alle enheder i en virksomhed;

- at bruge en global handling ved at trykke på den øverste bjælke for at låse alle enheder i Access Commander;
- i widgetten på dashboardet.

Det er muligt at foruddefinere en gruppe af enheder, der er underlagt nødlåsning, i widgetten til nødlåsning.

Offline-enheder, inaktive enheder, enheder med inkompatibel firmware og enheder med FW-version, der er lavere end 2.32, låses ikke efter anmodningen om nødlåsning. Offlineenheder låses ned, når de bliver tilgængelige igen.

9.3 Konfiguration af enhed

Du kan se og administrere enhedsoplysninger i enhedsoplysningerne. Klik på det valgte enhedslisteelement for at åbne enhedsoplysningerne. I henhold til enhedstypen kan detaljerne opdeles i *Oversigt*, *Opkald* og *Lift*.

Klik på knappen **Configure hardware** (Konfigurer hardware) i øverste højre hjørne af enhedsoplysningerne for at gå fra enhedsoplysningerne til webkonfigurationen. Se konfigurationsmanualen for den valgte enhed for dens konfiguration. Klik på krydset i den blå øverste bjælke for at afslutte konfigurationen web interface og vend tilbage.

9.3.1 Overblik

9.3.1.1 Stat

Dette kort viser forbindelsestilstanden til en enhed. Online-enheder er sådanne enheder, der er forbundet med Access Commander og udstyret med den acceptable firmware. Datasynkronisering kan finde sted takket være den etablerede forbindelse til enheden. Hvis den er inkompatibel, kan firmware tillades i Enheder > firmware.

Automatisk synkronisering startes ved hver ændring, der skal afspejles i slutenhedskonfigurationen. Synkronisering finder kun sted over de enheder, den vedrører. Det er kun de synkroniseringsanmodninger, der skyldes de ændringer, der kan påvirke slutenhederne, der sættes i kø. Sådanne ændringer omfatter ændringer af adgangsrettigheder, telefonnumre, tidsprofiler osv. En navneændring for brugeren, der ikke er tildelt nogen gruppe, starter f.eks. aldrig automatisk synkronisering. Synkroniseringstiden (nødvendig for alle de ændringer, der skal anvendes på slutenheder) afhænger af antallet af enheder, der skal synkroniseres, og mængden af data, der skal uploades til enheden.

9.3.1.2 Adgangskontrol

Indstil den zone, som enheden skal tildeles.

Hvis enheden har konfigureret 2 adgangspunkter, og hvis registrering af adgangspunkt er aktiveret (se Indstilling af enhedsadgangpunkter (se afsnit 12.2.1 side 53)), vises muligheden for at tildele 2 zoner. Et enhedsadgangspunkt kan kun være i én zone.

9.3.1.3 Konfiguration

Kortet viser den aktuelle firmwareversion, MAC-adresse og IP-adresse og giver dig mulighed for at ændre web konfigurationsadgangskode.

På fanen er det muligt at ændre IP-adressen, som enheden er placeret på, hvilket gør det muligt at pege Access Commander på den enhed, der er blevet afbrudt og tilsluttet igen på en anden IP-adresse.

9.3.1.4 Dør kontrol

Dette kort viser billeder fra enhedens kameraer og giver fjernåbning af dørkontakten, der styres af denne enhed. Klik ⋮ for at åbne en avanceret menu for at indstille døråbning i et bestemt tidsrum.

Den aktuelle dørkontakttilstand vises ved siden af knappen **Open** (Åbn).

Brug Emergency Lockdown (se afsnit 9.2 side 40) til at låse døren, selv for grupper med gyldig adgang.

9.3.1.5 Sikkerhedskopi

Backup hjælper dig med at sikkerhedskopiere enhedskonfigurationen i en xml-fil. Start sikkerhedskopieringen ved hjælp af **Start backup** (Start sikkerhedskopiering). Hvis sikkerhedskopien gemmes i det lokale lager, gemmes den i den dedikerede Access Commander-hukommelse. Hvis den er gemt i en fil, åbnes en dialogboks, hvor du kan sikre sikkerhedskopifilen med en adgangskode. Da filen indeholder følsomme data, anbefales filbeskyttelse. Backup-kryptering er tilgængelig på enheder med firmware 2.45 og højere.

Hver sidste sikkerhedskopi vises på fanen. Enheden kan automatisk synkroniseres med den sidste sikkerhedskopi ved hjælp af menuen i **Restore** (Gendan). I rullemenuen i denne menu kan du også vælge at gendanne fra sikkerhedskopien af en anden tilsluttet enhed eller fra en ekstern fil.

Alle tilgængelige enheder (online-enheder og tilsluttede enheder med inkompatibel firmware) kan sikkerhedskopieres.

9.3.2 Opkald

Denne mappe vises i detaljerne på den enhed, hvorfra opkald kan foretages.

9.3.2.1 Telefonbog med berøringsskærm

Brug kortet Kontakter til at administrere telefonbogsskærme på enheder, der er udstyret med en skærm. Kortet viser et træ af kontakter som vist i enhedens bibliotek. Klik på **Change** (Skift) for at åbne en dialogboks til redigering af kontakttræ. Rækkefølgen af kontaktelementerne vises i venstre del af dialogboksen. Kontakterne indstilles i den valgte mappe i højre del. Rodmappen er den første side, der vises, når enhedsbiblioteket åbnes. Alle de kontakter, der er gemt i denne rodmappe, vises på en mappeside. Kontakterne kan også grupperes i mapper, og mapperne kan tildeles rodmappen.

9.3.2.2 Tilføjelse af kontakter til enhedens skærm

1. Gå til Enheder > Enhedsoplysninger > Opkald > telefonbog med berøringsskærm.
2. Klik på **Change** (Skift) for at åbne visningsadministration.
3. Vælg den mappe, du vil tilføje kontakter, i højre del af den åbne dialogboks.
   Du kan føje følgende til mappen:
   1.**Brugere**
   Du kan vælge flere brugere samtidigt.
   2.**Grupper**
   Du kan bruge massetilføjelse til grupper af brugere. Biblioteket viser alle brugere i gruppen under brugernavnet. Du kan vælge flere grupper samtidigt.
   3.**Opkald til grupper**
   Opkaldsgrupper er grupper af kontakter, der skal ringes op samtidigt. Når du opretter en opkaldsgruppe, skal du indtaste det gruppenavn, der skal vises i telefonbogen. Brugerkontakter føjes til opkaldsgrupper på samme måde, som kontakter føjes til mapper.
   Du kan omdøbe en opkaldsgruppe i en udvidet menu i den mappe, der åbnes, ved at klikke på ⋮.
4. Du kan omdøbe en mappe i en udvidet menu i den mappe, der åbnes, ved at klikke på ⋮. Du kan også føje et billede til en valgt mappe i den udvidede menu, som derefter vises i denne mappe på enheden.
5. Fastgør de mapper/opkaldsgrupper, der skal vises første steder i den udvidede menu ⋮ i den givne mappe ved hjælp af 📌.

9.3.2.3 Yderligere virtuelle numre

Det er muligt at starte et udgående opkald ved at ringe til et virtuelt nummer på en enhed med et numerisk tastatur. På dette kort kan du tilføje de brugere, der kan ringes op ved hjælp af virtuelle numre, selvom disse brugere ikke har adgang til enheden. Opkald til de virtuelle numre på de brugere, der har adgang til enheden, tillades automatisk.

Ved udvælgelsen af brugere vises kun de brugere, hvis virtuelle numre er udfyldt.

9.3.2.4 Knapper

Dette kort vises i detaljerne for de enheder, der er udstyret med knapper, der bruges til at ringe til brugertelefonnumre. Kortet Knapper hjælper dig med at tildele brugere til knapperne på enheden. Et tryk på enhedsknappen starter et udgående opkald til destinationen for den tildelte bruger. Brugeren tildeles knappen ved at klikke på og vælge brugeren.

9.3.3 Elevator

For at styre adgangen til gulvliften skal du tilslutte AXIS A9188-relæmodulet til et 2N IP-intercom (2N IP Verso, 2N IP Force, 2N IP Safety, 2N IP Vario) eller til en adgangsenhed. Op til 8 relæmoduler kan tilsluttes et 2N IP-samtaleanlæg eller adgangsanlæg, som hver kan styre op til 8 etager, hvilket giver i alt 64 etager. Sørg for, at licenserne til 2N IP-samtaleanlæg (delnr. 9137916) og adgangsenhed (delnr. 9160401) er aktive for denne funktion.

9.3.3.1 Indstillinger for elevatorkontrol

1. Gå til detaljerne for den enhed, der skal bruges til gulvadgangskontrol. Aktiver løftestyring i den avancerede menu ⋮. **Lift** (Elevator) vises i enhedens detaljer.
2. Gå til ⚙ **hardware configuration** (hardwarekonfiguration) af enheden i enhedsdetaljeoverskriften. Aktiver elevatoradgangskontrolmodulerne i Hardware > Liftkontrol. Hvis modulerne kræver godkendelse, skal du indtaste brugernavn og adgangskode. Gem indstillingerne. Klik på krydset i den øverste blå bjælke for at afslutte konfigurationen.
3. Gå til fanen Løft i enhedsoplysningerne.
4. Vælg relæudgangen for den etage, som der skal indstilles adgang til, på kortet Elevatorgulve. Angiv output(s) som følger: *io_module_relay output*. Klik ✎.
5. Navngiv etagerne og vælg en etagezone, der skal åbnes i den åbne dialogboks. Det er således kun de brugere, der har gyldig zoneadgang baseret på de definerede adgangsregler, der kan få adgang til netop denne etage. Hvis adgangsreglerne ikke skal anvendes, skal du vælge **public access allowed** (offentlig adgang tilladt). Vælg en tidsprofil for at begrænse den offentlige adgang til en tidsperiode, der er defineret af den valgte tidsprofil. Ud over denne tidsprofil vil der kun blive givet adgang til de brugere med gyldig adgang baseret på adgangsreglerne.

ⓘ Hvis adgangen er indstillet i henhold til zoneadgangsreglerne, overtager løfteanordningen ikke nogen af de andre zoneindstillinger (PIN-kode, multifaktorgodkendelse, lydløs alarm osv.)

9.3.3.2 Elevator etager

Hvis den er aktiveret, vises en liste over alle konfigurerbare etager på dette kort. Hver etage har sin betegnelse i rækkefølgen af modulet og relæudgangen. Hver etage kan tildeles sit eget navn.

9.3.3.3 Elevator kontrolmoduler

Dette kort viser alle de tilsluttede AXIS A9188-moduler inklusive deres aktuelle tilstande. Aktiver modulerne i enhedskonfigurationen i Hardware > Lift-kontrol.

9.4 Overvågning

Siden hjælper dig med at finde oplysninger om de tilsluttede enheder. Hver administrator kan konfigurere tabellen efter behov ved hjælp af . Hver konto har en unik opsætning. Vælg de viste kolonner for at foretage indstillingen. Klik på en række for at få vist detaljerne om den valgte enhed.

9.5 Firmware

Firmwaresiden giver en massefirmwareopgradering til alle typer tilsluttede enheder for at holde dem i optimal stand. Du kan afbryde masseadministration af enhederne. Nogle enheder kan eventuelt udelukkes fra masseadministration.

Den aktuelle firmwareversion er tilgængelig online via 2N-opdateringsserveren, og eventuelt kan opgraderingsfilen uploades manuelt. Implementeringen af en ny version er altid underlagt administratorens godkendelse, så hele opgraderingsprocessen er under administratorens fulde kontrol.

Versionen viser en liste over tilsluttede 2N samtaleanlægstyper, 2N telefonsvarer og 2N adgangsenheder i masseadministration.

En ny firmwareversion kan installeres for en eller flere udvalgte enheder i testtilstand, og først derefter kan opgradering tillades for de andre enheder.

9.5.1 Udelukkelse af enhed

Hvis du vil udelukke en enhed fra masseadministration af firmware, skal du føje den til listen i Enheder > firmware > Udeladt Enheder.

