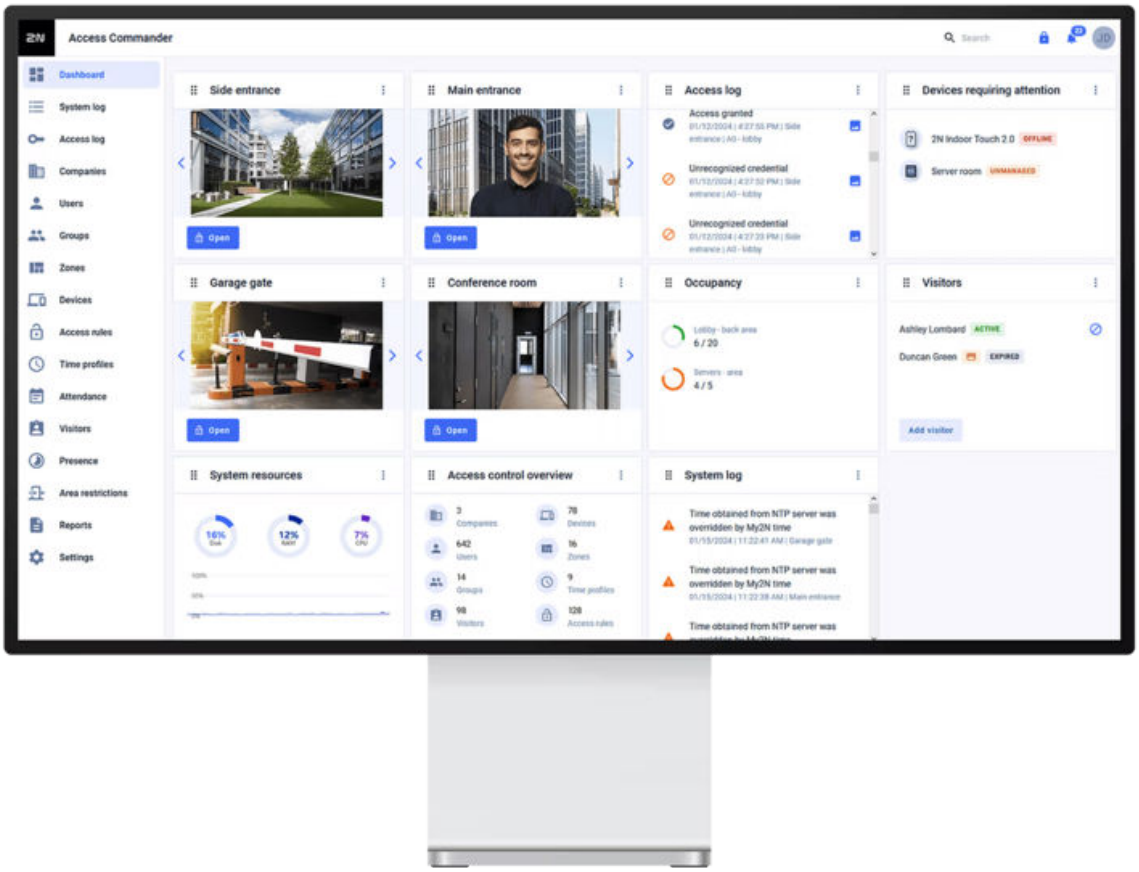
2N Access Commander

Installationshandbuch



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

2N.com

Inhaltsverzeichnis

Verwendete Symbole und Begriffe 6

allgemeine Informationen 7
- Benutzerberechtigungen 7
- Unterstützte Geräte und Anwendungen 8
  - Unterstützte Geräte 8
  - Internetbrowser 9
  - Virtualisierungsplattformen 9
- Verwendete Ports 10
- Übersicht der Lizenzen 10

Installation 13
- Verteilung über Access Commander Box 13
- Fortis Commander 14
  - Stecker und Installation 14
  - Projektdatei 14
  - Serviceleistungen 17
- Verteilung über virtuelle Maschine 17
  - Empfohlene Hardware der virtuellen Maschine 19
- Technische Parameter 19
  - Empfohlene Hardware der virtuellen Maschine 20
- Lizenzaktivierung 21
  - Erhalten der Lizenzdatei 21
  - Lizenz hochladen 21
- Lizenzerneuerung 21
- Elektronische Schlösser 22
  - Fortis Commander 23
  - Aktualisieren Sie die Karte 26
  - Kompatible Karten 26
  - Zeitprofile auf elektronischen Schlössern 26
  - Fortis Commander 27
  - IP-Gerätelesereinstellungen 30
  - Sperren in Access Commander einstellen 31
  - Karten für die Wartung 32
  - Unterstützung für DESFire-Karten von Drittanbietern (Anonyme App-Erstellung) 33

Grundlegender Zugriff auf die Schnittstelle 34
- Armaturenbrett 35
- Sprachwechsel 35
- Passwortänderung des Kontos 35
- Ändere dein Profilbild 36

Logos 37
- Systemprotokolle 37
  - Export von Logos 37
  - Lebensdauer der Protokolle 37
- Zugriffsprotokolle 38
  - Export von Logos 39
  - Lebensdauer der Protokolle 39
- Anrufprotokoll 39
  - Export von Logos 40
  - Lebensdauer der Protokolle 40
- Benachrichtigung 40
  - Benachrichtigungseinstellungen 41
- Lebensdauer der Protokolle 41

Unternehmen 43

Gründung eines neuen Unternehmens 43
Unternehmeneinstellungen 43
Die Sprache der Gesellschaft 43
Zonen 43
My2N app 43
Besuche 44
Arbeitsfonds 44
Feiertage 44
E-Mails, die an Unternehmenmitglieder gesendet werden 44
Synchronisierung des Unternehmens (LDAP) 45
Benutzer in das Unternehmen importieren 47
Benutzer 49
Erstellen Sie einen neuen Benutzer 50
Benutzereinstellungen 50
Namen und Foto des Benutzers ändern 50
Authentifizierung 50
Konto 52
persönliche Daten 53
Ansätze 53
Telefonnummern 53
Zugriffsprotokoll 53
Änderungsprotokoll 53
Hochladen von Fingerabdrücken 54
Bluetooth-Authentifizierung 54
Benutzerberechtigungen 56
Verfolgung der Benutzeranwesenheit 57
Gruppen 58
Erstellen Sie eine neue Gruppe 58
Gruppeneinstellungen 58
Mitglieder 58
Zugriffsregeln 58
Zonen 59
Erstellen einer neuen Zone 59
Zoneneinstellungen 59
Multi-Faktor-Authentifizierung 59
Zugriffseinstellungen 60
Gerät 60
Schlössergruppen 60
Unternehmen 60
Zugriffsregeln 60
Gerät 61
Hinzufügen eines neuen IP-Geräts 61
Schlössergruppen 62
Gruppen ansehen 62
Eine neue Sperrgruppe erstellen 62
Sperren in Access Commander einstellen 62
Notabschaltung 64
Geräteeinstellungen 64
Überblick 65
Anruf 66
Aufzug 67
Überwachung 68
Firmware 68
Geräteausschluss 69
Inkompatible Firmware-Version 69

Sicherheit 69
So verwalten Sie Zertifikate 70
Einstellungen für den Gerätezugriffspunkt 70
Gerätevorlagen 71
Vorlagen erstellen und verwalten 72
Ändern der Vorlage 72
Anwenden einer Vorlage auf ein Gerät 73
Zugriffsregeln 74
Matrixanzeige 74
Ein Beispiel für eine Matrixdarstellung 75
Liste der Regeln 75
Zeitprofile 76
Zeitprofile auf elektronischen Schlössern 76
Erstellen eines Zeitprofils 76
Zeitprofil einstellen 77
Teilnahme 78
Anwesenheit eines bestimmten Benutzers 78
Benutzeranwesenheit ändern 78
Anwesenheitseinstellungen 79
Einstellungen für den Gerätezugriffspunkt 80
Besuche 81
Festlegen der Aufbewahrung von Besucherdaten 81
Einen neuen Besuch erstellen 81
Ende des Besuchs 81
Besuchen Sie die Einstellungen 82
Ansätze 82
Besuchen 82
persönliche Daten 82
Authentifizierung 82
Zugriffsprotokoll 82
Karten 82
Verwalten einer sicheren Karte mit einem USB-Lesegerät 83
Gegenwart 84
Ablauf der Benutzerpräsenz 84
Berichte 85
Gebietsbeschränkungen 86
Gebietsbeschränkungen festlegen 86
Eingabe und Ausgabe 86
Belegung 86
Anti-Passback 87
Eine Ausnahme festlegen 87
Liste der blockierten Benutzer 87
Beschränkungen zurücksetzen 88
Erstellen Sie einen Sperrbereich 88
Die häufigsten Einrichtungsfehler 88
Ein Beispiel für das Festlegen von Einschränkungen 89
Systemeinstellungen 90
Linux-Einstellungen 90
Systemupdate 91
Downgrade 92
Beta-test 92
Systemsicherung 92
Synchronisierung von Benutzern mit FTP 94

Datum (und Uhrzeit 95
Zeitsynchronisierung mit Geräten 96
Automatisierung 96
Automatisierungen erstellen 97
Abgesicherter Modus 98
Access Commander Nodes 98
Beispiele für Flüsse 100
Streams exportieren/importieren 102
Fehlerzustände 103
Installationsname 103
E-Mail-Funktion (SMTP) aktivieren und einrichten 103
Zwei-Faktoren-Authentifizierung 104
Anwesenheitseinstellungen 105
Einstellungen für den Gerätezugriffspunkt 106
Erlauben Sie den SSH-Zugriff 107
Verschlüsselungsschlüssel für die My2N-Anwendung 108
RFID-Karten-Kompatibilitätsmodus 109
PICard-Schlüssel 109
Aktivierte USB-Lesegeräte 110
CAM-Protokolle 110
CAM-Logos einstellen 111
Elektronische Schlösser 111
Fortis Commander 111
Aktualisieren Sie die Karte 114
Kompatible Karten 115
Zeitprofile auf elektronischen Schlössern 115
Karten für die Wartung 116
Fehlerbehebung 116
Diagnoseprotokolle 116
Nutzungsstatistiken 116
Benachrichtigung 117
Benachrichtigungseinstellungen 117

Netzwerkeinstellungen 118
Erkennung einer Änderung der Geräte-IP-Adresse 118
Network Discovery 118
Proxy Einstellung 119
Verwendung von NodeRED 119

Weitere Informationen 120
HTTP API 120
SignalR 120
Lizenzen Dritter 120

Verwendete Symbole und Begriffe

Im Handbuch werden folgende Symbole und Piktogramme verwendet:

GEFAHR
Halten Sie sich stets daran Beachten Sie diese Hinweise, um Verletzungsgefahren zu vermeiden.

WARNUNG
Halten Sie sich stets daran Beachten Sie diese Hinweise, um Schäden am Gerät zu vermeiden.

ACHTUNG
Wichtige Warnung. Die Nichtbeachtung der Anweisungen kann zu Fehlfunktionen des Geräts führen.

TIPP
Nützliche Informationen für eine einfachere und schnellere Verwendung oder Einrichtung.

ANMERKUNG
Verfahren und Ratschläge zur effektiven Nutzung der Gerätefunktionen.

allgemeine Informationen

2N Access Commander ist ein Softwaretool für die Verwaltung von Massenzugriffssystemen. Schnittstelle Access Commander ist über einen Webbrowser zugänglich.

Innerhalb einer einzelnen Installation können die **Access Commander**-Einstellungen in Unternehmen unterteilt werden, die separat verwaltet werden.Teilen in **Unternehmen**. Diese Methode ermöglicht es, die Administration auf die Administratoren einzelner Unternehmen aufzuteilen. Ein Administrator eines Unternehmens hat keinen Zugriff auf Informationen über ein anderes Unternehmen. Administratoren eines Unternehmens sehen keine Benutzer eines anderen Unternehmens.

Um den Zugang zu verwalten, müssen Sie das Gerät zum Access Commander **hinzufügen. Geräte sind physische Einheiten im Gebäude, die Eingänge kontrollieren (2N Sprechanlagen, 2N Zutr**

Zonen oder Einrichtungen können unternehmensübergreifend gemeinsam genutzt werden, sodass der Unternehmenszugang zu Gemeinschaftsbereichen (Eingänge, Restaurants, Konferenzräume usw.) verwaltet werden kann.

Benutzer sind einzelne Personen, deren Bewegung im Gebäude verwaltet werden muss oder die von angeschlossenen Geräten aus angerufen werden können. Benutzer werden gruppiert in **Gruppen**, in dem eine Massenverwaltung ihres Zugangs zu Zonen durchgeführt wird. Der Benutzer authentifiziert sich am Gerät und das Gerät wertet dann aus, ob der Benutzer gültigen Zugriff auf das Gerät hat. Die Zugriffsgültigkeit richtet sich nach **Zutrittsregeln**. Ausgewählte Benutzer können auch über Administratorrechte verfügen **Access Commander** oder Teile davon.

Zeitprofile Sie legen die Zeiten fest, zu denen das Gerät den Zugriff ermöglicht oder zu denen Benutzer angerufen werden können.

Zeiterfassung ermöglicht die Überwachung der Benutzeranwesenheit.

Anwesenheit ermöglicht es Ihnen, zu verfolgen, in welchen Zonen sich Benutzer gerade befinden.

Besuche sind Personen, deren Zugangsrechte nur für eine begrenzte Zeit gültig sind.

Benutzerberechtigungen

Melden Sie sich **Access Commander** kann von mehreren Benutzern durchgeführt werden, abhängig von den ihnen zugewiesenen Berechtigungen.

Erhöhte Konten werden über eine Rolle in den Benutzereinstellungen eingerichtet. Einem Benutzer können mehrere Rollen zugewiesen werden.

ANMERKUNG
Benutzerberechtigungen gelten für die Verwaltung innerhalb des Unternehmens des Benutzers. Der Administrator hat Zugriff auf die komplette unternehmensübergreifende Verwaltung.

Administrator

- Einstellung des Systems und einzelner Module entsprechend der gültigen Lizenz.

- Lizenzwechsel
- Alle Berechtigungen anderer Rollen gelten für alle Unternehmen.

Zugriffsmanager

- Erstellen und verwalten Sie Gruppen.
- Benutzer zu Gruppen hinzufügen.
- Besuche erstellen und verwalten.
- Zeitprofile erstellen und verwalten.
- Zeiterfassung festlegen.

Benutzer Manager

- Benutzer erstellen und verwalten.
- Besuche erstellen und verwalten.
- Benutzer zu Gruppen hinzufügen.
- Besuche erstellen und verwalten.

Besuchsleiter

- Besuche erstellen und verwalten.
- Verwalten Sie ihre Gruppenmitgliedschaften (in der vereinfachten Benutzeroberfläche nicht verfügbar).
- Anzeigen des Zugriffsprotokolls von Besuchen (in der vereinfachten Benutzeroberfläche nicht verfügbar).

Türmanager

- Überwachung der Kameraübertragung von zugewiesenen Geräten.
- Fernöffnen zugewiesener Geräte.
- Notsperre zugewiesener Geräte.
- Anzeigen des Zugriffsprotokolls zugewiesener Geräte.
- Überwachung von Status und Sicherheitsereignissen im Systemprotokoll.

Anwesenheitsmanager

- Überwachung und Verwaltung der Anwesenheit zugewiesener Gruppen.
- Anzeigen des Zugriffsprotokolls von Benutzern zugewiesener Gruppen.

Firmenadministrator

- Einstellung der Standardsprache des Unternehmens.
- Überwachung des Systemprotokolls (beschränkt auf Unternehmensereignisse).
- Die Möglichkeit, ein Widget für das Systemprotokoll und die Notfallsperrfunktion auf Geräten einzurichten, die vom Unternehmen verwendet werden (einschließlich gemeinsam genutzter Geräte mit anderen Unternehmen).

Unterstützte Geräte und Anwendungen

In diesem Kapitel werden die unterstützten Geräte, unterstützten Webbrowser und kompatiblen Virtualisierungsplattformen aufgeführt, über die Access Commander installiert werden kann.

Unterstützte Geräte

Nachfolgend finden Sie eine Übersicht der vom Zutrittssystem unterstützten Geräte **Access Commander**. Diese Geräte können im System verwaltet werden.

ANMERKUNG
Die unterstützten Firmware-Versionen dieser Geräte sind im Kapitel aufgeführt Firmware (S. 68).

Gegensprechanlagen 2N

- 2N IP Style – unterstützt das Lesen von QR-Codes
- 2N IP Verso 2.0 – unterstützt das Lesen von QR-Codes
- 2N IP Force 2.0 – unterstützt das Lesen von QR-Codes
- 2N IP Verso
- 2N LTE Verso
- 2N IP One
- 2N IP Force
- 2N IP Safety
- 2N IP Vario
- 2N IP Base
- 2N IP Solo
- 2N IP Uni
- 2N IP Video Kit
- 2N IP Audio Kit
- 2N IP Audio Kit Lite

Zugangseinheiten 2N

- Access Unit QR – unterstützt das Lesen von QR-Codes
- 2N Access Unit 2.0
- 2N Access Unit
- 2N Access Unit M

2N Elektronische Schlösser

- 2N Fortis Handle
- 2N Fortis Cylinder

Reaktionseinheiten 2N

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

Internetbrowser

Aufbau **Access Commander** erfolgt über die Weboberfläche. Das System wurde für den Google Chrome-Browser (Version 90 und höher) optimiert.

Andere unterstützte Browser:

- Mozilla Firefox (Version 78 und höher)
- Microsoft Edge (Version 91 und höher)
- Safari (Version 14 und höher)

Andere Browser wurden nicht getestet, daher kann deren volle Funktionalität nicht gewährleistet werden.

Virtualisierungsplattformen

- Virtual Box
- VMware Player (Version 6.5 und höher)

- VMware vShpere (Version 6.5 und höher)
- Hyper-V

Verwendete Ports

Liste der Dienste und erforderlichen Ports

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

[a.] Es dient sowohl der Kommunikation mit dem Kunden als auch der Kommunikation mit den Gatekeepern.

[b.] Der Benutzer kann in den Einstellungen **Access Commander** Wählen Sie einen anderen Port für den LDAP-Dienst.

Übersicht der Lizenzen

Nach der Erstinstallation **Access Commander** eine Testlizenz ist verfügbar. Mit der Testlizenz können Sie alle Funktionen bei der Verwaltung von 1 Gerät und 5 Benutzern testen. Für die vollständige Administration müssen Sie eine der vier Lizenzen aktivieren: *Basic* (frei), *Advanced*, *Pro* oder *Unlimited*.

Lizenz:	Trial	Basic	Advanced	Pro	Unlimited
Best. Nr.	n/a	n/a	91379031	91379032	91379033
Maximale Anzahl Benutzer	5	50	300	1000	Unbegrenzt[a.]
Maximale Anzahl an Geräten (sowohl aktiviert als auch deaktiviert)	1	5	30	100	Unbegrenzt

Lizenz:	Trial	Basic	Advanced	Pro	Unlimited
Best. Nr.	n/a	n/a	91379031	91379032	91379033
Maximale Anzahl von Administratoren/Managern	5	1	5	1000	Unbegrenzt
Zugriffs- und Systemprotokolle	✓	✓	✓	✓	✓
Zugriffsregeln	✓	✓	✓	✓	✓
API-Verwaltung	✓	✓	✓	✓	✓
Aktivierung/Deaktivierung des Kontos	✓	✓	✓	✓	✓
Begrenzung der Anzahl fehlgeschlagener Zugriffe	✓	✓	✓	✓	✓
Stiller Alarm	✓	✓	✓	✓	✓
Zonencode	✓	✓	✓	✓	✓
Geräteüberwachung	✓	✓	✓	✓	✓
Protokollverwaltung	✓	✓	✓	✓	✓
Verwaltung von elektronischen Schlössern	✓	✓	✓	✓	✓
Importieren Sie Benutzer aus CSV oder von Geräten	✓	×	✓	✓	✓
Massen-Firmware-Verwaltung	✓	×	✓	✓	✓
Mehrfachauthentifizierung	✓	×	✓	✓	✓
Benutzerautorisierung	✓	×	✓	✓	✓

Lizenz:	Trial	Basic	Advanced	Pro	Unlimited
Best. Nr.	n/a	n/a	91379031	91379032	91379033
Benachrichtigung	✓	×	✓	✓	✓
Gegenwart	✓	×	✓	✓	✓
API-Zugriffsschlüssel	✓	×	✓	✓	✓
CAM-Protokolle	✓	×	✓	✓	✓
Aufzugssteuerung	✓	×	✓	✓	✓
Armaturenbrett	✓	×	✓	✓	✓
Notabschaltung	✓	×	✓	✓	✓
Unterstützung für mobile Anmeldeinformationen	✓	×	✓	✓	✓
Besuchsmanagement	✓	×	✓	✓	✓
Automatisierung	✓	×	✓	✓	✓
Belegungsmanagement	✓	×	×	✓	✓
Synchronisierung (LDAP & CSV)	✓	×	×	✓	✓
Anti-Passback	✓	×	×	✓	✓
Teilnahme	✓	Optional	Optional	Optional	Optional

[a] Unbegrenzt im Rahmen der maximalen Möglichkeiten der Softwareplattform, nämlich Empfohlene Hardware der virtuellen Maschine (S. 20)

Installation

Access Commander kann auf zwei Arten verteilt werden:

- 2N Access Commander Box 2.0, ein kleiner Desktop-Computer (Teilenummer 91379030)
- Virtueller Computer

Lösung Access Commander Box ist auf 2000 angeschlossene Geräte begrenzt. Die weiteren Softwarefunktionen sind bei beiden Lösungen identisch.

Verteilung über Access Commander Box

Access Commander Box 2.0 (1120120xx, 03129-00) ist ein kompakter Desktop-Minicomputer mit vorinstallierter Software. Es handelt sich um eine "Plug and Play"-Lösung, bei der Sie lediglich ein Netzteil und ein Ethernet-Kabel an diesen Minicomputer anschließen müssen. Damit das System ordnungsgemäß und in vollem Umfang funktioniert, empfiehlt es sich, diesen Minicomputer an einem sicheren Ort aufzustellen und ihn dauerhaft laufen zu lassen. Die Access Commander Box 2.0 dient als Server, um Daten, Ereignisse und Protokolle des gesamten Zutrittskontrollsystems zu sammeln.

Wir empfehlen, die Anzahl von 1500 Benutzern in der Gruppe nicht zu überschreiten. Wenn es Einschränkungen für Bereiche gibt, wie z. B. Anti-Passback oder Belegungskontrolle für eine große Anzahl von Benutzern, kann es zu einer Verlangsamung der Anwendung kommen.

Einloggen in Access Commander mit einer dynamischen IP-Adresse

1. Verbinden Access Commander Box über ein Ethernet-Kabel mit dem Netzwerk verbinden.
2. Verwenden Sie 2N IP Network Scanner und Axis IP Utility, um Access Commander Box im Netzwerk zu lokalisieren.
3. Gehen Sie in Ihrem Webbrowser zur IP-Adresse Access Commander Box und melden Sie sich an **Access Commander**.
   Das Standardpasswort für den Benutzer Admin lautet 2n und muss nach der Anmeldung geändert werden.

> **ANMERKUNG**
> Im Falle einer Weitergabe per Access Commander Box Stellen Sie von einem anderen Computer im Netzwerk aus eine Verbindung zur Weboberfläche her. Betriebssystem Access Commander Box stellt den Betrieb sicher **Access Commander** und sein grundlegendes Linux-Setup lässt die Ausführung des Webbrowsers nicht zu.

Einrichten einer statischen Adresse auf der Access Commander Box durch direkte Verbindung mit dem Computer

1. Schließen Sie die Access Commander Box über ein Netzwerkkabel direkt an Ihren Computer an.
2. Nach ca. **15 Sekunden wird** automatisch die link-local Adresse einstellen.
3. Öffnen Sie **accesscommander.local** in Ihrem Browser.
   Alternativ können Sie 2N IP Network Scannder oder Axis IP Utility verwenden, um das Gerät zu finden, auch wenn es keine IP-Adresse über DHCP erhalten hat.
4. Legen Sie in der Weboberfläche eine statische Adresse nach Bedarf fest.

Einstellen einer statischen Access Commander-Adresse auf der Access Commander-Box

1. Verbinden Access Commander Box über ein Ethernet-Kabel mit dem Netzwerk verbinden.
2. Verbunden mit Access Commander Box Tastatur und Monitor. Es erscheint ein schwarzer Bildschirm.
3. Melden Sie sich am System als „root“ mit dem Passwort „2n“ an. Wenn der blaue Bildschirm erscheint, ändern Sie das Standardpasswort.
4. Wählen Sie im Menü Erweitert „Netzwerk“ und dann „Statische IP“.
5. Legen Sie statische IP-Adresse, Gateway und DNS fest.
6. Speichern Sie diese Einstellung und verlassen Sie das Konsolenmenü mit der Abmeldung.
7. Stellen Sie über einen Webbrowser eine Verbindung zur eingestellten IP-Adresse her.

TIPP
Eine direkte Verbindung mit dem Computer und die Verwendung der Adresse **accesscommander.local** ist der empfohlene und einfachste Weg, um eine statische Adresse auf der Access Commander Box einzurichten.

ANMERKUNG
Die in 2N Network Scanner oder Axis IP Utility angezeigte Seriennummer kann von der Seriennummer auf dem Etikett der Access Commander Box abweichen.

Fortis Commander

Fortis Commander ist eine eigenständige Anwendung, die die elektronischen Schlösser **Fortis** mit dem System **Access Commander** verbindet. Die Anwendung setzt Sperren entsprechend der in **Access Commander**u erstellten Projektdatei, die die Sperrkonfiguration enthält. Die Datei ist verschlüsselt und kann nur auf einer bestimmten Installation verwendet werden.

Stecker und Installation

Fortis Commander ist für die Installation auf einem Windows-Computer mit Bluetooth Low Energy (BLE) Unterstützung konzipiert.

Die App finden Sie auf der Website 2N Download Centre.

Verlauf der Installierung

1. Laden Sie das Installationspaket über den angegebenen Link herunter.
2. Starten Sie das Installationsprogramm und schließen Sie die Installation ab, indem Sie den Anweisungen auf dem Bildschirm folgen.

Projektdatei

Die Projektdatei wird in **Access Commander** erstellt und enthält die vollständige Projektkonfiguration. Die Datei ist verschlüsselt und passwortgeschützt.

Sperren in Access Commander einstellen

Bevor Sie Schlüssel zu einzelnen Schlössern hochladen können, müssen Sie **Access Commander** mit **Fortis Commander** koppeln.

Generierung des Master Encryption Key (MEK) und Projektvorbereitung

1. Melden Sie sich bei Access Commander an.
2. Gehen Sie zu **Einstellungen > Elektronische Schlösser**.
3. Auf der Registerkarte **Ersteinstellungen** klicken Sie auf Schlüssel generieren.
4. Erstellen Sie den Hauptverschlüsselungscode.

ACHTUNG
Der Hauptverschlüsselungscode kann später weder eingesehen noch geändert werden .

ANMERKUNG
Anhand des Hauptchiffrierschlüssels (MEK) generiert **2N Access Commander** eine Reihe von Chiffrierschlüsseln. Der Schlüssel sollte also eindeutig und ausreichend sicher sein. Der Schlüsselsatz basiert auf dem Hauptchiffrierschlüssel, so dass Projekte mit demselben Hauptchiffrierschlüssel dieselben Schlüsselsätze erzeugen. Wenn ein Projekt verloren geht, kann ein neues Projekt mit demselben Hauptschlüssel erstellt werden und die Verschlüsselung fortsetzen.

5. Nachdem Sie die Schlüssel erzeugt und das Passwort für die Projektdatei festgelegt haben, können Sie **die Projektdatei** herunterladen, die ein Abbild der Konfiguration des elektronischen Schlosses im System **Access Commander** ist.
6. Klicken Sie auf der Registerkarte **von Fortis Commander** auf Anwendung herunterladen, von wo aus das Herunterladen von **Fortis Commander** (Anwendung zur Konfiguration von elektronischen Schlössern) gestartet wird.

ACHTUNG
Projektinformationen sind sensible Daten. Schützen Sie sie vor Missbrauch.

Konfigurieren des elektronischen Schlosses mit Fortis Commander

1. Installieren Sie **Fortis Commander** und öffnen Sie es.
2. Klicken Sie auf Projekt öffnen und öffnen Sie die heruntergeladene Projektdatei im Datei-Explorer.
3. Geben Sie in dem daraufhin angezeigten Dialogfeld das Passwort für die Projektdatei ein.
4. Nachdem Sie die Projektdatei geöffnet haben, wählen Sie Mit Gerät verbinden und verbinden Sie die Servicekarte mit dem Schloss.
5. Klicken Sie auf **Zuweisen**, wodurch die Sperre dem Projekt zugewiesen wird.
6. Trennen Sie die Verbindung zum Gerät und klicken Sie auf **Datei > Projekt schließen**.
7. Wenn die Konfiguration abgeschlossen ist, öffnen Sie das System **Access Commander**. Gehen Sie auf die Registerkarte **Einstellungen > Elektronische Schlösser** und klicken Sie erneut auf Fortis Commander. Laden Sie die Projektdatei hoch.

ANMERKUNG
Wenn Sie das Schloss zwischen Installationen verschieben oder einen Anspruch geltend machen, müssen Sie einen **Factory Reset** durchführen. Dieser Vorgang setzt das Schloss auf die Werkseinstellungen zurück und löscht alle vorherigen Konfigurationen.

Verfahren zur Aktualisierung der Konfiguration

1. Nehmen Sie Änderungen in **Access Commander** vor.
2. Laden Sie die neue Projektdatei herunter.
3. Laden Sie die Datei auf **Fortis Commander** hoch und nehmen Sie die erforderlichen Änderungen an den Schlössern vor.
4. Wenn Sie andere Änderungen an **Access Commander**u vornehmen, laden Sie immer eine neue Projektdatei herunter.

ACHTUNG
Für jede Konfigurationsänderung in **Access Commander**u müssen Sie eine neue Projektdatei herunterladen - Sie können keine ältere Datei verwenden, die bereits auf **Fortis Commander** hochgeladen wurde.

Dauerhaftes Ver- und Entriegeln

Die App ermöglicht es Ihnen, das Schloss dauerhaft zu sperren und zu entsperren. Die Funktion wird für Service-Einsätze oder Notfallkontrollen ohne Verwendung einer Karte verwendet.

Erfassung von Ereignissen aus elektronischen Schlössern mit RFID-Karten/ Chips

Einstellungen für die Ereignissammlung

1. Öffnen Sie **Einstellungen > Elektronische Schlösser > Registerkarte Ereignisse**.
2. Wählen Sie den Ereignistyp:
   - **Sammeln von Zugangs- und Systemereignissen** - Alle Zugangs- und Systemereignisse werden auf der Karte/dem Chip aufgezeichnet und in das **System Log** und **Access Log** geschrieben.
   - **Nur Systemereignisse sammeln** - nur Systemereignisse werden protokolliert, Zugriffsereignisse werden nicht auf Karten gespeichert.
   - **Sammeln Sie keine Ereignisse auf** Registerkarten - es werden keine Ereignisse auf die Registerkarte geschrieben; sie können nur über **Fortis Commander**u aufgerufen werden.

TIPP
Wenn Sie geeigneten Ereignissatzes auswählen, können Sie die Systemlast und die Nutzung des Speicherplatzes verringern. Eine detaillierte Protokollierung ist jedoch für Diagnosen und Sicherheitsaudits wichtig.

Ereignisse von einer Karte exportieren

Die Karte speichert maximal **16 erste Ereignisse**. Ereignisse können auf zwei Arten gelesen werden:

- Klicken Sie in **Access Commander** auf das Symbol im Suchfeld in der Kopfzeile und laden Sie die Registerkarte.
- Wenn Sie ein Gerät mit **2N OS** verwenden, werden Ereignisse von der Karte gelesen und an **Access Commander**u gesendet.

Hochladen von Ereignissen auf das Schloss

1. Öffnen Sie **Einstellungen > Elektronische Schlösser > Fortis Commander** und klicken Sie auf Datei herunterladen.

2. Öffnen Sie die Datei in **Fortis Commander**.
3. Verbinden Sie sich über die App **Fortis Commander** mit dem elektronischen Schloss.
4. Laden Sie die aktualisierte Datei wieder auf **Access Commander** hoch.
5. Nach dem Hochladen werden die Ereignisse in **Zugriffsprotokolle** und **Systemprotokolle** angezeigt.

Serviceleistungen

Diese Funktionen sind verfügbar für **Fortis Cylinder**:

- **Demontage** - Demontage von Schlössern zu Servicezwecken.
- **Auswechseln der Batterie** - Auswechseln der Batterie im Schloss.

ACHTUNG
Servicevorgänge sind für andere Arten von Sperren nicht relevant.

ANMERKUNG
Aus dem Servicemodus kehrt das Schloss in den normalen Modus zurück, indem Sie die Taste Lock drücken, um es dauerhaft zu sperren.

Verteilung über virtuelle Maschine

Access Commander kann als virtuelle Maschine verteilt werden. Im Folgenden finden Sie die Installationsverfahren für unterstützte Virtualisierungsplattformen.

Virtual Box

TIPP
Es wird empfohlen, die VT-X-Virtualisierungstechnologie im BIOS zu aktivieren.

1. Laden Sie die neueste Version von VirtualBox von https://www.virtualbox.org/wiki/Downloads herunter. Es wird empfohlen, die Version inklusive VirtualBox Extension Pack herunterzuladen.
2. Laden Sie die entsprechende Software aus dem Bereich Support > Download Center > herunter Software und Firmware auf 2N.com. Entpacken Sie die Datei nach dem Herunterladen.
3. Öffnen Sie VirtualBox und wählen Sie „Datei – App importieren…“.
4. Bearbeiten Sie den Titel.
5. Überprüfen Sie die CPU-Einstellungen (mindestens 2), die RAM-Einstellungen (mindestens 2048 MB) und die Auswahl der Netzwerkkarte.
6. Bestätigen Sie die Lizenzbedingungen.
   Nach der Installation öffnet sich die Linux-Konfigurationskonsole, in der Sie grundlegende Systemeinstellungen vornehmen können. Die komplette Konfiguration erfolgt im Webinterface.

VMware Player

ACHTUNG
Die unterstützte Version von VMWare ist 6.5 und höher.

1. Laden Sie die entsprechende Software aus dem Bereich Support > Download Center > herunter Software und Firmware auf 2N.com. Entpacken Sie die Datei nach dem Herunterladen.
2. Wählen Sie im VMware Player „Datei – Öffnen…“ den Pfad zur OVA-Datei aus.
3. Benennen Sie es nach Bedarf um und klicken Sie auf „Importieren“.
4. Überprüfen Sie die CPU-Einstellungen (mindestens 2), die RAM-Einstellungen (mindestens 2048 MB) und die Auswahl der Netzwerkkarte.
   Nach der Installation öffnet sich die Linux-Konfigurationskonsole, in der Sie grundlegende Systemeinstellungen vornehmen können. Die komplette Konfiguration erfolgt im Webinterface.

VMware vSphere

ACHTUNG
Die unterstützte Version von VMWare ist 6.5 und höher.

1. Laden Sie die entsprechende Software aus dem Bereich Support > Download Center > herunter Software und Firmware auf 2N.com. Entpacken Sie die Datei nach dem Herunterladen.
2. Wählen Sie in VMware vSphere „Datei – OVF-Vorlage bereitstellen …“ und folgen Sie dem Assistenten.
3. Überprüfen Sie nach dem Import die Einstellungen „Einstellungen bearbeiten…“
   Bearbeiten Sie den Namen (auf der Registerkarte „Optionen“).
4. Überprüfen Sie die CPU-Einstellungen (mindestens 2), die RAM-Einstellungen (mindestens 2048 MB) und die Auswahl der Netzwerkkarte.
   Nach der Installation öffnet sich die Linux-Konfigurationskonsole, in der Sie grundlegende Systemeinstellungen vornehmen können. Die komplette Konfiguration erfolgt im Webinterface.

Hyper-V

1. Laden Sie die entsprechende Software aus dem Bereich Support > Download Center > herunter Software und Firmware auf 2N.com. Entpacken Sie die Datei nach dem Herunterladen.
2. Starten Sie den Hyper-V-Manager und wählen Sie die Option für den gewünschten Host aus Virtuelle Maschine importieren.
3. Überprüfen Sie in der Installationsanleitung die angezeigten Informationen und bestätigen Sie das Lesen mit der Schaltfläche Nächste.
4. Wählen Sie den Ordnerpfad aus Schritt 1 aus.
5. Bestätigen Sie die Auswahl der virtuellen Maschine.
6. Wählen Sie den Importtyp aus.
7. Wählen Sie die virtuelle Netzwerkkarte für die virtuelle Maschine aus.
8. Überprüfen Sie die Zusammenfassung der Einstellungen, die in den vorherigen Schritten ausgewählt wurden, und bestätigen Sie mit der Schaltfläche Finish.
   Nach der Installation öffnet sich die Linux-Konfigurationskonsole, in der Sie grundlegende Systemeinstellungen vornehmen können. Die komplette Konfiguration erfolgt im Webinterface.

Empfohlene Hardware der virtuellen Maschine

Die Anzahl der angeschlossenen Geräte wirkt sich aus **Access Commander**. Stellen Sie daher die Größe der Hardwareelemente entsprechend der tatsächlichen Situation ein. Die folgende Tabelle zeigt die empfohlene Mindestanzahl an CPU-Kernen und RAM-Größen für eine unterschiedliche Anzahl verwalteter Geräte und Benutzer**Access Commander**.

ACHTUNG
Es wird empfohlen, eine kontinuierliche Verbindung zwischen ihnen aufrechtzuerhalten **Access Commander**und Geräte. Bei getrennter Verbindung speichern Geräte Ereignisprotokolle offline und bei erneuter Verbindung werden die Protokolldaten mit synchronisiert **Access Commander**. Während des Synchronisierungsvorgangs läuft die Anwendung weiter, bei einer größeren Anzahl an Geräten kann der gesamte Vorgang jedoch länger dauern.

Hardware der virtuellen Maschine

Anzahl der Geräte	Anzahl der Nutzer	Mindestanzahl an CPU-Kernen	Mindest-RAM-Größe	Minimale Festplattenzuweisung
1 000	10 000	2	2 GB	120 GB
2 000	100 000	2	4GB	120 GB
2 000	200 000	4	8 GB	120 GB
7 000	200 000	4	16 Gigabyte	120 GB

Technische Parameter

Programmoptionen auf der Access Commander Box 2.0

Anzahl der angeschlossenen Geräte	Anzahl der Nutzer	Anzahl der Benutzer in der Gruppe
7 000	200 000	1 500

Technische Parameter Access Commander Box

1. Generation Best.-Nr. 91379030	2. Generation Bestell-Nr. 1120120E, 1120120GB, 1120120US
• Ultrakompaktes Design – 0,69 l (56,1 x 107,6 x 114,4 mm) • Intel-Prozessor®Celeron®J3160 (2 MB Cache; max. 2,24 GHz) • 2,5" SSD SATA III Festplatte (120 GB) • DDR3 SODIMM-Speicher (4 GB) – 1,35 V, 1600 MHz • Dual-Display-Unterstützung über VGA- und HDMI-Anschluss • Gigabit-LAN-Anschluss für Ethernet-Verbindung • VESA-Montagerahmen (75 x 75 mm + 100 x 100 mm) • Lagertemperatur: -20 °C bis +60 °C • Umgebungstemperatur: 0 °C bis +35 °C	• Abmessungen: 127,5 x 132 x 57,6 mm (5,02 " x 5,20" x 2,27") • Intel® Processor N100, 6W TDP • SSD 980 NVMe M.2 – 250 GB • DDR4 SO-DIMM-Speicher – 16 GB, 1,2 V, 3200 MHz • HDMI 2.1, DisplayPort 1.4 und VGA-Unterstützung • 2,5G RJ45 LAN-Anschluss für Ethernet-Verbindung • Lagertemperatur: −40 °C bis +85 °C • Betriebstemperatur: 0 °C bis +50 °C

Empfohlene Hardware der virtuellen Maschine

Die Anzahl der angeschlossenen Geräte wirkt sich aus **Access Commander**. Stellen Sie daher die Größe der Hardwareelemente entsprechend der tatsächlichen Situation ein. Die folgende Tabelle zeigt die empfohlene Mindestanzahl an CPU-Kernen und RAM-Größen für eine unterschiedliche Anzahl verwalteter Geräte und Benutzer**Access Commander**.

ACHTUNG
Es wird empfohlen, eine kontinuierliche Verbindung zwischen ihnen aufrechtzuerhalten **Access Commander**und Geräte. Bei getrennter Verbindung speichern Geräte Ereignisprotokolle offline und bei erneuter Verbindung werden die Protokolldaten mit synchronisiert **Access Commander**. Während des Synchronisierungsvorgangs läuft die Anwendung weiter, bei einer größeren Anzahl an Geräten kann der gesamte Vorgang jedoch länger dauern.

Hardware der virtuellen Maschine

Anzahl der Geräte	Anzahl der Nutzer	Mindestanzahl an CPU-Kernen	Mindest-RAM-Größe	Minimale Festplattenzuweisung
1 000	10 000	2	2 GB	120 GB
2 000	100 000	2	4GB	120 GB

Anzahl der Geräte	Anzahl der Nutzer	Mindestanzahl an CPU-Kernen	Mindest-RAM-Größe	Minimale Festplattenzuweisung
2 000	200 000	4	8 GB	120 GB
7 000	200 000	4	16 Gigabyte	120 GB

Lizenzaktivierung

Zur Aktivierung müssen Lizenzen erworben werden Lizenzdatei und laden Sie es hoch **Access Commander**. Die Basic-Lizenz kann direkt aktiviert werden **Access Commander** auf der Seite „Einstellungen“ > Registerkarte „Lizenz“.

Erhalten der Lizenzdatei

Um eine Lizenz zu erhalten, müssen Sie dem Vertriebspartner die Seriennummer eines der an den **Access Commander** angeschlossenen 2N Geräte mitteilen. Die Lizenzdatei wird auf der Grundlage der Seriennummer dieses lizenzierten Geräts erstellt. Dabei muss es sich um die Seriennummer der Hauptsprechstelle, der Zutrittseinheit oder der Anrufbeantwortereinheit handeln (2N Indoor Touch kann nicht verwendet werden).

Verbindung lizenziertes Gerät stellt die Gültigkeit der Lizenz sicher. Im Falle einer Trennung des lizenzierten Geräts beginnt eine Schutzfrist, nach deren Ablauf die Lizenz ausgesetzt wird.

Lizenz hochladen

ACHTUNG

- Nach dem Wechsel von der Trial-lizenz ist eine Reaktivierung der Trial-lizenz nicht mehr möglich.
- Erweiterte Funktionseinstellungen, die von der neuen Lizenz nicht unterstützt werden, werden nicht gespeichert.

1. Gehe zu **Einstellungen > Registerkarte Lizenz**.
2. Klicke auf Lizenz einspielen und laden Sie im geöffneten Fenster die aus dem Repository erhaltene Lizenzdatei hoch.
3. Klicken Sie nach dem Hochladen der Datei auf Aktivieren Sie die Lizenz.
4. Stellen Sie sicher, dass das lizenzierte Gerät, für das die Lizenz generiert wurde, aktiviert ist.

Lizenzdatei	Eine Datei mit einer Lizenz, deren Hochladen die Lizenz aktiviert. Die Lizenzdatei wird vom Distributor auf Basis der Seriennummer des Lizenzgeräts generiert.
Lizenzgerät	Ausgewähltes 2N-Gerät verbunden mit **Access Commander**, was die Gültigkeit der Lizenz gewährleistet. Das Lizenzgerät dient als Hardwareschlüssel für die Lizenz.

Lizenzerneuerung

Um eine ausgesetzte Lizenz wiederherzustellen, müssen Sie das lizenzierte Gerät anschließen und aktivieren oder eine neue Lizenzdatei für ein anderes Gerät erstellen und hochladen lassen. Wenn Sie eine neue

Lizenz hochladen, müssen Sie zuerst das lizenzierte Gerät aktivieren, für das die neue Lizenz generiert wird. Sobald das lizenzierte Gerät aktiviert ist, können auch alle anderen Geräte aktiviert werden.

Die Lizenz wird ausgesetzt, wenn das lizenzierte Gerät über einen längeren Zeitraum als die Lizenzschutzzeit von **Access Commander** getrennt wird. Die Länge des Schutzzeitraums hängt davon ab, wie lange das lizenzierte Gerät in **Access Commander** verbunden war. Die Länge der Schutzzeiträume ist in der nachstehenden Tabelle aufgeführt. Wenn eine Lizenz ausgesetzt wird, werden alle angeschlossenen Geräte automatisch aus der Verwaltung entfernt und als nicht verwaltet gekennzeichnet.

ANMERKUNG
Das Entfernen von Geräten aus der Verwaltung bedeutet, dass Sie keine Änderungen an deren Konfiguration über **Access Commander** vornehmen können. In **Access Commander** vorgenommene Änderungen werden nicht an das Gerät weitergegeben. Die Geräte arbeiten jedoch weiterhin auf der Grundlage der Daten der letzten von **Access Commander** übertragenen Konfiguration. Das bedeutet, dass Zugänge und andere Einstellungen auf den Geräten so bleiben, wie sie waren, bevor die Lizenz ausgesetzt wurde.

Sie können die Konfiguration eines nicht verwalteten Geräts nur in der Webkonfigurationsoberfläche des jeweiligen Geräts ändern. Wenn das Gerät erneut mit der **Access Commander**-Verwaltung verbunden wird, wird das Gerät synchronisiert und die direkt in der Webkonfigurationsoberfläche des Geräts vorgenommenen Änderungen werden durch die Einstellungen in A**ccess Commander** überschrieben.

Die Zeitspanne, mit der das lizenzierte Gerät verbunden war Access Commander	Der Schutzzeitraum, für den es gelten wird Access Commander im Betrieb ohne angeschlossenes Lizenzgerät
weniger als 24 Stunden	1 Tag
1 Tag - 30 Tage	10 Tage
31 Tage - 180 Tage	1 Monat
mehr als 180 Tage	3 Monate

Elektronische Schlösser

Das System **Access Commander** ermöglicht die Zugangsverwaltung über elektronische Schlösser 2N Fortis, die durch RFID-Karten mit MIFARE-Technologie® DESFire® entriegelt werden. Bei der Konfiguration von elektronischen Schlössern wird jedem Schloss ein Verschlüsselungscode zugewiesen. Die Schlossschlüssel werden dann auf den RFID-Karten der berechtigten Benutzer gespeichert. Wenn die Schlüssel auf der Karte und im Schloss übereinstimmen, wird der Schließmechanismus entriegelt.

Eine RFID-Zugangskarte kann für den Zugang zu bis zu 90 Türen mit Schlössern 2N Fortis verwendet werden, abhängig von der Anzahl der angewendeten Zeitprofile. Wenn die Speicherkapazität der Karte überschritten wird, schlägt das Schreiben von Daten auf die Karte fehl. Das Ereignis des Schreibfehlers wird im

Zugriffsprotokoll des Systems aufgezeichnet. Wenn Schlossgruppen verwendet werden, können mehr Türen auf eine einzelne Karte geschrieben werden als bei einer individuellen Zuweisung. Wenn Schlossgruppen verwendet werden, können mehr Türen pro Karte registriert werden als bei einer individuellen Zuweisung.

Fortis Commander

Fortis Commander ist eine eigenständige Anwendung, die die elektronischen Schlösser **Fortis** mit dem System **Access Commander** verbindet. Die Anwendung setzt Sperren entsprechend der in **Access Commander**u erstellten Projektdatei, die die Sperrkonfiguration enthält. Die Datei ist verschlüsselt und kann nur auf einer bestimmten Installation verwendet werden.

Stecker und Installation

Fortis Commander ist für die Installation auf einem Windows-Computer mit Bluetooth Low Energy (BLE) Unterstützung konzipiert.

Die App finden Sie auf der Website 2N Download Centre.

Verlauf der Installierung

1. Laden Sie das Installationspaket über den angegebenen Link herunter.
2. Starten Sie das Installationsprogramm und schließen Sie die Installation ab, indem Sie den Anweisungen auf dem Bildschirm folgen.

Projektdatei

Die Projektdatei wird in **Access Commander** erstellt und enthält die vollständige Projektkonfiguration. Die Datei ist verschlüsselt und passwortgeschützt.

Sperren in Access Commander einstellen

Bevor Sie Schlüssel zu einzelnen Schlössern hochladen können, müssen Sie **Access Commander** mit **Fortis Commander** koppeln.

Generierung des Master Encryption Key (MEK) und Projektvorbereitung

1. Melden Sie sich bei Access Commander an.
2. Gehen Sie zu **Einstellungen > Elektronische Schlösser**.
3. Auf der Registerkarte **Ersteinstellungen** klicken Sie auf Schlüssel generieren.
4. Erstellen Sie den Hauptverschlüsselungscode.

ACHTUNG
Der Hauptverschlüsselungscode kann später weder eingesehen noch geändert werden .

ANMERKUNG
Anhand des Hauptchiffrierschlüssels (MEK) generiert **2N Access Commander** eine Reihe von Chiffrierschlüsseln. Der Schlüssel sollte also eindeutig und ausreichend sicher sein. Der Schlüsselsatz basiert auf dem Hauptchiffrierschlüssel, so dass Projekte mit demselben Hauptchiffrierschlüssel dieselben Schlüsselsätze erzeugen. Wenn ein Projekt verloren geht, kann ein neues Projekt mit demselben Hauptschlüssel erstellt werden und die Verschlüsselung fortsetzen.

5. Nachdem Sie die Schlüssel erzeugt und das Passwort für die Projektdatei festgelegt haben, können Sie **die Projektdatei** herunterladen, die ein Abbild der Konfiguration des elektronischen Schlosses im System **Access Commander** ist.
6. Klicken Sie auf der Registerkarte **von Fortis Commander** auf Anwendung herunterladen, von wo aus das Herunterladen von **Fortis Commander** (Anwendung zur Konfiguration von elektronischen Schlössern) gestartet wird.

ACHTUNG
Projektinformationen sind sensible Daten. Schützen Sie sie vor Missbrauch.

Konfigurieren des elektronischen Schlosses mit Fortis Commander

1. Installieren Sie **Fortis Commander** und öffnen Sie es.
2. Klicken Sie auf Projekt öffnen und öffnen Sie die heruntergeladene Projektdatei im Datei-Explorer.
3. Geben Sie in dem daraufhin angezeigten Dialogfeld das Passwort für die Projektdatei ein.
4. Nachdem Sie die Projektdatei geöffnet haben, wählen Sie Mit Gerät verbinden und verbinden Sie die Servicekarte mit dem Schloss.
5. Klicken Sie auf **Zuweisen**, wodurch die Sperre dem Projekt zugewiesen wird.
6. Trennen Sie die Verbindung zum Gerät und klicken Sie auf **Datei > Projekt schließen**.
7. Wenn die Konfiguration abgeschlossen ist, öffnen Sie das System **Access Commander**. Gehen Sie auf die Registerkarte **Einstellungen > Elektronische Schlösser** und klicken Sie erneut auf Fortis Commander. Laden Sie die Projektdatei hoch.

ANMERKUNG
Wenn Sie das Schloss zwischen Installationen verschieben oder einen Anspruch geltend machen, müssen Sie einen **Factory Reset** durchführen. Dieser Vorgang setzt das Schloss auf die Werkseinstellungen zurück und löscht alle vorherigen Konfigurationen.

Verfahren zur Aktualisierung der Konfiguration

1. Nehmen Sie Änderungen in **Access Commander** vor.
2. Laden Sie die neue Projektdatei herunter.
3. Laden Sie die Datei auf **Fortis Commander** hoch und nehmen Sie die erforderlichen Änderungen an den Schlössern vor.
4. Wenn Sie andere Änderungen an **Access Commander**u vornehmen, laden Sie immer eine neue Projektdatei herunter.

ACHTUNG
Für jede Konfigurationsänderung in **Access Commander**u müssen Sie eine neue Projektdatei herunterladen - Sie können keine ältere Datei verwenden, die bereits auf **Fortis Commander** hochgeladen wurde.

Dauerhaftes Ver- und Entriegeln

Die App ermöglicht es Ihnen, das Schloss dauerhaft zu sperren und zu entsperren. Die Funktion wird für Service-Einsätze oder Notfallkontrollen ohne Verwendung einer Karte verwendet.

Erfassung von Ereignissen aus elektronischen Schlössern mit RFID-Karten/Chips

Einstellungen für die Ereignissammlung

1. Öffnen Sie **Einstellungen > Elektronische Schlösser > Registerkarte Ereignisse**.
2. Wählen Sie den Ereignistyp:
   - **Sammeln von Zugangs- und Systemereignissen** - Alle Zugangs- und Systemereignisse werden auf der Karte/dem Chip aufgezeichnet und in das **System Log** und **Access Log** geschrieben.
   - **Nur Systemereignisse sammeln** - nur Systemereignisse werden protokolliert, Zugriffsereignisse werden nicht auf Karten gespeichert.
   - **Sammeln Sie keine Ereignisse auf** Registerkarten - es werden keine Ereignisse auf die Registerkarte geschrieben; sie können nur über **Fortis Commander**u aufgerufen werden.

TIPP
Wenn Sie geeigneten Ereignissatzes auswählen, können Sie die Systemlast und die Nutzung des Speicherplatzes verringern. Eine detaillierte Protokollierung ist jedoch für Diagnosen und Sicherheitsaudits wichtig.

Ereignisse von einer Karte exportieren

Die Karte speichert maximal **16 erste Ereignisse**. Ereignisse können auf zwei Arten gelesen werden:

- Klicken Sie in **Access Commander** auf das Symbol im Suchfeld in der Kopfzeile und laden Sie die Registerkarte.
- Wenn Sie ein Gerät mit **2N OS** verwenden, werden Ereignisse von der Karte gelesen und an **Access Commander**u gesendet.

Hochladen von Ereignissen auf das Schloss

1. Öffnen Sie **Einstellungen > Elektronische Schlösser > Fortis Commander** und klicken Sie auf Datei herunterladen.
2. Öffnen Sie die Datei in **Fortis Commander**.
3. Verbinden Sie sich über die App **Fortis Commander** mit dem elektronischen Schloss.
4. Laden Sie die aktualisierte Datei wieder auf **Access Commander** hoch.
5. Nach dem Hochladen werden die Ereignisse in **Zugriffsprotokolle** und **Systemprotokolle** angezeigt.

Serviceleistungen

Diese Funktionen sind verfügbar für **Fortis Cylinder**:

- **Demontage** - Demontage von Schlössern zu Servicezwecken.
- **Auswechseln der Batterie** - Auswechseln der Batterie im Schloss.

ACHTUNG
Servicevorgänge sind für andere Arten von Sperren nicht relevant.

ANMERKUNG
Aus dem Servicemodus kehrt das Schloss in den normalen Modus zurück, indem Sie die Taste Lock drücken, um es dauerhaft zu sperren.

Aktualisieren Sie die Karte

Benutzerzugangskarten müssen regelmäßig aktualisiert werden. Der Benutzer aktualisiert die Karte, indem er die Karte an das 2N IP-Gerät anschließt, für das er gültige Zugriffsrechte besitzt. Die Karte muss so lange am Gerätelesegerät gehalten werden, bis der Türöffnungsschalter eingeschaltet wird. Der Türöffnungsschalter wird erst aktiviert, nachdem der Zugang zu den Schlössern aktualisiert wurde

Sie können die standardmäßige zehntägige Gültigkeit der Karten unter **Einstellungen > Elektronische Schlösser > Registerkarte Kartenparameter** ändern.

ACHTUNG
Wenn Sie die Zutrittsrechte zu den Schlössern in **Access Commander** ändern, werden die Änderungen auf der Zutrittskarte des Benutzers erst nach der Aktualisierung auf dem Kartenleser des 2N Geräts sichtbar! Aus Sicherheitsgründen empfiehlt es sich, die Gültigkeitsdauer der Karten zu verkürzen, damit sie regelmäßig aktualisiert werden.

IP-Lesegeräte, Geräte, die Kartenaktualisierungen ermöglichen, und deren Einstellungen werden im Kapitel IP-Gerätelesereinstellungen (S. 30).

Kompatible Karten

ANMERKUNG
Für die Zwecke dieser Dokumentation bezeichnet der Begriff **Karte** jeder kompatible Identifikator mit MIFARE DESFire-Technologie.

Zum Öffnen elektronischer Schlösser 2N Fortis Karten mit Zufalls-ID können nicht verwendet werden.

Karten mit PICard-Technologie können nicht zum Öffnen elektronischer Schlösser verwendet werden 2N Fortis.

Zeitprofile auf elektronischen Schlössern

Elektronische Schlösser unterstützen Zeitprofile mit den folgenden Einschränkungen:

- Feiertage gelten nicht.
- Innerhalb eines Tages können bis zu 4 verschiedene Zeitintervalle eingestellt werden.
- Innerhalb eines Zeitprofils können 4 tägliche Intervallpläne definiert werden.

TIPP
Dies bedeutet, dass Sie beispielsweise für Montag, Dienstag, Mittwoch und Donnerstag unterschiedliche Einstellungen haben können, für Freitag, Samstag und Sonntag jedoch eine der vorhandenen Einstellungen verwenden müssen.

ACHTUNG
Verstößt das Zeitprofil gegen die festgelegten Einschränkungen, wird die Zutrittsregel ignoriert und dem Benutzer der Zutritt verweigert.

Fortis Commander

Fortis Commander ist eine eigenständige Anwendung, die die elektronischen Schlösser **Fortis** mit dem System **Access Commander** verbindet. Die Anwendung setzt Sperren entsprechend der in **Access Commander**u erstellten Projektdatei, die die Sperrkonfiguration enthält. Die Datei ist verschlüsselt und kann nur auf einer bestimmten Installation verwendet werden.

Stecker und Installation

Fortis Commander ist für die Installation auf einem Windows-Computer mit Bluetooth Low Energy (BLE) Unterstützung konzipiert.

Die App finden Sie auf der Website 2N Download Centre.

Verlauf der Installierung

1. Laden Sie das Installationspaket über den angegebenen Link herunter.
2. Starten Sie das Installationsprogramm und schließen Sie die Installation ab, indem Sie den Anweisungen auf dem Bildschirm folgen.

Projektdatei

Die Projektdatei wird in **Access Commander** erstellt und enthält die vollständige Projektkonfiguration. Die Datei ist verschlüsselt und passwortgeschützt.

Sperren in Access Commander einstellen

Bevor Sie Schlüssel zu einzelnen Schlössern hochladen können, müssen Sie **Access Commander** mit **Fortis Commander** koppeln.

Generierung des Master Encryption Key (MEK) und Projektvorbereitung

1. Melden Sie sich bei Access Commander an.
2. Gehen Sie zu **Einstellungen > Elektronische Schlösser**.
3. Auf der Registerkarte **Ersteinstellungen** klicken Sie auf Schlüssel generieren.
4. Erstellen Sie den Hauptverschlüsselungscode.

ACHTUNG
Der Hauptverschlüsselungscode kann später weder eingesehen noch geändert werden .

ANMERKUNG
Anhand des Hauptchiffrierschlüssels (MEK) generiert **2N Access Commander** eine Reihe von Chiffrierschlüsseln. Der Schlüssel sollte also eindeutig und ausreichend sicher sein. Der Schlüsselsatz basiert auf dem Hauptchiffrierschlüssel, so dass Projekte mit demselben Hauptchiffrierschlüssel dieselben Schlüsselsätze erzeugen. Wenn ein Projekt verloren geht, kann ein neues Projekt mit demselben Hauptschlüssel erstellt werden und die Verschlüsselung fortsetzen.

5. Nachdem Sie die Schlüssel erzeugt und das Passwort für die Projektdatei festgelegt haben, können Sie **die Projektdatei** herunterladen, die ein Abbild der Konfiguration des elektronischen Schlosses im System **Access Commander** ist.
6. Klicken Sie auf der Registerkarte **von Fortis Commander** auf Anwendung herunterladen, von wo aus das Herunterladen von **Fortis Commander** (Anwendung zur Konfiguration von elektronischen Schlössern) gestartet wird.

ACHTUNG
Projektinformationen sind sensible Daten. Schützen Sie sie vor Missbrauch.

Konfigurieren des elektronischen Schlosses mit Fortis Commander

1. Installieren Sie **Fortis Commander** und öffnen Sie es.
2. Klicken Sie auf Projekt öffnen und öffnen Sie die heruntergeladene Projektdatei im Datei-Explorer.
3. Geben Sie in dem daraufhin angezeigten Dialogfeld das Passwort für die Projektdatei ein.
4. Nachdem Sie die Projektdatei geöffnet haben, wählen Sie Mit Gerät verbinden und verbinden Sie die Servicekarte mit dem Schloss.
5. Klicken Sie auf **Zuweisen**, wodurch die Sperre dem Projekt zugewiesen wird.
6. Trennen Sie die Verbindung zum Gerät und klicken Sie auf **Datei > Projekt schließen**.
7. Wenn die Konfiguration abgeschlossen ist, öffnen Sie das System **Access Commander**. Gehen Sie auf die Registerkarte **Einstellungen > Elektronische Schlösser** und klicken Sie erneut auf Fortis Commander. Laden Sie die Projektdatei hoch.

ANMERKUNG
Wenn Sie das Schloss zwischen Installationen verschieben oder einen Anspruch geltend machen, müssen Sie einen **Factory Reset** durchführen. Dieser Vorgang setzt das Schloss auf die Werkseinstellungen zurück und löscht alle vorherigen Konfigurationen.

Verfahren zur Aktualisierung der Konfiguration

1. Nehmen Sie Änderungen in **Access Commander** vor.
2. Laden Sie die neue Projektdatei herunter.
3. Laden Sie die Datei auf **Fortis Commander** hoch und nehmen Sie die erforderlichen Änderungen an den Schlössern vor.
4. Wenn Sie andere Änderungen an **Access Commander**u vornehmen, laden Sie immer eine neue Projektdatei herunter.

ACHTUNG
Für jede Konfigurationsänderung in **Access Commander**u müssen Sie eine neue Projektdatei herunterladen - Sie können keine ältere Datei verwenden, die bereits auf **Fortis Commander** hochgeladen wurde.

Dauerhaftes Ver- und Entriegeln

Die App ermöglicht es Ihnen, das Schloss dauerhaft zu sperren und zu entsperren. Die Funktion wird für Service-Einsätze oder Notfallkontrollen ohne Verwendung einer Karte verwendet.

Erfassung von Ereignissen aus elektronischen Schlössern mit RFID-Karten/Chips

Einstellungen für die Ereignissammlung

1. Öffnen Sie **Einstellungen > Elektronische Schlösser > Registerkarte Ereignisse**.
2. Wählen Sie den Ereignistyp:
   - **Sammeln von Zugangs- und Systemereignissen** - Alle Zugangs- und Systemereignisse werden auf der Karte/dem Chip aufgezeichnet und in das **System Log** und **Access Log** geschrieben.
   - **Nur Systemereignisse sammeln** - nur Systemereignisse werden protokolliert, Zugriffsereignisse werden nicht auf Karten gespeichert.
   - **Sammeln Sie keine Ereignisse auf** Registerkarten - es werden keine Ereignisse auf die Registerkarte geschrieben; sie können nur über **Fortis Commander**u aufgerufen werden.

> **TIPP**
> Wenn Sie geeigneten Ereignissatzes auswählen, können Sie die Systemlast und die Nutzung des Speicherplatzes verringern. Eine detaillierte Protokollierung ist jedoch für Diagnosen und Sicherheitsaudits wichtig.

Ereignisse von einer Karte exportieren

Die Karte speichert maximal **16 erste Ereignisse**. Ereignisse können auf zwei Arten gelesen werden:

- Klicken Sie in **Access Commander** auf das Symbol im Suchfeld in der Kopfzeile und laden Sie die Registerkarte.
- Wenn Sie ein Gerät mit **2N OS** verwenden, werden Ereignisse von der Karte gelesen und an **Access Commander**u gesendet.

Hochladen von Ereignissen auf das Schloss

1. Öffnen Sie **Einstellungen > Elektronische Schlösser > Fortis Commander** und klicken Sie auf Datei herunterladen.
2. Öffnen Sie die Datei in **Fortis Commander**.
3. Verbinden Sie sich über die App **Fortis Commander** mit dem elektronischen Schloss.
4. Laden Sie die aktualisierte Datei wieder auf **Access Commander** hoch.
5. Nach dem Hochladen werden die Ereignisse in **Zugriffsprotokolle** und **Systemprotokolle** angezeigt.

Serviceleistungen

Diese Funktionen sind verfügbar für **Fortis Cylinder**:

- **Demontage** - Demontage von Schlössern zu Servicezwecken.
- **Auswechseln der Batterie** - Auswechseln der Batterie im Schloss.

> **ACHTUNG**
> Servicevorgänge sind für andere Arten von Sperren nicht relevant.

> **ANMERKUNG**
> Aus dem Servicemodus kehrt das Schloss in den normalen Modus zurück, indem Sie die Taste Lock drücken, um es dauerhaft zu sperren.

IP-Gerätelesereinstellungen

Einstellungen in der Weboberfläche des IP-Geräts

ACHTUNG
Wenn Sie ein neues RFID-Kartenleser-Erweiterungsmodul über ein VBUS-Kabel an das 2N Gerät anschließen, müssen Sie dieses Modul mit dem Gerät koppeln. Das Pairing des Leser-Erweiterungsmoduls kann über die Weboberfläche des Geräts unter **Zugriff > Module** durchgeführt werden.

1. Geben Sie die Webkonfiguration des Geräts ein.

   TIPP
   Sie können auf die webbasierte Konfigurationsschnittstelle zugreifen, indem Sie in der Liste auf der Seite Geräte klicken .

2. Gehen Sie zu Hardware > Erweiterungsmodule.
3. Gehen Sie auf der Seite zu den Einstellungen des RFID-Kartenlesermoduls.
4. Klicken Sie auf Paarmodul.
5. Aus dem Menü **Erlaubte Kartentypen** Wählen Sie eine Option „Elektronische Schlösser von 2N“.

   ACHTUNG
   Für eine optimale Funktionalität aktivieren Sie nur die Kartentypen, die Sie tatsächlich verwenden.

6. Speichern Sie die Änderungen.

Kompatible Module

Synchronisierung von Schlüsseln mit elektronischen Schlössern 2N Fortis Die Überprüfung kann mit allen 2N RFID-Lesegeräten durchgeführt werden, die ab Februar 2023 auf den Markt kommen. Die meisten nach diesem Datum hergestellten Lesegeräte sind ebenfalls kompatibel, mit Ausnahme der unten aufgeführten Modelle.

Die folgenden Modelle **sind nicht kompatibel**:

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

Bei den folgenden Modulen ist die Kompatibilität nur für Geräte gewährleistet, die im Herbst 2023 oder später hergestellt wurden:

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

Sperren in Access Commander einstellen

Bevor Sie Schlüssel zu einzelnen Schlössern hochladen können, müssen Sie **Access Commander** mit **Fortis Commander** koppeln.

Generierung des Master Encryption Key (MEK) und Projektvorbereitung

1. Melden Sie sich bei Access Commander an.
2. Gehen Sie zu **Einstellungen > Elektronische Schlösser**.
3. Auf der Registerkarte **Ersteinstellungen** klicken Sie auf Schlüssel generieren.
4. Erstellen Sie den Hauptverschlüsselungscode.

ACHTUNG
Der Hauptverschlüsselungscode kann später weder eingesehen noch geändert werden .

ANMERKUNG
Anhand des Hauptchiffrierschlüssels (MEK) generiert **2N Access Commander** eine Reihe von Chiffrierschlüsseln. Der Schlüssel sollte also eindeutig und ausreichend sicher sein. Der Schlüsselsatz basiert auf dem Hauptchiffrierschlüssel, so dass Projekte mit demselben Hauptchiffrierschlüssel dieselben Schlüsselsätze erzeugen. Wenn ein Projekt verloren geht, kann ein neues Projekt mit demselben Hauptschlüssel erstellt werden und die Verschlüsselung fortsetzen.

5. Nachdem Sie die Schlüssel erzeugt und das Passwort für die Projektdatei festgelegt haben, können Sie **die Projektdatei** herunterladen, die ein Abbild der Konfiguration des elektronischen Schlosses im System **Access Commander** ist.
6. Klicken Sie auf der Registerkarte **von Fortis Commander** auf Anwendung herunterladen**,** von wo aus das Herunterladen von **Fortis Commander** (Anwendung zur Konfiguration von elektronischen Schlössern) gestartet wird.

ACHTUNG
Projektinformationen sind sensible Daten. Schützen Sie sie vor Missbrauch.

Konfigurieren des elektronischen Schlosses mit Fortis Commander

1. Installieren Sie **Fortis Commander** und öffnen Sie es.
2. Öffnen Sie die Datenbank, die Sie mit der Anwendung heruntergeladen haben.
3. Klicken Sie auf Projekt öffnen und öffnen Sie die heruntergeladene Projektdatei im Datei-Explorer.
4. Geben Sie in dem daraufhin angezeigten Dialogfeld das Passwort für die Projektdatei ein.
5. Wenn die Konfiguration abgeschlossen ist, öffnen Sie das System **Access Commander**. Gehen Sie auf die Registerkarte **Einstellungen > Elektronische Schlösser** und klicken Sie erneut auf Fortis Commander. Laden Sie die Projektdatei hoch.
6. Trennen Sie die Verbindung zum Gerät und klicken Sie auf **Datei > Projekt schließen**.
7. Speichern Sie die Einstellungen, indem Sie auf das Haussymbol mit dem ✓-Symbol klicken.