9.5.2 Inkompatible firmwareversioner

Når den tilføjes eller opgraderes, går en enhed med inkompatibel firmware i inkompatibel tilstand. Inkompatibel tilstand betyder, at der ikke gemmes nye brugere i enheden. Hændelser kan stadig downloades fra enheden, og dens konfiguration eller backup kan stadig bruges. Der oprettes en ny post i tabellen, og administratoren kan aktivere brugen af inkompatibel firmware.

Access Commander udelukker automatisk en enhed med firmware, der ikke understøttes af den nyeste firmwareversion. Kortet viser disse ikke-understøttede firmwareversioner på de tilsluttede enheder. Se listen over understøttede firmwareversioner nedenfor.

Access Commander kan styre alle de enheder, der bruger en ikke-understøttet firmwareversion, når denne version er godkendt. Godkend versionen i Enheder > firmware > inkompatibel firmwareversion ved hjælp af .

Godkendelse af en ikke-understøttet version kan føre til problemer som datatab eller en form for funktionsfejl.

9.5.2.1 Understøttede firmwareversioner

- 2.45
- 2.44
- 2.43

- 2.42
- 2.41
- 2.40

9.6 Sikkerhed

Når SSL-certifikatbekræftelse er aktiveret, finder synkronisering kun sted på de enheder, der har et SSL-certifikat, der er signeret af et nøglecenter, der er tillid til. Synkronisering af enheder uden sådanne SSL-certifikater er deaktiveret.

For at blive verificeret skal enhedscertifikaterne være signeret af et nøglecenter og indeholde en IP-adresse/domænenavn på enheden. CA-certifikatet skal være pålideligt på den server, hvor Access Commander kører. Enhedscertifikaterne skal uploades via enhedens webgrænseflade (System > Certifikater > Brugercertifikater) og indstilles som HTTPS-servercertifikat i Tjenester > Web Server > Avancerede indstillinger.

Det er umuligt at uploade egne SSL-certifikater til 2N Indoor Touch-enhederne, da forbindelsen til dem vil gå tabt, når certifikatbekræftelse er aktiveret.

9.7 Indstilling af enhedsadgangspunkter

Enhederne (2N samtaleanlæg eller 2N adgangsenheder) kan have op til to adgangspunkter. Hvert adgangspunkt giver mulighed for passage i én retning. Adgangspunkter differentierer passageretningen gennem enheden. Hvert adgangspunkt kan tildeles en eller flere læsere, der er tilsluttet enheden og arbejder i retning af punktet. Adgangspunkter bruges til at optage en zoneind-/udgang. De skal bruges, hvis enheden er placeret på en zonegrænse.

Derudover hjælper adgangspunkter med at overvåge brugerne i Tilstedeværelsesmodulet (se afsnit 14 side 57). Adgangspunkter bruges også til overvågning af ind-/udgange i områderestriktioner (se afsnit 16 side 61).

Adgangspunktindstillingerne i Access Commander overføres til Services > Access Control i enhedens webgrænseflade:

- Adgangspunkt 1 = Adgangsregler
- Adgangspunkt 2 = Udgangsregler

9.7.1 Angive adgangsregler

1. Gå ind i web konfiguration af den valgte enhed.

Klik på listen på siden Enheder for at gå ind i web konfigurationsgrænseflade.

2. Gå til Hardware > udvidelse af moduler.
3. Find det modul, der giver adgangen, der skal bruges som adgangspunkt 1 (Indgang) eller adgangspunkt 2 (Udgang).
4. Indstil den ønskede retning i parameteren Dør, og gem indstillingen.
5. Gå til Zoner i Access Commander.
6. Presse i øverste højre hjørne og aktivere brugen af adgangspunkter.

10 Adgangsregler

Adgangsregler er et overskueligt administrationsværktøj til brugergruppeadgang til zoner. Adgange kan tildeles baseret på tidsprofiler.

Adgangsreglerne definerer TIL HVEM, HVOR og HVORNÅR der gives adgang.

- **WHO** (HVEM) defineres af gruppen og de brugere, der er tildelt den (en bruger kan være i flere grupper, der er tildelt en virksomhed på samme tid).
- **WHERE** (HVOR) er defineret af zonen eller enhederne (en enhed kan kun tildeles én zone).
- **WHEN** (HVORNÅR) er defineret af den tildelte tidsprofil. Dette punkt er ikke obligatorisk. En tom tidsprofil betyder en ubegrænset adgang (24/7).

En gruppe kan have adgang til flere zoner, og flere grupper kan have adgang til én zone.

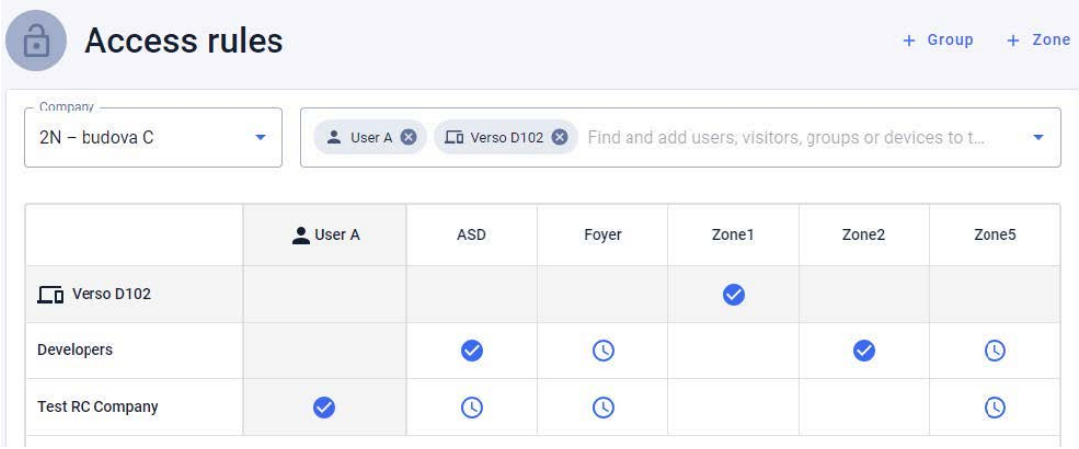
10.1 Matrix-skærm

Matrixvisningen af regler på siden Adgangsregler giver en oversigt over adgange og deres indstillingsindstillinger. Matrixen er tilgængelig for alle eksisterende virksomheder og viser alle de grupper og zoner, der er tildelt den. Administratoren kan skifte virksomhed i menuen over matrixen.

Klik på den celle, der svarer til den valgte zone og gruppe for at indstille gruppeadgangen til zonen. Der vises en menu, hvor du kan vælge enten en ubegrænset adgang eller adgang begrænset af en tidsprofil. Tidsprofilerne skal være forudindstillet på siden Tidsprofiler (se afsnit 11 side 49). En ny gruppe/zone kan tilføjes til virksomhedsmatrixen, hvis det er nødvendigt.

En bruger/enhed kan tilføjes til matrixen i søgefeltet over matrixen. Brugere kan føjes til grupper ved at forene brugeren og gruppen. Enheder kan føjes til en zone ved at forene enheden og zonen.

10.1.1 Eksempel på matrixvisning



Figuren viser en matrixundersøgelse for 2N Telekomunikace. Det fremgår tydeligt af undersøgelsen, at:

- Den filtrerede enhed Verso 2.0 D102 er en del af Zone1.
- Den filtrerede bruger A er en del af Test RC Company-gruppen.
- Brugerne fra Developers-gruppen har ubegrænset adgang til ASD og Zone2, begrænset adgang til Foyer og Zone5 (i henhold til den indstillede tidsprofil) og ingen adgang til Zone1.
- Brugerne fra Test RC Company gruppen har begrænset adgang til ASD, Foyer og Zone5 (i henhold til den indstillede tidsprofil) og ingen adgang til Zone1 og Zone2.

10.2 Regelliste (Rule List)

Siden Rule List (Regelliste) viser en liste over alle de aktuelt gyldige adgangsregler. Klik på en regel for at redigere den. Klik på knappen Tilføj i øverste højre hjørne for at tilføje en ny adgangsregel. Husk at angive regelparametrene, før du opretter en regel.

Regellisten og matrixen viser de samme adgangsregler. En ændring i den ene skærm vil automatisk forplante sig til den anden. Adgangsreglerne redigeres også i zone- og gruppeindstillingerne.

11 Tidsprofiler

Udvalgte enhedsfunktioner kan være tidsbegrænsede. En tidsprofil kan tildeles en valgt funktion for at definere når funktionen er tilgængelig.

Tidsprofiler kan opfylde følgende krav:

- blokere alle opkald til en valgt bruger ud over det indstillede tidsinterval;
- blokere opkald til udvalgte brugertelefonnumre ud over det indstillede tidsinterval;
- bloker brugeradgang ud over det indstillede tidsinterval.

Hver tidsprofil definerer funktionens tilgængelighed baseret på en ugekalender. Du skal blot indstille Fra-Til og angive ugedage for tilgængelighed. Den tidsprofilbaserede adgang defineres af adgangsreglerne. Begrænsning af brugertilgængelighed ud over tidsprofilen indstilles sammen med brugerens telefonnummer.

Eventuelt kan der oprettes op til 20 generelle tidsprofiler, som ud over adgangskontrol kan bruges til særlige lokale konfigurationssager. Disse tidsprofiler uploades til alle synkroniserede enheder.

11.1 Oprettelse af tidsprofil

1. Gå til **Time Profiles** (Tidsprofiler) side.
2. Klik på knappen til tilføjelse af tidsprofil i øverste højre hjørne.
3. Angiv navnet på tidsprofilen i den åbne dialogboks.
4. Vælg **Add time periods** (Tilføj tidsperioder) for tidsbegrænsning. Grønne dage identificerer de dage, der falder ind under tidsprofilen.
   Klik på en dag for at vælge den. Du kan angive et tidsinterval inden for få dage for at definere tidsprofilens gyldighed. Forskellige tidspunkter for hver dag kan ikke indstilles, før tidsprofilen er oprettet.
5. Den nye tidsprofil føjes til listen, og dens detaljer åbnes, så du kan indstille andre parametre. Du kan indstille profilpositionen på enhederne i tidsprofildetaljerne.

11.2 Indstillinger for tidsprofil

Tidsprofiloplysningerne viser en tidsplan for dag og klokkeslæt. Blå intervaller viser, hvornår den givne tidsprofil er aktiv. Du kan indstille en hvilken som helst optælling af tidsintervaller pr. dag.

Klik på timeintervallet, og indstil tidsprofilens aktive tid for at tilføje et interval. Klik på intervallet for at ændre intervallets tidsværdi. For at gøre en profil aktiv hele dagen skal du tilføje et interval, der dækker en hel dag, dvs. 00:00-23:59.

Klik ⋮ for at åbne en udvidet menu for at indstille positionen på en enhed. Positionen på en enhed definerer positionen på tidsprofillisten, som uploades til alle de enheder, der er tildelt tidsprofiler.

Begrænsning af brugertilgængelighed ud over tidsprofilen indstilles sammen med telefonnummeret i brugerindstillingerne.

12 Deltagelse

Access Commander hjælper dig med at overvåge brugernes deltagelse. Brugerens ind- og udrejsetider registreres i Fremmødetilstand.

Indstil fremmøde og dets tilstande i Indstillinger > Konfiguration > fremmøde, se Indstillinger for fremmøde (se afsnit 12.2 side 52).

Sørg for, at licensen til overvågning af brugerdeltagelse er aktiv i Access Commander for at overvåge fremmøde korrekt. Husk at aktivere tilstedeværelsesovervågning for hver bruger i brugerindstillingerne.

Siden Deltagelse indeholder en liste over brugere, hvis deltagelse skal overvåges. Der er et ikon i øverste højre hjørne, som hjælper dig med at downloade en CSV-fil med oversigtsdata for alle brugere. Angiv tidsintervallet for generering af fremmødedata før download.

12.1 Specifik brugerdeltagelse

Vælg en bruger på brugerlisten på siden Deltagelse for at få vist deltagelsesoplysninger for denne pågældende bruger. Listen viser kun de brugere, som tilstedeværelsesovervågning er tilladt for, se Brugere (se afsnit 6 side 27).