ANMERKUNG
Wenn Sie das Schloss zwischen Installationen verschieben oder einen Anspruch geltend machen, müssen Sie einen **Factory Reset** durchführen. Dieser Vorgang setzt das Schloss auf die Werkseinstellungen zurück und löscht alle vorherigen Konfigurationen.

Verfahren zur Aktualisierung der Konfiguration

1. Nehmen Sie Änderungen in **Access Commander** vor.
2. Laden Sie die neue Projektdatei herunter.
3. Laden Sie die Datei auf **Fortis Commander** hoch und nehmen Sie die erforderlichen Änderungen an den Schlössern vor.
4. Wenn Sie andere Änderungen an **Access Commander**u vornehmen, laden Sie immer eine neue Projektdatei herunter.

ACHTUNG
Für jede Konfigurationsänderung in **Access Commander**u müssen Sie eine neue Projektdatei herunterladen - Sie können keine ältere Datei verwenden, die bereits auf **Fortis Commander** hochgeladen wurde.

Dauerhaftes Ver- und Entriegeln

Die App ermöglicht es Ihnen, das Schloss dauerhaft zu sperren und zu entsperren. Die Funktion wird für Service-Einsätze oder Notfallkontrollen ohne Verwendung einer Karte verwendet.

Karten für die Wartung

Wartungskarten ermöglichen den autorisierten Zugang zum Schloss. Sie ermöglichen es, das Schloss in Betrieb zu nehmen, die Batterie zu wechseln und das Schloss zu demontieren.

ACHTUNG
Die Wartungskarte kann nicht gleichzeitig als Benutzerzugangskarte verwendet werden.

Einstellungen auf der Registerkarte Wartung

1. Gehen Sie in **Access Commander** zu **Einstellungen > Elektronische Schlösser**.
2. Klicken Sie auf der Registerkarte **Wartung** auf Erstellen.

3. Wählen Sie in dem sich öffnenden Dialogfeld die Art der Karte aus, die Sie erstellen möchten.
   - Einstellung neuer Schlösser - aktiviert zuvor konfigurierte neue Schlösser in den Werkseinstellungen im Servicemodus.
   - Service - aktiviert den Servicemodus für das bereits eingestellte Schloss.
   - Demontage - gibt das bereits eingestellte 2N Fortis Zylinderschloss zur Demontage frei, siehe 2N Fortis Installationshandbuch.
   - Batteriewechsel - gibt das bereits eingestellte 2N Fortis Zylinderschloss zum Batteriewechsel frei, siehe 2N Fortis Installationshandbuch.

   TIPP
   Eine physische Karte kann gleichzeitig mit **Setting New Locks** und einer anderen Servicekarte geladen werden. Wir empfehlen eine Kombination aus **Einstellung neuer Schlösser** und **Service**.
4. Klicken Sie auf . Weiter zu.
5. Schließen Sie die Karte an das angeschlossene USB-RFID-Lesegerät an. Warten Sie, bis die Daten auf die Karte geladen sind.

Die Gültigkeit der Daten auf der Wartungskarte beträgt ein Jahr. Nach Ablauf dieser Zeit müssen die Daten gelöscht und die Karte neu eingerichtet werden.

Unterstützung für DESFire-Karten von Drittanbietern (Anonyme App-Erstellung)

Access Commander ermöglicht Ihnen die Arbeit mit MIFARE DESFire-Karten. Es unterstützt Karten, die bereits in anderen Zugangskontrollsystemen im Einsatz sind, und ermöglicht deren Wiederverwendung, ohne dass Sie den Hauptschlüssel (PICC Master Key) kennen müssen.

Dies ist ein spezieller Modus, in dem die Karte die Erstellung einer neuen, unabhängigen Anwendung ermöglicht, ohne dass der Hauptschlüssel (PICC Master Key) bekannt sein muss.

Mit dieser Funktion können Administratoren:

- Verwenden Sie vorhandene physische Karten wieder.
- Schreiben Sie die OSO-Anwendung für **Access Commander** zu ihnen.
- Sie müssen den PICC Master Key der Originalsysteme nicht mehr kennen oder verwalten.

So erstellen Sie eine OSO-Anwendung auf einer Registerkarte

1. Schließen Sie die vorhandene DESfire-Karte des Benutzers an ein Lesegerät an, das an **Access Commander** angeschlossen ist.
2. Erstellen Sie Benutzeranmeldeinformationen.
3. Access Commander erkennt automatisch, ob die Karte die Erstellung anonymer Anwendungen unterstützt.
4. Wenn der Modus unterstützt wird, schreibt **Access Commander** eine neue anonyme Anwendung auf die Karte, ohne bestehende Daten oder Anwendungen von Drittanbietern zu beeinträchtigen.

   ACHTUNG
   Wenn der Modus unterstützt wird, schreibt Access Commander eine neue anonyme Anwendung ohne die Möglichkeit, die Karte später über eine Funktion im Bereich Einstellungen zu formatieren. Nur der Inhalt der Anwendung kann gelöscht werden, nicht der zuvor belegte Speicherplatz auf der Karte.

Grundlegender Zugriff auf die Schnittstelle

In diesem Kapitel werden die Inbetriebnahme und die grundlegende Verwendung beschrieben ***Access Commander****. Die Installation wird im Kapitel beschrieben* *Installation (S. 13)**.*

Die Schnittstelle **des Access Commander** ist über einen Webbrowser zugänglich. Die IP-Adresse der Webschnittstelle können Sie mit 2N Network Scanner oder Axis IP Utility abrufen. Die Weboberfläche kann auch direkt unter **accesscommander.local** aufgerufen werden. Diese Funktion ist standardmäßig aktiviert.

ANMERKUNG

- Wenn mehrere Access Commander-Instanzen im Netzwerk ausgeführt werden, vergibt das System automatisch eindeutige Namen: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local** und andere Instanzen auf der Grundlage der Anzahl der Server im Netzwerk.
- Für die Verteilung über Access Commander Box verbinden Sie sich von einem anderen Computer im Netzwerk mit der Webschnittstelle. Das Betriebssystem Access Commander Box führt den **Access Commander** und seine grundlegenden Linux-Einstellungen aus, erlaubt Ihnen aber nicht, einen Webbrowser zu verwenden.

ANMERKUNG
Im Falle einer Weitergabe per Access Commander Box Stellen Sie von einem anderen Computer im Netzwerk aus eine Verbindung zur Weboberfläche her. Betriebssystem Access Commander Box stellt den Betrieb sicher **Access Commander** und sein grundlegendes Linux-Setup lässt die Ausführung des Webbrowsers nicht zu.

Die Standard-Anmeldedaten sind:

Benutzername: **Admin**

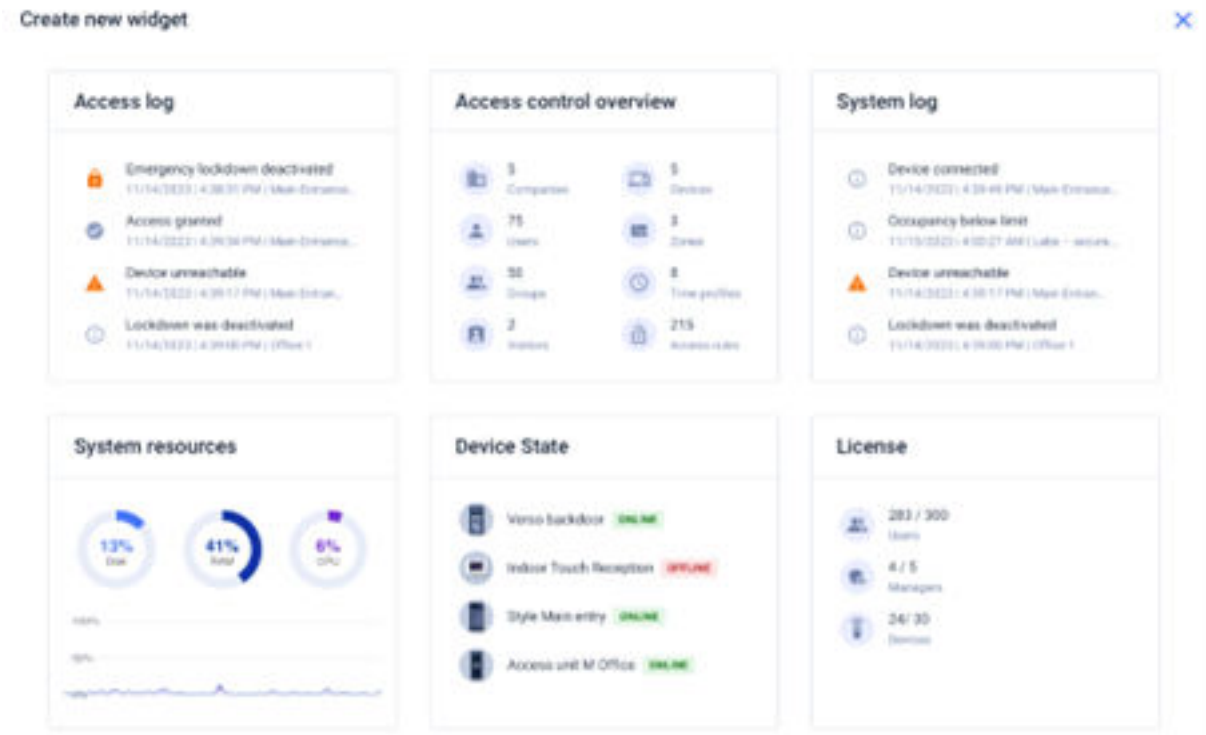
Passwort: **2n**

Nach der ersten Anmeldung ist unverzüglich das Passwort zu ändern.

ANMERKUNG
Aktivieren Sie die Option **Nicht abmelden**, wenn Sie vermeiden möchten, dass Sie Ihre Anmeldedaten bei der nächsten Anmeldung erneut eingeben müssen. Die Anmeldung ist maximal 7 Tage lang gültig, danach müssen Sie sich erneut anmelden.

Möglicherweise ist eine Anmeldung erforderlich Zwei-Faktoren-Authentifizierung (S. 104).

Armaturenbrett



Das Dashboard ist eine grundlegende Ansicht der Webschnittstelle **Access Commander**. Es handelt sich um ein konfigurierbares Dashboard, das Echtzeitdaten anzeigt. **Access Commander** bietet verschiedene Widgets, die über die Schaltfläche + zum Dashboard hinzugefügt werden. Die Widgets auf dem Dashboard können verschoben, umbenannt oder ihre Grundeinstellungen auf verschiedene Weise geändert werden. Die Verwaltung und das Löschen von Widgets erfolgt über das erweiterte Menü ⋮ in der Kopfzeile jedes Widgets.

Jeder Benutzer mit einem Konto bei **Access Commander** Sie können Ihr eigenes Dashboard einrichten. Die Verfügbarkeit von Widgets ist abhängig von der Rolle des Benutzers und der verfügbaren Lizenz begrenzt.

Sprachwechsel

Nach der ersten Anmeldung se **Access Commander** wird in der Sprache angezeigt, die für das Unternehmen des angemeldeten Benutzers eingestellt ist. Jeder Benutzer kann die Sprache ändern. Nach dem nächsten Login wird die Oberfläche in der neu eingestellten Sprache angezeigt.

1. Mit einem Klick auf das Bild des Benutzers in der oberen rechten Ecke öffnet sich das Benutzermenü.
2. Wählen Sie Sprache ändern.
3. Wählen Sie die entsprechende Sprache aus und bestätigen Sie mit Sprache ändern.

Passwortänderung des Kontos

1. Mit einem Klick auf das Bild des Benutzers in der oberen rechten Ecke öffnet sich das Benutzermenü.
2. Wählen Sie Profil anzeigen.
3. Klicken Sie auf das ✎ neben dem Parameter Passwort.

4. Bestätigen Sie Ihr bestehendes Passwort und geben Sie ein neues ein.

ANMERKUNG
Wenn das Passwort für das "admin"-Konto dasselbe ist wie das Passwort des Root-Benutzers des Systems (für die Anmeldung bei der Linux-Setup-Konsole), wird bei einer Änderung des Passworts für das "admin"-Konto automatisch auch das Passwort für das Root-Konto geändert.

Ändere dein Profilbild

1. Mit einem Klick auf das Bild des Benutzers in der oberen rechten Ecke öffnet sich das Benutzermenü.
2. Wählen Sie Profil anzeigen.
3. Klicken Sie auf das Bild in der Kopfzeile der Benutzerdetails.
4. Legen Sie im geöffneten Dialogfeld das Foto fest.
   Die Bildauflösung wird automatisch auf 432 × 432 Pixel angepasst.

Logos

Hier ist eine Übersicht über den Inhalt des Kapitels:

- Systemprotokolle (S. 37)
- Zugriffsprotokolle (S. 38)
- Benachrichtigung (S. 40)
- Lebensdauer der Protokolle (S. 37)

Systemprotokolle

ANMERKUNG

- Dem Benutzer werden die Protokolle angezeigt, die er je nach Benutzerberechtigung anzeigen darf.
- Die Daten werden auf Englisch in die Protokolle geschrieben.

Die Seite Systemprotokolle zeigt eine Liste der Ereignisse und Benachrichtigungen an, die das System erzeugt hat.

In der Liste der Systemprotokolle wird für jedes Ereignis und jede Benachrichtigung Folgendes angezeigt:

- Schweregrad (Info, Warnung, Fehler).
- die Zeit, zu der das Ereignis eingetreten ist.
- die Kategorie, zu der die Aktion gehört (Gerätestatus, Import, Benutzersynchronisierung, System, Benutzeraktionen, Bereichseinschränkungen).
- Subjekt, auf das sich die Aktion bezieht (Anlage, Benutzer, Zone, Besuch...).
- kurze Beschreibung des Ereignisses.
- Veranstaltungsautor.

Durch Klicken auf eine Zeile werden detaillierte Informationen zum jeweiligen Datensatz angezeigt.

Die Liste kann mit gefiltert werden oberhalb der Liste. Alternativ können im erweiterten Menü, das sich durch Klicken auf öffnet, Filter für einzelne Spalten gesetzt werden in der Kopfzeile jeder Spalte. Erweitertes Spaltenmenü Außerdem können Spalten verschoben, an der ersten oder letzten Position angeheftet oder ausgeblendet werden.

Die Spalten „Schweregrad“ und „Zeit“ können nicht ausgeblendet werden.

Export von Logos

Die Datensätze können in eine CSV-Datei heruntergeladen werden, indem Sie auf die Schaltfläche Export oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 angegeben.

Lebensdauer der Protokolle

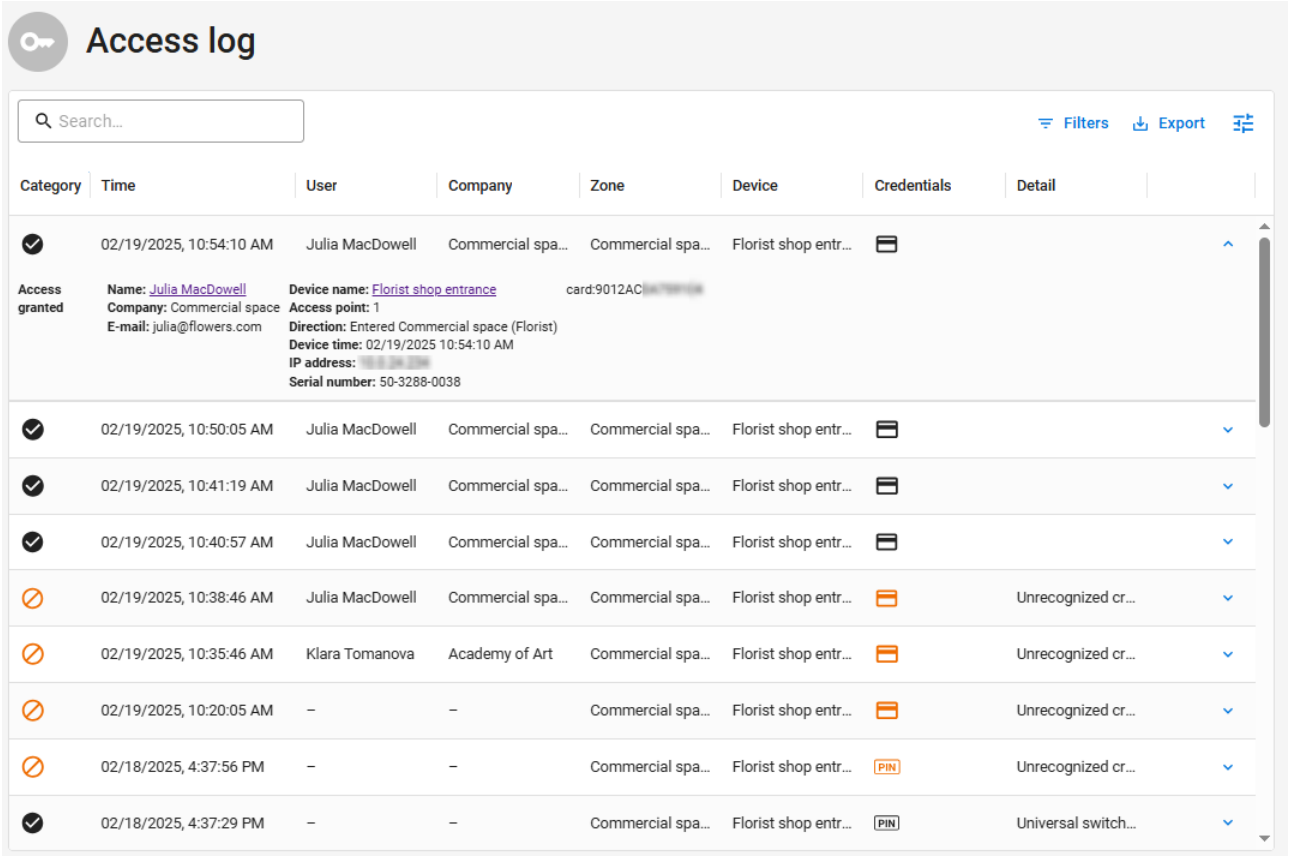
Sobald die Festplattenkapazitätsauslastung 80 % erreicht, beginnt die automatische Protokolllöschung. Die Festplattenkapazität kann auf der Seite „Einstellungen“ überwacht werden. Protokolle des ersten Typs wer-

den zuerst der Reihe nach gelöscht, andere Protokolle werden nach und nach gelöscht, bis die Speicherplatznutzung auf 75 % sinkt oder bis nur noch Protokolle mit unvollständiger minimal möglicher Speicherzeit des angegebenen Protokolltyps übrig bleiben.

Die Speicherzeit für einen bestimmten Protokolltyp wird auf der **Registerkarte Einstellungen > Speicherung der Aufzeichnungen**. Die Aufbewahrung von Kameraaufzeichnungen darf nicht länger sein als die Aufbewahrung von System- und Zugriffsprotokollen.

TIPP
Wenn Sie ständig 70 % der Festplattenkapazität nutzen, empfehlen wir, die maximale Protokollspeicherzeit zu verkürzen.

Zugriffsprotokolle



ANMERKUNG

- Dem Benutzer werden die Protokolle angezeigt, die er je nach Benutzerberechtigung anzeigen darf.
- Die Daten werden auf Englisch in die Protokolle geschrieben.

Auf der Seite „Zugriffsprotokolle“ werden Aufzeichnungen erfolgreicher und fehlgeschlagener Authentifizierungsversuche sowie Notfallsperrungen angezeigt.

In der Liste der Zugriffsprotokolle heißt es:

- **Kategorie**
  - Zugriff erlaubt
  - Zugriff abgelehnt
  - Öffentlichen Zugang ermöglichen
  - Sperren des Geräts
- **Zeit**, als das Ereignis eintrat
- **Benutzer**, der die Aktion ausgeführt hat
- **Unternehmen** des angegebenen Benutzers
- **Zone**, in dem die Aktion stattgefunden hat
- **Gerät**, an dem das Ereignis aufgetreten ist
- **Authentifizierung**, der für das Experiment verwendet wurde (PIN, QR-Code usw.)

Durch Klicken auf eine Zeile werden detaillierte Informationen zum jeweiligen Datensatz angezeigt.

Die Liste kann mit gefiltert werden oberhalb der Liste. Alternativ können im erweiterten Menü, das sich durch Klicken auf öffnet, Filter für einzelne Spalten gesetzt werden in der Kopfzeile jeder Spalte. Erweitertes Spaltenmenü Außerdem können Spalten verschoben, an der ersten oder letzten Position angeheftet oder ausgeblendet werden.

Export von Logos

Die Datensätze können in eine CSV-Datei heruntergeladen werden, indem Sie auf die Schaltfläche Export oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 angegeben.

Lebensdauer der Protokolle

Sobald die Festplattenkapazitätsauslastung 80 % erreicht, beginnt die automatische Protokolllöschung. Die Festplattenkapazität kann auf der Seite „Einstellungen“ überwacht werden. Protokolle des ersten Typs werden zuerst der Reihe nach gelöscht, andere Protokolle werden nach und nach gelöscht, bis die Speicherplatznutzung auf 75 % sinkt oder bis nur noch Protokolle mit unvollständiger minimal möglicher Speicherzeit des angegebenen Protokolltyps übrig bleiben.

Die Speicherzeit für einen bestimmten Protokolltyp wird auf der **Registerkarte Einstellungen > Speicherung der Aufzeichnungen**. Die Aufbewahrung von Kameraaufzeichnungen darf nicht länger sein als die Aufbewahrung von System- und Zugriffsprotokollen.

TIPP
Wenn Sie ständig 70 % der Festplattenkapazität nutzen, empfehlen wir, die maximale Protokollspeicherzeit zu verkürzen.

Anrufprotokoll

Auf der Seite Anrufprotokoll werden alle Anrufe von angeschlossenen Gegensprechanlagen und anderen SIP-Geräten (z. B. Anrufbeantwortern oder Aufzugskommunikatoren) aufgezeichnet.

ANMERKUNG
Das Anrufprotokoll ist nur mit der Benutzerberechtigung Administrator verfügbar.

Die Anrufprotokollliste für jedes Ereignis gibt an:

- Gesprächstyp
- die Uhrzeit, zu der der Anruf erfolgte
- ob die Tür entriegelt ist
- Gerätetyp
- Gegenpartei
- Gesprächsdauer
- Grund für die Beendigung des Gespräches

Durch Klicken auf eine Zeile werden detaillierte Informationen zum jeweiligen Datensatz angezeigt.

Die Liste kann mit gefiltert werden oberhalb der Liste. Alternativ können im erweiterten Menü, das sich durch Klicken auf öffnet, Filter für einzelne Spalten gesetzt werden in der Kopfzeile jeder Spalte. Erweitertes Spaltenmenü Außerdem können Spalten verschoben, an der ersten oder letzten Position angeheftet oder ausgeblendet werden.

Export von Logos

Die Datensätze können in eine CSV-Datei heruntergeladen werden, indem Sie auf die Schaltfläche Export oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 angegeben.

Lebensdauer der Protokolle

Die Aufbewahrungszeit für einen bestimmten Protokolltyp wird auf der Registerkarte *Einstellungen* > *Protokollaufbewahrung* festgelegt.

TIPP
Wenn Sie ständig 70 % der Festplattenkapazität nutzen, empfehlen wir, die maximale Protokollspeicherzeit zu verkürzen.

ACHTUNG
Es wird empfohlen, dass Sie die neueste Firmware-Version auf Ihren Geräten verwenden, damit alle Funktionen des Anrufprotokolls ordnungsgemäß funktionieren. Einige Informationen und Spalten sind möglicherweise nicht verfügbar oder werden auf Geräten mit älteren Firmware-Versionen nicht korrekt angezeigt.

- **Gesprächsdauer:** Die Spalte Anruflänge wird von älteren Firmware-Versionen nicht unterstützt. Diese Informationen sind ab Firmware-Version 2.49 und höher verfügbar.
- **Identifizierung der Gegenpartei:** Die Firmware-Version 2.50 und höher ist erforderlich, um die Gegenpartei aus dem Geräteverzeichnis korrekt zu identifizieren. Bei älteren Versionen verhält sich die Suche im Geräteverzeichnis möglicherweise nicht korrekt.

Benachrichtigung

Mit dem Benachrichtigungsmodul können Sie die Überwachung ausgewählter Ereignisse und Systemeigenschaften einrichten, die ihm bekannt sind **Access Commander** Informieren Sie per E-Mail oder Benachrichtigung in der oberen Leiste neben dem Benutzermenü.

Die Liste der Benachrichtigungen wird auch auf der **Seite Systemprotokolle > Benachrichtigungen angezeigt**.

Die Datensätze können in eine CSV-Datei heruntergeladen werden, indem Sie auf die Schaltfläche Export oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 angegeben.

Einrichten eines neuen Benachrichtigungstyps

1. Gehen Sie zur Seite **Einstellungen > Benachrichtigungen**.
2. Klicken Sie oben rechts auf der Seite auf die Schaltfläche „Hinzufügen“.
3. Geben Sie einen Namen für den neuen Benachrichtigungstyp ein.
   Nach der Erstellung werden die Details der Benachrichtigung angezeigt, in der die Geräte ausgewählt werden können, für die die Benachrichtigung überwacht werden soll; Benutzer hinzufügen, an die die Benachrichtigung gesendet werden soll; Wählen Sie die Zustellungsmethode für die Benachrichtigung.

Benachrichtigungseinstellungen

Die Benachrichtigungsarten werden in den Details der Benachrichtigungsart festgelegt. Um die Details der Benachrichtigungsart zu öffnen, klicken Sie auf die ausgewählte Benachrichtigung in der Liste auf der Seite **Einstellungen > Benachrichtigungen**.

Art der Benachrichtigung

Auf dieser Registerkarte werden die Benachrichtigungsmethoden und die Liste der E-Mail-Benachrichtigungsempfänger festgelegt.

In **Access Commander** erscheinen die Benachrichtigungen unter dem in der oberen Leiste, neben dem Benutzermenü oder unter **Systemprotokoll > Benachrichtigungen**.

Benachrichtigungs-E-Mails können an die in verwalteten Benutzer gesendet werden **Access Commander** und Empfänger außerhalb des Systems. Benutzer können aus der Liste ausgewählt werden. Die E-Mail-Adressen der anderen Empfänger müssen manuell eingegeben werden.

ANMERKUNG
Für die korrekte Funktion von E-Mail-Benachrichtigungen ist die korrekte Einstellung von SMTP erforderlich, siehe E-Mail-Funktion (SMTP) aktivieren und einrichten (S. 103).

Überwachte Geräte

Der angegebene Benachrichtigungstyp kann sowohl für alle Geräte als auch nur für einige Geräte generiert werden. Wenn „Alle Geräte überwachen“ aktiviert ist, kann das Ereignis auf jedem Gerät auftreten und es wird eine Benachrichtigung generiert. Wenn die Überwachung aller Geräte deaktiviert ist, wird nur dann eine Benachrichtigung generiert, wenn das Ereignis auf dem ausgewählten Gerät auftritt. Die Auswahl des Gerätes erfolgt im Menü, das mit geöffnet wird .

Lebensdauer der Protokolle

Sobald die Festplattenkapazitätsauslastung 80 % erreicht, beginnt die automatische Protokolllöschung. Die Festplattenkapazität kann auf der Seite „Einstellungen“ überwacht werden. Protokolle des ersten Typs werden zuerst der Reihe nach gelöscht, andere Protokolle werden nach und nach gelöscht, bis die Speicherplatznutzung auf 75 % sinkt oder bis nur noch Protokolle mit unvollständiger minimal möglicher Speicherzeit des angegebenen Protokolltyps übrig bleiben.

Die Speicherzeit für einen bestimmten Protokolltyp wird auf der **Registerkarte Einstellungen > Speicherung der Aufzeichnungen**. Die Aufbewahrung von Kameraaufzeichnungen darf nicht länger sein als die Aufbewahrung von System- und Zugriffsprotokollen.

TIPP
Wenn Sie ständig 70 % der Festplattenkapazität nutzen, empfehlen wir, die maximale Protokollspeicherzeit zu verkürzen.

Unternehmen

Innerhalb einer einzelnen Installation können die **Access Commander**-Einstellungen in Unternehmen unterteilt werden, die separat verwaltet werden.Teilen in **Unternehmen**. Diese Methode ermöglicht es, die Administration auf die Administratoren einzelner Unternehmen aufzuteilen. Ein Administrator eines Unternehmens hat keinen Zugriff auf Informationen über ein anderes Unternehmen. Administratoren eines Unternehmens sehen keine Benutzer eines anderen Unternehmens.

Zonen oder Einrichtungen können unternehmensübergreifend gemeinsam genutzt werden, sodass der Unternehmenszugang zu Gemeinschaftsbereichen (Eingänge, Restaurants, Konferenzräume usw.) verwaltet werden kann.

Gründung eines neuen Unternehmens

1. Gehen Sie zur Seite **Unternehmen**.
2. Klicken Sie oben rechts auf die Schaltfläche „Unternehmen hinzufügen“.
3. Geben Sie den Unternehmennamen ein.
4. Sie können ein Unternehmen gründen, indem Sie auf klicken Erstellen.
   Das neu erstellte Unternehmen wird in der Liste angezeigt. In den Details des Unternehmens müssen dessen Einstellungen vorgenommen werden. Das Hinzufügen von Benutzern zum Unternehmen erfolgt in den Einstellungen der einzelnen Benutzer.

Unternehmeneinstellungen

Unternehmeninformationen können in den Unternehmendetails eingesehen und bearbeitet werden. Ein Unternehmendetail wird geöffnet, indem Sie auf der Seite „Unternehmen“ auf ein ausgewähltes Unternehmen in seiner Liste klicken.

In der Kopfzeile des Firmendetails befindet sich eine Schaltfläche Sperren, die die Notabschaltung (S. 64) für alle Geräte in den Zonen dieser Firma aktiviert.

Die Unternehmensdetails sind in die Registerkarten „Übersicht“, „E-Mails“ und „Benutzersynchronisierung“ unterteilt.

Die Sprache der Gesellschaft

Im Reiter „Allgemein“ können Sie die Unternehmenssprache auswählen, in der die Oberfläche genutzt werden soll **Access Commander**Benutzern in diesem Unternehmen angezeigt werden. Benutzer können die Sprache der Benutzeroberfläche später ändern. Die Wahl der Sprache durch das Unternehmen wirkt sich auch auf die E-Mail-Vorlagen aus, die an Benutzer gesendet werden. Der Wortlaut von E-Mails kann im Reiter E-Mails geändert werden.

Zonen

Durch die Zuweisung von Zonen zu einem Unternehmen wird der Satz von Einrichtungen definiert, auf die Benutzer des Unternehmens Zugriff haben (z. B. die Gemeinschaftsbereiche und die Zone im 4. Stock, einschließlich der Eingangstür zur Rezeption und aller Eingänge im vierten Stock).). Zonen können mehreren Unternehmen gleichzeitig zugewiesen werden, und mehrere Zonen können einem Unternehmen zugewiesen werden.

My2N app

Im Unternehmen besteht die Möglichkeit, Pairing-Parameter festzulegen My2N App, was die Bluetooth-Authentifizierung ermöglicht. Es werden sowohl die Geräte festgelegt, mit denen Benutzer eine Kopplung durchführen können, als auch die für die Kopplung erforderliche Gültigkeitsdauer des mobilen Zugriffs. Der mobile Zugang selbst wird in den Benutzereinstellungen generiert.

Besuche

Auf dieser Registerkarte werden Gruppen eingerichtet, denen der Besuchsadministrator neue Besuche zuordnen kann. Eine der Gruppen kann als Standard festgelegt werden. Sofern nicht anders festgelegt, wird der neue Besuch automatisch der Standardgruppe zugeordnet.

ACHTUNG
Ohne eine korrekt eingestellte Standardgruppe ist es nicht möglich, Besuchern in der vereinfachten Benutzeroberfläche Zugriff zu gewähren.

Es besteht auch die Möglichkeit auszuwählen, auf welche Weise der Besuch gewährt werden kann.

Weitere Informationen zum Einrichten von Besuchen in Besuche (S. 81).

Arbeitsfonds

Arbeitspool und Feiertage werden zur Berechnung des monatlichen Arbeitspools der Benutzer im Anwesenheitsmodul verwendet. Durch die Auswahl der Tage kann festgelegt werden, welche Wochentage als Arbeitstage gezählt werden. Durch Anklicken wird der Tag ausgewählt. Grüne Tage geben an, welche Tage als Arbeitstage gelten.

Die Arbeitszeitanpassung legt fest, wie viel Zeit eine Tagesschicht hat.

Feiertage

Durch die Festlegung von Feiertagen legen Sie fest, welche Tage bei der Berechnung des monatlichen Arbeitspools nicht berücksichtigt werden. An Feiertagen geleistete Arbeitsstunden werden genauso gezählt wie an Wochenenden geleistete Arbeitsstunden – die geleistete Arbeitszeit wird zusätzlich zur normalen Arbeitszeit erfasst.

Erweitertes Angebot ⋮ ermöglicht es Ihnen, Feiertage von einem anderen Unternehmen zu kopieren. Feiertage werden inklusive Datum und Namen kopiert. Das Kopieren kann wiederholt verwendet werden, wenn der neu kopierte Feiertag jedoch bereits im Unternehmen festgelegt ist, wird sein Name überschrieben.

E-Mails, die an Unternehmenmitglieder gesendet werden

Für die E-Mail-Einstellungen gibt es in den Unternehmendetails eine eigene Registerkarte. **Access Commander** ermöglicht den automatischen Versand von E-Mails an Unternehmenmitglieder (auch Besucher) mit Informationen über die Zuweisung einer Authentifizierungsmethode. Eine E-Mail mit der eingestellten E-Mail-Adresse wird an den Benutzer oder Besucher gesendet.

Access Commander ermöglicht Ihnen das Versenden von E-Mails mit den folgenden Informationen:

- PIN-Code für den Besuch
- QR-Code für den Besuch
- PIN-Code für den Benutzer
- QR-Code für Benutzer
- My2N app zum Einrichten der Bluetooth-Authentifizierung für den Benutzer

In den **Unternehmensdetails > Registerkarte „E-Mails“ > Registerkarte „Vorlagen“** können Sie das Erscheinungsbild dieser E-Mails festlegen und ihren Wortlaut bearbeiten. Das Bearbeiten des Wortlauts einer E-Mail erfolgt in einem Dialogfenster, das sich durch Klicken auf den ausgewählten E-Mail-Typ öffnet. Im Dialogfeld können Sie Folgendes bearbeiten:

- Betreff – der Betreff der E-Mail
- Kopfzeile – wird im farbigen Feld des E-Mail-Texts angezeigt

- Einleitung – der Text, der vor den automatisch generierten Daten angegeben wird **Access Commander**
- nächste Nachricht – der Text, der auf die von generierten Daten folgt **Access Commander**
- Signatur – die Signatur am Ende der E-Mail

Synchronisierung des Unternehmens (LDAP)

Die Synchronisierung mit LDAP wird zum Herunterladen von Benutzern und ihren Änderungen von einem externen LDAP-System verwendet. Zu den Benutzerdaten gehören Benutzername, ID, Kartenkennungen, PIN/QR-Code, Bild, E-Mail-Adresse, Telefonnummer, Passwort und Login sowie Fahrzeugkennzeichen.

ANMERKUNG
Weitere Informationen zu LDAP finden Sie unter www.ldap.com.

1. Gehen Sie zu **Firmen > ausgewählte Firmendetails > Registerkarte Benutzersynchronisierung**.
2. Wenn keine Verbindung festgelegt ist, erstellen Sie eine.
   Ausfüllen:

   - **Der Name des Servers** – Wenn DNS richtig eingestellt ist, geben Sie einfach den Namen des Servers ein („WIN-9ABEB4AUOHD“). Wenn DNS nicht eingestellt ist, wird im Servernamen die IP-Adresse des Servers eingetragen, auf dem der LDAP-Dienst läuft.
   - **Hafen** – Die Standardeinstellung ist LDAP-Port 389 (ohne SSL). Wenn Sie in Ihrem Unternehmen eine verschlüsselte Verbindung nutzen möchten, geben Sie die Portnummer 636 ein. Auch auf der LDAP-Serverseite muss die SSL-Unterstützung aktiviert sein. Wenn der Administrator eine andere Portnummer festlegt, muss diese ebenfalls in v geändert werden **Access Commander**.
   - **Benutzername** – der Anmeldename des Benutzers, der die entsprechenden Rechte für den angegebenen Root oder den gesamten Baum hat. Der Anmeldename muss in der Form eingegeben werden: „administrator@domain.com“
   - **Passwort** – das Passwort des angegebenen Benutzers auf dem LDAP-Server.
   - **Kommunikationssicherheit (SSL)** – Wenn SSL deaktiviert ist, ist es nicht erforderlich, die Portnummer neu zu schreiben. Bei der Aktivierung von SSL muss die Portnummer auf 636 geändert werden.
   - **Basis-DN** – der Stammpunkt, von dem aus die Verzeichnissuche beginnt. Es kann eine Erweiterung oder das Stammverzeichnis eines Verzeichnisses sein, wie zum Beispiel: CN=Administrator, CN=Benutzer, DC=Domäne, DC=com.

   Durch die Aktivierung von TLS wird die Transport Layer Security (TLS) für Ihre FTP-Verbindung aktiviert. TLS verschlüsselt die Daten, die zwischen dem **Access Commander** und dem Server übertragen werden.
   Aktivieren Sie TLS-Zertifikatsauthentifizierung, um die TLS-Authentifizierung der vom Server bereitgestellten Zertifikate zu aktivieren. Wenn diese Funktion aktiviert ist, prüft **Access Commander**, ob er mit einem vertrauenswürdigen Server kommuniziert, was die Sicherheit der Verbindung erhöht.
3. Es öffnet sich das Detail der eingestellten LDAP-Verbindung. Verbindungseinstellungen können getestet werden. Mit der Taste Jetzt synchronisieren Sie starten eine einmalige Synchronisierung.
4. Auf der Registerkarte **Optionen von** können Sie festlegen, wie die Daten synchronisiert werden sollen.

   Im erweiterten Menü können Sie die eingestellte Verbindung löschen ⋮ Karten **Importieren**. Auf Karte **Optionen** andere Synchronisationsparameter werden eingestellt.

TIPP
Auf der Karte ist die automatische Synchronisierung eingestellt **Importieren**. Wenn Sie die automatische Synchronisierung aktivieren, geben Sie die Intervalle ein, in denen die Synchronisierung erfolgen soll. Wählen Sie je nach Häufigkeit aus, in welcher Minute oder Zeit die Daten synchronisiert werden sollen.

Einstellungen für die LDAP-Datensynchronisierung

Importierte Attribute - Durch die Änderung des Schemas wird die Zuordnung der Attribute vom LDAP-Server zu den **Access Commander** Parametern festgelegt.

ANMERKUNG
Die Telefonnummernattribute werden mit einem Filter erweitert, der die Nummern in das gewünschte Format konvertiert, das mit der Benutzerliste des Unternehmens in **Access Commander** kompatibel ist. Es sind zwei Filter verfügbar:

- `toPhoneNumber` - entfernt unnötige Zeichen (Leerzeichen, Bindestriche usw.) aus Telefonnummern.
- `skipExtension` - entfernt die Durchwahl aus den Rufnummern.

Beispiel für die Verwendung: Wenn Sie das Attribut `{telephoneNumber|toPhoneNumber|skipExtension}` eingeben, wird der ursprüngliche Wert der Telefonnummer in Active Directory „+420 123 456 789 x2222“ in „+420123456789“ umgewandelt.

Benutzer aus LDAP entfernt – legt fest, was mit Benutzern passieren soll, die in LDAP gelöscht wurden. Aus LDAP gelöschte Benutzer können sein **Access Commander** Behalten oder löschen Sie sie ebenfalls. Wenn Benutzer deaktiviert werden sollen, bleiben ihre Daten nach dem Löschen von Benutzern aus LDAP erhalten **Access Commander**, wird aber nicht mit Geräten synchronisiert.

Aus LDAP entfernte Benutzer - legt fest, was mit Benutzern geschehen soll, die aus LDAP gelöscht wurden. Aus LDAP gelöschte Benutzer können in **Access Commander** beibehalten oder auch gelöscht werden. Wenn Benutzer deaktiviert werden sollen, bleiben ihre Daten nach dem Löschen aus LDAP in **Access Commander** erhalten, werden aber nicht mit Geräten synchronisiert. Deaktivierte Benutzer haben keine Zugriffsrechte, sind nicht erreichbar, etc.

Gruppensynchronisierung - ermöglicht das Hochladen von Gruppenmitgliedschaften aus LDAP auf **Access Commander**. Über die Einstellungen des Synchronisierungsschemas können Sie einen benutzerdefinierten Basis-DN und Filter für die Synchronisierung von Gruppen definieren. In den Schemaeinstellungen können Sie die Synchronisierung von Benutzern aus verschachtelten Gruppen aktivieren.

Avatar-Synchronisierung – Legt den Foto-Download des Benutzers vom LDAP-System fest.

Linkverfolgung – legt fest, ob Daten von LDAP-Links synchronisiert werden sollen.

Verschachtelte Suche - ermöglicht die Benutzersynchronisation aus dem gesamten Baum. Wenn sie deaktiviert ist, werden nur die Daten der Wurzel durchsucht und synchronisiert.

Paging aktiviert – Für die Paginierung wird die LDAP-Erweiterung „Simple Paged Results Control“ verwendet. Dadurch können Ergebnisse auf mehrere Seiten aufgeteilt werden, was für große Verzeichnisdienste unerlässlich ist. Parameter **Seitengröße** bestimmt, wie viele Datensätze eine Seite enthalten wird.

Benutzer in das Unternehmen importieren

Erweitertes Angebot ⋮ Im Firmendetail-Header ermöglicht es den einmaligen Import neuer Benutzer in das Unternehmen, entweder aus einer CSV-Datei oder von einem anderen 2N-Gerät.

Importieren Sie Benutzer aus einer CSV-Datei

TIPP
Sie können eine Beispiel-CSV-Datei zum Importieren von Benutzern herunterladen diesen Link.

Mit **Access Commander** können Sie Benutzer in großen Mengen in Ihr Unternehmen hochladen. Grundlegende Benutzerinformationen können in einer externen Datei vorbereitet werden, und dann kann der Benutzer einfach importiert werden. Benutzer können jeweils nur in einer einzigen Datei in ein bestimmtes Unternehmen hochgeladen werden.

Mit dieser Funktion ist das Löschen von Benutzern nicht möglich.

ANMERKUNG
Benutzer mit der Administratorrolle können eine umfassende, wiederholbare Synchronisierung der Benutzerliste unternehmensübergreifend durchführen, d. h Synchronisierung von Benutzern mit FTP (S. 94).

Import vom 2N-Gerät

Sie können eine Liste von Benutzern von einem 2N-Gerät in **Access Commander** übertragen. Sie können nur von einem Gerät importieren, das noch nicht zu **Access Commander** hinzugefügt wurde. Ein Gerät kann keine Benutzer enthalten, die bereits in **Access Commander** vorhanden sind (d.h. dieselbe UUID haben). Alle Benutzer können nur in einer bestimmten Firma importiert werden.

1. Es ist ratsam, die Konfiguration vor dem Importieren zu sichern. Die Sicherung des Access Commander-Systems erfolgt auf der Registerkarte **Einstellungen > System-Backup**. Die Sicherung der Gerätekonfiguration erfolgt in der Web-Konfigurationsoberfläche unter **System > Wartung**.
2. Fügen Sie das Gerät, von dem Sie die Benutzerliste importieren möchten, als **Access Commander**-Gerät hinzu.

   ACHTUNG
   Fügen Sie noch keine Geräte zu Zonen hinzu! Das Gerät würde die Zugriffsregeln erben und die Benutzerliste würde auf dem Gerät überschrieben.

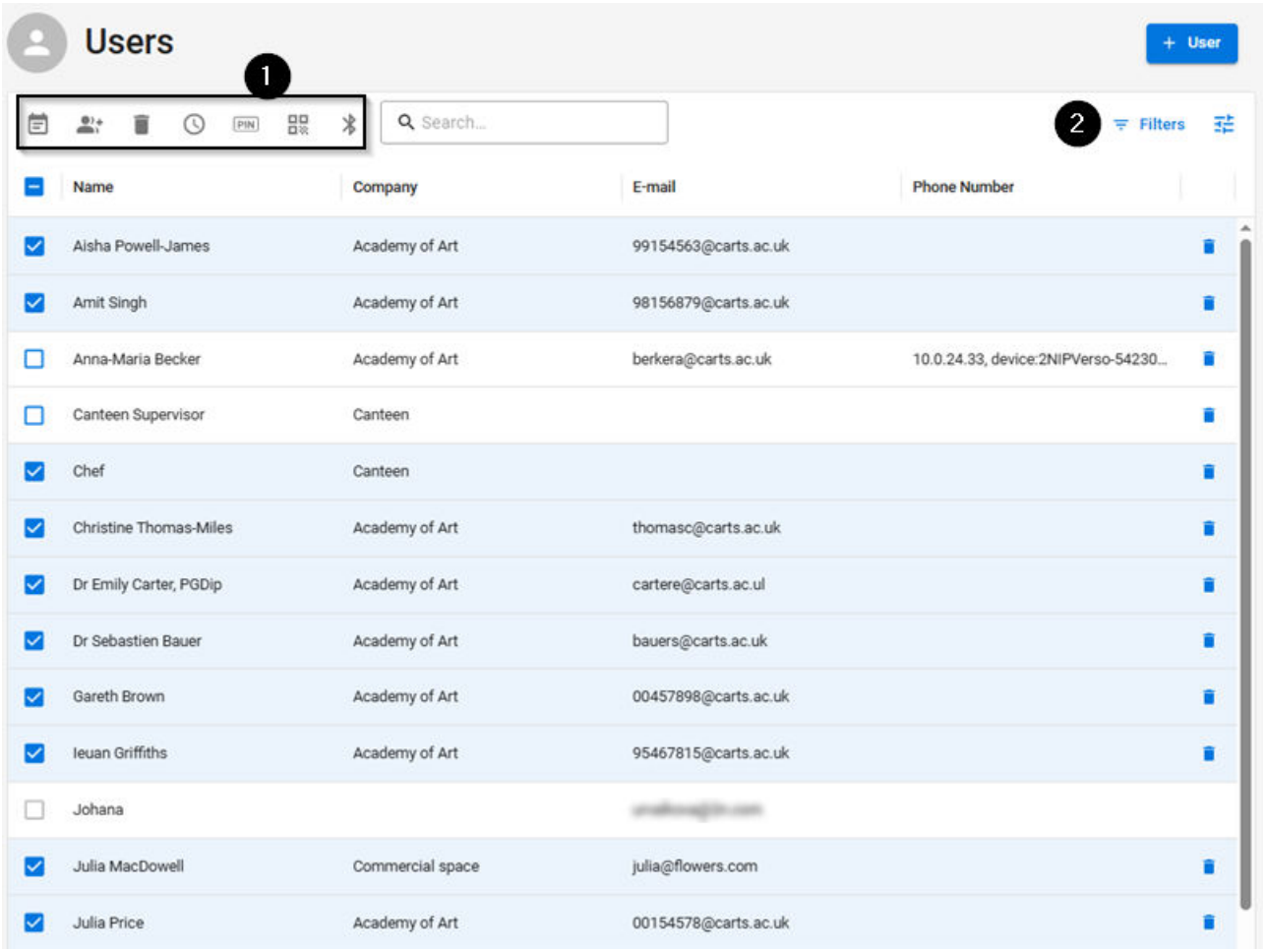
3. Gehen Sie zu den Details des Unternehmens, in das Sie den Benutzer importieren möchten. Im erweiterten Menü ⋮ wählen Vom Gerät importieren.
4. Es öffnet sich ein Dialogfenster. Wählen Sie aus der Dropdown-Liste der verfügbaren Geräte das Gerät aus, von dem Sie die Benutzerliste importieren möchten.
5. Klicken Sie auf Import, um den Import im Hintergrund zu starten. Der Abschluss des Prozesses wird im Systemprotokoll protokolliert.
6. Nach erfolgreichem Import kann das Gerät zu Zonen hinzugefügt und in Zutrittsregeln einbezogen werden.

ACHTUNG
Der Importvorgang funktioniert nur für bestimmte Benutzer (UUID) auf dem Gerät und importiert alle Benutzer vom Gerät auf einmal in ein Unternehmen.

Benutzer

Helfen **Access Commander** verwaltet werden kann **Benutzer**, ihren Zugang ändern, ihre Kontaktinformationen verwalten usw.

In der Benutzerliste werden alle Benutzer angezeigt, die erstellt wurden. Oberhalb der Liste können Sie die Benutzer filtern (Nummer 2 im Bild) oder Sie können nach einem bestimmten Benutzer nach Name, E-Mail oder Telefonnummer suchen.



Massenaktionen

Sie können mehrere Benutzer auswählen, indem Sie sie markieren und die folgenden Massenaktionen durchführen (Nummer 1 in der Abbildung):

- Aktivieren Sie die Anwesenheitsverfolgung für Benutzer
- Benutzer zur Gruppe hinzufügen
- Benutzer löschen
- Legen Sie das Zeitintervall für die Zugriffsgültigkeit fest
- Weisen Sie denjenigen Benutzern einen Zugangs-PIN-Code zu, denen noch kein PIN- oder QR-Code zugewiesen wurde

- Weisen Sie denjenigen Benutzern einen Zugangs-QR-Code zu, denen noch keine PIN oder kein QR-Code zugewiesen wurde
- Weisen Sie den Benutzern in der Auswahl den mobilen Zugriff zu, denen noch kein mobiler Zugriff zugewiesen wurde.

ANMERKUNG
Um einem Benutzer einen PIN/QR-Code oder einen mobilen Zugang zuzuweisen, ist es erforderlich, dass der Benutzer über eine gültige E-Mail-Adresse verfügt.

Erstellen Sie einen neuen Benutzer

1. Gehen Sie zur Seite **Benutzer**.
2. Klicken Sie oben rechts auf die Schaltfläche „Benutzer hinzufügen“.
3. Geben Sie die erforderlichen Informationen ein: Benutzername und Unternehmen, zu dem er gehört.
   Der neu erstellte Benutzer wird in der Liste angezeigt und die Benutzerdetails werden geöffnet. Weitere Benutzereinstellungen werden im Detail vorgenommen, wie z. B. die Zuweisung einer Telefonnummer, das Festlegen von Authentifizierungsmethoden, die Zuweisung zu Gruppen usw.

ANMERKUNG
Mit **Access Commander** können Sie Benutzer in großen Mengen in Ihr Unternehmen hochladen. Grundlegende Benutzerinformationen können in einer externen Datei vorbereitet werden, und dann kann der Benutzer einfach importiert werden. Benutzer können jeweils nur in einer einzigen Datei in ein bestimmtes Unternehmen hochgeladen werden.

Der Massenimport erfolgt in den Details des Unternehmens, nämlich Benutzer in das Unternehmen importieren (S. 47).

Benutzereinstellungen

Benutzerinformationen können im Benutzerdetail eingesehen und verwaltet werden. Die Benutzerdetails werden geöffnet, indem Sie auf der Seite „Benutzer“ auf den ausgewählten Benutzer in der Liste klicken.

Die Benutzerdetails sind in die Registerkarten „Übersicht“, „Anwesenheit“ und „Änderungsprotokoll“ unterteilt. Die Registerkarte „Anwesenheit“ wird nur den Benutzern angezeigt, für die die Nachverfolgung aktiviert ist, siehe Verfolgung der Benutzeranwesenheit (S. 57). Das Anwesenheitsmodul ist lizenzabhängig verfügbar.

Namen und Foto des Benutzers ändern

Optionen zum Umbenennen des Benutzers und Einstellen des Fotos finden Sie im erweiterten Menü im Benutzerdetail-Header.

Die Bildauflösung wird automatisch auf 432 × 432 Pixel angepasst.

Authentifizierung

Auf dieser Registerkarte werden Benutzerauthentifizierungsmethoden auf Geräten festgelegt. Der Benutzer muss sich beim Gerät authentifizieren und erhält bei gültigem Zugriff Zugriff auf das Gerät.

RFID-Karte – fügt dem Benutzer eine vorhandene RFID-Karte hinzu. Es öffnet sich ein Dialogfenster, in dem Sie die Kartenkennung eingeben müssen. Der Identifikator kann geladen werden, indem man die Karte an einen USB-Leser hält oder indem man den Ausweis über die Tastatur eingibt. Der Bezeichner muss eine hexadezimale Zahl mit mindestens 6 Zeichen sein. Einem Benutzer können bis zu 2 Zutrittskarten zugewiesen werden.

Eine RFID-Zugangskarte kann für den Zugang zu bis zu 90 Türen mit Schlössern 2N Fortis verwendet werden, abhängig von der Anzahl der angewendeten Zeitprofile. Wenn die Speicherkapazität der Karte überschritten wird, schlägt das Schreiben von Daten auf die Karte fehl. Das Ereignis des Schreibfehlers wird im Zugriffsprotokoll des Systems aufgezeichnet. Wenn Schlossgruppen verwendet werden, können mehr Türen auf eine einzelne Karte geschrieben werden als bei einer individuellen Zuweisung. Wenn Schlossgruppen verwendet werden, können mehr Türen pro Karte registriert werden als bei einer individuellen Zuweisung.

TIPP
Benutzermanager und Administratoren können die Kartenkennung im Zugriffsprotokoll einsehen. Somit ist es möglich, ein neues/nicht zugewiesenes Auto auf ein zugängliches Gerät zu laden und dann dessen Kennung aus dem Protokoll zu kopieren. Nach dem Einfügen des Identifikators zwischen den RFID-Karten kann der Benutzer mit der Nutzung der Karte beginnen. Die Anzeige von Kennungen im Zugriffsprotokoll muss in aktiviert werden **Einstellungen > Authentifizierung**.

ANMERKUNG
Wenn **Access Commander** meldet, dass die soeben hinzugefügte Karte bereits im System verwendet wird, kann dies daran liegen, dass der RFID-Kartenkompatibilitätsmodus aktiviert ist. Dieser Modus wird vom Administrator auf der **Registerkarte Einstellungen > Authentifizierung > Kompatibilitätsmoduseinstellungen** aktiviert.

My2N app – Wird für die Verbindung mit der Anwendung verwendet My2N app Aktivieren der Authentifizierung über Bluetooth, siehe Kapitel Bluetooth-Authentifizierung (S. 54).

PIN-Code – generiert automatisch eine 5-stellige PIN.

Dem Benutzer kann für den Zugriff eine PIN oder ein QR-Code zugewiesen werden, beides gleichzeitig ist jedoch nicht möglich.

QR-Code – generiert automatisch einen QR-Code. Geräte, die das Lesen von QR-Codes ermöglichen, sind in aufgeführt Unterstützte Geräte und Anwendungen (S. 8).

Dem Benutzer kann für den Zugriff eine PIN oder ein QR-Code zugewiesen werden, beides gleichzeitig ist jedoch nicht möglich.

Fingerabdruck – öffnet einen Dialog zum Hochladen eines Fingerabdrucks, mit dem sich der Benutzer auf Geräten authentifizieren kann, die das Lesen des Fingerabdrucks unterstützen. Jeder Benutzer kann bis zu 2 Fingerabdrücke hochladen. Die Vorgehensweise ist im Kapitel beschrieben Hochladen von Fingerabdrücken (S. 54).

Kennzeichen – legt das Kennzeichen des Fahrzeugs des Benutzers fest, das das Gerät scannen und zur Authentifizierung des Benutzers verwenden kann.

Virtuelle Karte – ermöglicht Ihnen das Festlegen der virtuellen Zugangskarten-ID des Benutzers. Jedem Benutzer kann genau eine virtuelle Karte zugewiesen werden. Die virtuelle Karten-ID ist eine Folge von 6–32

Zeichen aus der Menge 0–9, A–F. Die virtuelle Kartennummer dient zur Identifizierung des Benutzers in Geräten, die über die Wiegand-Schnittstelle angeschlossen sind.

Schaltercode – ermöglicht die Einstellung von bis zu 4 Codes zur Aktivierung von Schaltern (z. B. Türschloss). Der Schaltcode dient zum Öffnen des Schlosses über die Tastatur am Gerät sowie ein DTMF-Code.

ACHTUNG
Bei der Multi-Faktor-Authentifizierung ist es notwendig, die Reihenfolge der Authentifizierungsmethoden einzuhalten.

TIPP
Beim Ausfüllen der E-Mail-Adresse besteht die Möglichkeit, den generierten Zugangs-PIN/QR-Code an die angegebene Adresse zu senden.

Konto

Durch Festlegen eines Anmeldenamens und eines einmaligen Passworts können Sie einem Benutzer Zugriff auf die **Access Commander**-Schnittstelle gewähren. Nach der Anmeldung kann der Benutzer seine Anwesenheit verfolgen (sofern verfügbar), seine E-Mail-Adresse ändern oder sein Profilbild ändern. Beim ersten Anmelden wird der Benutzer aufgefordert, sein Passwort zu ändern. Wenn für einen Benutzer eine Zwei-Faktoren-Authentifizierung erforderlich ist, wird der Benutzer aufgefordert, eine Verbindung zu einer benutzerdefinierten Authentifizierungsanwendung herzustellen, siehe Zwei-Faktoren-Authentifizierung (S. 104). Auf dieser Registerkarte können Sie auch die Verbindung zur Authentifizierungsanwendung entfernen.

Auf der Registerkarte „Konto“ besteht die Möglichkeit, Benutzern mit Anmeldedaten administrative Berechtigungen zu erteilen **Access Commander** Verwendung von Benutzerrollen. Die Berechtigungen der einzelnen Rollen werden im Kapitel beschrieben Benutzerberechtigungen (S. 7).

Vereinfachte Schnittstelle

Für den Besuchsadministrator eines einzelnen Unternehmens kann eine vereinfachte Benutzerschnittstelle eingerichtet werden. Eine vereinfachte Schnittstelle ermöglicht es dem Besuchsadministrator, Besuche hinzuzufügen, zu entfernen und zu verwalten. In der vereinfachten Schnittstelle können Protokolle und Anwesenheit nicht angezeigt werden. Der Zweck der vereinfachten Schnittstelle besteht in erster Linie darin, es den Wohnungsbenutzern zu erleichtern, ihren Besuchern Zugang zu gewähren. Alle Besuche, die über die vereinfachte Schnittstelle angelegt werden, werden immer der *Standardgruppe für neue Besuche zugeordnet*. Der Besuchsmanager hat keine Möglichkeit, diese Gruppe zu ändern. Die Standardgruppe für neue Besucher muss im Voraus in den Unternehmenseinstellungen ausgewählt werden, und die Gruppe muss mit gültigen Zugangsregeln für den Zugang zur Wohnung, einschließlich des Weges zu dieser, eingerichtet werden. Der Wohnungsbenutzer kann dann die Authentifizierungsmethoden und die Dauer der Besuche über eine vereinfachte Schnittstelle verwalten.

ACHTUNG
Bevor Sie die vereinfachte Schnittstelle aktivieren **Der Systemadministrator muss die Standardgruppe für neue Besuche festlegen** In Unternehmeneinstellungen (S. 43). Solche Zugangsregeln müssen der Standardgruppe zugeordnet werden, damit der Besucher Zugang zu den besuchten Bereichen hat. Ohne eine korrekt eingestellte Standardgruppe ist es nicht möglich, Besuchern in der vereinfachten Benutzeroberfläche Zugriff zu gewähren.

persönliche Daten

Wird verwendet, um grundlegende Informationen über den Benutzer hinzuzufügen. Ermöglicht das Hinzufügen der E-Mail-Adresse des Benutzers, an die Informationen zum Benutzerkonto gesendet werden, sowie das Hinzufügen einer Telefonnummer zur Kontaktaufnahme mit dem Benutzer.

Auf der Karte kann Folgendes geschrieben werden:

- **E-Mail** - die Adresse, an die der Benutzer Informationen zu seinem **Access Commander**-Konto erhalten wird;
- **Benutzernummer** - eine spezifische Kennung, die für die Massensynchronisierung mit einer CSV-Datei erforderlich ist (siehe Synchronisierung von Benutzern mit FTP (S. 94))
- **Notiz an**

Ansätze

Über die Registerkarte Zugänge wird der Benutzer einer Gruppe zugeordnet und das Zeitintervall eingestellt, in dem die Zugangsdaten des Benutzers gültig sein sollen. Das Zeitintervall wird im erweiterten Menü der Karte eingestellt, das sich durch Klicken auf öffnet ⋮. Die Einstellung für den Beginn der Gültigkeit gilt nur für Zugriffe auf IP-Geräte. Der Zugang zu elektronischen Schlössern 2N Fortis ist ab dem Zeitpunkt gültig, an dem die Zugangskarte dem Benutzer zugewiesen wird.

TIPP
Zeitlimits für den Gerätezugriff werden über Zeitprofile festgelegt.

Wenn der Benutzer Mitglied einer Gruppe ist, wird auf der Registerkarte diese Gruppe angezeigt. Ist der Benutzer keiner Gruppe zugeordnet, kann er im Reiter hinzugefügt werden. Die Gruppe kann im erweiterten Menü geändert oder gelöscht werden ⋮.

Telefonnummern

Mit dieser Karte wird die Verbindung zum Benutzer hergestellt. Die Telefonnummer ist das Anrufziel des Geräts dieses Benutzers.

Virtuelle Nummer

Eine virtuelle Telefonnummer kann verwendet werden, um Benutzer über die numerische Tastatur des Geräts anzurufen. Virtuelle Nummern sind nicht mit den eigenen Telefonnummern der Benutzer verknüpft, sodass die eigenen Telefonnummern der Benutzer auf dem Gerät verborgen bleiben können. Virtuelle Nummern können beispielsweise nach Wohnungsnummern eingerichtet werden. Virtuelle Nummern können somit in Installationen verwendet werden, in denen die Anzahl der Kurzwahltasten nicht ausreicht.

Eine virtuelle Nummer kann 1 bis 7 Ziffern haben. Die erste und letzte Stelle kann entweder eine Ziffer oder ein Buchstabe sein, der Rest darf nur aus Ziffern bestehen (z. B. A123, 456B, C12E).

Stellvertreter

In diesem Reiter können Sie auch einen Stellvertreter festlegen, an den der Anruf weitergeleitet wird, falls dieser Benutzer nicht erreichbar ist. Der Vertreter kann aus anderen Benutzern innerhalb des Unternehmens ausgewählt werden.

Zugriffsprotokoll

Das Zugriffsprotokoll zeigt den Zugriffsverlauf an.

Änderungsprotokoll

Alle Änderungen an den Benutzereinstellungen können im Tab „Änderungsprotokoll“ eingesehen werden. Die Grundsortierung erfolgt nach dem Zeitpunkt der Änderung. Im Protokoll ist es möglich herauszufinden,

wer die Änderung vorgenommen hat. Nach einem Klick auf die Zeile ist es möglich, die Details der vorgenommenen Änderung zu erfahren.

Hochladen von Fingerabdrücken

Jeder Benutzer kann bis zu 2 Fingerabdrücke hochladen. Verwenden Sie zum Hochladen einen externen Fingerabdruckleser. Überprüfen Sie, ob Sie den Treiber installiert haben 2N USB Driver. Der Treiber steht zum Download bereit Hier.

Der hochgeladene Fingerabdruck eines Benutzers kann für die folgenden Aktionen verwendet werden:

- Öffne die Tür;
- Einen stillen Alarm starten – kann nur eingestellt werden, wenn die Türöffnungsfunktion aktiv ist;
- Automatisierung F1 und F2 – generiert das FingerEntered-Ereignis in der Automatisierung. F1 und F2 werden verwendet, um den angebrachten Finger in der Automatisierung zu unterscheiden.

Hochladen von Fingerabdrücken

1. Vergewissern Sie sich, dass der USB-Fingerabdruckleser unter **Einstellungen > Zugriff** aktiviert ist.
2. In den Benutzereinstellungen v **Registerkarte „Authentifizierung“.** Wählen Sie Authentifizierung Fingerabdruck.
3. Wählen Sie den Finger aus, für den Sie einen Fingerabdruck hochladen möchten.
   Es erscheint ein Fenster mit dem Titel „Fingerabdruck-Upload“.
4. Legen Sie den ausgewählten Finger auf das Lesegerät. Wiederholen Sie diesen Schritt dreimal, jedes Mal, wenn Sie dazu aufgefordert werden.
   Nach dem letzten Scan werden Sie über den erfolgreichen Scan des Fingerabdrucks informiert.
5. Durch Drücken der Taste**Erstellen**Der Vorgang ist abgeschlossen.

Bluetooth-Authentifizierung

Die Benutzerauthentifizierung über Bluetooth erfolgt über die My2N app, die der Nutzer auf sein Mobiltelefon heruntergeladen haben muss.

Dieser Vorgang ist durch den **vertrauenswürdigen Bluetooth-Kopplungsmechanismus** gesichert. Der Kopplungsprozess variiert je nach Firmware-Version des angeschlossenen Geräts.

GET IT ON Google Play Download on the App Store

Die Verbindung der App auf dem Telefon des Benutzers mit den 2N Geräten erfolgt durch Eingabe des Pairing-Codes in der My2N App.

Der Pairing-Code kann auf zwei Arten erhalten werden:

- durch Verbindung mit dem Gerät **2N OS**
- über ein an Ihren Computer angeschlossenes USB-Bluetooth-Lesegerät

ACHTUNG
Für ein erfolgreiches vertrauenswürdiges Pairing muss das Gerät die Firmware-Version 2.50 (oder 3.0) oder höher haben. Wenn das Gerät über eine ältere Firmware verfügt, erfolgt die Kopplung über den älteren Mechanismus mit **PIN** ohne **QR-Code**.

TIPP
Für ein höheres Maß an Sicherheit ist es besser, den **QR-Code** zu verwenden. Wenn **QR-Code** nicht verfügbar ist oder von Ihrem Gerät nicht unterstützt wird, verwenden Sie **PIN**.

Erstellen eines Pairing-Codes per Computer

1. Auf Ihren Computer herunterladen 2N IP USB Driver und installieren Sie es.
2. Stellen Sie sicher, dass das USB-Bluetooth-Lesegerät unter **Einstellungen > Authentifizierung > Registerkarte Aktivierte USB-Lesegeräte** aktiviert ist.
3. Verbinden Sie den USB-Bluetooth-Leser mit dem Computer.
4. In den Benutzereinstellungen v **Registerkarte „Authentifizierung“.** Wählen Sie Authentifizierung My2N app.
5. Wählen Sie im sich öffnenden Dialogfeld aus Koppeln Sie mit einem Lesegerät.
   Im Dialogfeld wird ein Kopplungscode angezeigt.
6. Folgen Sie dem unten stehenden Verfahren (Pairing in der mobilen App My2N (S. 55)), um in der App zu koppeln.

Erstellen Sie einen Pairing-Code auf dem Gerät

1. Sei sicher, dass
   - Das Pairing-Gerät ist für das Unternehmen des jeweiligen Benutzers eingestellt, siehe???;
   - Das Pairing-Gerät befindet sich in einer Zone, zu der der Benutzer gültigen Zugriff hat, sieheZugriffs-regeln (S. 74);
   - Eine angemessene Zeit für das Pairing eingestellt ist, siehe ???.
2. In den Benutzereinstellungen v **Registerkarte „Authentifizierung“.** Wählen Sie Authentifizierung My2N app.
3. Wählen Sie im sich öffnenden Dialogfeld aus Mithilfe des Geräts koppeln.
4. Der generierte Pairing-Code wird zusammen mit der verbleibenden Pairing-Zeit auf der Karte angezeigt. Geben Sie den Pairing-Code an den Benutzer weiter. Wenn der Benutzer über eine vollständige E-Mail-Adresse verfügt, können Sie den mobilen Schlüssel an die E-Mail senden, indem Sie auf klicken .
5. Folgen Sie dem unten stehenden Verfahren (Pairing in der mobilen App My2N (S. 55)), um in der App zu koppeln.

Pairing in der mobilen App My2N

1. Laden Sie es herunter My2N-Anwendung auf Ihr Mobiltelefon. Den Antrag gibt es unter App Store Und Google Play.
2. Öffnen Sie die App und geben Sie die Kopplungs-PIN ein.

   ANMERKUNG
   Wenn die App **QR-Code** anzeigt, das Gerät aber mit einer Firmware älter als 2.50.0 betrieben wird, kann die Kopplung nur durch Eingabe von **PIN** erfolgreich durchgeführt werden.

3. Aktivieren Sie alle wichtigen Berechtigungen, um sicherzustellen, dass My2N ordnungsgemäß funktio-niert.
4. Folgen Sie den Anweisungen auf dem Mobiltelefon – nähern Sie sich dem Gerät im Pairing-Modus und klicken Sie auf Beginnen Sie mit dem Pairing. Das Mobiltelefon sucht dann nach einem Gerät zum Koppeln.

5. Gewähren Sie Zugriff auf das ausgewählte Mobiltelefon. Anschließend können Sie im gesamten Standort Türen öffnen.

WARNUNG
Bei Mobiltelefonen mit älteren Betriebssystemen (Android 9 / iOS 17 und niedriger) müssen Sie zum Koppeln die Anwendung verwenden Mobiler Schlüssel.

Kopplung in der mobilen App Mobiler Schlüssel

1. Laden Sie die App herunter Mobile Key auf Ihr Mobiltelefon. Den Antrag gibt es unter App Store Und Google Play.
2. Öffnen Sie die App und aktivieren Sie die App Mobiler Schlüssel Zugriff auf Bluetooth.
3. Je nach Art des mobilen Schlüssels nähern Sie sich dem USB-Leser oder dem Kopplungsgerät mit dem Mobiltelefon.
4. In der App Mobiler Schlüssel Klicken Sie zum Koppeln auf das angebotene Gerät.
5. Die Anwendung fordert Sie zur Eingabe eines PIN-Codes auf. Geben Sie den Pairing-Code ein und bestätigen Sie die Eingabe.