Vælg en måned i den øverste del af listen, hvor fremmøde skal vises. Derudover vises den indstillede arbejdstid for den givne måned, saldo og arbejdstimer.

Der er en avanceret menu ⋮ ud for brugernavnet, hvilket gør det muligt at eksportere den givne brugers tilstedeværelsesdata til en CSV/PDF-fil. Begge filer indeholder daglige optegnelser.

Brugerdeltagelse kan også ses i brugeroplysningerne, som er valgt på brugerlisten på siden Brugere (se afsnit 6 side 27).

12.1.1 Ændring af brugerdeltagelse

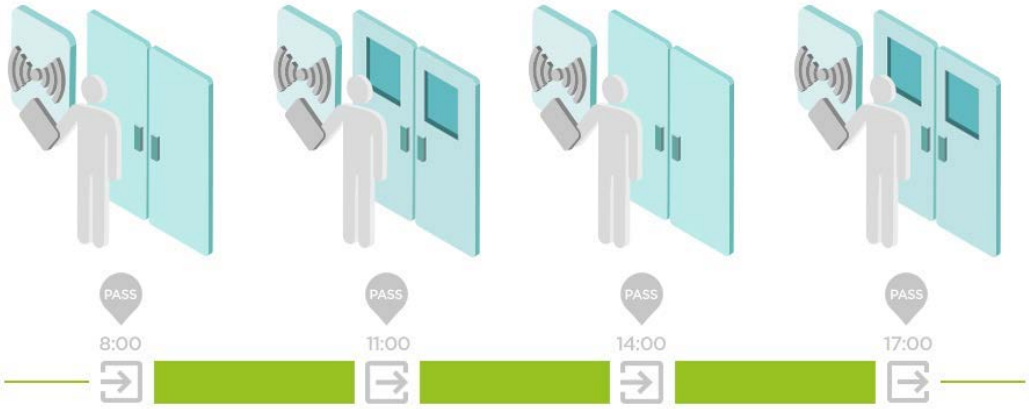
Tilstedeværelsesadministratoren kan redigere brugerens tilstedeværelsesdata. Det gør du ved at klikke på det tidsinterval, der skal ændres. Du kan også redigere grænsetiderne og tilføje en note til et interval.

12.2 Indstillinger for fremmøde

Access Commander hjælper dig med at overvåge brugernes deltagelse. Brugerens ind- og udrejsetider registreres i Fremmødetilstand.

FREMMØDETILSTANDE

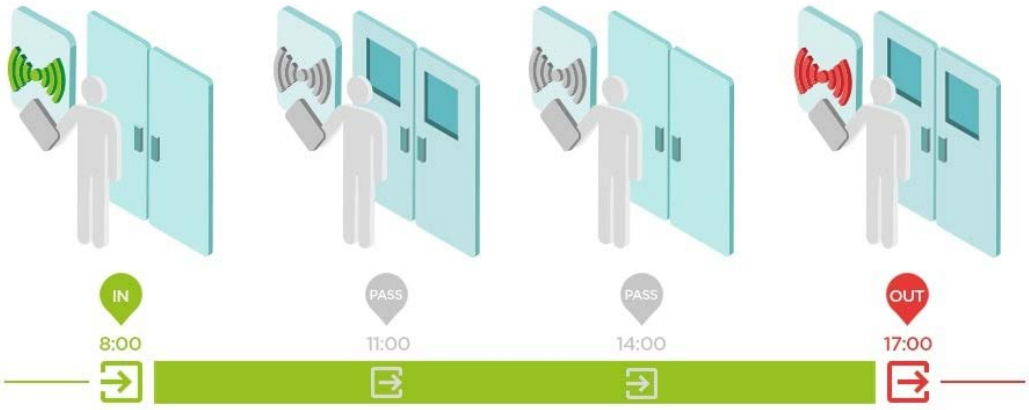
- **FREE** (gratis)



Ankomster/afgange registreres af den første og sidste godkendelse af brugeren på en hvilken som helst enhed på en dag. Tilstedeværelsesmodulet er deaktiveret i denne tilstand.

- **IN-OUT** (ind-ud)

Det er nødvendigt at indstille ankomst- og afgangsenhederne til en korrekt funktion.



- **IN-OUT til alle enheder**

Denne tilstand gør det muligt at overvåge tilstedeværelse. Ankomster registreres på indgangsenhederne, afgange registreres på udgangsenhederne. Færdsel på tværs af zoner registreres ikke som ankomst/afgang.

- **IN-OUT for udvalgte enheder**

Denne tilstand gør det muligt at overvåge tilstedeværelse. Ankomster og afgange registreres på udvalgte enheder, der er indstillet som ind- eller udrejse. Ankomster og afgange registreres kun på disse valgte enheder. Ankomst-/afgangsregistrering kan således kun indstilles for f.eks. bygningens hovedindgang.

12.2.1 Indstilling af enhedsadgangspunkter

Enhederne (2N samtaleanlæg eller 2N adgangsenheder) kan have op til to adgangspunkter. Hvert adgangspunkt giver mulighed for passage i én retning. Adgangspunkter differentierer passageretningen gennem enheden. Hvert adgangspunkt kan tildeles en eller flere læsere, der er tilsluttet enheden og arbejder i retning af punktet. Adgangspunkter bruges til at optage en zoneind-/udgang. De skal bruges, hvis enheden er placeret på en zonegrænse.

Derudover hjælper adgangspunkter med at overvåge brugerne i Tilstedeværelsesmodulet (se afsnit 14 side 57). Adgangspunkter bruges også til overvågning af ind-/udgange i områderestriktioner (se afsnit 16 side 61).

Adgangspunktindstillingerne i Access Commander overføres til Services > Access Control i enhedens webgrænseflade:

- Adgangspunkt 1 = Adgangsregler
- Adgangspunkt 2 = Udgangsregler

12.2.1.1 Angive adgangsregler

1. Gå ind i web konfiguration af den valgte enhed.

Klik på listen på siden Enheder for at gå ind i web konfigurationsgrænseflade.

2. Gå til Hardware > udvidelse af moduler.
3. Find det modul, der giver adgangen, der skal bruges som adgangspunkt 1 (Indgang) eller adgangspunkt 2 (Udgang).
4. Indstil den ønskede retning i parameteren Dør, og gem indstillingen.
5. Gå til Zoner i Access Commander.
6. Presse i øverste højre hjørne og aktivere brugen af adgangspunkter.

13 Besøgende

I Access Commander er det muligt at oprette profiler for de besøgende, der er autoriseret til at komme ind i anlægget i en begrænset periode. En besøgende kan få tildelt et adgangskort og en adgangskode, og den besøgendes køretøjsnummerplade kan registreres. Fremmøde beregnes ikke for en besøgende. Antallet af besøgende er ikke begrænset af nogen licens.

13.1 Indstillinger for opbevaring af besøgsdata

Administratoren kan indstille opbevaringsperioden for besøgsdata. Opbevaringsperioden for besøgendes data indstilles i dage ved at klikke på ikonet ud for knappen Oprettelse af besøgende.

Når tidsintervallet for besøgendes adgang og den forudindstillede dataopbevaringsperiode er udløbet, er de besøgende slettes automatisk ved midnat hver dag. De besøgende, der stadig er tildelt besøgskort, slettes ikke.

Indstillingen kan bruges til at opfylde de lokale databeskyttelsesregler. Den besøgendes navn og note vil blive bevaret i adgangsloggen i henhold til levetidsindstillingen i logadministrationen.

13.2 Oprettelse af besøgende

1. Gå til **Visitors** (Besøgende) side.
2. Klik på knappen til tilføjelse af besøgende i øverste højre hjørne.
3. Udfyld den besøgendes navn, vælg den gruppe, der skal besøges, og indstil besøgets start/slut i den åbne dialogboks. Hvis du ikke fuldfører besøgets start- og sluttidspunkter, starter tidsintervallet for besøgsadgang med det samme og slutter sidst på dagen.

Tidsintervallet for besøgsadgang må ikke være længere end en måned.

4. Før du opretter en besøgende, kan du indstille godkendelsesmetoderne for besøgendes adgang.
   Den nye besøgende vises på listen. Du kan tilføje godkendelsesmetoder og administrere besøgendes adgang i besøgsoplysningerne.

13.3 Afslutning af besøget

Den besøgendes adgangsgyldighed udløber, når tidsintervallet udløber.

Hvis administratoren afslutter et besøg ved at trykke på knappen **End now** (Afslut nu) i besøgsindstillingerne på kortet Adgange, blokeres den besøgendes adgang med det samme. Knappen Afslut er tilgængelig, når en besøgendes adgang er blevet afbrudt automatisk på grund af mulige forskellige tidszoner på enhederne. Det skyldes, at den besøgende kan have en ugyldig adgang på én enhed, men en gyldig adgang på en anden. Dette sker, når der er indstillet forskellige tidszoner for forskellige enheder.

Hvis en besøgende har fået tildelt et besøgskort, vil kortet blive frigivet til en anden besøgende.

13.3.1 Indstillinger for besøgende

Se og rediger de besøgendes oplysninger i besøgsoplysningerne. Klik på det valgte element på listen over besøgende for at åbne oplysninger om besøgende.

ADGANG

Adgangskortet viser den adgangsgruppe og det tidsinterval, hvor den besøgende har en gyldig adgang. Tidsintervallet for besøgsadgang kan nulstilles ved at vælge Forny besøg i den udvidede menu ⋮.

Et besøg kan afsluttes på dette kort, se End of Visit (Afslutning af besøget).

BESØGENDE

Kortet viser personen og virksomheden, der skal besøges. Den person, der skal besøges, kan ændres.

En note kan tilføjes til en besøgende på dette kort.

PERSONLIGE OPLYSNINGER

Kortet viser den besøgendes kontaktdata og gør det muligt at redigere dataene. Den indstillede e-mail gør det muligt at sende godkendelseskoder.

LEGITIMATIONSOPLYSNINGER

En besøgende kan tildeles et adgangskort og en PIN/QR-adgangskode, og den besøgendes køretøjsnummer kan registreres. Der kan kun tilføjes én nummerplade til én besøgende. En besøgende kan tildeles et besøgsadgangskort, se Kort.

Det er muligt at sende den genererede adgangskode/QR-kode til en e-mailadresse, hvis den er tilgængelig. Det tildelte besøgskort kan returneres her.

ADGANGSLOG

Adgangsloggen viser adgangshistorikken.

13.4 Kort

Undersiden Kort hjælper dig med at administrere de adgangskort for besøgende, der er tilgængelige for tildeling. Klik på knappen Tilføj i øverste højre hjørne for at tildele et kort.

Husk at tildele kortene til en virksomhed. Et kort kan kun bruges til de besøgende, der får adgang til denne virksomhed.

Et eksisterende kort kan overskrives eller slettes i den avancerede menu ⋮.

ⓘ Et kort, der er tildelt en aktiv besøgende, kan ikke slettes.

14 Tilstedeværelse

Tilstedeværelsesmodulet er en udvidelse til tilstedeværelsesmodulet og viser listen over aktuelt tilstedeværende

Medarbejdere. Husk at indstille fremmøde IN-OUT-tilstand i Indstillinger > Konfiguration > fremmødekort, se Fremmødeindstillinger (se afsnit 12.2 side 52), for at få modulet til at fungere.

- Hvis ankomst (**IN**-begivenhed) er dagens sidste begivenhed, anses brugeren for at være til stede.
- Hvis en bruger passerer en læser med en uspecificeret retning, ændres brugerzonen. Det samme sker, hvis brugeren passerer læseren i **IN**-tilstand.
- Hvis afrejse (**OUT**-begivenhed) er dagens sidste begivenhed, betragtes brugeren som fraværende.

ⓘ Tilstedeværelsesmodulet fungerer ikke korrekt, hvis FREE (GRATIS) fremmødetilstand er valgt. Den eneste tilstand, der skal vælges, er IN-OUT.