Benutzerberechtigungen

Melden Sie sich **Access Commander** kann von mehreren Benutzern durchgeführt werden, abhängig von den ihnen zugewiesenen Berechtigungen.

Erhöhte Konten werden über eine Rolle in den Benutzereinstellungen eingerichtet. Einem Benutzer können mehrere Rollen zugewiesen werden.

ANMERKUNG
Benutzerberechtigungen gelten für die Verwaltung innerhalb des Unternehmens des Benutzers. Der Administrator hat Zugriff auf die komplette unternehmensübergreifende Verwaltung.

Administrator

- Einstellung des Systems und einzelner Module entsprechend der gültigen Lizenz.
- Lizenzwechsel
- Alle Berechtigungen anderer Rollen gelten für alle Unternehmen.

Zugriffsmanager

- Erstellen und verwalten Sie Gruppen.
- Benutzer zu Gruppen hinzufügen.
- Besuche erstellen und verwalten.
- Zeitprofile erstellen und verwalten.
- Zeiterfassung festlegen.

Benutzer Manager

- Benutzer erstellen und verwalten.
- Besuche erstellen und verwalten.

- Benutzer zu Gruppen hinzufügen.
- Besuche erstellen und verwalten.

Besuchsleiter

- Besuche erstellen und verwalten.
- Verwalten Sie ihre Gruppenmitgliedschaften (in der vereinfachten Benutzeroberfläche nicht verfügbar).
- Anzeigen des Zugriffsprotokolls von Besuchen (in der vereinfachten Benutzeroberfläche nicht verfügbar).

Türmanager

- Überwachung der Kameraübertragung von zugewiesenen Geräten.
- Fernöffnen zugewiesener Geräte.
- Notsperre zugewiesener Geräte.
- Anzeigen des Zugriffsprotokolls zugewiesener Geräte.
- Überwachung von Status und Sicherheitsereignissen im Systemprotokoll.

Anwesenheitsmanager

- Überwachung und Verwaltung der Anwesenheit zugewiesener Gruppen.
- Anzeigen des Zugriffsprotokolls von Benutzern zugewiesener Gruppen.

Firmenadministrator

- Einstellung der Standardsprache des Unternehmens.
- Überwachung des Systemprotokolls (beschränkt auf Unternehmensereignisse).
- Die Möglichkeit, ein Widget für das Systemprotokoll und die Notfallsperrfunktion auf Geräten einzurichten, die vom Unternehmen verwendet werden (einschließlich gemeinsam genutzter Geräte mit anderen Unternehmen).

Verfolgung der Benutzeranwesenheit

Access Commander ermöglicht die Überwachung der Benutzeranwesenheit. Im Anwesenheitsmodus werden die Ein- und Austrittszeiten der einzelnen Benutzer erfasst.

Die Aufzeichnung der Benutzeranwesenheit muss aktiviert sein. Die Aktivierung erfolgt im erweiterten Menü ⋮ im Benutzerdetail-Header. Die gleichzeitige Aktivierung der Anwesenheitserfassung für mehrere Benutzer kann durch die Auswahl von Benutzern in der Liste auf der Seite „Benutzer“ und die Verwendung einer Massenaktion erfolgen .

Der Anwesenheitsmanager kann die Anwesenheitsdaten der Benutzer bearbeiten. Die Bearbeitung erfolgt durch Anklicken des zu ändernden Zeitintervalls. Nach dem Öffnen können die Cut-off-Zeiten bearbeitet und dem Intervall eine Notiz hinzugefügt werden.

ACHTUNG
Für das ordnungsgemäße Funktionieren der Anwesenheit ist es notwendig, Folgendes zu haben **Access Commander**Verfügbare aktive Lizenz zur Verfolgung der Benutzeranwesenheit. Die Anwesenheitsverfolgung muss in den individuellen Benutzereinstellungen aktiviert werden.

Die Überwachung und Anpassung der Anwesenheit wird im Kapitel beschrieben Teilnahme (S. 78).

Gruppen

Die Gruppe dient der Gruppierung von Benutzern und der einfacheren Festlegung der Zugriffsrechte ihrer Mitglieder auf die Zone. Rechte müssen nicht auf der Ebene einzelner Benutzer und Besuche festgelegt werden, sondern die Gruppe wird der Zone zugeordnet.

Die Liste kann mit gefiltert werden oberhalb der Liste. Alternativ können im erweiterten Menü, das sich durch Klicken auf öffnet, Filter für einzelne Spalten gesetzt werden in der Kopfzeile jeder Spalte. Erweitertes Spaltenmenü Außerdem können Spalten verschoben, an der ersten oder letzten Position angeheftet oder ausgeblendet werden.

Erstellen Sie eine neue Gruppe

1. Gehen Sie zur Seite **Gruppen**.
2. Klicken Sie oben rechts auf die Schaltfläche zum Hinzufügen einer Gruppe.
3. Im sich öffnenden Dialogfenster müssen Sie den Namen der Gruppe eingeben und auswählen, zu welchem Unternehmen sie gehört.

> **ACHTUNG**
> Sobald eine Gruppe erstellt wurde, kann die Muttergesellschaft nicht mehr geändert werden.

Die neu erstellte Gruppe wird in der Liste angezeigt und ihre Details werden geöffnet. In den Gruppendetails müssen Sie Mitglieder hinzufügen und deren Zugriffsregeln festlegen.

Gruppeneinstellungen

Gruppeninformationen können in den Gruppendetails angezeigt und bearbeitet werden. Die Gruppendetails werden durch Klicken auf die ausgewählte Gruppe in der Gruppenliste geöffnet. Im Detail gibt es eine Übersicht über die Gruppenmitglieder und eine Übersicht über deren Zugriffsregeln.

Mitglieder

Auf der Registerkarte werden alle Benutzer angezeigt, die zur Gruppe gehören. Der Gruppe können nur Benutzer oder Besucherkarten hinzugefügt werden, die zum gleichen Unternehmen wie die Gruppe gehören.

Zugriffsregeln

Es zeigt eine Übersicht aller bereits erstellten Zugriffsregeln und bietet die Möglichkeit, diese zu ändern oder zu erstellen. Durch das Erstellen einer Zugriffsregel wird einer bestimmten Gruppe Zugriff auf die Zone gewährt. Beim Erstellen einer Regel müssen Sie eine Gruppe und ein Zeitprofil angeben, in dem die Gruppe Zugriff auf die Zone haben soll.

Zonen

Zonen dienen der einfacheren Verwaltung des Zugriffs auf einzelne Geräte. Zonen fassen Geräte zu logischen Einheiten zusammen. Auf der Seite wird eine Liste aller Zonen angezeigt.

Die Liste kann mit gefiltert werden oberhalb der Liste. Alternativ können im erweiterten Menü, das sich durch Klicken auf öffnet, Filter für einzelne Spalten gesetzt werden in der Kopfzeile jeder Spalte. Erweitertes Spaltenmenü Außerdem können Spalten verschoben, an der ersten oder letzten Position angeheftet oder ausgeblendet werden.

Zugangspunkte aktivieren

Helfen Es öffnet sich ein Dialogfenster, in dem die Access-Point-Unterstützung gestartet wird, mehr v Einstellungen für den Gerätezugriffspunkt (S. 80).

Erstellen einer neuen Zone

1. Gehen Sie zur Seite **Zonen**.
2. Klicken Sie auf die Schaltfläche zum Hinzufügen einer Zone in der oberen rechten Ecke.
3. Im geöffneten Dialogfeld müssen Sie den Namen der Zone eingeben und auswählen, zu welchen Unternehmen sie gehört.
   Die neu erstellte Zone erscheint in der Liste. Geräte können einer Zone im Zonendetail oder im Gerätedetail hinzugefügt werden. Im Zonendetail können weitere Einstellungen vorgenommen werden.

Zoneneinstellungen

Zoneninformationen können im Zonendetail angezeigt und bearbeitet werden. Zonendetails werden durch Klicken auf die ausgewählte Zone in der Liste geöffnet.

Multi-Faktor-Authentifizierung

Es besteht die Möglichkeit, die Notwendigkeit der Authentifizierung für alle Geräte in der Zone auf verschiedene Weise festzulegen. Es ist möglich, nur einige Authentifizierungsmethoden auszuwählen, bei deren Verwendung muss jedoch die folgende Reihenfolge unbedingt eingehalten werden:

1. My2N app
2. RFID-Karte
3. Fingerabdruck
4. PIN-Code

ACHTUNG
Bei der Multi-Faktor-Authentifizierung ist es notwendig, die Reihenfolge der Authentifizierungsmethoden einzuhalten.

Die Notwendigkeit einer Multi-Faktor-Authentifizierung kann durch ein Zeitprofil begrenzt werden. Wenn die Multi-Faktor-Authentifizierung aktiviert ist, wird eine Option angezeigt **Verwenden Sie die Multi-Faktor-Authentifizierung**, in dem Sie verwenden können Wählen Sie ein Zeitprofil aus. Wenn Sie den Modus „Beliebig“ wählen, ist immer eine Multi-Faktor-Authentifizierung erforderlich.

Nur für den Zutritt zur Zone kann eine Multi-Faktor-Authentifizierung erforderlich sein. Diese Einstellung ist nur bei Verwendung von Access Points gültig.

Zugriffseinstellungen

Es ist möglich, im Tab eine Menge festzulegen **PIN-Code für den Zugriff auf die Zone** oder anzeigen, wenn bereits ein PIN-Code erstellt wurde.

Darüber hinaus können in den Zugangseinstellungen folgende Funktionen aktiviert und deaktiviert werden:

Stiller Alarm – Bei Verwendung eines speziellen Codes wird eine stille Aktion aktiviert, die eine Alarmmeldung sendet; Bei einem stillen Alarm gibt das Gerät keine Alarmtöne ab. Die Einstellung des speziellen Codes für den stillen Alarm und seiner genauen Funktion erfolgt in der Gerätekonfiguration.

Zugriff blockieren – Nach fünf erfolglosen Versuchen wird der nächste Zugriffsversuch erst nach 30 Sekunden zugelassen.

Überprüfung des Kennzeichens – Fahrzeuge erhalten Zugang zur Zone, basierend auf der Kennzeichenüberprüfung auf allen Geräten, die diese Funktion unterstützen.

Gerät

Auf der Registerkarte wird eine Übersicht über die der jeweiligen Zone hinzugefügten Geräte angezeigt. In dieser Registerkarte können weitere Geräte hinzugefügt werden.

Bei der Verwendung von Access Points werden einzelne Access Points zur Zone hinzugefügt. Der Zugangspunkttyp des jeweiligen Geräts wird als Zoneneintritt beschrieben.

Für jedes Gerät/jeden Access Point werden die verfügbaren Authentifizierungsmethoden angezeigt.

Schlössergruppen

Die Registerkarte zeigt eine Übersicht über die Sperrgruppe. Sie können auf dieser Registerkarte eine weitere Gruppe hinzufügen.

Für jede Sperrgruppe können Sie die Gruppendetails einsehen.

Unternehmen

Die Karte verwaltet, zu welchen Unternehmen die jeweilige Zone gehört. Eine Zone kann mehreren Unternehmen gehören.

Zugriffsregeln

Es zeigt eine Übersicht aller bereits erstellten Zugriffsregeln und bietet die Möglichkeit, diese zu ändern oder zu erstellen. Durch das Erstellen einer Zugriffsregel wird einer bestimmten Gruppe Zugriff auf die Zone gewährt. Beim Erstellen einer Regel müssen Sie eine Gruppe und ein Zeitprofil angeben, in dem die Gruppe Zugriff auf die Zone haben soll.

Das Bearbeiten einer Zugriffsregel kann durch Klicken auf die entsprechende Regel erfolgen.

Gerät

Auf der Seite „Geräte“ werden alle dort hinzugefügten Geräte angezeigt **Access Commander**.

Die Liste kann mit gefiltert werden oberhalb der Liste. Alternativ können im erweiterten Menü, das sich durch Klicken auf öffnet, Filter für einzelne Spalten gesetzt werden in der Kopfzeile jeder Spalte. Erweitertes Spaltenmenü Außerdem können Spalten verschoben, an der ersten oder letzten Position angeheftet oder ausgeblendet werden.

Die Datensätze können in eine CSV-Datei heruntergeladen werden, indem Sie auf die Schaltfläche Export oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 angegeben.

Durch das Markieren ist es möglich, mehrere Geräte auszuwählen und die folgenden Massenaktionen auf sie anzuwenden:

- Ausgewählte Geräte verwalten
- Ausgewählte Geräte aus der Verwaltung entfernen
- Ausgewählte Geräte sichern

Das Symbol in der Geräteleiste leitet Sie zur Web-Konfigurationsschnittstelle des Geräts weiter.

Gerätezustände

- Online
- Nicht verwaltet — Die Geräteverwaltung wurde vom Benutzer deaktiviert.
- Inkompatibel — das Gerät hat keine unterstützte Firmware-Version.
- Nicht konfiguriert — Sie müssen die Konfiguration der elektronischen Schlösser aus einem Drittanbieterprogramm hochladen.
- Offline
  - Anmeldung fehlgeschlagen – In der Webkonfiguration des Geräts wurden falsche Anmeldeinformationen eingegeben.
  - Nicht zugänglich - **Access Commander** Es kann keine Verbindung zum Gerät hergestellt werden.
  - Ungültiges Zertifikat – Eine Validierung des SSL-Zertifikats ist erforderlich und das Gerät verfügt nicht über ein gültiges SSL-Zertifikat.

Hinzufügen eines neuen IP-Geräts

ANMERKUNG
Das Hinzufügen von elektronischen 2N Fortis Schlössern wird unter Elektronische Schlösser (S. 22) beschrieben.

1. Gehen Sie zur Seite **Gerät**.
2. Klicken Sie oben rechts auf die Schaltfläche „Gerät hinzufügen“.
3. Um eine 2N Gegensprechanlage, 2N Türsprechstelle oder 2N Anrufbeantworter hinzuzufügen, wählen Sie „2N IP-Geräte“.

4. Suchen Sie in dem sich öffnenden Dialogfeld das Gerät in Ihrem lokalen Netzwerk oder geben Sie seine IP-Adresse und seinen Port im Format „IP-Adresse:Port“ ein.
   Nach Eingabe der IP-Adresse des Geräts ist es möglich, durch Drücken der EINGABETASTE auf der Tastatur ein anderes Gerät einzugeben.
5. Nachdem Sie alle Geräte eingegeben haben, die Sie hinzufügen möchten, geben Sie das Passwort ein, um auf die Webkonfiguration dieser Geräte zuzugreifen. Es ist möglich, nur die Geräte hinzuzufügen, bei denen Sie sich gleichzeitig mit demselben Passwort anmelden.
6. Vorlage Anwendung (optional): Um eine Vorlage auf das hinzuzufügende Gerät anzuwenden, aktivieren Sie den Schalter **. Verwenden Sie nach dem Hinzufügen des Geräts die Konfigurationsvorlage**.
   - Das Prinzip der Auswahl und Anwendung einer Konfiguration aus einer Vorlage ist dasselbe wie die manuelle Anwendung einer Vorlage auf ein vorhandenes Gerät, wie unter Gerätevorlagen (S. 71) beschrieben.
7. Benennen Sie das Gerät, bevor Sie es erstellen.
8. Neu hinzugefügte Geräte erscheinen in der Liste. Weitere Geräteeinstellungen nehmen Sie in den Gerätedetails vor.

Schlössergruppen

Mit Sperrgruppen können Sie einzelne Sperren zu logischen Einheiten zusammenfassen, die dann zur Definition von Zugriffsregeln, zur Überwachung oder zur Verwaltung von Geräten verwendet werden können.

Gruppen ansehen

Öffnen Sie **Geräte > Gruppen sperren**.

ANMERKUNG
Die Liste zeigt alle erstellten Sperrgruppen an. Verwenden Sie das Suchfeld, um Datensätze nach Namen zu filtern.

Eine neue Sperrgruppe erstellen

1. Öffnen Sie **Geräte > Gruppen sperren**.
2. Klicken Sie auf + Locks Group.
3. Geben Sie einen Gruppennamen ein und wählen Sie die Registerkarte Erstellen.
4. Im Modul **Schlösser** klicken Sie auf Schlösser hinzufügen. Wählen Sie die Schlösser aus, die Teil der Gruppe sein sollen.
5. Im Modul **Zonen** klicken Sie auf Zonen hinzufügen. Wählen Sie die Zonen aus, die Teil der Gruppe sein sollen.
6. Wählen Sie ⋮, um eine Sperrgruppe hinzuzufügen, umzubenennen oder zu löschen.

WARNUNG
Das Ändern der Zuordnung der Sperre zu einer anderen Gruppe erfordert eine Neukonfiguration. Stellen Sie sicher, dass alle Systemänderungen abgeschlossen sind, bevor Sie die Konfigurationsdatei exportieren.

Sperren in Access Commander einstellen

Bevor Sie Schlüssel zu einzelnen Schlössern hochladen können, müssen Sie **Access Commander** mit **Fortis Commander** koppeln.

Generierung des Master Encryption Key (MEK) und Projektvorbereitung

1. Melden Sie sich bei Access Commander an.
2. Gehen Sie zu **Einstellungen > Elektronische Schlösser**.
3. Auf der Registerkarte **Ersteinstellungen** klicken Sie auf Schlüssel generieren.
4. Erstellen Sie den Hauptverschlüsselungscode.

ACHTUNG
Der Hauptverschlüsselungscode kann später weder eingesehen noch geändert werden .

ANMERKUNG
Anhand des Hauptchiffrierschlüssels (MEK) generiert **2N Access Commander** eine Reihe von Chiffrierschlüsseln. Der Schlüssel sollte also eindeutig und ausreichend sicher sein. Der Schlüsselsatz basiert auf dem Hauptchiffrierschlüssel, so dass Projekte mit demselben Hauptchiffrierschlüssel dieselben Schlüsselsätze erzeugen. Wenn ein Projekt verloren geht, kann ein neues Projekt mit demselben Hauptschlüssel erstellt werden und die Verschlüsselung fortsetzen.

5. Nachdem Sie die Schlüssel erzeugt und das Passwort für die Projektdatei festgelegt haben, können Sie **die Projektdatei** herunterladen, die ein Abbild der Konfiguration des elektronischen Schlosses im System **Access Commander** ist.
6. Klicken Sie auf der Registerkarte **von Fortis Commander** auf Anwendung herunterladen, von wo aus das Herunterladen von **Fortis Commander** (Anwendung zur Konfiguration von elektronischen Schlössern) gestartet wird.

ACHTUNG
Projektinformationen sind sensible Daten. Schützen Sie sie vor Missbrauch.

Konfigurieren des elektronischen Schlosses mit Fortis Commander

1. Installieren Sie **Fortis Commander** und öffnen Sie es.
2. Klicken Sie auf Projekt öffnen und öffnen Sie die heruntergeladene Projektdatei im Datei-Explorer.
3. Geben Sie in dem daraufhin angezeigten Dialogfeld das Passwort für die Projektdatei ein.
4. Nachdem Sie die Projektdatei geöffnet haben, wählen Sie Mit Gerät verbinden und verbinden Sie die Servicekarte mit dem Schloss.
5. Klicken Sie auf **Zuweisen**, wodurch die Sperre dem Projekt zugewiesen wird.
6. Trennen Sie die Verbindung zum Gerät und klicken Sie auf **Datei > Projekt schließen**.
7. Wenn die Konfiguration abgeschlossen ist, öffnen Sie das System **Access Commander**. Gehen Sie auf die Registerkarte **Einstellungen > Elektronische Schlösser** und klicken Sie erneut auf Fortis Commander. Laden Sie die Projektdatei hoch.

ANMERKUNG
Wenn Sie das Schloss zwischen Installationen verschieben oder einen Anspruch geltend machen, müssen Sie einen **Factory Reset** durchführen. Dieser Vorgang setzt das Schloss auf die Werkseinstellungen zurück und löscht alle vorherigen Konfigurationen.

Verfahren zur Aktualisierung der Konfiguration

1. Nehmen Sie Änderungen in **Access Commander** vor.
2. Laden Sie die neue Projektdatei herunter.
3. Laden Sie die Datei auf **Fortis Commander** hoch und nehmen Sie die erforderlichen Änderungen an den Schlössern vor.
4. Wenn Sie andere Änderungen an **Access Commander**u vornehmen, laden Sie immer eine neue Projektdatei herunter.

ACHTUNG
Für jede Konfigurationsänderung in **Access Commander**u müssen Sie eine neue Projektdatei herunterladen - Sie können keine ältere Datei verwenden, die bereits auf **Fortis Commander** hochgeladen wurde.

Dauerhaftes Ver- und Entriegeln

Die App ermöglicht es Ihnen, das Schloss dauerhaft zu sperren und zu entsperren. Die Funktion wird für Service-Einsätze oder Notfallkontrollen ohne Verwendung einer Karte verwendet.

Notabschaltung

Die Notverriegelung dient zur vollständigen Verriegelung der Tür, gesteuert durch die entsprechende Vorrichtung. Während der Notverriegelung ist ein Öffnen der Tür über die eingestellten Benutzerzugänge nicht möglich, auch wenn der Benutzer oder Besucher einen gültigen Zutritt mit gültigem Zeitprofil nutzt.

Die Notverriegelung kann aktiviert/deaktiviert werden:

- im Gerätedetail – sperrt das angegebene Gerät;
- im Zonendetail – sperrt alle Geräte in der Zone;
- im Unternehmendetail – sperrt alle Geräte im Unternehmen;
- Verwenden Sie die globale Aktion in der oberen Leiste, indem Sie auf die Schaltfläche klicken – sperrt alle Geräte ein **Access Commander**;
- im Dashboard-Widget.

Im Widget „Notfallsperre“ ist es möglich, eine bestimmte Gruppe von Geräten vorab zu definieren, die im Notfall gesperrt werden können.

ACHTUNG
Offline-Geräte, inaktive Geräte, Geräte mit inkompatibler Firmware und Geräte mit Firmware älter als 2.32 werden nach einer Notsperranforderung nicht gesperrt. Das Offline-Gerät wird gesperrt, sobald es wieder verfügbar ist.

Geräteeinstellungen

Geräteinformationen können im Gerätedetail eingesehen und verwaltet werden. Die Gerätedetails werden durch Klicken auf das ausgewählte Geräteelement in der Liste geöffnet. Abhängig vom Gerätetyp können die Details in die Registerkarten „Übersicht“, „Anruf“ und „Lift“ unterteilt werden.

Aus den Gerätedetails gelangen Sie über den Button in die Webkonfiguration des Geräts **Hardwarekonfiguration** im oberen rechten Teil der Gerätedetails. Die Konfiguration der einzelnen Geräte ist im jeweili-

gen Konfigurationshandbuch beschrieben. Sie können von der Konfigurations-Weboberfläche zurückkehren, indem Sie die Konfiguration mit einem Kreuz in der blauen oberen Leiste schließen.

Überblick

Zustand

Auf dieser Registerkarte wird der Status der Verbindung mit den Geräten angezeigt. Online-Geräte sind solche, mit denen Access Commander eine Verbindung hergestellt hat und auf denen eine akzeptierte Firmware geladen ist. Wenn eine Verbindung zu einem Gerät besteht, kann eine Datensynchronisation stattfinden. Inkompatible Firmware kann auf der **Seite Geräte > Firmware** aktiviert werden.

Nach jeder Änderung wird eine automatische Synchronisierung ausgelöst, die sich in der Konfiguration der Endgeräte widerspiegelt. Die Synchronisierung erfolgt nur über die betroffenen Geräte. Nur Anfragen, die durch Änderungen ausgelöst werden, die sich auf Endgeräte auswirken können, werden zur Synchronisierung in die Warteschlange gestellt. Bei solchen Änderungen handelt es sich in der Regel um Änderungen von Zugriffsrechten, Telefonnummern, genutzten Zeitprofilen usw. Wenn Sie beispielsweise den Namen eines Benutzers ändern, der keiner Gruppe zugeordnet ist, wird keine automatische Synchronisierung ausgelöst. Die Dauer der Synchronisierung selbst (Projektion aller Änderungen auf die Endgeräte) hängt von der Anzahl der Geräte ab, die synchronisiert werden müssen, sowie von der Datenmenge, die auf das Gerät hochgeladen wird.

Zugangskontrolle

Legt die Zone fest, zu der das Gerät gehört.

Wenn für das Gerät 2 Zugangspunkte eingestellt sind und die Zugangspunkterkennung aktiviert ist (siehe Einstellungen für den Gerätezugriffspunkt (S. 80)), wird die Möglichkeit angezeigt, 2 Zonen zuzuweisen. Ein Gerätezugangspunkt kann sich nur in einer Zone befinden.

Aufbau

Auf der Karte sind die aktuelle Firmware-Version, MAC-Adresse und IP-Adresse zu sehen und sie ermöglicht die Änderung des Passwortes für den Web-Konfigurationszugang.

Auf der Registerkarte können Sie die IP-Adresse ändern, unter der sich das Gerät befindet. Dadurch kann **Access Commander** auf ein Gerät verweisen, das vom Netz getrennt und unter einer anderen IP-Adresse wieder angeschlossen wurde.

Türsteuerung

Diese Karte zeigt Aufnahmen der Kameras des Geräts an und ermöglicht das Fernöffnen des vom Gerät gesteuerten Türschalters. Das Öffnen der Tür für eine bestimmte Zeit kann im erweiterten Menü eingestellt werden, das sich durch Klicken auf öffnet .

Der aktuelle Status des Türschalters wird neben der Taste angezeigt Öffnen.

Es dient zum Verriegeln von Türen auch für Gruppen mit gültigem Zutritt Notabschaltung (S. 64).

Sicherung

Auf dieser Registerkarte können Sie die Intercom-Konfiguration in einer XML-Datei sichern. Das Backup wird gestartet mit Starte ein Backup. Wenn ein Backup im lokalen Speicher gespeichert wird, wird es im getrennten Speicher gespeichert **Access Commander**. Beim Speichern in eine Datei öffnet sich ein Dialogfenster, in dem Sie die Backup-Datei mit einem Passwort verschlüsseln können. Die Datei enthält vertrauliche Informationen, daher wird empfohlen, die Datei zu schützen. Die Backup-Verschlüsselung ist auf Geräten mit Firmware 2.45 und höher verfügbar

Jedes letzte Backup wird auf der Registerkarte angezeigt. Es ist möglich, das Gerät automatisch mit dem letzten Backup zu synchronisieren, indem Sie das Menü unter Zurücksetzen. Im Dropdownmenü dieses Menüs können Sie auch wählen, ob Sie die Wiederherstellung aus einem Backup eines anderen angeschlossenen Geräts oder aus einer externen Datei durchführen

ANMERKUNG
Alle verfügbaren Geräte (Online-Geräte und angeschlossene Geräte mit inkompatibler Firmware) können gesichert werden.

Ruf an

Callcard wird angezeigt, wenn eine Telekommunikationsverbindung verfügbar und auf dem Gerät aktiviert ist. Auf der Registerkarte werden alle aktivierten Konten, die die Verbindung sichern, sowie deren Status angezeigt. Die Telekommunikationsverbindung wird direkt in der Konfigurationsoberfläche des betreffenden Geräts im Abschnitt Anrufe eingerichtet. Die Konfigurationsoberfläche wird über eine Schaltfläche aufgerufen Konfiguration der Hardware in der Kopfzeile der Gerätedetails.

Anruf

Diese Registerkarte wird im Detail des Geräts angezeigt, von dem aus Anrufe getätigt werden können.

Telefonbuchanzeige

Die Registerkarte Kontakte verwaltet die Anzeige des Adressbuchs auf Geräten mit Display. Die Karte zeigt den Kontaktbaum so an, wie er im Adressbuch auf dem Gerät erscheint. Durch Klicken auf Ändern Es öffnet sich ein Dialogfenster zum Bearbeiten des Kontaktbaums. Im linken Teil des geöffneten Dialogfensters wird die Sortierung der Kontaktordner angezeigt. Im rechten Teil werden die Kontakte innerhalb des ausgewählten Ordners eingestellt. Der Stammordner ist die erste Seite, die angezeigt wird, wenn Sie das Verzeichnis auf Ihrem Gerät öffnen. Kontakte werden alle auf einer Adressbuchseite angezeigt, wenn sie alle in diesem Stammordner gespeichert sind. Kontakte können weiter in Ordner gruppiert und im Stammordner sortiert werden.

Kontakte zur Geräteanzeige hinzufügen

1. Gehen Sie zu **Gerät > Gerätedetails > Registerkarte Anrufe > Registerkarte Kontakte**.
2. Öffnen Sie die Displayverwaltung, indem Sie auf klicken Ändern.
3. Wählen Sie im rechten Teil des geöffneten Dialogfelds den Ordner aus, zu dem Sie Kontakte hinzufügen möchten.
   Sie können dem Ordner Folgendes hinzufügen:

   1. **Benutzer**
      Es ist möglich, mehrere Benutzer gleichzeitig auszuwählen.
   2. **Gruppen**
      Benutzer können gruppenweise massenhaft zum Ordner hinzugefügt werden. Jeder Benutzer aus der Gruppe wird unter seinem Namen im Verzeichnis angezeigt. Es ist möglich, mehrere Gruppen gleichzeitig auszuwählen.
   3. **Rufgruppen an**
      Anrufgruppen sind Gruppen von Kontakten, die gleichzeitig angerufen werden. Beim Erstellen einer Anrufergruppe ist es notwendig, deren Namen einzugeben, unter dem die Anrufergruppe im Adressbuch angezeigt wird. Benutzerkontakte werden zu einer Anrufgruppe hinzugefügt, genau wie Kontakte zu Ordnern hinzugefügt werden.
      Sie können die Anrufgruppe im erweiterten Menü neben dem Ordner umbenennen, den Sie durch Klicken auf öffnen ⋮.
4. Sie können den Ordner im erweiterten Menü des Ordners umbenennen, das Sie durch Klicken auf öffnen ⋮. Im erweiterten Menü besteht die Möglichkeit, dem angegebenen Ordner ein Bild hinzuzufügen, das dann für diesen Ordner auf dem Gerät angezeigt wird.
5. Pinnen Sie die Ordner oder Anrufgruppen an, die an den ersten Stellen im erweiterten Menü angezeigt werden sollen ⋮ für den angegebenen Ordner mit 📌.

Andere virtuelle Nummern

Auf einem Gerät mit Ziffernblock ist es möglich, durch Eingabe einer virtuellen Nummer einen ausgehenden Anruf einzuleiten. Auf dieser Registerkarte können Benutzer hinzugefügt werden, die virtuelle Nummern anrufen können, auch wenn diese Benutzer keinen Zugriff auf das Gerät haben. Anrufe an virtuelle Nummern von Benutzern, die Zugriff auf das Gerät haben, werden automatisch zugelassen.

Bei der Benutzerauswahl werden nur die Benutzer angezeigt, die über eine ausgefüllte virtuelle Nummer verfügen.

Tasten

Diese Registerkarte wird im Detail von Geräten angezeigt, die über Tasten verfügen, mit denen Benutzertelefonnummern gewählt werden können. Auf der Registerkarte „Tasten“ werden einzelnen Benutzern einzelne Tasten am Gerät zugewiesen. Durch Drücken einer Taste am Gerät wird ein ausgehender Anruf an das Ziel des zugewiesenen Benutzers eingeleitet. Durch Klicken auf wird der Benutzer dem Button zugeordnet und Auswahl des Benutzers.

Aufzug

Durch den Anschluss des Relaismoduls AXIS A9188 an eine 2N Sprechanlage (2N IP Verso, 2N IP Force, 2N IP Safety, 2N IP Vario) oder an eine Access Unit kann der Zugang zu den einzelnen Etagen eines Gebäudes über den Aufzug gesteuert werden. Maximal 8 dieser Relaismodule können an eine 2N Sprechanlaege oder Access Unit angeschlossen werden, von denen jedes 8 Etagen steuern kann, also insgesamt 64 Etagen. Um diese Funktion nutzen zu können, müssen Sie über eine aktive 2N IP Intercom Lizenz (Best.-Nr. 9137916) und Access Unit Lizenz (Best.-Nr. 9160401) verfügen.

Einstellungen zur Aufzugssteuerung

1. Bevor Sie die Konfiguration in **Access Commander** vornehmen, vergewissern Sie sich, dass das AXIS A9188 Relaismodul an das 2N-Gerät angeschlossen ist, das die Zugangsberechtigung für die Etage erteilt. Stellen Sie außerdem sicher, dass HTTPS auf dem Modul eingestellt und das Root-Passwort geändert ist.
2. Gehen Sie zu den Details des Geräts, das den Zugang zu einzelnen Etagen steuern soll. Im erweiterten Menü Aktivieren Sie in der Kopfzeile die Aufzugssteuerung. In den Gerätedetails wird eine Registerkarte angezeigt **Aufzug**.
3. Navigieren Sie in der Kopfzeile der Gerätedetails zu hardware configuration device. Navigieren Sie zu **Integration > Zugangskontrolle > Registerkarte Aufzug**. Aktivieren Sie alle Relaismodule, die den Zugang vom Aufzug aus kontrollieren sollen. Wenn die Module eine Authentifizierung erfordern, geben Sie den Benutzernamen und das Passwort ein. Speichern Sie die Einstellungen. Verlassen Sie die Hardwarekonfiguration über das Kreuz in der oberen blauen Leiste.
4. Gehen Sie in den Gerätedetails zur Registerkarte Aufzug.
5. Wählen Sie auf der Registerkarte „Aufzugsetage“ den Relaisausgang für die Etage aus, für die Sie den Zugang einrichten möchten. Die Beschriftung der Ausgänge erfolgt im Format: *io_module_relay-Ausgabe*. Klicke auf .

6. Benennen Sie im geöffneten Dialogfeld die Etage und wählen Sie die Zone aus, die auf dieser Etage eingegeben wird. Nur Benutzer, die gemäß den definierten Zugangsregeln zum Betreten der jeweiligen Zone berechtigt sind, dürfen diese Etage betreten. Wenn der Zugang zur Etage nicht den Zonenregeln unterliegen soll, aktivieren Sie das Kontrollkästchen **öffentlicher Zugang erlaubt**. Durch die Auswahl eines Zeitprofils beschränken Sie den öffentlichen Zugriff nur auf die durch das ausgewählte Zeitprofil definierte Zeit. Außerhalb dieses Zeitprofils ist der Zutritt wieder nur Benutzern mit gültigem Zugang gemäß den Zugangsregeln gestattet.

ACHTUNG
Wenn der Zutritt gemäß den Zutrittsregeln der Zone eingestellt ist, übernimmt die Aufzugsanlage keine weiteren Einstellungen dieser Zone (PIN-Code, Mehrfachauthentifizierung, stiller Alarm, ...).