14.1 Udløb af brugertilstedeværelse

Klik på ikonet ⚙ i den øverste højre del for at indstille udløbet af brugertilstedeværelse. Udløb af brugertilstedeværelse angiver automatisk sletning af brugerens tilstedeværelsespost, hvis brugeren ikke registrerer afgangen. Denne timeout udtrykkes i timer og definerer den timeout, hvorefter tilstedeværelsesposten slettes automatisk efter den sidste passage for en nuværende bruger. Denne timeout hjælper med at definere, hvor længe en tilstedeværelsespost kan opbevares i systemet, hvis brugeren ikke betragtes som fraværende. Dette sikrer, at listen over nuværende brugere forbliver opdateret og fri for registreringer af dem, der har forladt bygningen uden at tjekke ud.

15 Rapporter

Oversigtsdata om tilføjede brugere kan downloades fra siden Rapporter. Downloads er i CSV-filen format (kommaseparerede værdier). Filen indeholder altid dato og klokkeslæt for rapportgenerering.

Nogle regnearksprogrammer bruger forskellige separatorer, og CSV-filen afspilles muligvis ikke korrekt i dem. I sådanne tilfælde anbefales det, at CSV-fildataene importeres til en åben projektmappe.

- **My2N-app** – Parrede og ikke-parrede brugere med parringstid tilbage
  Rapporten indeholder statusdata om brugerparring via My2N-appen eller parringskodens gyldighedsdata, hvis det er nødvendigt.
- **Brugere** – Adgangsregler med grupper, zoner, enheder og tidsprofiler
  Rapporten indeholder data om brugertildelinger til grupper, brugeradgang til zoner og zoneenheder og tidsprofiler for brugeradgange. Hver eneste kombination er skrevet på kun én række i tabellen.
- **Brugere** – Detaljeret eksport
  Rapporten indeholder alle de brugeroplysninger, der er udfyldt i brugerprofilerne, herunder brugerens personlige data og adgangsdata.

Filen indeholder følsomme data!

- **Brugere** – eksport af global synkronisering
  Rapporten indeholder data om brugertildelinger til grupper, brugeradgang til zoner og zoneenheder og tidsprofiler for brugeradgange. Hver eneste kombination er skrevet på kun én række i tabellen.
  Denne rapport kan bruges som en CSV-fil til brugersynkronisering, se Brugersynkronisering (se afsnit 17.7 side 69).

Filen indeholder følsomme data!

16 Områdebegrænsninger

Områdebegrænsninger hjælper med at definere de områder, hvor funktionerne Anti-passback og Occupancy/Belægning kan bruges. Disse foranstaltninger øger beskyttelsesniveauet og forhindrer potentielle sikkerhedstrusler. Specifikt hjælper de med at forhindre uautoriseret adgang til udvalgte steder, tillade sporing af folks bevægelser inden for et givet område og registrere ind- og udgange, hvilket kan være nyttigt til overvågning og analyse af sikkerhedshændelser.

Listen viser de områder, der er oprettet i systemet. Du kan oprette og slette områder og åbne deres oplysninger i denne mappe. Du kan også deaktivere et område og få vist dets tilstand.

16.1 Oprettelse af områdebegrænsninger

1. Gå til **Area Restrictions** (Områdebegrænsninger) side.
2. Klik på knappen til tilføjelse af område i øverste højre hjørne.
3. Navngiv området i den åbne dialogboks.
4. Føj en enhed til området i detaljen om det åbne område. Brug knappen i områdedetaljeoverskriften til at tilføje en enhed.
   Det nye område vises på listen. Du kan definere ind- og udgangsenhederne, indstille den tilladte belægning, aktivere Anti-passback og blokere områdeadgang for udvalgte brugere i områdedetaljerne.

16.2 Indstillinger for områdebegrænsning

En ny enhed føjes til området ved hjælp af knappen i områdedetaljeoverskriften.

16.2.1 Ind- og udrejse

Disse kort definerer, hvilke enheder der er ind- og udgangsenheder i det valgte område. Brug den udvidede menu under ⋮ for at flytte enheder mellem kortene eller fjerne dem fra området.

Ved at autentificere brugeren ved indgangsanordningen registreres indgangen til området. Ved at autentificere brugeren på udgangsenheden, forlader brugeren området. Med dette er det muligt at overvåge, om brugeren stadig er i området, og om han ønsker at komme ind i det igen.

Hvis den tilføjede enhed har to adgangspunkter indstillet, kan hvert punkt bruges i en anden retning (Ind-/udgang). Indstillinger for adgangspunkter er beskrevet i kapitlet Indstilling af enhedsadgangspunkter (se afsnit 12.2.1 side 53). Adgangspunktegenskaber udvides ved at klikke på pilen.

16.2.2 Belægning

Det er nødvendigt at indstille ankomst- og afgangsenhederne til en korrekt funktion.

Belægningskortet hjælper med at overvåge og kontrollere antallet af personer i et område. Belægningsbegrænsninger hjælper med at kontrollere antallet af personer i et område. Når belægningsgrænsen er nået, kan yderligere adgang nægtes, eller enhver overskridelse kan kun registreres. Ind- og udgangsanordningerne er nødvendige til denne funktion.

16.2.3 Anti-Passback

Det er muligt at aktivere Anti-passback for områder, hvilket udvider adgangskontrollen til også at omfatte overvågning og misbrug af retten til at komme ind i de forbudte områder. De områder, der skal overvåges, er defineret af grænseanordninger, som gør det muligt at komme ind i eller ud af områderne. Forbipasserende personer kontrolleres for autoriseret adgang på disse enheder i henhold til de definerede regler for områdeadgang. Når brugeren har forladt et område gennem en kantenhed, kan brugeren ikke vende tilbage til området, før timeouten, hvis den er defineret, udløber. Hvis brugeren forsøger at vende tilbage til området tidligere, vil systemet nægte adgang eller kun registrere hændelsen i loggen.

Anti-passback-området ophører med at give mening og kan være potentielt farligt, hvis der er en enhed i området udstyret med en aktiv REX-knap, som giver mulighed for uautoriseret adgang.

16.2.4 Indstillinger for undtagelser

Nogle gange er det ønskeligt, at Anti-passback-betingelserne ikke gælder for udvalgte brugere. Disse brugere omfatter typisk bygningsadministratorer, administrerende direktører, VIP-brugere osv. Indstil de brugere/grupper, der er undtaget fra Anti-passback-betingelserne i Indstillinger > Anti-Passback > Undtagelser.

Afsnittet Indstillinger er kun tilgængeligt for brugeren med administratorrollen.

16.2.5 Liste over blokerede brugere

Blokerede brugere er de brugere, der forsøgte at få adgang til et Anti-passback-område før udløbet af timeout. Brug ✕ for at udelukke en bruger fra listen over blokerede brugere for at give brugeren adgang til området igen.

Ved nægtelse af adgang på grund af aktiv Anti-passback kan brugeren få tilsendt en automatisk informations-e-mail. Aktivér denne e-mail-afsendelse i Indstilling > Anti-Passback > E-mail-meddelelse til blokeret bruger.

16.2.6 Nulstilling af begrænsning

Indstil de dage og tidspunkter i Indstillinger > Anti-Passback > Nulstil områdebegrænsninger, hvor områdeposterne skal slettes, dvs. alle brugere vil kunne bestå uanset deres tidligere overtrædelse af reglerne.

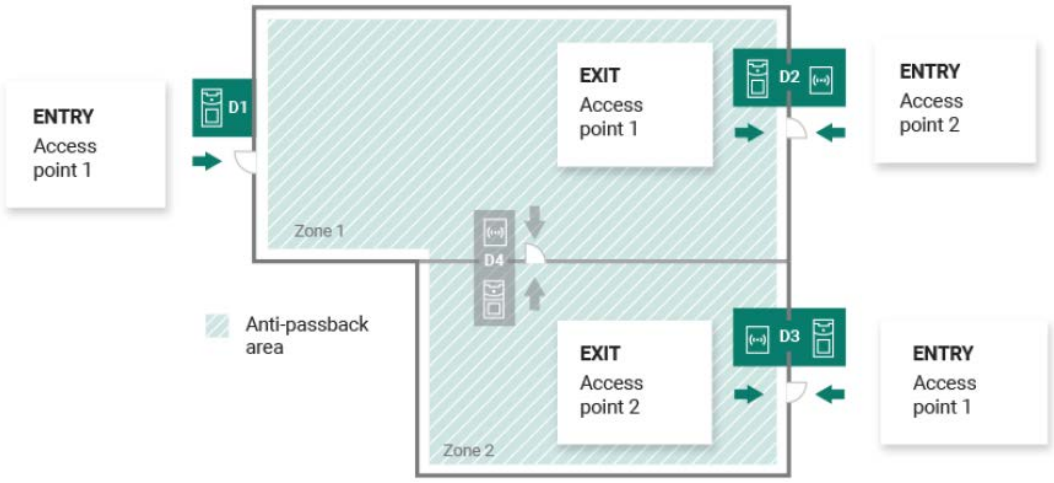
16.3 De mest almindelige opsætningsfejl

Skulle der opstå en fejl i et Anti-passback-område, vil hele området blive deaktiveret og genaktiveret, når fejlen er fjernet.

Følgende tilfælde kan forhindre korrekt anvendelse af områdebegrænsninger.

- Der føjes ingen enhed til APB-området. Tildel mindst én enhed.
- En ind-/udgangsenhed er ikke konfigureret korrekt eller indeholder ikke en læser.
- En APB-områdeindgangsenhed er blevet brugt til at komme ind i et andet område. Rediger tildelingerne for at få funktionen til at fungere korrekt.
- En enhed har ikke den korrekte licens.
- En enhed er blevet deaktiveret.
- En enhed er blevet afbrudt.
- En enhed har en inkompatibel firmwareversion.
  En enhed er udstyret med REX-knappen, der giver brugeren mulighed for at forlade APB-området uden tilladelse. Deaktiver REX-knappen for at få funktionen til at fungere korrekt.

16.4 Eksempel på begrænsningsindstilling



Figuren viser et Anti-passback-område med tre kantenheder D1, D2 og D3. De eneste enheder, der kan indstille Anti-passback-funktionen, er kantenheder. Enhed D4 inde i Anti-passback-området bruges ikke til områdeind-/udgangskontrol. Både ind- og udgangsvejledningen er indstillet for enhederne D2 og D3.

Enhed D1 bruges kun til adgang til Anti-passback-området. Enheden er indstillet som en indgangsenhed.

Enhed D2 bruges både til ind- og udrejse. Enheden har et udvidelsesmodul til indstigning og den indstillede hovedenhed til udgang.

Enhed D3 bruges både til ind- og udkørsel. Enheden har den indstillede hovedenhed til indstigning og et udvidelsesmodul til udgang.

17 Systemopsætning

Dato og klokkeslæt (side 65)
Konfiguration af netværk (side 66)
E-mail (SMTP) aktivering og indstilling (side 66)
Systemopdatering (side 67)
Sikkerhedskopiering af systemet (side 68)
Synkronisering af brugere (side 69)
Aktiverede USB-læsere (side 71)
PICard-nøgler (side 71)
Krypteringsnøgler til My2N-appen (side 71)
CAM-logfiler (side 72)
Overvågede enheder (side 73)
To-faktor-godkendelse (side 73)
Aktiver SSH-adgang (side 74)
Linux-indstillinger (side 74)
Automatisering (side 76)

17.1 Dato og klokkeslæt

Dato og klokkeslæt kan synkroniseres med internettet eller indstilles manuelt i Access Commander. Skift dato/klokkeslæt hentningsmetode i Indstillinger > Konfiguration > kort Server dato og klokkeslæt. Hvis Access Commander er afbrudt fra internettet, skal du indstille dato, klokkeslæt og tidszone manuelt. Hvis du er tilsluttet, skal du skifte til NTP og få tid fra NTP-serveren. I så fald skal du kun indstille tidszonen. NTP-serveren opdaterer automatisk dato og klokkeslæt.

ⓘ Når tidsændringen er gemt, genstarter Access Commander automatisk.

17.1.1 Tidssynkronisering med enheder

Det er muligt at synkronisere enhedens tidsværdier med Access Commander-tiden . Aktivér parameteren Synkronisering af enhedstid i Indstillinger > Konfiguration > Serverdato- og tidskort for at dele tid med enhederne.

Når tidssynkronisering med enheder er slået til, skal du vælge en af følgende synkroniseringsmetoder:

- **Enheder bruger samme NTP-server** – enhedstiden adlyder den NTP-server, der er angivet i Access Commander.
- **Enheder bruger Access Commander som NTP-server** – enhedens tid synkroniseres med Access Commander-tiden.

17.2 Konfiguration af netværk

Indstil netværksforbindelsen i Indstillinger > Konfiguration > netværkskort. Netværkskortet viser og hjælper med at indstille de aktuelle parametre for Access Commander. Husk at aktivere manuel konfiguration, før du indstiller parametrene.

Konfigurationsmetoderne omfatter indstilling af netværksparametrene automatisk fra DHCP-serveren eller manuelt. Når den automatisk indstillede IP-adresse fra DHCP ændres til en manuelt indstillet IP-adresse, foretages omdirigering til den manuelt indtastede IP-adresse i web browser. Efter omdirigering genstartes Access Commander, og systemlogin er påkrævet.

- Ved at ændre konfigurationsmetoden til DHCP ændrer du serverens IP-adresse og kan forårsage forbindelsesafbrydelse.
- Hvis du ændrer HTTP-proxyserveren, genstarter Access Commander automatisk.

17.3 E-mail (SMTP) aktivering og indstilling

E-mail-funktionen hjælper dig med at sende meddelelser eller få adgang til adgangskoder til brugere. E-mails sendes ved hjælp af SMTP.

Indstil funktionen i Indstillinger > konfiguration > e-mail-kort.

1. Når e-mail-funktionen er slået til, åbnes en dialogboks, hvor du kan indstille følgende parametre:
   - **SMTP-serveradresse**, hvortil e-mails skal sendes.
   - **Serverport**, forudindstillet til 25.
   - **Brugernavn og adgangskode til SMTP**-serverkontoen, hvis SMTP-serveren kræver godkendelse.
   - Standard afsenderadresse, hvorfra e-mails skal sendes.
2. Tænd om nødvendigt:
   - **SSL** til e-mail-kryptering;
   - **Bekræftelse af SSL-servercertifikat;**
   - **Legacy Mode** i tilfælde af forbindelse til ældre SMTP-servere, der ikke understøtter nye funktioner (GSSAPI).
3. Når du har gemt, kan du indstille **Basisadresse for e-mail-links**, som vil være en del af de sendte e-mails og henvise til en udvalgt del af Access Commander grænseflade på e-mail-kortet.
4. Send en test-e-mail for at kontrollere indstillingerne.

17.4 Installationsnavn

Navnet på den pågældende Access Commander-installation vises i webgrænsefladens overskrift for alle de brugere, der er logget på. Du kan ændre standardnavnet på Access Commander, f.eks. til adressen på den bygning, som den pågældende installation administrerer.

Skift navnet i Indstillinger > Konfiguration > Installationsnavn. Ved at ændre navnet kan du adskille flere installationer, hvis de administreres af én person. Installationsnavnet skrives også ind i de e-mails, der sendes til virksomhederne.

17.5 Systemopdatering

Access Commander kontrollerer opdateringsserveren og informerer regelmæssigt om tilgængelige opdateringer og nye firmwareversioner til de tilsluttede enheder. Du kan deaktivere automatisk opdateringskontrol i Indstillinger > Systemopdateringskort.

17.5.1 Installation af opdatering til Access Commander

⚠ *Det anbefales, at der foretages en sikkerhedskopi af systemet (se afsnit 17.6 side 68) før opdatering. Udfør sikkerhedskopieringen uden for arbejdstiden for at undgå midlertidig systemutilgængelighed for brugerne.*

1. Gå til Indstillinger > systemopdateringskort.
2. Hvis Automatisk opdateringskontrol er deaktiveret, skal du klikke på **Check for Updates** (Søg efter opdateringer).
3. Klik på **Download** i meddelelsen om tilgængelighed af opdateringer, og bekræft overførslen.
   Kortet informerer om, at opdateringen er klar til installation.
4. Klik på **Install** (Installer) i informationsmeddelelsen, og bekræft installationen i den åbne dialogboks.
   Når installationen starter, vil du blive omdirigeret til siden Vedligeholdelse. Siden Vedligeholdelse informerer den administrator, der startede installationen, om de igangværende installationstilstande. De andre brugere får oplysninger om, at opdateringen er i gang. det er umuligt at logge ind på Access Commander under installationen.
5. Når installationen er fuldført, skal du klikke på **Go to login** (Gå til login) for at komme til login-siden.

17.5.2 Beta-test

Brugeren kan vælge at deltage i betatest af Access Commander-softwareopdateringerne, før opdateringerne udsendes officielt. Aktivér dette i Indstillinger > Systemopdateringskort > Opdateringsserverparameter.

⚠ *Testfunktionerne er ikke garanteret, og 2N TELEKOMUNIKACE a.s. kan ikke holdes ansvarlig for eventuelle funktionalitetsbegrænsninger og potentielle skader, der opstår som følge af funktionsbegrænsninger i betaversionen. Betaversionerne leveres udelukkende til testformål. Betaversionen er ikke beregnet til arbejde med vigtige data.*

Når betaversionerne er aktiveret, vises de i tilgængelige opdateringer på systemopdateringskortet.

⚠ *Når Access Commander er opdateret til den nyeste betaversion, kan der ikke foretages nedgradering til den tidligere version.*

17.6 Sikkerhedskopiering af systemet

Du kan udføre, indstille og kontrollere Access Commander-datasikkerhedskopiering og -gendannelse i Indstillinger > System Backup-kort. Data kan gemmes på det lokale lager eller Server Message Block (SMB). SMB er velegnet til langvarig opbevaring af sikkerhedskopier.

Sikkerhedskopiering af data kan udføres én gang eller automatisk i forudindstillede periodiske intervaller.

Hver sikkerhedskopi kan gendannes, downloades eller fjernes i en menu, der åbnes ved at klikke på ⋮ på sikkerhedskopilisten.

17.6.1 Engangs sikkerhedskopiering af data

1. Gå til Indstillinger > System Backup-kort.
2. Klik på **Back Up Now** (Sikkerhedskopier nu) i den nederste del af kortet.
3. Vælg, om du vil bruge datakryptering eller ej. Hvis det er tilfældet, skal du udfylde den adgangskode, der skal indtastes til sikkerhedskopiering.

17.6.2 Indstillinger for automatisk sikkerhedskopiering af data

1. Gå til Indstillinger > System Backup-kort.
2. Klik ✎ ved parameteren Periodisk sikkerhedskopiering.
3. Indstil de nødvendige backupparametre:
   - Frekvens – periodisk backup-interval
   - Tid – backup-tid
   - Dag – dag i en uge/måned til backup
4. Vælg, om du vil bruge datakryptering eller ej. Hvis det er tilfældet, skal du udfylde den adgangskode, der skal indtastes til sikkerhedskopiering.
5. Gem indstillingerne for at få sikkerhedskopier til at blive udført automatisk som indstillet.

17.6.3 Indstillinger for SMB-sikkerhedskopiering af data

1. Gå til Indstillinger > System Backup-kort.
2. Klik ✎ ved parameteren Storage.
3. Vælg lagertype: SMB.
4. Udfyld serveradressen, login-data og protokolversion.
5. Gem indstillingerne for at få sikkerhedskopierne sendt til den forudindstillede servermeddelelsesblok.

17.6.4 Gendannelse af sikkerhedskopiering af data

1. Gå til Indstillinger > System Backup-kort.
2. Åbn den udvidede menu ⋮ på den valgte sikkerhedskopi, og vælg ⟲ Genskabe.

17.6.5 Gendan fra sikkerhedskopifil

1. Gå til Indstillinger > System Backup-kort.
2. Klik på **Restore from file** (Gendan fra fil) i den nederste del af kortet.
3. Vælg sikkerhedskopifilen fra dit lager, og klik på **Restore** (Genskabe).

17.6.6 Dataoverførsel fra en anden Access Commander

1. Gå til Indstillinger > System Backup-kort.
2. Klik **Migrate** (Overflytte) i den nederste del af kortet.
3. Indtast Access Commander IP-adresse, hvorfra dataene vil blive overført.
4. Udfyld administratorkontoens logindata for Access Commander hvorfra dataene vil blive overført.

Sørg for, at SSH-tjenesten er aktiveret på Access Commander , hvorfra data skal overføres, for at importere dataene.

17.7 Synkronisering af brugere

Brugerlisten inklusive de grundlæggende brugerindstillinger og virksomheds-/gruppetildelinger kan synkroniseres ved hjælp af en eksternt opbevaret CSV-fil.

Synkroniser i Indstillinger > Brugersynkronisering. Download en CSV-skabelon fra kortet (på forhånd menu ⋮).

Download den aktuelle brugerliste, der matcher CSV-skabelonstrukturen, på Rapporter (s. 54).

Den forberedte CSV-fil kan importeres direkte på kortet. Fildata begynder at synkronisere automatisk med Access Commander.

Se systemloggen for detaljerede oplysninger om hvert synkroniseringsresultat. Logfilen informerer om, hvorvidt synkroniseringen var vellykket eller ej. Klik på ikonet i slutningen af rækken for at downloade en detaljeret informationsfil.

17.7.1 Automatisk brugersynkronisering med FTP

Brugersynkronisering i Indstillinger hjælper dig med at forbinde Access Commander med FTP-lageret, hvor CSV-filen med brugerlisten er gemt. Kortet viser derefter oplysninger om dette FTP-lager.

1. Klik ✎ i parameteren Storage.
2. Angiv den FTP-serveradresse, som CSV-filen er gemt på, i dialogboksen Åbn
3. Ved at aktivere TLS aktiverer du TLS (Transport Layer Security) for din FTP-forbindelse. TLS krypterer de data, der overføres mellem Access Commander og serveren. Ved at aktivere TLS-certifikatgodkendelse aktiverer du godkendelse af de TLS-certifikater, der leveres af serveren. Når denne indstilling er aktiveret, kontrollerer Access Commander , at den kommunikerer med en server, der er tillid til, hvilket øger forbindelsessikkerheden.
4. Indtast FTP-serverens logindata.

17.7.2 CSV-fil

Nogle regnearksprogrammer bruger forskellige separatorer, og CSV-filen afspilles muligvis ikke korrekt i dem. I sådanne tilfælde anbefales det, at CSV-fildata importeres til en åben projektmappe. Klik her til tom testfil

Behold altid CSV-filstrukturen. Alle værdierne er adskilt med et komma, gruppelisten er adskilt med et semikolon. CSV-filstrukturen er som følger:

- **EmployeeID** – primær nøgle, der skal opfyldes hver gang. Det er en unik brugeridentifikator.
- **Brugernavn** – navnet på den bruger, der er oprettet i Access Commander.
- **Firma** – navnet på den virksomhed, som brugeren er tilknyttet. Sørg for, at virksomheden er oprettet i Access Commander. De små og store bogstaver, der anvendes i virksomheds-/koncernnavnene, er ikke udskiftelige.
- **Bruger-e-mail** – bruger-e-mail-adresse.
- **Kortnumre** – brugerkort-id. Der kan indstilles op til to kort pr. bruger. Kort-id'erne skal adskilles med et semikolon (;).
- **Skift kode** – skift kode; Koden er altid indstillet til Switch 1.
- **Telefonnummer 1** – telefonnummer til position 1.
- **Gruppeopkald** – gruppeopkald til ovenstående udfyldte telefon.Værdierne er Sand/Falsk.
  Hvis Sand er valgt, aktiveres gruppeopkaldet. Hvis Falsk er valgt, deaktiveres gruppeopkaldet.
- **Telefonnummer 2** – telefonnummer til position 2.
- **Gruppeopkald** – gruppeopkald til ovenstående udfyldte telefon.Værdierne er Sand/Falsk. Hvis Sand er valgt, aktiveres gruppeopkaldet. Hvis Falsk er valgt, deaktiveres gruppeopkaldet.
- **Telefonnummer 3** – telefonnummer til position 3.
- **Virtuelt nummer** – brugerens virtuelle nummer.
- **Grupper** – liste over de grupper, som brugeren skal tildeles. Sørg for, at alle grupperne er oprettet i Access Commander. Gruppelisten er adskilt med et semikolon. De små og store bogstaver, der anvendes i virksomheds-/koncernnavnene, er ikke udskiftelige.
- **Slettes** – brugeren bør/bør ikke slettes. Hvis FALSK er valgt, oprettes brugeren, og dens data opdateres kun ved næste synkronisering. Hvis TRUE er valgt, slettes brugeren ved næste synkronisering. Hvis FALSK er valgt, gendannes brugeren.
- **Nummerplader** – nummerplader. Der kan indstilles flere nummerplader, adskilt med et semikolon.