Boden
Sobald diese Registerkarte aktiviert ist, wird eine Liste aller konfigurierbaren Etagen angezeigt. Jede Etage hat eine eigene Bezeichnung in der Reihenfolge Modul- und Relaisausgang. Anschließend kann jeder Etage ein eigener Name zugewiesen werden.

Module
Auf dieser Registerkarte werden alle angeschlossenen AXIS A9188-Module und ihr aktueller Status angezeigt. Die einzelnen Module werden in der Gerätekonfiguration unter **Hardware > Elevator Control** aktiviert.

Überwachung
Auf dieser Seite finden Sie Informationen zu den angeschlossenen IP-Geräten (Sprechanlagen, Zugangseinheiten, Innensprechstellen). Jeder Administrator kann die Tabelle nach seinen eigenen Bedürfnissen einrichten. Die Einstellungen sind für jedes Konto individuell. Die Einstellungen werden durch Auswahl der anzuzeigenden Spalten vorgenommen.

Klicken Sie auf die Zeile, um zu den Details des angegebenen Geräts zu gelangen.

Firmware
Die Firmware-Seite sorgt für ein Massen-Upgrade der Firmware einzelner Arten angeschlossener Geräte und trägt so dazu bei, diese in optimalem Zustand zu halten. Die Massenverwaltung von Geräten kann ausgesetzt werden. Optional können einige Geräte von der Massen-Firmware-Verwaltung ausgeschlossen werden.

TIPP
Die neue Firmware-Version kann zunächst im Testmodus auf einem oder mehreren ausgewählten Geräten bereitgestellt werden und erst dann das Upgrade anderer Geräte ermöglichen.

Die aktuelle Firmware-Version ist online über den 2N Update Server verfügbar, optional ist es auch möglich, die Upgrade-Datei manuell hochzuladen. Die Bereitstellung einer neuen Version bedarf immer der Genehmigung durch den Administrator, der somit die volle Kontrolle über den Upgrade-Prozess hat.

Das Abrufen der Firmware-Versionen von 2N-Update-Server kann einige Minuten dauern.

Die Massenverwaltungsversion zeigt eine Liste der angeschlossenen 2N-Intercom-Typen, 2N-Antworteinheiten und 2N-Zugangseinheiten an.

Geräteausschluss

Sie können Geräte von der Bulk-Firmware-Verwaltung ausschließen, indem Sie sie der Liste unter **Geräte > Firmware > Registerkarte Ausgeschlossene Geräte hinzufügen**.

Inkompatible Firmware-Version

Wenn Sie ein Gerät hinzufügen oder aktualisieren, das über keine kompatible Firmware verfügt, wechselt das Gerät in den Status „Inkompatibel“. Ein inkompatibler Status bedeutet, dass keine neuen Benutzer auf dem Gerät gespeichert werden. Darüber hinaus werden Ereignisse vom Gerät heruntergeladen und es besteht die Möglichkeit, die Konfiguration oder Sicherung des Geräts zu nutzen. In der Tabelle wird ein neuer Eintrag erstellt und der Administrator hat die Möglichkeit, die Verwendung inkompatibler Firmware zuzulassen.

Access Commander Deaktiviert automatisch Geräte mit Firmware, die von der aktuellen Version nicht unterstützt wird. Auf der Registerkarte werden diese nicht unterstützten Firmware-Versionen auf angeschlossenen Geräten angezeigt. Die Liste der unterstützten Firmware-Versionen finden Sie unten.

Access Commander kann alle Geräte mit einer nicht unterstützten Firmware-Version steuern, wenn diese Version zugelassen ist. Die Freigabe erfolgt unter **Geräte > Firmware > Registerkarte "Inkompatible Firmware-Versionen"** mit dem Symbol  .

ACHTUNG
Die Genehmigung einer nicht unterstützten Version kann zu Problemen wie Datenverlust führen oder auf andere Weise den ordnungsgemäßen Betrieb verhindern.

Unterstützte Firmware-Versionen

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

Sicherheit

Die Methode zur Sicherung der Kommunikation zwischen Access Commander und Geräten wird unter **Geräte > Sicherheit > Registerkarte Gerätezertifikatsüberprüfung** eingestellt.

Access Commander bietet drei Sicherheitsstufen für die Kommunikation mit Geräten:

1. **Verschlüsselte Kommunikation ohne Zertifikatsprüfung** – **Access Commander** verwendet ein selbstsigniertes Zertifikat für die HTTPS-Kommunikation. Dieses Zertifikat wird von Webbrowsern als nicht vertrauenswürdig eingestuft.
2. **Überprüfung des Zertifikatsaufdrucks –** Die Kommunikation wird gewährleistet, indem das auf dem Gerät aufgezeichnete Zertifikat überprüft wird. Bei der Kommunikation wird der Aufdruck dieses Zertifikats überprüft
   Wenn die Fingerabdruckauthentifizierung aktiviert ist, muss der Geräteadministrator die Gültigkeit des Zertifikatsabdrucks bestätigen, wenn ein neues Gerät hinzugefügt wird. Der Geräteadministrator wird aufgefordert, den Fingerabdruck zu überprüfen, auch wenn das Zertifikat eines bereits hinzugefügten Geräts geändert wird

3. **Vollständige Zertifikatsüberprüfung** - Die Kommunikation ist durch ein von einer so genannten Zertifizierungsstelle unterzeichnetes Zertifikat gesichert. Während der Kommunikation wird die gesamte Zertifizierungskette gemäß den Anforderungen der PKI überprüft.

ACHTUNG
Sie können keine eigenen SSL-Zertifikate auf das 2N Indoor Touch-Gerät hochladen, die Verbindung mit ihnen geht verloren, nachdem die Zertifikatsauthentifizierung aktiviert wurde.

So verwalten Sie Zertifikate

Die Methode zur Sicherung der Kommunikation zwischen Access Commander und Geräten wird unter **Geräte > Sicherheit > Registerkarte Gerätezertifikatsüberprüfung** eingestellt.

Wenn die SSL-Zertifikatsauthentifizierung aktiviert ist, erfolgt die Synchronisierung nur auf Geräten, die über ein SSL-Zertifikat mit einer signierten vertrauenswürdigen Stelle verfügen. Die Synchronisierung von Geräten ohne solche SSL-Zertifikate wird deaktiviert. Geräte wechseln in den Offline-Status

Das Zertifikat der Signaturstelle muss auf dem Server, auf dem **Access Commander** ausgeführt wird, vertrauenswürdig sein.

TIPP
Der Vorgang des Hochladens von Zertifikaten auf den Server wird in den FAQ beschrieben.

Für eine erfolgreiche Authentifizierung müssen Gerätezertifikate von der Zertifizierungsstelle signiert werden und die IP-Adresse oder den Domänennamen des Geräts enthalten.

Laden Sie ein Gerätezertifikat hoch

1. Geben Sie die Webkonfiguration des Geräts ein.
2. Gehen Sie zu **System > Zertifikate > Registerkarte Benutzerzertifikate**.
3. Laden Sie das vorbereitete Zertifikat hoch.
4. Gehen Sie zu **System > Netzwerkverbindung > Registerkarte Webserver**.
5. Wählen Sie im Parameter **HTTPS Server-Zertifikat** das von Ihnen hochgeladene Zertifikat aus.
6. Speichern Sie die Änderungen.

Einstellungen für den Gerätezugriffspunkt

Sie können jedes Gerät logisch in zwei Zugangspunkte unterteilen - Ankunft und Abfahrt. Jeder Zugangspunkt stellt einen Durchgang in eine Richtung dar und bestimmt, ob der Gerätebenutzer die Zone betritt oder verlässt. Ein Zugangspunkt kann von einem oder mehreren Gerätemodulen kontrolliert werden. Alle zugewiesenen Module verwalten dann die Durchgänge in der Richtung des spezifischen Zugangspunkts. Zugangspunkte werden vor allem in Situationen verwendet, in denen sich ein Gerät an der Grenze zwischen zwei Zonen befindet und die Bewegungsrichtung zwischen diesen Zonen genau erfasst werden muss (z.B. für Anti-Passback-Funktionen).

Zugangspunkte werden auch verwendet, um Benutzer im Modul zu verfolgen Gegenwart (S. 84). Access Points werden auch zur Überwachung des Ein- und Ausgangs verwendet Gebietsbeschränkungen (S. 86).

ANMERKUNG
In der Web-Konfigurationsoberfläche jedes Geräts werden die Zugangspunkte als **Ankunft** und **Abreise** bezeichnet. Um sie einzurichten, gehen Sie zu **Zutritt> Zutrittsregeln> Zutritt und Abreise tabs**.

Aktivieren von Access Points in Access Commander

1. Gehen Sie zur Seite Zonen v **Access Commander**.
2. Drücken Sie in der oberen rechten Ecke und ermöglichen die Nutzung von Access Points.

Modulzuweisung für Ankunft oder Abreise

1. Geben Sie die Webkonfiguration des Geräts ein.

TIPP
Sie können auf die webbasierte Konfigurationsschnittstelle zugreifen, indem Sie in der Liste auf der Seite Geräte klicken .

2. Gehen Sie zu **Zugriff > Zugriffsregeln**.
3. Klicken Sie auf der Registerkarte **Ankunft** oder **Abreise** unter **Module** auf Verwalten.
4. Es öffnet sich ein Dialogfenster mit einer Liste der verfügbaren Zugangsverwaltungsmodule.
5. Ziehen Sie die Module per Drag & Drop in Gruppen entsprechend der Richtung, die sie bieten sollen.

TIPP
Klicken Sie auf , um ein bestimmtes Modul zu finden. Das Modul löst je nach seinen Fähigkeiten ein optisches oder akustisches Signal aus.

Gerätevorlagen

Die Funktion Gerätevorlagen ermöglicht es Ihnen, mehrere Geräte zu konfigurieren. Vorlagen vereinfachen die Erstinstallation des Systems und vereinheitlichen die Einstellungen für alle Projekte.

Schablonen funktionieren nach dem Prinzip der Muster. Mit den Vorlagen können Sie die gesamte Konfiguration eines beliebigen Geräts mit **2N OS** oder nur ausgewählte Teile der Konfiguration speichern und dann auf andere Geräte anwenden. Die Konfiguration kann auf einem bereits konfigurierten Gerät, einer Sicherungskopie des Geräts oder einer zuvor exportierten Vorlage basieren.

Wenn Sie eine Vorlage erstellen, können Sie wählen, welche Teile der Konfiguration enthalten sein sollen. Die einzelnen Teile unterscheiden sich je nach Gerätetyp (z. B. Relaiseinstellungen, Audioausgänge, Automatisierung). Diese Auswahl ist Teil des Erstellungsprozesses der Vorlage und kann nicht mehr geändert werden, sobald die Vorlage gespeichert ist.

ANMERKUNG
Die Verwendung von Vorlagen kann den Zeitaufwand für die Erstinbetriebnahme erheblich reduzieren.

Vorlagen erstellen und verwalten

Um auf die Funktion Vorlagen zuzugreifen, gehen Sie zu Geräte > Vorlagen.

1. Klicken Sie auf + Vorlage erstellen von.
2. Das Dialogfeld **Vorlage erstellen** wird geöffnet.
3. Wählen Sie aus dem Dropdown-Menü **Geräte*** ein vorhandenes Gerät aus, das als Basisgerät für Ihre Vorlage dienen soll. Nur Geräte, die mit den Vorlagen kompatibel sind, werden angezeigt.
4. Klicken Sie auf Weiter, um mit der Konfiguration der Vorlage fortzufahren.

ACHTUNG
Bei einigen Konfigurationen werden möglicherweise Warnungen angezeigt. Diese weisen darauf hin, dass die ausgewählten Konfigurationen Einschränkungen oder potenzielle Risiken haben können. Die Auswahl ist weiterhin aktiviert, aber es wird empfohlen, die Benachrichtigung zu überprüfen.

Importieren einer Vorlage oder eines Backups aus einer Datei

Wenn Sie bereits eine Vorlage oder eine Gerätesicherung in einer Datei gespeichert haben, können Sie diese einfach importieren:

1. Gehen Sie zu Geräte > Schablonen.
2. Klicken Sie oben rechts auf Importieren von.
3. Wählen Sie die Vorlage oder die Sicherungsdatei von Ihrem Computer aus und klicken Sie auf Importieren.

ANMERKUNG
Beim Importieren können einige Abschnitte deaktiviert erscheinen. Dies sind Teile der Konfiguration, die unerwünschte Änderungen verursachen oder die Funktion des Geräts beeinträchtigen könnten. Diese Abschnitte werden beim Import automatisch entfernt und der Benutzer kann sie beim Laden kurz sehen.

Ändern der Vorlage

Die Vorlage kann nach der Erstellung weiter bearbeitet werden. Die Oberfläche zeigt nur die Teile der Konfiguration an, die bei der Erstellung der Vorlage enthalten waren.

1. Gehen Sie zu Geräte > Vorlagen.
2. Wählen Sie eine Vorlage aus der Liste.
3. Klicken Sie auf Schablone bearbeiten.

Es wird ein Dialog mit den Konfigurationsabschnitten angezeigt.

Anpassung der Werte

- Der Wert wird durch einen Doppelklick angepasst.
- Der geänderte Artikel wird sofort als geändert markiert.
- Das Warnsymbol ⚠ weist auf Werte hin, die möglicherweise nicht vollständig auf dem Gerät validiert werden können.

ACHTUNG
Die bei der Bearbeitung einer Vorlage durchgeführte Validierung ist nur indikativ und erfolgt **auf der Elementebene**. Die Prüfung erfasst nicht alle Konflikte zwischen Geräten und Firmware-Versionen und entspricht nicht der vollständigen Validierung, die unter **2N OS** stattfindet.

Ein mit einer Warnung gekennzeichneter Artikel kann auf dem Gerät noch verwendbar sein, und ein Artikel ohne Warnung kann bei der Anwendung abgelehnt werden. Die eigentliche Auswertung findet auf dem Gerät statt.

Anwenden einer Vorlage auf ein Gerät

Die Vorlage kann auf ein oder mehrere Geräte angewendet werden. Sie kann auch über Massenaktionen in der Geräteliste oder direkt über die Gerätedetails angewendet werden.

1. Gehen Sie zu Geräte > Vorlagen.
2. Wählen Sie die Vorlage, die Sie auf das Gerät anwenden möchten.
3. Klicken Sie auf Auf das Gerät anwenden.
4. Wählen Sie das Gerät und bestätigen Sie.
5. Die Konfigurationsübersicht wird angezeigt. Diese Abschnitte entsprechen den bei der Erstellung der Vorlage getroffenen Auswahlen, können aber geändert werden.
6. Klicken Sie auf Anwenden.

ACHTUNG
Wenn bei der Anwendung der Vorlage eine Abweichung zwischen der Firmware-Version oder dem Gerätetyp, für den die Vorlage erstellt wurde, und der Version oder dem Typ des Zielgeräts festgestellt wird, wird eine Warnmeldung angezeigt. Die Diskrepanz muss bestätigt werden, bevor Sie fortfahren.

ANMERKUNG

- Der Status bestätigt nur den erfolgreichen Start des Prozesses. Sie informiert nicht über den tatsächlichen Fortschritt oder die Fertigstellung des Antrags.
- Anweisungen zur Verwendung der Vorlage beim Hinzufügen eines Geräts finden Sie unter Hinzufügen eines neuen Geräts (S. 61).

Zugriffsregeln

Zugriffsregeln sind ein Werkzeug zur übersichtlichen Verwaltung des Zugriffs von Benutzergruppen auf Zonen. Der Zutritt kann auf Basis von Zeitprofilen gewährt werden.

Zugriffsregeln legen fest, wer WO und WANN Zugriff hat.

- **WER** wird durch die Gruppe und die ihr zugeordneten Benutzer bestimmt (ein Benutzer kann gleichzeitig mehreren Gruppen eines Unternehmens angehören).
- **WO** wird durch die Zone oder die Geräte bestimmt (ein Gerät kann sich jeweils nur in einer Zone befinden).
- **WANN**wird durch das zugeordnete Zeitprofil bestimmt. Dieser Artikel ist optional. Ein unbefülltes Zeitprofil bedeutet unbegrenzten Zugriff (24/7).

ANMERKUNG
Eine Gruppe kann Zugriff auf mehrere Zonen haben, ebenso können mehrere Gruppen Zugriff auf eine Zone haben.

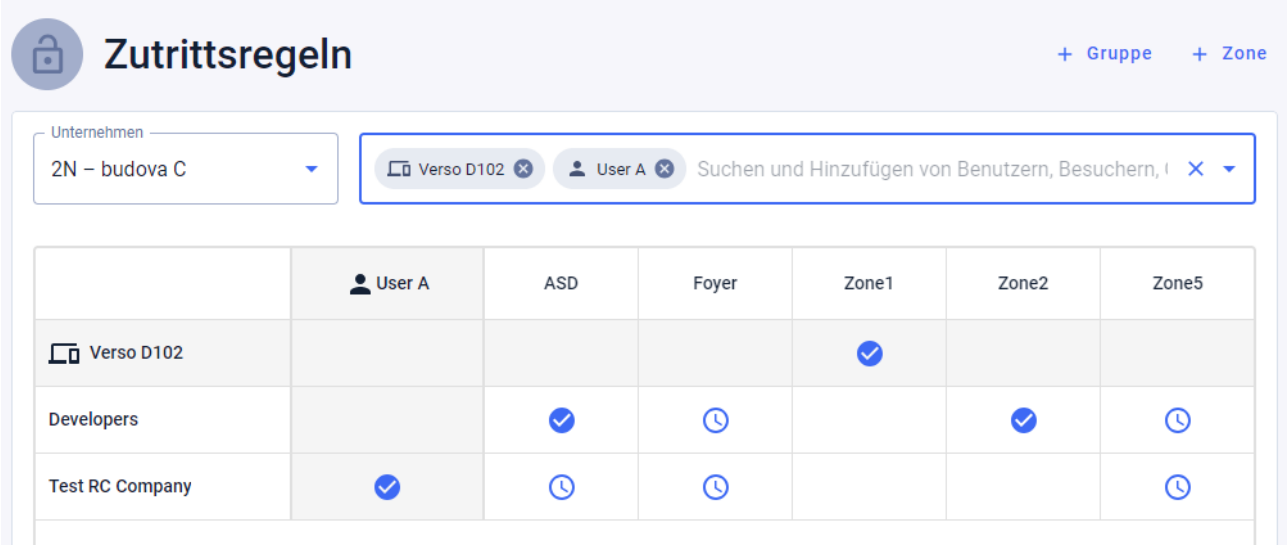
Matrixanzeige

Die Matrixansicht der Regeln auf der Seite Zugriffsregeln zeigt einen Überblick über die Zugriffe und ermöglicht deren Festlegung. Die Matrix ist für jedes bestehende Unternehmen verfügbar und zeigt alle ihm zugeordneten Gruppen und Zonen. Der Administrator kann die Firma im Menü oberhalb der Matrix wechseln.

Durch Klicken auf die Zelle, die der ausgewählten Zone und Gruppe entspricht, wird der Zugriff der Gruppe auf die Zone festgelegt. Es erscheint ein Menü, in dem Sie zwischen unbegrenztem Zugang und zeitlich begrenztem Zugang wählen können. Zeitprofile müssen auf der Seite voreingestellt sein Zeitprofile (S. 76). Bei Bedarf kann der Unternehmensmatrix eine neue Gruppe oder Zone hinzugefügt werden.

Im Suchfeld oberhalb der Matrix besteht die Möglichkeit, Benutzer oder Geräte zur Matrix hinzuzufügen. Benutzer können über die Schnittstelle von Benutzer und Gruppe zu einer Gruppe hinzugefügt werden. Durch die Überschneidung eines Geräts mit einer Zone werden Geräte zur Zone hinzugefügt.

Ein Beispiel für eine Matrixdarstellung



Das Bild bietet einen Überblick über die Matrix für das Unternehmen 2N Telekomunikace as. Aus der Übersicht geht klar hervor, dass:

- Das gefilterte Gerät Verso 2.0 D102 ist Teil von Zone1.
- Der gefilterte Benutzer Benutzer A ist Teil der Gruppe Test RC Company.
- Benutzer aus der Entwicklergruppe haben uneingeschränkten Zugriff auf die Zonen ASD und Zone2, eingeschränkten Zugriff auf die Zonen Foyer und Zone5 (gemäß dem eingestellten Zeitprofil) und keinen Zugriff auf die Zone Zone1.
- Benutzer aus der Gruppe „Test RC Company“ haben eingeschränkten Zugriff auf die Zonen ASD, Foyer und Zone5 (gemäß dem eingestellten Zeitprofil) und keinen Zugriff auf die Zonen Zone1 und Zone2.

Liste der Regeln

Auf der Seite „Regelliste“ wird eine Liste aller derzeit gültigen Zugriffsregeln angezeigt. Klicken Sie auf die Regel, um sie zu bearbeiten. Eine neue Zugriffsregel kann durch Klicken auf die Schaltfläche „Hinzufügen“ in der oberen rechten Ecke hinzugefügt werden. Vor dem Erstellen müssen Sie die Parameter der Regel festlegen.

Sowohl die Regelliste als auch die Matrix zeigen die gleichen Zugriffsregeln an. Eine Änderung in einer Ansicht wird automatisch in die andere Ansicht kopiert. Zugriffsregeln werden auch in den Zoneneinstellungen und Gruppeneinstellungen angepasst.

Zeitprofile

Ausgewählte Intercom-Funktionen können zeitlich begrenzt sein. Den genannten Funktionen kann ein sogenanntes Zeitprofil zugeordnet werden, das bestimmt, wann die jeweilige Funktion verfügbar ist.

Zeitprofile können die folgenden Anforderungen erfüllen:

- Anrufe an den ausgewählten Benutzer außerhalb der reservierten Zeit vollständig blockieren
- Blockieren Sie Anrufe an ausgewählte Telefonnummern des Benutzers außerhalb der reservierten Zeit
- Blockieren Sie den Benutzerzugriff außerhalb der vorgegebenen Zeit

Jedes Zeitprofil definiert die Verfügbarkeit der Funktion, der es zugeordnet ist, mithilfe eines Wochenkalenders. Sie können ganz einfach die Zeit von-bis und evtl. einstellen Wochentage, an denen die Funktion verfügbar sein soll. Die Zutrittsbestimmung anhand des Zeitprofils wird durch Zutrittsregeln festgelegt. Die Einschränkung der Erreichbarkeit des Benutzers außerhalb des Zeitprofils wird zusammen mit der Telefonnummer des Benutzers festgelegt.

Optional können bis zu 20 allgemeine Zeitprofile erstellt werden, die neben der Zutrittskontrolle auch für Sonderfälle der lokalen Konfiguration genutzt werden können. Diese Zeitprofile werden auf alle synchronisierten Geräte hochgeladen.

Zeitprofile auf elektronischen Schlössern

Elektronische Schlösser unterstützen Zeitprofile mit den folgenden Einschränkungen:

- Feiertage gelten nicht.
- Innerhalb eines Tages können bis zu 4 verschiedene Zeitintervalle eingestellt werden.
- Innerhalb eines Zeitprofils können 4 tägliche Intervallpläne definiert werden.

TIPP
Dies bedeutet, dass Sie beispielsweise für Montag, Dienstag, Mittwoch und Donnerstag unterschiedliche Einstellungen haben können, für Freitag, Samstag und Sonntag jedoch eine der vorhandenen Einstellungen verwenden müssen.

ACHTUNG
Verstößt das Zeitprofil gegen die festgelegten Einschränkungen, wird die Zutrittsregel ignoriert und dem Benutzer der Zutritt verweigert.

Erstellen eines Zeitprofils

1. Gehen Sie zur Seite **Zeitprofile**.
2. Klicken Sie auf die Schaltfläche zum Hinzufügen eines Zeitprofils in der oberen rechten Ecke.
3. Legen Sie im geöffneten Dialogfenster den Namen des Zeitprofils fest.

4. Wählen Sie Zeitfenster hinzufügen, um eine Zeitbeschränkung auszuwählen. Blau hervorgehobene Tage kennzeichnen Tage, die in das Zeitprofil fallen. Um einen Tag auszuwählen, klicken Sie ihn an. Sie können ein Zeitintervall innerhalb der Tage festlegen, um die Gültigkeit des Zeitprofils zu bestimmen.

   ANMERKUNG
   Sie können ein Zeitintervall innerhalb von Tagen festlegen, um die Gültigkeit des Zeitprofils zu bestimmen.

   ACHTUNG
   Nachdem das Zeitprofil erstellt wurde, können Sie für jeden Tag unterschiedliche Zeiten festlegen.

5. Das neu erstellte Zeitprofil wird zur Liste hinzugefügt und dessen Detail geöffnet, in dem weitere Einstellungen vorgenommen werden können. Im Detail des Zeitprofils besteht die Möglichkeit, die Position des Profils auf den Geräten einzustellen.

ANMERKUNG
Globale Profile können den Zugang zu allen Unternehmen beeinflussen. Nur der Administrator kann sie bearbeiten.

Ein Zugangsverwalter kann nur die Zeitprofile seiner Firma korrigieren.

Zeitprofil einstellen

Die Aufteilung nach Tagen und Uhrzeiten wird im Detail des Zeitprofils angezeigt. Die blauen Intervalle zeigen an, wann das Profil aktiv ist. Es können beliebig viele Intervalle innerhalb eines Tages eingestellt werden.

Das Intervall wird hinzugefügt, indem Sie auf das Stundenfenster klicken und den genauen Zeitpunkt festlegen, zu dem das Profil aktiv sein soll. Die Zeit eines einzelnen Intervalls kann durch Klicken auf das Intervall geändert werden. Soll das Profil den ganzen Tag aktiv sein, muss ein ganztägiges Intervall angelegt werden, also 00:00-23:59.

Im erweiterten Menü, das sich durch Klicken auf öffnet ⋮ Die Position am Gerät kann eingestellt werden. Die Position auf dem Gerät definiert die Position in der Liste der Zeitprofile, die auf alle Geräte hochgeladen wird, denen das Zeitprofil zugewiesen ist.

Die Begrenzung der Erreichbarkeit des Benutzers außerhalb des Zeitprofils wird zusammen mit der Telefonnummer in den Einstellungen des Benutzers festgelegt.

Teilnahme

Access Commander ermöglicht die Überwachung der Benutzeranwesenheit. Im Anwesenheitsmodus werden die Ein- und Austrittszeiten der einzelnen Benutzer erfasst.

Die Einstellung der Anwesenheit und des Anwesenheitsmodus erfolgt unter **Einstellungen > Konfiguration > Registerkarte Anwesenheit**, sehen Anwesenheitseinstellungen (S. 79).

ACHTUNG
Für das ordnungsgemäße Funktionieren der Anwesenheit ist es notwendig, Folgendes zu haben **Access Commander**Verfügbare aktive Lizenz zur Verfolgung der Benutzeranwesenheit. Die Anwesenheitsverfolgung muss in den individuellen Benutzereinstellungen aktiviert werden.

Die Anwesenheitsseite bietet eine Liste von Benutzern mit erfasster Anwesenheit. In der oberen rechten Ecke befindet sich ein Symbol , mit dem es möglich ist, eine CSV-Datei mit zusammenfassenden Daten über die Anwesenheit aller Benutzer in der CSV-Datei herunterzuladen. Beim Herunterladen der Daten müssen Sie den Zeitraum angeben, für den die Anwesenheit generiert werden soll.

Anwesenheit eines bestimmten Benutzers

Sie können einen bestimmten Benutzer aus der Benutzerliste auf der Seite „Anwesenheit“ auswählen und detailliertere Informationen nur zu seiner Anwesenheit anzeigen. In der Liste werden nur die Benutzer angezeigt, für die die Anwesenheitsverfolgung aktiviert ist, siehe Benutzer (S. 49).

Im oberen Teil der Abrechnung können Sie den Monat auswählen, für den Sie die Anwesenheit anzeigen möchten. Neben der Monatsauswahl werden der eingestellte Arbeitsfonds für den jeweiligen Monat, der Saldo und die geleisteten Arbeitsstunden angezeigt.

Neben dem Namen des Benutzers befindet sich ein Erweiterungsmenü Ermöglicht das Herunterladen von Daten über die Anwesenheit des angezeigten Benutzers in einer CSV- oder PDF-Datei. Beide Dateien enthalten Aufzeichnungen einzelner Tage.

TIPP
Es ist auch möglich, die Anwesenheit des Benutzers in den Benutzerdetails anzuzeigen, auf die Sie zugreifen können, indem Sie ihn aus der Benutzerliste auf der Seite auswählen **Benutzer**.

Benutzeranwesenheit ändern

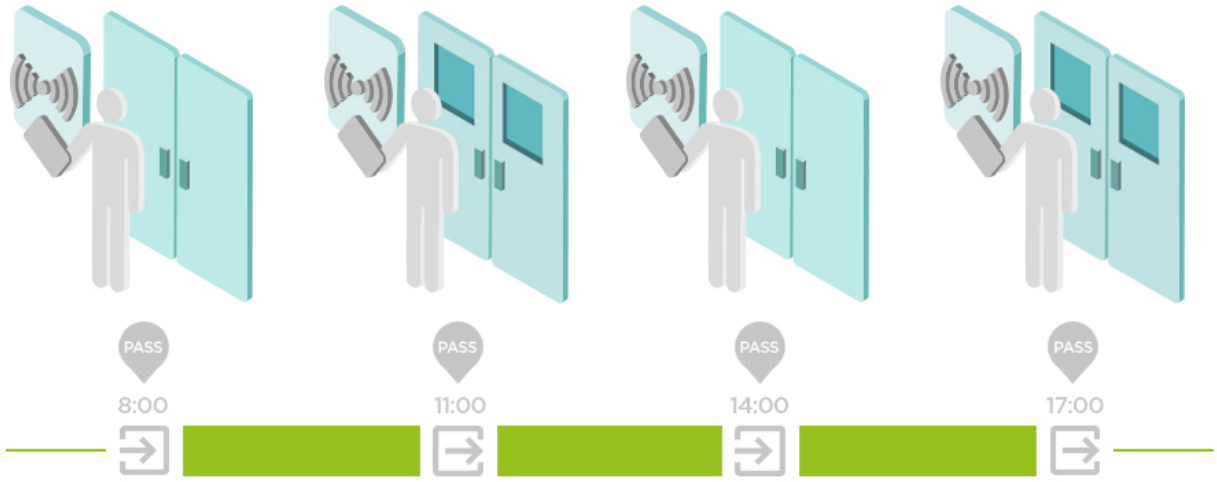
Der Anwesenheitsmanager kann die Anwesenheitsdaten der Benutzer bearbeiten. Die Bearbeitung erfolgt durch Anklicken des zu ändernden Zeitintervalls. Nach dem Öffnen können die Cut-off-Zeiten bearbeitet und dem Intervall eine Notiz hinzugefügt werden.

Anwesenheitseinstellungen

Access Commander ermöglicht die Überwachung der Benutzeranwesenheit. Im Anwesenheitsmodus werden die Ein- und Austrittszeiten der einzelnen Benutzer erfasst.

Anwesenheitsmodi

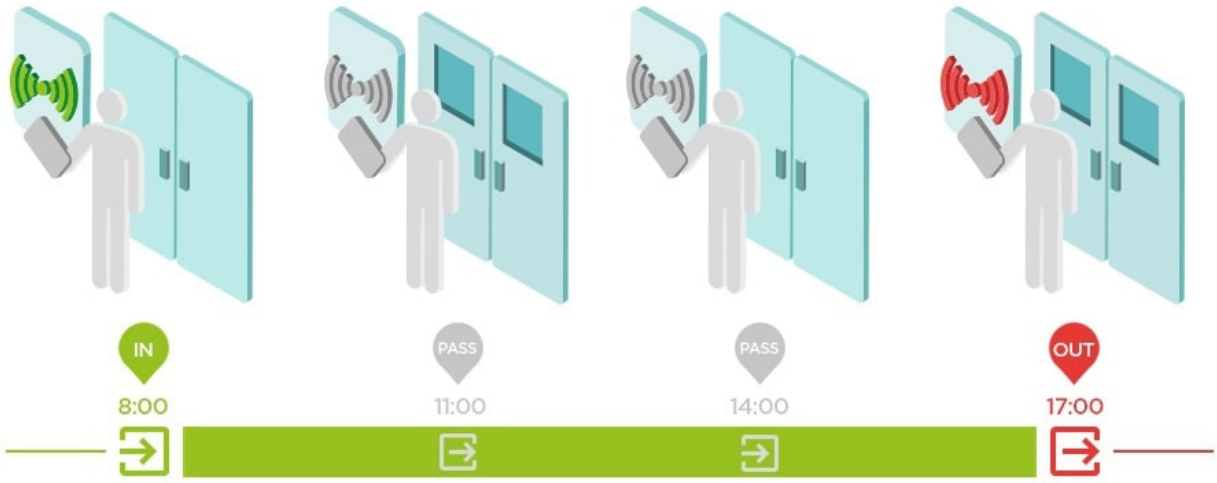
- **FREI**



Ankünfte und Abgänge werden ab der ersten und letzten Benutzerauthentifizierung auf einem beliebigen Gerät an einem Tag gezählt. Das Präsenzmodul funktioniert in diesem Modus nicht.

- **IN-OUT**

Für einen ordnungsgemäßen Betrieb muss das Gerät so eingestellt sein, dass es den Bereich betreten und verlassen kann.



- **IN-OUT für alle Geräte**
  Dieser Modus ermöglicht die Anwesenheitsüberwachung. Ankünfte werden auf eingehenden Geräten erfasst, Abgänge werden auf ausgehenden Geräten erfasst. Bewegungen zwischen Zonen werden nicht als Ankunft/Abfahrt registriert.
- **IN-OUT für ausgewählte Geräte**
  Dieser Modus ermöglicht die Anwesenheitsüberwachung. An- und Abreisen werden auf ausgewählten Geräten erfasst, die als An- bzw. Abgänge eingestellt sind. An- und Abreisen werden nur auf diesen ausgewählten Geräten erfasst. Somit kann die Erfassung der Ankunft/Abfahrt beispielsweise nur am Haupteingang des Gebäudes eingestellt werden.

Einstellungen für den Gerätezugriffspunkt

Sie können jedes Gerät logisch in zwei Zugangspunkte unterteilen - Ankunft und Abfahrt. Jeder Zugangspunkt stellt einen Durchgang in eine Richtung dar und bestimmt, ob der Gerätebenutzer die Zone betritt oder verlässt. Ein Zugangspunkt kann von einem oder mehreren Gerätemodulen kontrolliert werden. Alle zugewiesenen Module verwalten dann die Durchgänge in der Richtung des spezifischen Zugangspunkts. Zugangspunkte werden vor allem in Situationen verwendet, in denen sich ein Gerät an der Grenze zwischen zwei Zonen befindet und die Bewegungsrichtung zwischen diesen Zonen genau erfasst werden muss (z.B. für Anti-Passback-Funktionen).

Zugangspunkte werden auch verwendet, um Benutzer im Modul zu verfolgen Gegenwart (S. 84). Access Points werden auch zur Überwachung des Ein- und Ausgangs verwendet Gebietsbeschränkungen (S. 86).

ANMERKUNG
In der Web-Konfigurationsoberfläche jedes Geräts werden die Zugangspunkte als **Ankunft** und **Abreise** bezeichnet. Um sie einzurichten, gehen Sie zu **Zutritt> Zutrittsregeln> Zutritt und Abreise tabs**.

Aktivieren von Access Points in Access Commander

1. Gehen Sie zur Seite Zonen v **Access Commander**.
2. Drücken Sie in der oberen rechten Ecke und ermöglichen die Nutzung von Access Points.

Modulzuweisung für Ankunft oder Abreise

1. Geben Sie die Webkonfiguration des Geräts ein.

   TIPP
   Sie können auf die webbasierte Konfigurationsschnittstelle zugreifen, indem Sie in der Liste auf der Seite Geräte klicken .

2. Gehen Sie zu **Zugriff > Zugriffsregeln**.
3. Klicken Sie auf der Registerkarte **Ankunft** oder **Abreise** unter **Module** auf Verwalten.
4. Es öffnet sich ein Dialogfenster mit einer Liste der verfügbaren Zugangsverwaltungsmodule.
5. Ziehen Sie die Module per Drag & Drop in Gruppen entsprechend der Richtung, die sie bieten sollen.

   TIPP
   Klicken Sie auf , um ein bestimmtes Modul zu finden. Das Modul löst je nach seinen Fähigkeiten ein optisches oder akustisches Signal aus.

Besuche

In **Access Commander**Es besteht die Möglichkeit, Besucherprofile zu erstellen, die über zeitlich begrenzte Zugriffsrechte verfügen. Während des Besuchs besteht die Möglichkeit, eine Zugangskarte und einen Zugangscode hinzuzufügen und das Fahrzeugkennzeichen auszufüllen. Die Anwesenheit wird für den Besuch nicht angerechnet. Die Anzahl der Besuche ist durch keine Lizenz begrenzt.

Festlegen der Aufbewahrung von Besucherdaten

Der Administrator kann die Aufbewahrungsfrist für Besucherdaten festlegen. Der Zeitraum für die Speicherung der Besucherdaten wird durch Klicken auf das Symbol in Tagen eingestellt neben der Schaltfläche zum Erstellen eines neuen Besuchs.

Nach Ablauf des Besuchszeitintervalls und der eingestellten Datenaufbewahrungsfrist werden Besuche automatisch alle Mitternacht gelöscht. Besuche, denen noch Besucherkarten zugeordnet sind, werden nicht gelöscht.

ANMERKUNG
Die Einstellungen können zur Einhaltung lokaler Datenschutzbestimmungen verwendet werden. Der Besuchsname und die Notiz werden entsprechend den Lebensdauereinstellungen in der Protokollverwaltung im Zugriffsprotokoll gespeichert.

Einen neuen Besuch erstellen

1. Gehen Sie zur Seite **Besuche**.
2. Klicken Sie oben rechts auf die Schaltfläche „Besuch hinzufügen“.
3. Im sich öffnenden Dialogfenster müssen Sie den Namen des Besuchs eingeben, die besuchte Gruppe auswählen und den Beginn und das Ende des Besuchs festlegen. Wenn Sie den Beginn und das Ende des Besuchs nicht festlegen, beginnt das Zeitintervall für den Zugriff auf den Besuch sofort und endet am Ende des Tages.

   ACHTUNG
   Das Zeitintervall für den Besuchszugang darf 90 Tage nicht überschreiten.
4. Bevor Sie einen Besuch erstellen, können Sie die Authentifizierungsmethoden festlegen, die der Besuch für den Zugang verwenden soll.
   Der neu erstellte Besuch erscheint in der Liste. In den Details des Besuchs ist es möglich, dem Besuch Authentifizierungsmethoden hinzuzufügen und seinen Zugriff zu verwalten.

Ende des Besuchs

Nach Ablauf des Zeitintervalls erlischt der Zugriff für den Besuch.

Wenn der Administrator bzw. die Administratorin den Besuch über den Button beendet Ende Auf der Registerkarte „Zugriff“ in den Besuchseinstellungen wird der Zugriff für diesen Besuch sofort gesperrt. Für einen Besucher, dessen Besuch automatisch beendet wurde, steht eine Stopp-Schaltfläche zur Verfügung, da die Zeitzone auf den Geräten unterschiedlich sein kann. Es kann vorkommen, dass ein Besucher zwar auf

einem Gerät keinen gültigen Zugriff hat, auf einem anderen aber schon. Dies passiert, wenn für das Gerät unterschiedliche Zeitzonen eingestellt sind.

Wenn einem Besuch eine Besucherkarte zugeordnet ist, wird die Karte entbunden und kann für einen weiteren Besuch verwendet werden.

Besuchen Sie die Einstellungen

Informationen zum Besuch können in den Details zum Besuch eingesehen und bearbeitet werden. Die Besuchsdetails werden durch Klicken auf den ausgewählten Besuch in der Liste geöffnet.

Ansätze

Auf der Registerkarte Zutritte werden die Zutrittsgruppe und das Zeitintervall angezeigt, in dem der Besuch gültigen Zutritt hat. Das Zeitintervall für den Besuchszugriff kann über die Auswahl „Besuch zurücksetzen“ im erweiterten Menü neu eingestellt werden ⋮ .

In dieser Registerkarte ist es möglich, den Besuch zu beenden, siehe Ende des Besuchs (S. 81).

Besuchen

Die Karte zeigt die besuchte Person und das besuchte Unternehmen. Es ist möglich, die besuchte Person zu ändern.

In dieser Registerkarte ist es möglich, dem Besuch eine Notiz hinzuzufügen.

persönliche Daten

Auf der Karte werden die Kontaktdaten des Besuchs angezeigt und können geändert werden. Die eingestellte E-Mail ermöglicht den Versand von Authentifizierungscodes.

Authentifizierung

Während des Besuchs besteht die Möglichkeit, eine Zugangskarte, Zugangs-PIN oder QR-Code hinzuzufügen und das Fahrzeugkennzeichen auszufüllen. Es ist möglich, pro Besuch nur ein Kennzeichen auszufüllen. Es besteht die Möglichkeit, dem Besuch eine Besucherzugangskarte zuzuordnen, siehe Karten (S. 82).

Beim Ausfüllen der E-Mail-Adresse besteht die Möglichkeit, den generierten Zugangs-PIN/QR-Code an die angegebene Adresse zu senden.

Die zugewiesene Besucherkarte kann hier zurückgegeben werden.

Zugriffsprotokoll

Das Zugriffsprotokoll zeigt den Zugriffsverlauf an.

Karten

Auf der Seite Karten können Sie die Zugangskarten verwalten, die für das Hinzufügen eines Besuchs verfügbar sind. Eine neue Karte wird über die Schaltfläche Hinzufügen in der oberen rechten Ecke hinzugefügt.

Karten müssen immer einer Firma zugeordnet werden. Die Karte kann nur für Besuche verwendet werden, bei denen dieses Unternehmen besucht wird.

Durch Auswahl im erweiterten Menü kann eine bestehende Karte überschrieben oder gelöscht werden ⋮ .

ACHTUNG
Eine einem aktiven Besuch zugeordnete Karte kann nicht gelöscht werden.

ANMERKUNG
Wenn **Access Commander** meldet, dass die soeben hinzugefügte Karte bereits im System verwendet wird, kann dies daran liegen, dass der RFID-Kartenkompatibilitätsmodus aktiviert ist. Dieser Modus wird vom Administrator auf der **Registerkarte Einstellungen > Authentifizierung > Kompatibilitätsmoduseinstellungen** aktiviert.

Verwalten einer sicheren Karte mit einem USB-Lesegerät

Das USB-Lesegerät kann zur Diagnose und Verwaltung der sicheren Karte im Suchfeld in der Kopfzeile verwendet werden.

TIPP
Bevor Sie das USB-Lesegerät verwenden können, muss es unter **Access Commander** aktiviert werden. Weitere Informationen finden Sie unter Aktivierte USB-Lesegeräte (S. 110).

1. Schließen Sie das USB-Lesegerät an Ihren Computer an.
2. Klicken Sie auf das Symbol im Suchfeld in der Kopfzeile.
3. Befestigen Sie es am Lesegerät.

Verfügbare Operationen

- Abrufen von Daten von der Karte
- Suchen Sie einen Benutzer nach Karte
- So zeigen Sie die auf der Registerkarte gespeicherten Ereignisse an
- Aktualisieren der Zugangsdaten
- Löschen oder Formatieren einer Anwendung
- Erweiterung der Servicekarte

Gegenwart

Mit dem Modul **Präsenz** können Sie Benutzeraktivitäten in Echtzeit überwachen. Es funktioniert unabhängig vom Modul **Anwesenheit**, das separat lizenziert wird. Die Anwesenheit kann auch ohne eine aktive Anwesenheitslizenz überwacht werden.

Die beiden Funktionen werden zusammen auf den Registerkarten **Anwesenheit und Präsenz** in der Access Commander-Benutzeroberfläche angezeigt, aber jede hat ihren eigenen Zweck und funktioniert unabhängig.

Damit das Modul funktioniert, müssen Sie den IN-OUT-Anwesenheitsmodus unter **Einstellungen > Konfiguration > Registerkarte Anwesenheit** einstellen, siehe Anwesenheitseinstellungen (S. 79).

- Wenn das letzte Ereignis des Benutzers an einem bestimmten Tag eine Ankunft ist (**IN** Ereignis) wird als vorhanden angesehen.
- Wenn ein Benutzer ein Lesegerät passiert, das auf eine unbestimmte Richtung eingestellt ist, ändert sich die Zone des Benutzers. Das Gleiche passiert, wenn er ein Lesegerät im Modus **IN** passiert.
- Wenn das letzte Ereignis des Benutzers an einem bestimmten Tag eine Abmeldung ist (**OUT**), wird er als abwesend behandelt.

ACHTUNG
Das Anwesenheitsmodul funktioniert nicht, wenn der FREE-Modus innerhalb des Anwesenheitsverfolgungssystems verwendet wird. Es können nur IN-OUT-Einstellungen verwendet werden.

Ablauf der Benutzerpräsenz

Klicken Sie auf das Symbol Oben rechts wird der Ablauf der Benutzeranwesenheit eingestellt. Der Ablauf der Anwesenheit des Benutzers legt die automatische Löschung des Anwesenheitsdatensatzes des Benutzers fest, wenn der Benutzer vergisst, seine Abreise zu markieren. Dieses Zeitlimit wird in Stunden ausgedrückt und bestimmt, wie lange nach dem letzten Durchgang des aktuellen Benutzers sein Anwesenheitsdatensatz automatisch gelöscht wird. Durch die Festlegung dieses Zeitlimits können Sie festlegen, wie lange ein Anwesenheitsdatensatz im System verbleiben kann, wenn der Benutzer nicht als abwesend markiert ist. Dadurch wird sichergestellt, dass die Liste der aktuellen Benutzer aktuell bleibt und keine Einträge von Benutzern enthält, die das Gebäude bereits verlassen und vergessen haben, sich abzumelden.

Berichte

Es ist möglich, zusammenfassende Daten über hinzugefügte Benutzer von der Seite „Berichte“ herunterzuladen. Die heruntergeladenen Dateien liegen im CSV-Format (Comma-Separated Values) vor. Der Dateiname gibt immer das Datum und die Uhrzeit der Berichterstellung an.

ANMERKUNG
Einige Tabellenkalkulationsprogramme verwenden unterschiedliche Trennzeichen und die CSV-Datei wird möglicherweise nicht korrekt angezeigt, wenn sie darin geöffnet wird. In solchen Fällen empfiehlt es sich, die Daten aus der CSV-Datei in eine geöffnete Arbeitsmappe zu importieren.

- **My2N app** – Gekoppelte und nicht gekoppelte Benutzer mit verbleibender Kopplungszeit
  Der Bericht listet Daten zum Status der Benutzer-Kopplung über die Anwendung auf My2N app, oder Daten zur Gültigkeitsdauer des aktiven Pairing-Codes.
- **Benutzer** – Zutrittsregeln mit Gruppen, Zonen, Geräten und Zeitprofilen
  Der Bericht listet Daten zur Zuordnung der Benutzer zu Gruppen, ihrem Zugriff auf Zonen und Geräte in den Zonen sowie die Zeitprofile auf, in denen Benutzern der Zugriff gewährt wird. Jede Kombination ist in genau einer Zeile der Tabelle aufgeführt.
- **Benutzer** – Detaillierter Export
  Der Bericht listet alle Informationen über Benutzer auf, die in ihren Profilen eingegeben werden, einschließlich ihrer persönlichen Daten und Zugangsdaten.

  ACHTUNG
  Die Datei enthält sensible Daten!
- **Benutzer** – Globaler Synchronisationsexport
  Der Bericht listet Daten zur Zuordnung von Benutzern zu Gruppen, ihrem Zugriff auf Zonen und Geräte in den Zonen sowie die Zeitprofile auf, in denen Benutzern der Zugriff gewährt wird. Jede Kombination ist in genau einer Zeile der Tabelle aufgeführt.
  Dieser Bericht kann als CSV-Datei zur Benutzersynchronisierung dienen, siehe Synchronisierung von Benutzern mit FTP (S. 94).

  ACHTUNG
  Die Datei enthält sensible Daten!

Gebietsbeschränkungen

Verwenden Sie Bereichsbeschränkungen, um Bereiche zu definieren, in denen die Belegungs- und Anti-Passback-Funktionen verwendet werden können.

ANMERKUNG
Das Modul Bereichsbeschränkungen und das Präsenzmodul (einschließlich Anwesenheit) sind unabhängig voneinander. Die Module „Belegung“ und „Anti-Passback“ können nicht für die Module „Anwesenheit“ und „Präsenz“ verwendet werden. Belegung und Anti-Passback funktionieren nur im

Gebietsbeschränkungen festlegen

Über die Schaltfläche im Bereichsdetail-Header wird dem Bereich ein neues Gerät hinzugefügt.

Eingabe und Ausgabe

Diese Karten zeigen an, welche Geräte in einem bestimmten Bereich als Eingang oder Ausgang weitergeleitet werden. Verwenden Sie das erweiterte Menü unten ⋮ Geräte können zwischen Registerkarten verschoben oder aus dem Bereich entfernt werden.

Durch die Authentifizierung des Benutzers am Zutrittsgerät wird das Betreten des Bereichs erfasst. Durch die Authentifizierung des Benutzers am Ausgangsgerät verlässt der Benutzer den Bereich. Damit lässt sich überwachen, ob sich der Nutzer noch im Bereich aufhält und diesen erneut betreten möchte.

Wenn auf dem hinzugefügten Gerät zwei Zugangspunkte eingerichtet sind, kann jeder Punkt für eine andere Richtung (In/Out) verwendet werden. Die Einstellungen für den Zugangspunkt werden im Kapitel Einstellungen für den Gerätezugriffspunkt (S. 80) beschrieben. Die Eigenschaften des Zugangspunkts werden durch Klicken auf den Pfeil erweitert.

Belegung

Für einen ordnungsgemäßen Betrieb muss das Gerät so eingestellt sein, dass es den Bereich betreten und verlassen kann.

Die Registerkarte Belegung bietet einen Überblick über die Anzahl der Personen in der Gegend und ermöglicht es Ihnen, Belegungsgrenzen festzulegen. Wenn das Belegungslimit erreicht ist, ist es möglich, entweder zusätzliche Eingaben zu verweigern oder nur diese Eingaben im Systemprotokoll aufzuzeichnen. Die Belegungsfunktion verfolgt nicht, welche Personen sich in der Gegend aufhalten. Ein separates Präsenzmodul dient zur Überwachung der Anwesenheit einzelner Personen

ACHTUNG
Wenn Sie einen Benutzer wiederholt autorisieren, zählt jede Autorisierung als ein Eintritt. Das heißt, wenn ein Benutzer dreimal hintereinander am Zutrittsgerät angemeldet wird, wird dies als drei Personen im Bereich gezählt. Wenn die physische Installation des Geräts den wiederholten Abruf einer einzigen Benutzerkarte ermöglicht, ist es daher ratsam, die Belegungsfunktion mit der Anti-Passback-Funktion zu kombinieren.

Anti-Passback

Für einen ordnungsgemäßen Betrieb muss das Gerät so eingestellt sein, dass es den Bereich betreten und verlassen kann.

Es ist möglich, die Anti-Passback-Funktion für den Bereich zu aktivieren, die eine Erweiterung der Zugangskontrolle gewährleistet, indem sie die Nichtnutzung von Rechten für den erneuten Zutritt zu den reservierten Bereichen überwacht und verhindert. Die zu überwachenden Bereiche werden durch die Begrenzungsvorrichtungen definiert, die in die oder aus den Bereichen führen. An diesen Geräten wird der Durchgang von Personen auf Berechtigungen gemäß den für den Bereich definierten Regeln überprüft. Nach dem Verlassen des Bereichs durch eine Begrenzungsvorrichtung kann der Benutzer erst nach einer Zeitüberschreitung in den Bereich zurückkehren, wenn eine Zeitüberschreitung eingestellt ist. Wenn der Benutzer versucht, früher in den Bereich zurückzukehren, verweigert das System den Zugang oder protokolliert das Ereignis einfach.

WARNUNG

- Der Anti-Passback-Bereich wird bedeutungslos und potenziell gefährlich, wenn sich in diesem Bereich ein Gerät befindet, an das eine aktive REX-Taste angeschlossen ist, die unbefugten Zugriff ermöglicht.

Eine Ausnahme festlegen

Manchmal kann es wünschenswert sein, dass die Anti-Passback-Bedingungen für bestimmte Benutzer nicht gelten. In der Regel handelt es sich dabei um Benutzer wie den Gebäudemanager, den Geschäftsführer, VIP-Benutzer usw. Benutzer oder ganze Gruppen, für die die Anti-Passback-Bedingungen nicht gelten sollen, werden unter **Einstellungen > Anti-Passback > Ausnahmen festgelegt.**

ANMERKUNG
Der Abschnitt „Einstellungen“ ist nur für Benutzer mit der Administratorrolle verfügbar.

Liste der blockierten Benutzer

Gesperrte Benutzer sind die Benutzer, die versucht haben, auf den Anti-Passback-Bereich zuzugreifen, bevor die Zeitüberschreitung abgelaufen ist. Mit ✕ können Sie Benutzer von der Liste ausschließen und ihnen den Zugriff auf den Bereich wieder erlauben.

TIPP
Wenn einem Benutzer der Zugang aufgrund eines aktiven Anti-Passback-Systems verweigert wird, kann eine automatische Informations-E-Mail an den Benutzer gesendet werden. Um den E-Mail-Versand zu aktivieren, gehen Sie zu **Einstellungen > Anti-Passback > Registerkarte Benachrichtigung** des gesperrten Benutzers per E-Mail.

Beschränkungen zurücksetzen

Unter **Einstellungen > Anti-Passback > Registerkarte Bereichsbeschränkungen zurücksetzen** legen Sie die Tage und Uhrzeiten fest, zu denen der Bereichsdatensatz gelöscht wird, d. h. alle Benutzer können den Bereich wieder passieren, unabhängig von früheren Regelverstößen.

Diese Maßnahmen verbessern das Schutzniveau und beugen potenziellen Sicherheitsbedrohungen vor. Genauer gesagt tragen sie dazu bei, unbefugten Zutritt zu ausgewählten Orten zu verhindern, ermöglichen die Verfolgung der Bewegung von Personen innerhalb eines bestimmten Raums und zeichnen Ein- und Ausgänge auf, was für die Überwachung und Analyse von Sicherheitsereignissen nützlich sein kann.

Die Liste zeigt die angelegten Bereiche im System. Auf dieser Registerkarte können Bereiche erstellt, gelöscht und auf deren Details zugegriffen werden. Gleichzeitig besteht die Möglichkeit, den Bereich zu deaktivieren und seinen Status anzuzeigen.

Erstellen Sie einen Sperrbereich

1. Gehen Sie zur Seite **Gebietsbeschränkungen**.
2. Klicken Sie auf die Schaltfläche, um in der oberen rechten Ecke eine Region hinzuzufügen.
3. Benennen Sie im geöffneten Dialogfeld den Bereich.
4. Fügen Sie im offenen Bereichsdetail ein Gerät zum Bereich hinzu. Geräte werden über die Schaltfläche im Bereichsdetail-Header hinzugefügt.
   Der neu erstellte Bereich erscheint in der Liste. In seinen Details ist es möglich, die Ein- und Ausgabegeräte einzustellen, die zulässige Belegung festzulegen, die Anti-Passback-Funktion einzuschalten und den Zugang zum Bereich für ausgewählte Benutzer zu sperren.

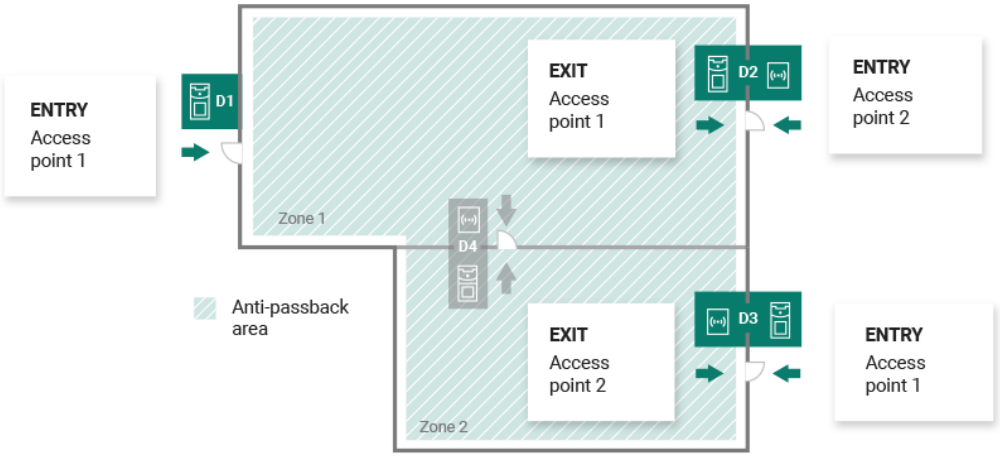
Die häufigsten Einrichtungsfehler

ACHTUNG
Tritt in einem Bereich ein Fehler auf, wird der gesamte Bereich gesperrt. Nach Behebung der Fehler wird es wieder aktiviert.

Die folgenden Fälle können dazu führen, dass Regionseinschränkungen nicht ordnungsgemäß funktionieren

- Dem Bereich wird kein Gerät hinzugefügt. Es muss mindestens ein Gerät zugewiesen sein.
- Einige Eingabe-/Ausgabegeräte sind nicht richtig konfiguriert oder enthalten kein Lesegerät.
- Ein Eingabegerät für diesen Bereich wird bereits als Eingabe für einen anderen Bereich verwendet. Die Zuordnung muss für einen korrekten Betrieb geändert werden.
- Einige Geräte verfügen nicht über die erforderliche Lizenz.
- Einige Geräte wurden deaktiviert.
- Einige Geräte wurden getrennt.
- Einige Geräte verfügen nicht über eine kompatible Firmware-Version.
  Einige Geräte sind mit einer REX-Taste ausgestattet, die das Verlassen des APB-Bereichs ohne Benutzerberechtigung ermöglicht. Für eine korrekte Funktion muss die REX-Taste deaktiviert sein.

Ein Beispiel für das Festlegen von Einschränkungen



Die Abbildung zeigt einen Anti-Passback-Bereich mit drei Grenzgeräten D1, D2 und D3. Zur Einstellung der Anti-Passback-Funktion werden ausschließlich Grenzgeräte verwendet. Das D4-Gerät innerhalb des Anti-Passback-Bereichs wird nicht zur Kontrolle der Ein-/Ausfahrt aus dem Bereich verwendet. Für die Geräte D2 und D3 sind Ein- und Ausgaberichtungen festgelegt.

Gerät D1 Es wird nur zum Betreten des Anti-Passback-Bereichs verwendet. Das Gerät ist als Eingang eingestellt.

Gerät D2 dient sowohl der Eingabe als auch der Ausgabe. Das Gerät verfügt über ein Erweiterungsmodul, das auf den Eintritt in den Bereich und eine Haupteinheit auf den Ausgang eingestellt ist.

Gerät D3 dient sowohl der Eingabe als auch der Ausgabe. Das Gerät verfügt über eine Haupteinheit, die auf das Betreten des Bereichs eingestellt ist, und ein Erweiterungsmodul, das auf das Verlassen des Bereichs eingestellt ist.

Systemeinstellungen

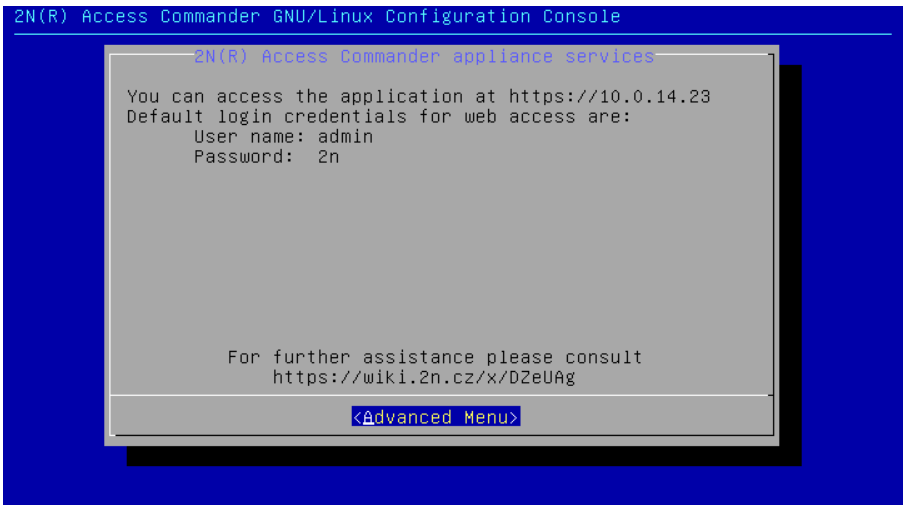
- Datum (und Uhrzeit (S. 95)
- Netzwerkeinstellungen (S. 118)
- E-Mail-Funktion (SMTP) aktivieren und einrichten (S. 103)
- Systemupdate (S. 91)
- Synchronisierung von Benutzern mit FTP (S. 94)
- Aktivierte USB-Lesegeräte (S. 110)
- PICard-Schlüssel (S. 109)
- Verschlüsselungsschlüssel für die My2N-Anwendung (S. 108)
- CAM-Protokolle (S. 110)
- Linux-Einstellungen (S. 90)

Linux-Einstellungen

Grundlegende Systemeinstellungen können in der Linux-Konfigurationskonsole vorgenommen werden.

ANMERKUNG
wenn ja **Access Commander** Über eine virtuelle Maschine verteilt, besteht die Möglichkeit, sich über eine SSH-Verbindung aus der Ferne mit der Linux-Version zu verbinden.

Durch die Anmeldung öffnet sich die Konfigurationskonsole **Access Commander** mit dem Root-Konto. Auf der Startseite werden grundlegende Informationen zum Administratorzugriff auf die Weboberfläche angezeigt und zum erweiterten Menü weitergeleitet.



Im erweiterten Menü können Sie Folgendes einstellen:

- **Vernetzung**
  Proxyservereinstellungen, Netzwerkeigenschaften, Synchronisierungsoptionen mit DHCP-Server.
- **Tim**
  Manuelle Zeiteinstellung, NTP-Server und Zeitzoneneinstellungen

- **SSH**
  Richtet eine Remote-Verbindung zu ein **Access Commander** über SSH. Um SSH zu aktivieren, muss ein anderes als das Standardpasswort festgelegt werden, das den Anforderungen für seinen Schwierigkeitsgrad entspricht.
- **KMU**
  Startet den Assistenten zum Einrichten von Verbindungen zu freigegebenen Ordnern. Legt die IP-Adresse oder den Domänennamen und den Ordnerpfad fest. Z.B. „192.168.1.1/Freigabe“. Für die Einstellungen ist es notwendig, den Benutzernamen des Benutzers anzugeben, der Zugriff auf den angegebenen Ordner und das Recht zum Schreiben erhält. Es ist notwendig, das Passwort des Benutzers einzugeben und die Version des Samba-Protokolls auszuwählen. Nach Abschluss aller obligatorischen Schritte wird die Verbindung zum Server überprüft und Informationen darüber angezeigt, ob die Einrichtung erfolgreich war oder fehlgeschlagen ist.
- **Passwort**
  Es ermöglicht die Änderung des Passworts des System-Root-Benutzers, um sich an der Konsole anzumelden oder über SSH darauf zuzugreifen.

  ANMERKUNG
  Das Ändern des Root-Passworts erfolgt in der Konfigurationskonsole, nicht in Access Commander.
- **Sichern und Wiederherstellen**
  Wird zum Importieren von Daten und Konfigurationen, zum Einrichten wiederholter Sicherungen und zum Wiederherstellen früherer Sicherungen verwendet.

Systemupdate

System **Access Commander** prüft regelmäßig den Update-Server und informiert über verfügbare Updates und verfügbare neue Firmware-Versionen angeschlossener Geräte. IN **Einstellungen > Registerkarte Systemaktualisierung** Die automatische Update-Prüfung kann ausgeschaltet werden.

Installieren Sie das Update Access Commander

WARNUNG
Es wird empfohlen, dies vor der Installation des Updates zu tun Systemsicherung (S. 92). Führen Sie die Sicherung außerhalb der Geschäftszeiten durch, um eine vorübergehende Nichtverfügbarkeit des Systems für Benutzer zu vermeiden.

1. Gehe zu **Einstellungen > Registerkarte Systemaktualisierung**.
2. Wenn die automatische Update-Überprüfung deaktiviert ist, klicken Sie auf Auf Updates prüfen.
3. Klicke auf Herunterladen in der verfügbaren Update-Informationsmeldung und bestätigen Sie den Download.
   Die Registerkarte informiert darüber, dass das Update zur Installation bereit ist.
4. Klicke auf Installieren Bestätigen Sie in der Informationsmeldung und im geöffneten Dialogfeld die Installation.
   Nach dem Start der Installation werden Sie auf die Wartungsseite weitergeleitet. Die Wartungsseite informiert den Administrator, der die Installation gestartet hat, über den aktuellen Status der Installation. Zeigt anderen Benutzern Informationen darüber an, dass ein Update ausgeführt wird. Während der Installation ist dies nicht möglich**Access Commander**Melden Sie sich an.
5. Klicken Sie nach Abschluss der Installation auf Gehen Sie zum Anmelden, wodurch Sie zur Anmeldeseite weitergeleitet werden.

Erforderliche Domänen für System-Updates

ACHTUNG
Die Verbindung des 2N Access Commander mit den unten aufgeführten Servern ist für eine erfolgreiche Systemaktualisierung unerlässlich. Wenn der Zugriff auf diese Domänen nicht aktiviert ist, schlägt der Aktualisierungsvorgang fehl und das System wird nicht aktualisiert.

Dieser Zugang ist entscheidend für das Herunterladen der neuesten Anwendungsversionen, Systempakete, Sicherheitspatches und anderer Komponenten, die Ihr System in einem optimalen und sicheren Zustand halten.

- .2n.cz
- .2n.com
- .deb.nodesource.com
- .packages.microsoft.com
- .security.debian.org
- .apt.postgresql.org
- .httpredir.debian.org

Downgrade
Ein Zurücksetzen auf eine frühere Firmware-Version ist nicht möglich.

Beta-test
Benutzer können sich für die Teilnahme am Betatest von Software-Updates entscheiden **Access Commander** vor der offiziellen Veröffentlichung von Updates. Die Autorisierung erfolgt in **Einstellungen > Registerkarte „Systemaktualisierung“ > Parameter „Server aktualisieren“.**.

WARNUNG
Für die Testversion besteht keine Garantie und das Unternehmen stellt sie nicht zur Verfügung 2N TELEKOMUNIKACE a.s. ist nicht verantwortlich für Funktionseinschränkungen und mögliche Schäden, die durch Funktionseinschränkungen der Beta-Version entstehen. Betaversionen werden nur zu Testzwecken bereitgestellt. Die Beta-Version ist nicht für die Arbeit mit wichtigen Daten gedacht.

Nach der Aktivierung werden Betaversionen in den verfügbaren Updates auf der Registerkarte „Systemaktualisierungen“ angezeigt.

WARNUNG
Nach dem Update **Access Commander** Die neueste Betaversion kann nicht auf eine frühere Version heruntergestuft werden.

Systemsicherung
Auf der **Registerkarte Einstellungen > Systemsicherung** können Sie die Datensicherung und -wiederherstellung des Access Commander durchführen, einrichten und steuern. Die Daten können auf einem lokalen

Speicher oder auf einem Server Message Block (SMB) gespeichert werden. Der SMB eignet sich für die langfristige Speicherung von Backups.

Die Datensicherung kann einmalig oder automatisch in regelmäßigen, voreingestellten Abständen erfolgen.

Jedes Backup kann im Menü, das sich nach einem Klick auf öffnet, wiederhergestellt, heruntergeladen oder gelöscht werden für ein Element in der Sicherungsliste.

Einmalige Datensicherung

1. Gehe zu **Einstellungen > Registerkarte Systemsicherung**.
2. Klicken Sie unten auf der Registerkarte auf Machen Sie jetzt ein Backup.
3. Wählen Sie aus, ob die Dateidaten verschlüsselt werden sollen. Wenn ja, geben Sie das Passwort ein, das zum Wiederherstellen der Sicherung erforderlich ist.

Automatische Datensicherungseinstellungen

1. Gehe zu **Einstellungen > Registerkarte Systemsicherung**.
2. Klicke auf  beim Parameter „Reguläre Sicherung“.
3. Legen Sie die erforderlichen Sicherungsparameter fest:
   - Häufigkeit – das Intervall, das angibt, wie oft die Sicherung durchgeführt wird
   - Uhrzeit – das Backup wird am entsprechenden Tag um diese Uhrzeit erstellt
   - Tag – Tag der Woche oder des Monats, in dem die Sicherung durchgeführt wird
4. Wählen Sie aus, ob die Dateidaten verschlüsselt werden sollen. Wenn ja, geben Sie das Passwort ein, das zum Wiederherstellen der Sicherung erforderlich ist.
5. Durch das Speichern werden die Backups automatisch entsprechend den gewählten Einstellungen durchgeführt.

Datensicherung auf SMB einrichten

1. Gehe zu **Einstellungen > Registerkarte Systemsicherung**.
2. Klicke auf  am Parameter Storage.
3. Wählen Sie den Speichertyp: SMB.
4. Geben Sie die Serveradresse, die Anmeldeinformationen und die Protokollversion ein.
5. Durch das Speichern werden alle Backups an den eingestellten Server Message Block gesendet.

Wiederherstellung aus Sicherungsdaten

1. Gehe zu **Einstellungen > Registerkarte Systemsicherung**.
2. Öffnen Sie das erweiterte Menü bei der ausgewählten Sicherung und wählen Sie  Wiederherstellen.