17.8 Aktiverede USB-læsere

USB-læsere, der er tilsluttet pc'en, og som bruges til at få adgang til Access Commander, kan gøre det lettere at overføre visse brugergodkendelsesmetoder. Husk at aktivere læserne i Indstillinger > legitimationsoplysninger > aktiverede USB-læsere i Access Commander.

Klik på **Allow readers** (Tillad læsere) at åbne en dialogboks for at aktivere/deaktivere brugen af en ekstern USB-enhed. Klik derefter på **Change** (Skift) for at redigere aktiveringen.

Access Commander giver dig mulighed for at bruge følgende USB-enheder:

- 125 kHz RFID-kortlæser – varenr. 9137420E, AXIS varenr. 01399-001
- 13.56 MHz og 125 kHz RFID-kortlæser – varenr. 9137421E, AXIS varenr. 01400-001
- Fingeraftrykslæser – Varenummer 9137423E, AXIS Varenummer 01401-001
- Ekstern USB Bluetooth-læser (dongle) – Vare nr. 9137422E, AXIS Varenummer 01402-001

17.9 PICard-nøgler

Krypteringsnøglerne til 2N PICard Commander gemmes på kortet Indstillinger > legitimationsoplysninger > PICard Keys. Hvis krypteringsnøglerne er blevet overført til Access Commander, vises PICard Commander-projektnavnet og det numeriske id for nøgleeksport på kortet. Kortet gør det muligt at slette de krypteringsnøgler, der er uploadet til Access Commander.

Når PICard-nøgler er fjernet, vil alle kort, der er krypteret ved hjælp af disse nøgler, ophøre med at fungere.

17.9.1 Import af PICard-krypteringsnøgle

1. Klik på **Import** (Importer) for at uploade filen med krypteringsnøgler fra dit lager.
2. Indtast adgangskoden til filbeskyttelsen, hvis den er indstillet under eksport fra PICard Commander.

PICard Commander er et softwareprogram, der bruges til kryptering af logindata på adgangskort. Applikationen opretter projekter, der genererer et sæt krypterings- og læsenøgler. Læsetasterne kan importeres til 2N-enheder eller Access Commander til distribution til de tilsluttede 2N-enheder.

17.10 Krypteringsnøgler til My2N-appen

Brugere kan bruge My2N-appen til forbindelse med 2N-enhederne. My2N-appen – enhedskommunikation er altid krypteret. My2N-appen kan ikke godkende en bruger uden at kende krypteringsnøglen. Den primære krypteringsnøglen genereres automatisk ved intercoms første lancering og kan genereres manuelt når som helst senere. Sammen med AuthID overføres den primære krypteringsnøgle til den mobile enhed til parring.

My2N-appen – enhedskommunikation er altid krypteret. My2N-appen kan ikke godkende en bruger uden at kende krypteringsnøglen. Den primære krypteringsnøgle genereres automatisk ved intercoms første lancering og kan genereres manuelt når som helst senere. Sammen med AuthID overføres den primære krypteringsnøgle til den mobile enhed til parring.

Du kan generere op til 4 krypteringsnøgler i Indstillinger > legitimationsoplysninger > krypteringsnøgler til My2N-appen. Den genererede nøgle uploades automatisk til My2N-appen ved første brug af mobiltelefonen med den enhed, der tidligere er parret. Når du forsøger at generere den femte tast, advarer Access Commander dig om, at den ældste nøgle fjernes. Kortet viser genereringstiden for hver nøgle.

Hvis My2N-appen ikke har adgang til nogen af de gyldige krypteringsnøgler, kan applikationen ikke bruges til brugergodkendelse. For at gendanne funktionen skal du parre applikationen igen med den enhed, der er tilsluttet Access Commander, hvilket resulterer i upload af de gyldige krypteringsnøgler til My2N-appen.

ⓘ Adgangen til enheden afhænger af den givne brugers adgangsrettigheder.

17.11 CAM-logfiler

CAM-logfiler bruges til automatisk optagelse af flere billeder før og efter en valgt hændelse. Du kan administrere forskellige typer hændelser i Indstillinger > CAM-logfiler, som CAM-logfiler skal genereres for.

CAM-logfiler kan f.eks. genereres, når et kort swipes. Således vil 5 snapshots før kortstrygningen og 3 snapshots efter kortstrygningen blive registreret i adgangslogfilerne. Billederne er taget i

1 sekunds intervaller. Der er oprettet et lager på størrelsen 1, 3 eller 5 GB til snapshots. Når lageret er fuldt, slettes de ældste snapshots. Adgangslogfilerne slettes ikke.

17.11.1 Oprettelse af CAM-logtype

1. Gå til Indstillinger > CAM-logfiler.
2. Klik på knappen Tilføj i øverste højre hjørne af siden.
3. Angiv navnet på CAM-loghændelsestypen.
   Den nye CAM-loghændelsestype vises på listen, og dens oplysninger åbnes i CAM-loggen. Indstil de hændelser og enheder, som kamerabillederne skal genereres for, i CAM-logoplysningerne.

17.11.2 Indstillinger for CAM-log

Du kan administrere oplysninger om CAM-logtypen i CAM-logoplysningerne. Klik på det valgte CAM-loglisteelement for at åbne CAM-logoplysningerne, eller oplysningerne åbnes, hver gang der oprettes en ny CAM-log.

17.11.3 Overvågede hændelser

Kortet hjælper dig med at vælge en liste over begivenheder, hvor kamerabilleder skal tages. De overvågede hændelser kan være som følger:

ADGANGE

- Bruger accepteret
- Køretøjets nummerplade anerkendt
- Bruger nægtet
- REX-knap trykket ned

SIKKERHED

- Tamper kontakt aktiveret
- Uautoriseret døråbning
- Fjernbetjent døråbning
- Adgang nægtet – gentagne forkerte indtastninger
- Lydløs alarm aktiveret

17.12 Overvågede enheder

Det anbefales, at CAM-logfiler kun optages fra en enhed udstyret med et kamera. Vælg en enhed i en dialogboks, der åbnes ved hjælp af . Samtidig tillader kortet, at CAM-logoptagelsen fra alle enheder aktiveres.

17.13 To-faktor-godkendelse

Tofaktorgodkendelse giver et højere sikkerhedsniveau for Access Commander-brugerkontoen. For at logge ind indtaster brugeren login-dataene og skal bekræfte login ved hjælp af et godkendelsesprogram. Når administratoren slår tofaktorgodkendelse til, bliver brugeren bedt om at forbinde brugerkontoen med sit eget godkendelsesprogram ved næste login.

Administratoren indstiller tofaktorgodkendelse i Indstillinger > konfiguration > tofaktor-godkendelse. Administratoren kan vælge, hvilke brugere der skal blive bedt om at bruge to-faktor-godkendelse.

17.13.1 Muligheder for anmodning om to-faktor-godkendelse

- **Valgfrit**
  To-faktor-godkendelse er frivillig. Brugere kan aktivere tofaktorgodkendelse i deres profiler.
- **Obligatorisk for bruger med rolle**
  Hver bruger, der har fået tildelt en rolle, skal bekræfte login ved hjælp af et godkendelsesprogram.
- **Obligatorisk**
  Alle brugere skal bekræfte deres logins ved hjælp af et godkendelsesprogram.

17.13.2 To-faktor-godkendelse aktiveret

Hvis administratoren indstiller valgfri tofaktorgodkendelse, aktiverer du selv totrinsgodkendelse på følgende måde:

1. Klik på brugerbilledet i øverste højre hjørne for at åbne brugermenuen.
2. Vælg Vis profil.
3. Forbind kontoen med godkendelsesapplikationen på tofaktorgodkendelseskortet. Følg vejledningen i guiden.

17.14 Aktiver SSH-adgang

SSH-adgangsaktivering anbefales kun til erfarne brugere. Enhver forkert brug udgør en sikkerhedsrisiko.

Indstillinger > Konfiguration > SSH-kort bruges til Secure Shell-aktivering, som giver sikker fjernkommunikation med systemkonsollen. Den aktiverede SSH-tjeneste giver sikkerhedskopiering og gendannelse af systemet eller fuld genstart af Access Commander.

SSH-klienten skal kende Access Commander-IP-adressen og root-brugeradgangskoden for at oprette forbindelse til Access Commander Box eller den virtuelle maskine. System-root-brugeradgangskoden kan indstilles i Indstillinger > konfiguration > SSH-kort.

Root-brugeradgangskoden ændres i konfigurationskonsollen, ikke via Access Commander.

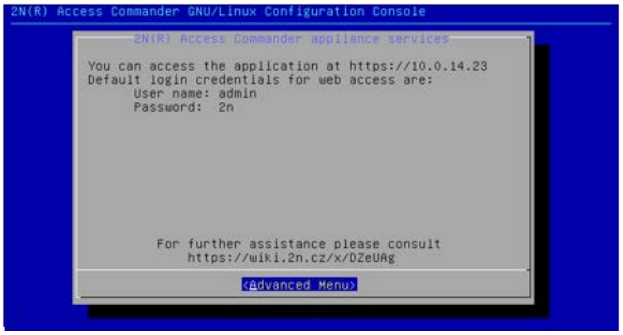
SSH-adgangen kan også aktiveres og administreres direkte i Linux-konfigurationskonsollen, se Linux Indstillinger.

17.15 Linux-indstillinger

De grundlæggende systemindstillinger kan foretages via en Linux-konfigurationskonsol.

Hvis Access Commander distribueres via en virtuel maskine, er det muligt at oprette forbindelse til Linux-version eksternt via SSH-forbindelse.

Konfigurationskonsollen åbnes ved at logge ind på Access Commander ved hjælp af root-kontoen. Den indledende side viser grundlæggende oplysninger om administratorens adgang til webgrænsefladen og omdirigerer til menuen Avanceret.



Følgende kan indstilles i menuen Avanceret

- **Netværk**
  Indstil indstillingerne for proxyserver, netværksegenskaber og DHCP-serversynkronisering.
- **Tid**
  Indstil tiden manuelt, indstil NTP-serveren og tidszonen.
- **SSH**
  Indstil fjernadgang til Access Commander via SSH. Sørg for, at SSH-aktiveringsadgangskoden er forskellig fra standardadgangskoden og opfylder SSH-kravene.
- **SMB**
  Aktivér guiden til forbindelse til delte mapper. Indstil IP-adressen/domænenavnet og

stien til mappen. Fx.: 192.168.1.1/aktie. Indstil brugernavnet for mappeadgang og skriverettigheder. Udfyld brugeradgangskoden, og vælg Samba-protokolversionen. Når alle de obligatoriske parametre er indstillet, kontrolleres serverforbindelsen, og oplysningerne om vellykket/forkert vises.

- **Adgangskode**
  Skift systemroot-brugeradgangskoden for konsollogin eller adgang via SSH.

Root-brugeradgangskoden ændres i konfigurationskonsollen, ikke via Access Commander.

- **Sikkerhedskopiering og gendannelse**
  Du kan importere data og konfiguration, indstille gentagen sikkerhedskopiering og gendanne fra tidligere sikkerhedskopiering.

17.16 Automatisering

Automatiseringsfunktionen er tilgængelig i 2N Access Commander fra firmwareversion 3.2 under licenserne Advanced, Pro og Unlimited. Denne tilføjelse er bygget på Node-RED-platformen og tilbyder direkte omfattende flowbaserede programmeringsfunktioner til Access Commander. Det giver brugerne mulighed for at forbinde Access Commander med forskellige tredjepartssystemer og automatisere brugerdefinerede arbejdsgange baseret på begivenheder inden for platformen.

For at udnytte dette alsidige automatiseringsværktøj fuldt ud er det nødvendigt at huske på følgende:

- **Kundeansvar for sikkerhed**: Brugere er ansvarlige for at sikre, at deres automatiseringskonfigurationer og arbejdsgange er sikre og i overensstemmelse med bedste praksis for cybersikkerhed. Dette omfatter sikring af Node-RED-miljøet, korrekt administration af tilladelser og beskyttelse af følsomme data i deres automatiseringer.
- **Brug af REST API-noden**: Hvis den ikke bruges korrekt, kan denne node føre til tab af data eller uforudsete ændringer. Det er brugerens ansvar at sikre, at noden er konfigureret og implementeret korrekt. Vær forsigtig og dobbelttjek dine indstillinger for at undgå potentielle risici for dine data.
- **Tredjepartsnoder og tilføjelser**: 2N Telekomunikace er ikke ansvarlig for brugen eller integrationen af tredjepartsnoder, tilføjelser eller brugerdefinerede ændringer til Node-RED i automatiseringsfunktionen. Kunder bør nøje evaluere og sikre sikkerheden og stabiliteten af eventuelle yderligere komponenter, de vælger at installere. Eventuelle problemer, der opstår som følge af tredjepartsudvidelser, skal løses af kunden eller den respektive tredjepartsudbyder.
- **Tekniske supportbegrænsninger**: Selvom vores supportteam vil hjælpe med problemer relateret til den grundlæggende funktionalitet af automatiseringsfunktionen i 2N Access Commander, herunder vores brugerdefinerede Access Commander-noder, vil de ikke være i stand til at yde hjælp med design, udvikling eller fejlfinding af brugerdefinerede Node-RED-flows. De brugere, der ønsker at oprette komplekse automatiseringer, skal muligvis søge yderligere support fra kvalificerede Node-RED-eksperter eller konsultere tilgængelige ressourcer.

For at komme i gang med Node-RED er det tilrådeligt at udforske tilgængelige online ressources, såsom detaljerede manualer og adskillige YouTube-tutorials om Node-RED, som giver vejledning i oprettelse og styring af flows.

Du kan finde flere oplysninger om brugerdefinerede Access Commander-noder og brug af automatiseringsfunktionen i Access Commander, se venligst denne vejledning.

Denne funktion forbedrer funktionerne i Access Commander. Det anbefales at udforske dets potentiale og samtidig sikre sikkerheden af konfigurationer.

17.16.1 Oprettelse af automatiseringer

Automatiserede opgaver oprettes i en ekstern editor. Få adgang til editoren fra Indstillinger > Konfiguration > Automatisering. Ændringer foretaget i editoren træder ikke i kraft, før de er implementeret på serveren, hvilket gøres ved at klikke på knappen **Deploy** (Implementer) i øverste højre hjørne af editoren.

Oprettelsen af automatiserede opgaver er baseret på kompilering af flows. Strømmene er dannet af knudepunkter, der er bundet til hinanden. Nodemenuen vises i venstre panel. Du kan søge efter noder efter navn i venstre panel. Du kan også tilføje en ny node, når du har oprettet en ny forbindelse fra en eksisterende node.

De data, der overføres mellem knudepunkterne, kaldes meddelelser. Der henvises til Her for meddelelsesoplysningerne. På denne side beskrives også de grundlæggende noder, der håndterer meddelelsesformater eller -sekvenser, f.eks. Noder. Automatiseringer kan ikke kun arbejde med de data, der er opnået i denne unikke opgave (msg.), men også med dynamiske værdier i forbindelse med hele flowhistorikken (flow.) eller endda alle flows i installationen (globalt.).

Knappen **Deploy** (Implementer) sender de angivne flow til serveren. De nye flows træder ikke i kraft, før de sendes til serveren!

17.16.2 Fejlsikret tilstand

Fejlsikret tilstand er et vigtigt fejlfindingsværktøj til automatisering. Hvis du kører editoren i fejlsikret tilstand, kan du foretage flowændringer (i testtilstand), uden at flowene kører i baggrunden. Det betyder, at du kan gå til editoren, redigere det, du har brug for, og derefter implementere ændringerne ved hjælp af knappen **Deploy** (Implementer). Denne tilstand er især nyttig, hvis nogen af flowene forårsager, at Node-RED ikke fungerer korrekt eller mislykkes, f.eks. på grund af en fejl i flowet eller en tredjepartsnode, eller hvis flowet skal stoppes med det samme.

17.16.3 Adgangskommandonoder

REST API

REST API-noden sender en defineret HTTP API-anmodning. Inputdataene i brødteksten bruges som anmodningstekst for denne anmodning. Nodeoutputtet indeholder data fra svaret på anmodningen. Du kan angive valg og arrangement af outputdata i parameteren **Query** (Forespørgsel).

Node-parametre

- **Metode** – tilbyder et udvalg af API-anmodningsmetoder.
- **Slutpunkt** – angiver hele det slutpunkt, som anmodningen skal rettes til. Slutpunktsstien kan fuldføres med parameteren Body.
  Arbejde med HTTP-anmodninger er beskrevet i HTTP API (se afsnit 19.1 side 87).
- **Forespørgsel** – angiver, hvilke dataparametre der skal adresseres i slutpunktet, og hvordan de skal returneres i outputtet. Denne parameter kan angives af inputværdien i Query. Se Tilpasning af dataforespørgsler (kun på engelsk) for at få oplysninger om oprettelse af forespørgsler.
- **Send kun ikke-2xx-svar til Catch-noden** – påvirker den type HTTP-svar, der skal registreres i Catch-noden.
- **Navn** – giver dig mulighed for at omdøbe en node for bedre orientering, når du arbejder med flowet.

17.16.3.1 Adgangslog

Noden indlæser poster i adgangsloggen og giver dig mulighed for at behandle disse poster yderligere.

Administratoren kan oprette automatiserede opgaver, der starter, når Access Commander registrerer en defineret logpost. Handlingen er defineret i nodeindstillingerne. Outputtet indeholder specifikke data om den registrerede begivenhed. Den SignalR-baserede funktionalitet kører på baggrund af denne funktion.

NODE-PARAMETRE

- **Filter** – angiver de poster, der skal behandles af noden. Poster, der ikke matcher dette filter, ignoreres af flowet. Filterformatet er et JSON-objekt. Denne parameter kan overskrives af en inputværdi.
- **Navn** – giver dig mulighed for at omdøbe en node for bedre orientering, når du arbejder med flowet.

17.16.3.2 Systemlog

Noden indlæser poster i systemloggen og giver dig mulighed for at behandle disse poster yderligere.

Administratoren kan oprette automatiserede opgaver, der starter, når Access Commander registrerer en defineret logpost. Handlingen er defineret i nodeindstillingerne. Outputtet indeholder specifikke data om den registrerede begivenhed. Den SignalR-baserede funktionalitet kører på baggrund af denne funktion.

NODE-PARAMETRE

- **Filter** – angiver de poster, der skal behandles af noden. Poster, der ikke matcher dette filter, ignoreres af flowet. Filterformatet er et JSON-objekt. Denne parameter kan overskrives af en inputværdi.
- **Navn** – giver dig mulighed for at omdøbe en node for bedre orientering, når du arbejder med flowet.

17.16.3.3 SignalR

SignalR-noden læser data i det samplede emne. Noden henter data i realtid og er velegnet til scenarier, hvor den automatiserede opgave er at udtrække oplysninger fra Access Commander uden konstant forespørgsel.

NODE-PARAMETRE

- **Emne** – tilbyder tilgængelige emner til abonnement.
- **Filter** – angiver de poster, der skal behandles af noden. Poster, der ikke matcher dette filter, ignoreres af flowet. Filterformatet er et JSON-objekt. Denne parameter kan overskrives af en inputværdi.
- **Navn** – giver dig mulighed for at omdøbe en node for bedre orientering, når du arbejder med flowet.

Se Udskiftninger. SignalR (se afsnit 19.2 side 87) for flere oplysninger om SignalR-funktionalitet.

17.16.3.4 Dynamisk SignalR

Sammenlignet med SignalR giver Dynamic SignalR-noden mulighed for dynamiske ændringer i datasampling. Dette kan omfatte ændring af emnet eller prøveudtagningsmetoden baseret på inputværdierne. Nodens outputværdier omfatter data, der er hentet fra emnerne (Data), og oplysninger om vellykket/mislykket udførelse af nodehandlingen.

NODE-PARAMETRE

- **Emne** – definerer det emne, som dataindsamlingen skal ændres til.

- **Filter** – angiver de poster, der skal behandles af noden. Poster, der ikke matcher dette filter, ignoreres af flowet. Filterformatet er et JSON-objekt. Denne parameter kan overskrives af en inputværdi.
- **Poster** – definer antallet af poster, der skal indlæses, når du bruger læsetypen Hent.
- **Hent når klar** – indstil, om værdierne skal hentes baglæns, når hentekommandoen er aktiveret.
- **Navn** – giver dig mulighed for at omdøbe en node for bedre orientering, når du arbejder med flowet.

GYLDIGE INPUTVÆRDIER

Noden accepterer følgende egenskaber som inputværdier. De gyldige inputværdier tilsidesætter midlertidigt de parametre, der er angivet i nodekonfigurationen.

- **Emne** – En streng, der angiver det emne, der skal abonneres på.
- **Filter**– chain i JSON-formatet, som angiver de hentede poster.
- **FetchWhenReady** – bootlean, der angiver nodeparameteren Fetch When Ready.
- **Handling** – En streng, der angiver den handling, der skal udføres. Det kan være abonner for at abonnere, afmelde...
- **Opdatering** – kan indeholde et tidsstempel (streng) og et timeWindow (objekt), der angiver, hvornår den handling, der skal ændres, fandt sted.

Se Udskiftninger. SignalR (se afsnit 19.2 side 87) for flere oplysninger om SignalR-funktionalitet.

17.16.3.5 Skriv systemlog

Noden Skriv systemlog opretter en post i systemloggen for Access Commander. Logposten indeholder den angivne alvorsgrad, hændelsesbeskrivelse og andre detaljer. Hvis der opstår en fejl under processen, registreres den, og nodestatus opdateres i overensstemmelse hermed. Noden har ingen outputværdier.

NODE-PARAMETRE

- **Alvorsgrad** – bestemmer alvorsgraden af posten. Denne parameter kan angives af forespørgselsinputværdien.
- **Filter** – angiver de poster, der skal behandles af noden. Poster, der ikke matcher dette filter, ignoreres af flowet. Filterformatet er et JSON-objekt. Denne parameter kan overskrives af en inputværdi.
- **Detalje** – giver en mere detaljeret beskrivelse af den post, der vises i systemloggen. Denne parameter kan overskrives af en inputværdi.
- **Navn** – giver dig mulighed for at omdøbe en node for bedre orientering, når du arbejder med flowet.

GYLDIGE INPUTVÆRDIER

Noden accepterer følgende egenskaber som inputværdier. De gyldige inputværdier tilsidesætter midlertidigt de parametre, der er angivet i nodekonfigurationen.

- **Alvorsgrad** – Den streng, der bestemmer postens alvorsgrad.
- **Begivenhed** – en streng, der kort beskriver den optagede handling.
- **Detail** – en kæde, der udfylder den detaljerede beskrivelse af posten, der vises i systemloggen.

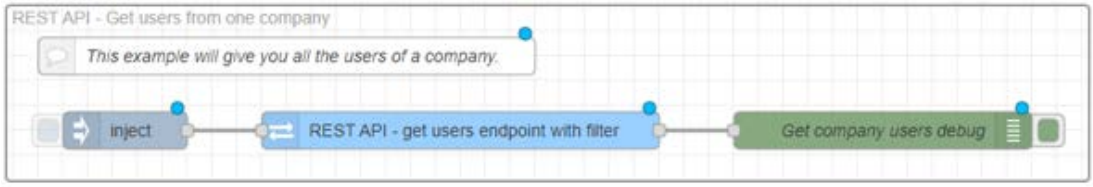
17.16.4 Eksempler på flows

Access Commander tilbyder flere grundlæggende automatiserede opgaver, der repræsenterer mulighederne for at bruge automatiseringer. Flowene for disse opgaver kan installeres, når du kører Automation første gang i Access Commander, men du kan importere dem senere, se Floweksport/import (se afsnit 17.16.5 side 82). Disse forudinstallerede flows kan nemt ændres til dine egne formål.

17.16.4.1 Få alle brugere

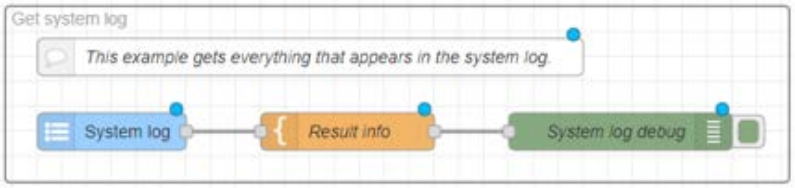
Dette flow genererer en liste over alle brugere, herunder brugeroplysninger. Opgaven startes af aktiveringen af Inject-noden. Du kan anvende et filter i REST API – hent brugeres slutpunktsnode for at angive de brugere, der skal returneres af processen. På denne måde kan du få procesoutputtet til at opfylde administratorens behov.

17.16.4.2 Få brugere fra én virksomhed



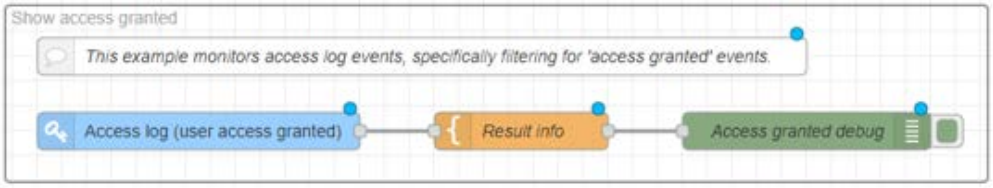
Dette flow genererer en liste over alle brugere i én virksomhed, herunder brugeroplysninger. Opgaven startes af aktiveringen af Inject-noden. Indstil virksomhedsvalget i REST API – hent brugernes slutpunkt med filter ved at indtaste virksomheds-id'et.

17.16.4.3 Hent systemlog



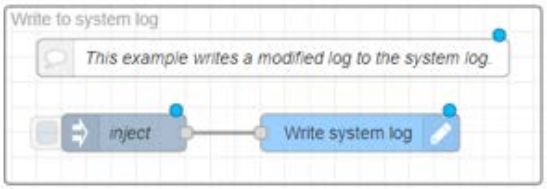
Dette flow indlæser alle de nye poster i systemloggen. Du kan angive et filter i systemloggen for at gøre hændelsesvalget mere præcist.

17.16.4.4 Vis adgang givet



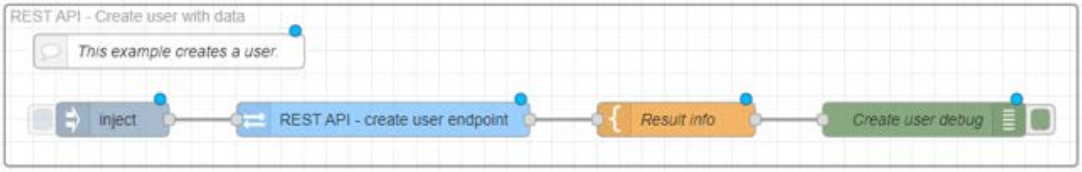
Dette flow indlæser alle de nye poster i Access-loggen. Flowet er indstillet til kun at indlæse tildelt adgang. Du kan ændre denne begrænsning i noden Adgangslog.

17.16.4.5 Skriv til systemlog



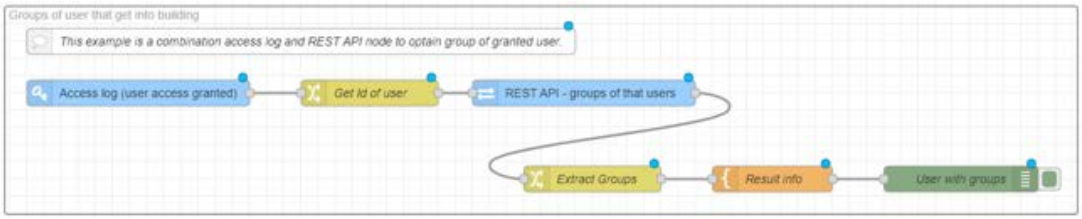
Dette flow opretter en post i systemloggen. Du kan angive posten Alvorsgrad, Navn og detaljeret Beskrivelse i lognoden Write System.

17.16.4.6 Opret bruger med data



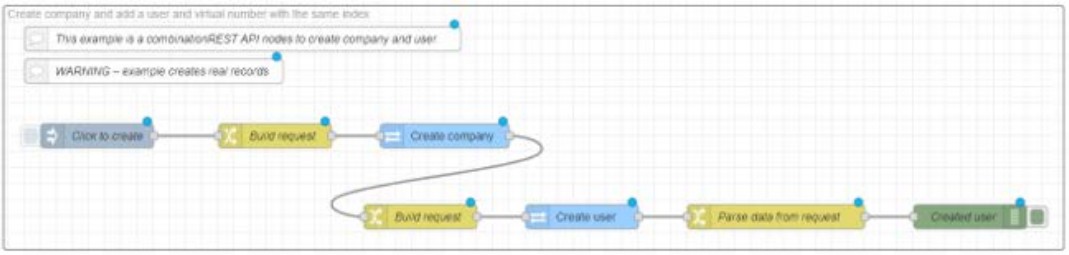
Brug dette flow til at oprette en ny bruger. Opgaven startes af aktiveringen af Inject-noden. Noden Inject indeholder en meddelelsestekst, der angiver brugernavnet Joe Doe og dets medtagelse i firmaet med ID 1. Denne brødtekst anvendes i REST API – opret brugerslutpunktsnode, og brugeren oprettes på dette grundlag. Noden Resultatoplysninger angiver, at meddelelsesteksten skal vises i fejlfindingsmeddelelserne.

17.16.4.7 Grupper af brugere, der kommer i gang med at bygge



Dette flow indlæser de brugergrupper, der har fået adgang. Tilladte adgange indlæses fra adgangsloggen. Efterfølgende henter flowet id'et for brugeren med den tildelte adgang og bruger REST API-noden – grupper af disse brugeres node til at hente data om denne bruger. Noden Udtræk grupper henter gruppenavnene for denne bruger, og noden Resultatoplysninger kompilerer teksten i den endelige meddelelse.

17.16.4.8 Opret virksomhed og tilføj en bruger og et virtuelt nummer med samme indeks



Dette flow opretter en ny virksomhed, den første bruger i virksomheden og dens virtuelle nummer. Opgaven startes af aktiveringen af Inject-noden. Ved start genereres et tilfældigt heltal, der skal bruges i firmanavnet og brugernavnet og fungere som brugerens virtuelle nummer. Noden Opret firma opretter et firma med det definerede navn. Fra svaret fra denne node opnås et firma-id, på grundlag af hvilket følgende Opret brugernode opretter en ny bruger i dette firma og tildeler samtidig brugeren et virtuelt nummer. Noden Parse data fra anmodning henter derefter firmanavnet, brugernavnet og brugerens virtuelle nummer.

17.16.5 Flow-eksport/-import

Flows kan eksporteres til .json filer og senere importeres igen til automatiseringsgrænsefladen. Eksport og import udføres i den udvidede menu i øverste højre hjørne. Flows, der flyttes fra én Access Commander-installation til en anden, kan kræve redigering.

Der er forudindlæste eksempelforløb for Access Commander i importindstillingerne. De er placeret på fanen Eksempler i mappen Access-Commander-nodes.

De avancerede indstillinger, der ikke understøttes af den nye licens, gemmes ikke. Husk derfor at eksportere de angivne flows, når prøvelicensen er afsluttet.

17.16.6 Fejl tilstande

Når du arbejder med automatiseringer, kan der lejlighedsvis opstå fejl, der påvirker deres stabilitet og funktionalitet. Når der opstår en fejl, giver fanen Automatisering i Access Commander dig besked om denne tilstand og giver dig mulighed for at genstarte Node-RED-platformen i fejlsikret tilstand. Den sikre tilstand stopper midlertidigt strømmene og giver mulighed for en sikker reparation af de strømme, der inducerer fejltilstanden. Klik på knappen Deploy (Implementer) for at genstarte flows.

Der er to grundlæggende fejltilstande:

- **Node-RED reagerer ikke**
  Denne situation opstår, når Node-RED holder op med at svare. Der er ingen automatiseringer i gang. Dette problem kan skyldes forskellige faktorer, såsom systemoverbelastning, fejl i flowindstillinger eller konflikter mellem de importerede tredjepartsmoduler.
- **Node-RED er ustabil**
  Node-RED-ustabiliteten manifesterer sig ved en gentagen genstart af platformen, hvilket kan forstyrre automatiseringsoperationer og forårsage tab af data. Som regel sker gentagne genstarter normalt, hvis et af flowene er forkert konfigureret og udløser genstart. Under genstarten afbrydes forløbet af alle flows.

18 Fejlfinding

18.1 Logfiler til diagnosticering

Diagnosticeringslogfiler hjælper teknisk supportpersonale med at identificere og løse rapporterede problemer. Logfilerne indeholder oplysninger om udførte handlinger, fejl, statusændringer og andre relevante hændelser.

18.1.1 Download af diagnosticeringslog

1. Gå til Indstillinger > Fejlfinding > diagnosticeringslogfiler.
2. Klik på **Generate logs** (Generer logfiler).
   Genereringsprocessen for logpakker tager et par minutter.
3. Når den er forberedt, vises pakken på kortet og er klar til **Download**.

18.2 Brugsstatistik

Hvis funktionen er aktiveret, sender Access Commander anonyme data om anvendte funktioner til en sikker 2N-server én gang om dagen. Hver afsendelse udføres med en unik identifikator, som regenereres automatisk for hver ny afsendelse. Dette forhindrer 2N-siden i at identificere den givne Access Commander-installation. De således opnåede oplysninger hjælper med at forbedre produktudviklingen, innovere funktioner og forbedre brugeroplevelsen.

19 Supplerende oplysninger

19.1 HTTP API

URL-adressen til Access Commander API er som følger: https://acom_ip_address/api/v3/.

Se http(s)://acom_ip_address/support/api (link) for listen over API-slutpunkter. Slutpunktslisten er tilgængelig uden for Access Commander-grænsefladen.

19.1.1 Godkendelse

HTTP API-kommandoerne sendes under brugerens logindata eller ved hjælp af tokengodkendelse. Autentificeringstokenet oprettes af administratoren i Indstillinger > konfiguration > API-adgangstokens. Det er ihændehavertokenet. Når der oprettes et nyt API-adgangstoken, kan administratoren begrænse tokenets gyldighed for kun at læse for at få tokenet til kun at godkende GET-kommandoerne. Tokenet kan begrænses til: 1 måned, 6 måneder, 1 år.

Kopier det oprettede adgangstoken til feltet. Senere kan tokenet ikke vises.

19.2 SignalR

SignalR er en protokol, der muliggør kommunikation mellem servere i realtid. Det betyder, at serveren kan sende beskeder til tilsluttede klienter, så snart de bliver tilgængelige, og ikke behøver at vente på en anmodning fra klienten. De grundlæggende principper for SignalR er beskrevet i SignalR-integrationsmanualen (kun på engelsk). En liste over tilgængelige SignalR-emner til brug med Access Commander er beskrevet i SignalR-emnereferencemanualen (kun på engelsk).

19.3 Tredjeparts licenser

En lang liste over de brugte tredjepartsbiblioteks licenser er inkluderet i brugermenuen til højre på den øverste bjælke i afsnittet Om applikation.

An ALLIED UNIVERSAL® Company

G4S Security Services A/S, Roskildevej 157, 2620 Albertslund
43 86 50 00, sikring@dk.g4s.com, www.g4s.dk