Wiederherstellung aus einer Sicherungsdatei

1. Gehe zu **Einstellungen > Registerkarte Systemsicherung**.
2. Klicken Sie unten auf der Registerkarte auf Aus Datei wiederherstellen.
3. Wählen Sie die Sicherungsdatei aus Ihrem Speicher aus und klicken Sie auf Wiederherstellen.

Übertragen Sie Daten von einem anderen Access Commander

1. Gehe zu **Einstellungen > Registerkarte Systemsicherung**.
2. Klicken Sie unten auf der Registerkarte auf Wandern.
3. Geben Sie die IP-Adresse des Access Commanders ein, von dem Sie die Daten übertragen möchten.
4. Geben Sie die Anmeldeinformationen des Access Commander-Administratorkontos ein, von dem Sie die Daten übertragen möchten.

ACHTUNG
Um Daten von einem anderen Access Commander zu importieren, muss der SSH-Dienst auf dem Server aktiviert sein, von dem die Daten heruntergeladen werden.

Synchronisierung von Benutzern mit FTP

Die Liste der Benutzer und deren Grundeinstellungen, inklusive Zuordnungen zu Unternehmen und Gruppen, können über eine extern gepflegte CSV-Datei synchronisiert werden.

Die Synchronisierung erfolgt auf der **Registerkarte Einstellungen > Benutzersynchronisierung**. Sie können eine CSV-Beispieldatei von der Registerkarte herunterladen.

TIPP
Die Liste der aktuellen Benutzer, die der Struktur der Beispiel-CSV-Datei entspricht, kann von der Seite heruntergeladen werden Berichte (S. 85).

Die vorbereitete CSV-Datei kann direkt auf die Karte importiert werden. Daten aus der Datei mit s **Access Commander** Sie beginnen automatisch mit der Synchronisierung.

Detaillierte Informationen über das Ergebnis jeder Synchronisierung werden im Systemprotokoll gespeichert. Das Protokoll selbst enthält grundlegende Informationen über den Erfolg oder Misserfolg der Synchronisierung. Detaillierte Informationen werden in einer Datei gespeichert, die über das Symbol am Ende der Zeile heruntergeladen werden kann.

Automatische Synchronisierung von Benutzern mit FTP

Auf der Registerkarte „Benutzersynchronisierung“ in den Einstellungen können Sie eine Verknüpfung herstellen **Access Commander** mit dem FTP-Speicher, in dem sich die CSV-Datei mit der Benutzerliste befindet. Auf der Registerkarte werden dann Informationen zu diesem FTP-Speicher angezeigt.

1. Gehen Sie zu **Einstellungen > Registerkarte Benutzersynchronisation**.
2. Klicke auf im Speicherparameter.
3. Legen Sie im geöffneten Dialogfeld die Adresse des FTP-Servers fest, auf dem die CSV-Datei gespeichert ist.
4. Durch die Aktivierung von TLS wird die Transport Layer Security (TLS) für Ihre FTP-Verbindung aktiviert. TLS verschlüsselt die Daten, die zwischen dem **Access Commander** und dem Server übertragen werden.
   Aktivieren Sie TLS-Zertifikatsauthentifizierung, um die TLS-Authentifizierung der vom Server bereitgestellten Zertifikate zu aktivieren. Wenn diese Funktion aktiviert ist, prüft **Access Commander**, ob er mit einem vertrauenswürdigen Server kommuniziert, was die Sicherheit der Verbindung erhöht.

   ACHTUNG
   Proxy für FTP mit TLS-Authentifizierung wird nicht unterstützt.
5. Geben Sie die Anmeldeinformationen ein, um auf den FTP-Server zuzugreifen.

CSV-Datei

ANMERKUNG
Einige Tabellenkalkulationsprogramme verwenden unterschiedliche Trennzeichen und die CSV-Datei wird möglicherweise nicht korrekt angezeigt, wenn sie darin geöffnet wird. In solchen Fällen empfiehlt es sich, die Daten aus der CSV-Datei in eine geöffnete Arbeitsmappe zu importieren.

Eine CSV-Datei hat eine vorgegebene Struktur, die eingehalten werden muss. Alle Werte werden durch ein Komma getrennt, nur die Liste der Gruppen wird durch ein Semikolon getrennt. Die CSV-Datei hat folgenden Aufbau:

- EmployeeID – Primärschlüssel, der ausgefüllt werden muss. Dies ist eine eindeutige Benutzerkennung.
- User Name – der Name des in Access Commander erstellten Benutzers.
- Company – der Name des Unternehmens, unter dem der Benutzer eingetragen wird. Das Unternehmen muss im Access Commander erstellt werden. Klein- und Großbuchstaben, die in Unternehmen- oder Gruppennamen verwendet werden, sind nicht austauschbar.
- User Mail – E-Mail-Adresse des Benutzers.
- Card Numbers – die Kartennummer des Benutzers. Für einen Benutzer können bis zu zwei Karten eingerichtet werden. Die Nummern der einzelnen Karten müssen durch ein Semikolon (;) getrennt werden.
- Switch Code – ein Schaltercode, ein Code wird immer unter dem ersten Schalter erstellt.
- Phone Number 1 – Telefonnummer an erster Stelle.
- Group Call – Gruppenanruf an die oben festgelegte Telefonnummer. Nimmt die Werte True/False an. Bei der Einstellung „True“ wird der Gruppenanruf aktiviert. Bei der Einstellung „Falsch“ sind Gruppenanrufe deaktiviert.
- Phone Number 2 – Telefonnummer an zweiter Stelle.
- Group Call – Gruppenanruf an die oben festgelegte Telefonnummer. Nimmt die Werte True/False an. Bei der Einstellung „True“ wird der Gruppenanruf aktiviert. Bei der Einstellung „Falsch“ sind Gruppenanrufe deaktiviert.
- Phone Number 3 – Telefonnummer an dritter Stelle.
- Virtual Number – virtuelle Nummer des Benutzers.
- Groups – Liste der Gruppen, zu denen der Benutzer hinzugefügt werden soll. Alle Gruppen müssen in eingerichtet sein **Access Commander**. Die Liste der Gruppen wird durch ein Semikolon getrennt. Klein- und Großbuchstaben, die in Unternehmen- oder Gruppennamen verwendet werden, sind nicht austauschbar.
- Is Deleted – Flag, ob der Benutzer gelöscht werden soll. Bei FALSE wird der Benutzer erstellt und nur seine Daten werden bei der nächsten Synchronisierung aktualisiert. Wenn auf TRUE gesetzt, wird der Benutzer bei der nächsten Synchronisierung gelöscht. Bei FALSE wird der Benutzer erneut erstellt.
- License Plates – Kennzeichen. Es ist möglich, mehrere Kennzeichen festzulegen, die durch ein Semikolon getrennt werden müssen.

Datum (und Uhrzeit

Um die Zeitabrufmethode zu ändern, gehen Sie zu **Einstellungen > Konfiguration > Registerkarte Datum und Uhrzeit**.

Das Datum und die Uhrzeit in **Access Commander** können mit dem Internet synchronisiert oder manuell eingestellt werden. Wenn **Access Commander** nicht mit dem Internet verbunden ist, müssen Sie das Datum, die Uhrzeit und die Zeitzone manuell einstellen. Andernfalls ist es möglich, auf NTP umzuschalten und die Zeit vom NTP-Server zu beziehen. In diesem Fall müssen Sie nur die Zeitzone einstellen. Der NTP-Server aktualisiert das Datum und die Uhrzeit automatisch.

ACHTUNG
Nach dem Speichern der Zeit ändern Sie se **Access Commander**automatisch neu gestartet.

Zeitsynchronisierung mit Geräten

Die Zeit der angeschlossenen Geräte kann mit der Zeit des **Access Commander** synchronisiert werden. Die gemeinsame Nutzung der Zeit mit den Geräten wird aktiviert, indem Sie den Parameter Gerätesynchronisierung in **Einstellungen > Konfiguration > Registerkarte Datum & Uhrzeit** aktivieren.

Wenn die Zeitsynchronisierung mit dem Gerät aktiviert ist, können Sie zwischen folgenden Synchronisierungsmethoden wählen:

- **Die Geräte nutzen denselben NTP-Server** – Die Zeit auf den Geräten richtet sich nach dem eingestellten NTP-Server **Access Commander**.

  TIPP
  Die Zeit vom NTP-Server bietet die beste Zeitgenauigkeit auf dem Gerät.

- **Die Geräte nutzen Access Commander als NTP-Server** – steuert die Zeit auf den Geräten entsprechend der eingestellten Zeit**Access Commander**.

Automatisierung

Die Automatisierungsfunktion ist im Programm enthalten **2N Access Commander** Verfügbar ab Firmware-Version 3.2 und unterliegt den Lizenzen Advanced, Pro oder Unlimited. Die Funktion basiert auf der Node-RED-Plattform und bietet umfangreiche Programmierfunktionen basierend auf der Erstellung von Streams im Programm **Access Commander**. Mit dieser Funktion können Benutzer eine Verbindung herstellen **Access Commander** mit Drittsystemen und automatisieren Sie Ihre eigenen Arbeitsabläufe basierend auf Ereignissen innerhalb der Plattform.

ACHTUNG
Um dieses vielseitige Automatisierungstool optimal nutzen zu können, sollten Sie Folgendes beachten:

- **Kundenverantwortung für Sicherheit**: Benutzer sind dafür verantwortlich, sicherzustellen, dass ihre Automatisierungskonfigurationen und Arbeitsabläufe sicher sind und den Best Practices für Cybersicherheit entsprechen. Der Verantwortungsbereich umfasst die Sicherheit der Node-RED-Umgebung, die angemessene Verwaltung von Berechtigungen und den Schutz sensibler Daten, mit denen die Automatisierungen arbeiten.
- **Verwendung der Knoten-REST-API**: Bei unsachgemäßer Verwendung des REST-API-Knotens besteht die Gefahr von Datenverlust oder unerwünschten Änderungen. Der Benutzer ist für die korrekte Konfiguration und Implementierung dieses Knotens verantwortlich. Es ist Vorsicht geboten und die Einstellungen müssen sorgfältig überprüft werden, um Datenrisiken zu vermeiden.
- **Knoten und Add-ons von Drittanbietern**: 2N Telekomunikace a.s. ist nicht verantwortlich für die Verwendung und Integration von Knoten oder Add-ons Dritter oder für die Anpassung des Node-RED-Systems innerhalb der Automatisierungsfunktion. Kunden sollten die Sicherheit und Stabilität aller zusätzlichen Komponenten, die sie installieren möchten, sorgfältig prüfen und sicherstellen. Alle Probleme, die sich aus Erweiterungen Dritter ergeben, müssen vom Kunden oder dem jeweiligen Drittanbieter gelöst werden.
- **Grenzen des technischen Supports**: Das Team des technischen Supports hilft bei Problemen im Zusammenhang mit den grundlegenden Automatisierungsfunktionen in 2N Access Commander und den Access Commander-Knotenfunktionen, kann jedoch keine Unterstützung beim Design, der Entwicklung oder dem Debuggen von benutzerdefinierten Abläufen in Node-RED leisten. Benutzer, die komplexe Automatisierungen erstellen möchten, werden zur Unterstützung an qualifizierte Node-RED-Experten verwiesen oder können öffentlich verfügbare Ressourcen nutzen.

Bevor Sie mit Node-RED arbeiten, empfiehlt es sich, sich mit den verfügbaren vertraut zu machen Online-Ressourcen, wie ausführliche Node-RED-Handbücher und zahlreiche YouTube-Tutorials. Diese Materialien bieten Anleitungen zum Erstellen, Verwalten von Streams usw.

Das folgende Handbuch konzentriert sich auf die Grundprinzipien der Erstellung automatisierter Aufgaben und auf die Beschreibung von Knoten, die speziell dafür erstellt wurden **Access Commander** und um die Beispiele zu beschreiben, mit denen er Automatisierung verwendet **Access Commander**.

Die Automatisierungsfunktion erweitert die Möglichkeiten des Programms **Access Commander**. Bei der Erkundung der Möglichkeiten muss jedoch auf die Sicherheit der damit verbundenen Einstellungen geachtet werden.

Automatisierungen erstellen

Automatisierte Aufgaben werden in einem externen Editor erstellt. Der Editor wird über die Registerkarte **Einstellungen > Konfiguration > Automatisierung aufgerufen**. Die im Editor vorgenommenen Änderungen werden erst nach der Bereitstellung auf dem Server übernommen, die über die Schaltfläche Deploy in der oberen rechten Ecke des Editors erfolgt.

Die Erstellung automatisierter Aufgaben basiert auf der Zusammenstellung von Abläufen. Flüsse werden von einzelnen Knoten abgeleitet, die miteinander verbunden sind. Im linken Bereich wird ein Menü mit Knoten angezeigt. Im linken Bereich ist es möglich, Knoten anhand ihres Namens zu suchen. Ein neuer Knoten kann auch hinzugefügt werden, nachdem eine neue Verbindung von einem vorhandenen Knoten erstellt wurde.

Die Daten, die zwischen den Knoten übermittelt werden, werden als Nachrichten bezeichnet. Ihre Beschreibung und Handhabung wird hier ausführlich beschrieben. Auf dieser Seite werden auch die Basisknoten

beschrieben, die das Format einzelner Nachrichten oder deren Sequenzen behandeln, wie z.B. Change, Split, Join,... Automatisierungen können nicht nur mit Daten arbeiten, die in dieser einen Aufgabe (msg.) gewonnen werden, sondern auch mit dynamischen Werten im Kontext der gesamten Bewegungshistorie (flow.) oder sogar aller Bewegungen in einer Instanz (global.).

ACHTUNG
Die Schaltfläche Deploy sendet die konfigurierten Abläufe an den Server. Erst durch das Senden an den Server werden die neuen Abläufe wirksam!

Abgesicherter Modus

Der abgesicherte Modus ist ein wichtiges Werkzeug zur Lösung von Automatisierungsproblemen. Wenn Sie den Editor im abgesicherten Modus ausführen, können Sie Änderungen an Streams vornehmen, ohne dass diese Streams im Hintergrund ausgeführt werden. Das bedeutet, dass Sie in den Editor gehen, das Gewünschte bearbeiten und die Änderungen dann mit einer Schaltfläche erneut bereitstellen können Deploy. Dieser Modus ist besonders nützlich, wenn einer der Flows zu Fehlfunktionen oder Abstürzen von Node-RED führt, beispielsweise aufgrund eines Fehlers im Flow oder in einem Drittanbieter-Knoten, oder wenn der Flow sofort gestoppt werden muss.

Access Commander Nodes

REST-API

Ein REST-API-Knoten sendet eine definierte HTTP-API-Anfrage. Die in der Eigenschaft enthaltenen Eingabedaten **Punkte** werden als Anforderungspunkte dieser Anforderung verwendet. Die Ausgabe des Knotens sind die Daten aus der Antwort auf die Anfrage. Im Parameter kann die Auswahl und Sortierung der Ausgabedaten festgelegt werden **Query**.

Knotenparameter

- **Method** – bietet eine Auswahl an API-Anforderungsmethoden
- **Endpoint** – wird verwendet, um den gesamten Endpunkt anzugeben, an den die Anfrage gerichtet werden soll. Der Pfad des Endpunkts kann mit dem Parameter points ergänzt werden.
  Das Arbeiten mit HTTP-Anfragen wird in beschrieben HTTP API (S. 120).
- **Query** – wird verwendet, um anzugeben, welche Datenparameter im Endpunkt angesprochen werden sollen und wie sie in der Ausgabe zurückgegeben werden sollen. Dieser Parameter kann durch Eingabewert, Eigenschaft angegeben werden **query**. Beschreibung des Builds **query** ist im Dokument beschrieben Data Query Customization (nur auf Englisch).
- **Only send non-2xx responses to Catch node** – Diese Option beeinflusst die Art der HTTP-Antworten, die im Catch-Knoten erfasst werden.
- **Name** – ermöglicht Ihnen, den Knoten zur besseren Orientierung beim Arbeiten mit dem Flow umzubenennen.

Access log

Der Knoten lädt die Einträge im Access Log und ermöglicht die weitere Verarbeitung dieser Einträge.

Der Administrator kann automatische Aufgaben einrichten, die ausgeführt werden, wenn **Access Commader** einen bestimmten Protokolleintrag sieht. Die Definition der Aktion erfolgt in den Knoteneinstellungen. Die Ausgabe sind spezifische Daten über das protokollierte Ereignis. Eine SignalR-basierte Funktion läuft im Hintergrund dieser Funktion.

Knotenparameter

- **Filter** – wird verwendet, um anzugeben, welche Datensätze der Knoten verarbeiten soll. Einträge, die diesem Filter nicht entsprechen, werden vom Flow ignoriert. Das Format des Filters ist ein JSON-Objekt. Dieser Parameter kann durch einen Eingabewert überschrieben werden.
- **Name** – ermöglicht Ihnen, den Knoten zur besseren Orientierung beim Arbeiten mit dem Flow umzubenennen.

System Log

Der Knoten lädt die Datensätze im Systemprotokoll und ermöglicht die weitere Verarbeitung dieser Datensätze.

Der Administrator kann automatische Aufgaben einrichten, die ausgeführt werden, wenn Access Commander einen bestimmten Protokolleintrag sieht. Die Definition der Aktion erfolgt in den Knoteneinstellungen. Die Ausgabe sind spezifische Daten über das protokollierte Ereignis. Eine SignalR-basierte Funktion läuft im Hintergrund dieser Funktion.

Knotenparameter

- **Filter** – wird verwendet, um anzugeben, welche Datensätze der Knoten verarbeiten soll. Einträge, die diesem Filter nicht entsprechen, werden vom Flow ignoriert. Das Format des Filters ist ein JSON-Objekt. Dieser Parameter kann durch einen Eingabewert überschrieben werden.
- **Name** – ermöglicht Ihnen, den Knoten zur besseren Orientierung beim Arbeiten mit dem Flow umzubenennen.

SignalR

Der SignalR-Knoten liest die Daten im abonnierten Thema. Der Knoten ruft Daten in Echtzeit ab und eignet sich daher für Szenarien, in denen er über eine automatisierte Aufgabe verfügt, Informationen von Access Commander abzurufen, ohne dass eine ständige Abfrage erforderlich ist.

Knotenparameter

- **Heizer** – bietet verfügbare Themen zum Abonnieren an.
- **Filter** – wird verwendet, um anzugeben, welche Datensätze der Knoten verarbeiten soll. Einträge, die diesem Filter nicht entsprechen, werden vom Flow ignoriert. Das Format des Filters ist ein JSON-Objekt. Dieser Parameter kann durch einen Eingabewert überschrieben werden.
- **Name** – ermöglicht Ihnen, den Knoten zur besseren Orientierung beim Arbeiten mit dem Flow umzubenennen.

Weitere Informationen zur SignalR-Funktionalität finden Sie im KapitelSignalR (S. 120).

Dynamic SignalR

Ein dynamischer SignalR-Knoten gegenüber einem SignalR-Knoten ermöglicht dynamische Änderungen im Datenverbrauch. Dies kann das Ändern des Themas oder der Abonnementmethode basierend auf Eingabewerten umfassen. Die Ausgabewerte des Knotens sind einerseits aus Themen gewonnene Daten (Data) und andererseits Informationen über die erfolgreiche oder fehlgeschlagene Ausführung der Aktion dieses Knotens.

Knotenparameter

- **Topic** – definiert das Thema, für das die Änderung der Datenabfrage erfolgen soll.
- **Filter** – wird verwendet, um anzugeben, welche Datensätze der Knoten verarbeiten soll. Einträge, die diesem Filter nicht entsprechen, werden vom Flow ignoriert. Das Format des Filters ist ein JSON-Objekt. Dieser Parameter kann durch einen Eingabewert überschrieben werden.
- **Records** – definiert die Anzahl der zu lesenden Datensätze bei Verwendung des Lesetyps fetch.
- **Fetch When Ready** – legt fest, ob die Werte zurückgelesen werden sollen, wenn der Befehl fetch aktiviert wird.

- **Name** – ermöglicht Ihnen, den Knoten zur besseren Orientierung beim Arbeiten mit dem Flow umzubenennen.

Gültige Eingabewerte

Der Knoten akzeptiert die folgenden Eigenschaften als Eingabewerte. Gültige Eingabewerte überschreiben vorübergehend die in der Knotenkonfiguration festgelegten Parameter.

- **topic** – Zeichenfolge, die das zu entfernende Thema angibt.
- **Filter** – verkettet im JSON-Format, das die abzurufenden Datensätze angibt.
- **fetchWhenReady** – Bootlean, das den Knotenparameter „Fetch When Ready“ angibt.
- **Aktion** – eine Zeichenfolge, die die auszuführende Aktion angibt. Es kann abonnieren, abbestellen .....
- **update** – kann einen Zeitstempel (String) und ein Zeitfenster (Objekt) enthalten, die angeben, wann die auszuführende Aktion geändert wurde.

Weitere Informationen zur SignalR-Funktionalität finden Sie im KapitelSignalR (S. 120).

Write system log

Der Knoten „Systemprotokoll schreiben“ erstellt einen Eintrag im Access Commander-Systemprotokoll. Der Protokolleintrag enthält den angegebenen Schweregrad, die Ereignisbeschreibung und andere Details. Tritt während des Prozesses ein Fehler auf, wird dieser protokolliert und der Knotenstatus entsprechend aktualisiert. Der Knoten hat keine Ausgabewerte.

Knotenparameter

- **Severity** – bestimmt den Schweregrad des Datensatzes. Dieser Parameter kann durch den Abfrage-Eingabewert angegeben werden.
- **Filter** – wird verwendet, um anzugeben, welche Datensätze der Knoten verarbeiten soll. Einträge, die diesem Filter nicht entsprechen, werden vom Flow ignoriert. Das Format des Filters ist ein JSON-Objekt. Dieser Parameter kann durch einen Eingabewert überschrieben werden.
- **Detail** – wird für eine ausführlichere Beschreibung des Datensatzes verwendet, die im Systemprotokoll angezeigt wird. Dieser Parameter kann durch einen Eingabewert übersteuert werden.
- **Name** – ermöglicht Ihnen, den Knoten zur besseren Orientierung beim Arbeiten mit dem Flow umzubenennen.

Gültige Eingabewerte

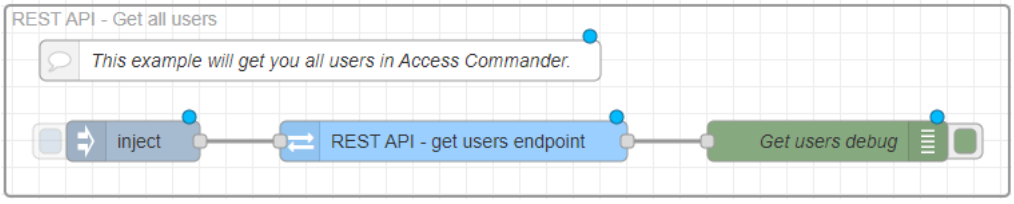
Der Knoten akzeptiert die folgenden Eigenschaften als Eingabewerte. Gültige Eingabewerte überschreiben vorübergehend die in der Knotenkonfiguration festgelegten Parameter.

- **severity** – eine Zeichenfolge, die den Schweregrad des Datensatzes angibt.
- **event** – eine Zeichenkette mit einer kurzen Beschreibung der aufgezeichneten Aktion.
- **detail** – String, der die detaillierte Beschreibung des Datensatzes enthält, die im Systemprotokoll angezeigt wird.

Beispiele für Flüsse

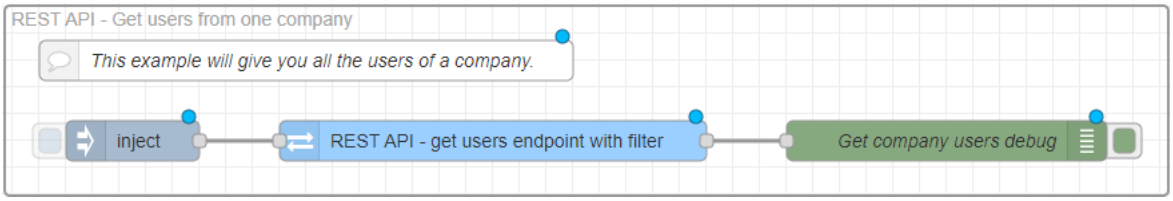
Access Commander bietet mehrere grundlegende automatisierte Aufgaben, die die Möglichkeiten der Automatisierung darstellen. Die Abläufe für diese Aufgaben können installiert werden, wenn Sie die Automatisierungsfunktion in **Access Commander** zum ersten Mal starten, sie können aber auch später importiert werden, siehe Streams exportieren/importieren (S. 102). Diese vordefinierten Abläufe können leicht für Ihre eigenen Zwecke geändert werden.

Get all users



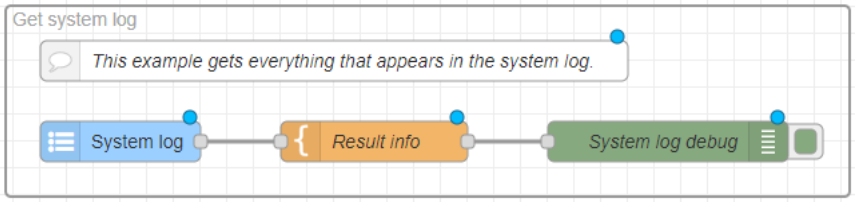
Dieser Ablauf generiert eine Liste aller Benutzer, einschließlich Informationen über sie. Die Aufgabe wird durch die Aktivierung des Inject-Knotens initiiert. Im Knoten **REST-API – Benutzerendpunkt abrufen** Es kann ein Filter angewendet werden, um anzugeben, welchen Benutzer der Prozess zurückgeben soll. Auf diese Weise kann die Ausgabe des Prozesses an die Bedürfnisse des Administrators angepasst werden.

Get users from one company



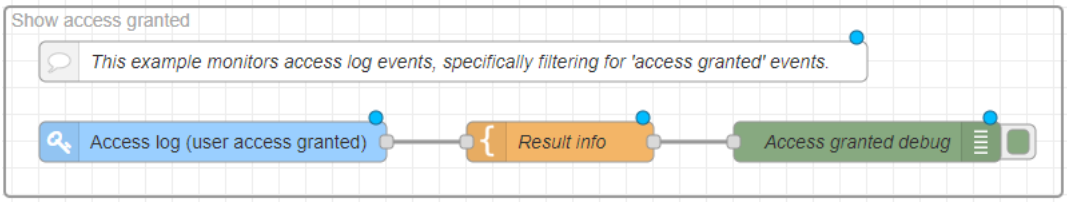
Dieser Ablauf generiert eine Liste aller Benutzer innerhalb eines Unternehmens, einschließlich Informationen über sie. Die Aufgabe wird durch die Aktivierung des Inject-Knotens initiiert. Die Firmenauswahl wird im Knoten eingestellt **REST-API – Benutzerendpunkt mit Filter abrufen** indem Sie ihre ID eingeben.

Get system log



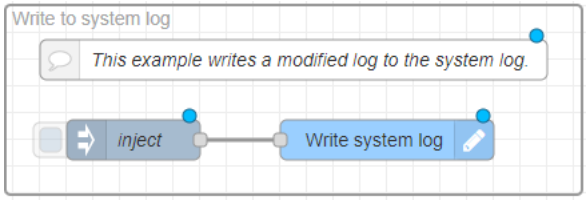
Dieser Stream ruft alle neuen Einträge im Systemprotokoll ab. Die Auswahl der Ereignisse kann durch die Angabe eines Filters im Knoten verfeinert werden **Systemprotokoll**.

Show access granted



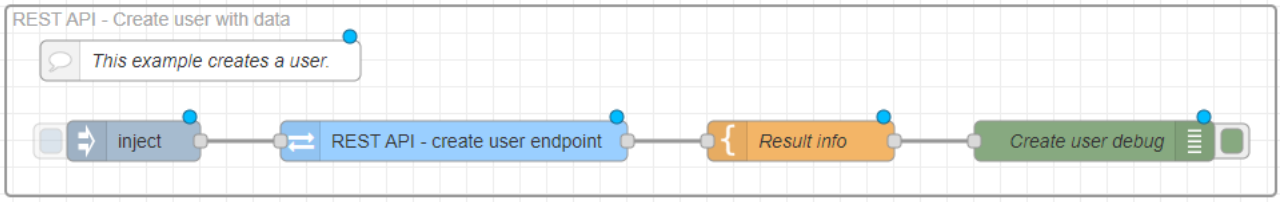
Dieser Ablauf ruft alle neuen Einträge im Zugriffsprotokoll ab. Der Stream ist so eingestellt, dass nur gewährter Zugriff geladen wird. Im Knoten **Zugriffsprotokoll** Es ist möglich, diese Einschränkung zu ändern.

Write to system log



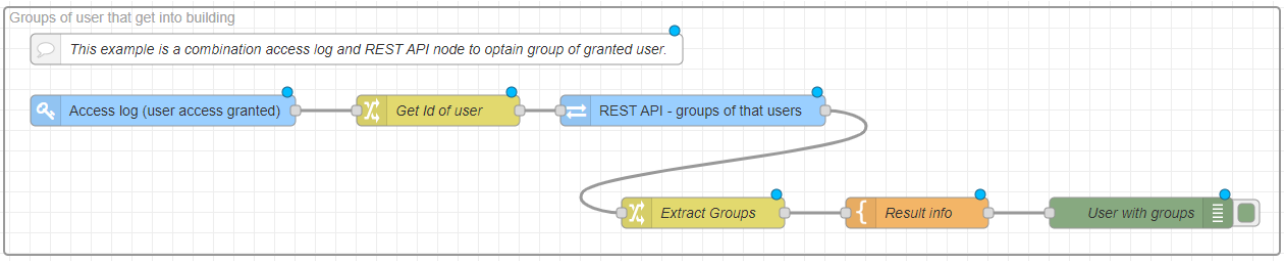
Dieser Ablauf erstellt einen Eintrag im Systemprotokoll. im Knoten **Systemprotokoll schreiben** Es können der Schweregrad, der Name und die detaillierte Beschreibung des Datensatzes festgelegt werden.

Create user with data



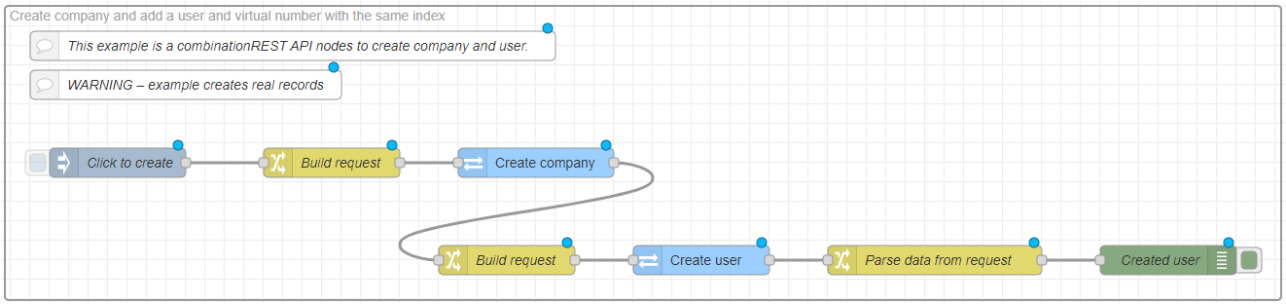
Dieser Ablauf wird verwendet, um einen neuen Benutzer zu erstellen. Eine Aufgabe wird durch die Aktivierung eines Knotens initiiert **Injizieren**. Knoten **Injizieren** enthält einen Nachrichtentext, der den Namen des Benutzers Joe Doe und seine Klassifizierung im Unternehmen mit der ID 1 angibt. Dieser Text wird im Knoten angewendet **Rest-API – Benutzerendpunkt erstellen** und auf dieser Grundlage erstellt der Benutzer sie. Knoten **Ergebnisinfo** Legt den Wortlaut der Nachricht fest, die in Debug-Nachrichten angezeigt wird.

Groups of users that get into building



Dieser Ablauf ruft Gruppen von Benutzern ab, denen Zugriff gewährt wurde. Erlaubte Zugriffe werden aus dem Zugriffsprotokoll geladen. Anschließend erhält der Flow die ID des Benutzers, dem Zugriff gewährt wurde, und nutzt den Knoten **REST-API – Gruppen dieser Benutzer** ruft Daten über diesen Benutzer ab. Knoten **Gruppen extrahieren** Ruft die Namen der Gruppen dieses Benutzers und des Knotens ab **Ergebnisinfo** erstellt den Wortlaut des Abschlussberichts.

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



Dieser Ablauf erstellt ein neues Unternehmen, den ersten Benutzer in diesem Unternehmen und seine virtuelle Nummer. Eine Aufgabe wird durch die Aktivierung eines Knotens initiiert **Injizieren**. Beim Start wird eine zufällige Ganzzahl generiert, die im Firmennamen und im Namen des Benutzers verwendet wird und als virtuelle Nummer dient. Knoten **Unternehmen gründen** erstellt ein Unternehmen mit einem definierten Namen. Aus der Antwort dieses Knotens wird die Firmen-ID ermittelt, auf deren Grundlage der nächste Knoten entsteht **Benutzer anlegen** legt in dieser Firma einen neuen Benutzer an und weist ihm gleichzeitig eine virtuelle Nummer zu. Knoten **Analysieren Sie Daten aus der Anfrage** Anschließend werden der Firmenname, der Benutzername und die virtuelle Nummer abgerufen.

Streams exportieren/importieren

Abläufe können in .json-Dateien exportiert und später wieder in die Automatisierungsschnittstelle importiert werden. Sowohl der Export als auch der Import werden über das erweiterte Menü in der oberen rechten Ecke durchgeführt. Flows, die von einer **Access Commander**-Installation zu einer anderen verschoben werden, müssen möglicherweise bearbeitet werden.

In den Importoptionen sind Beispielabläufe für **Access Commander** vorgeladen. Sie befinden sich auf der Registerkarte "Beispiele" im Ordner "Access-Commander-nodes".

ACHTUNG
Erweiterte Funktionseinstellungen, die von der neuen Lizenz nicht unterstützt werden, werden nicht gespeichert.

Vergessen Sie daher bei der Kündigung der Testlizenz nicht, Ihre eingestellten Streams zu exportieren.

Fehlerzustände

Bei der Arbeit mit Automatisierungen können gelegentlich Fehler auftreten, die deren Stabilität und Funktionalität beeinträchtigen. Wenn ein Fehlerzustand auftritt, werden Sie auf der Registerkarte "Automatisierung" in **Access Commander** auf den Zustand aufmerksam gemacht und es wird angeboten, die Node-RED-Plattform im Sicherheitsmodus neu zu starten. Der Sicherheitsmodus unterbricht vorübergehend die Ausführung der Abläufe und ermöglicht eine sichere Reparatur der Abläufe, die den Fehlerzustand verursacht haben. Der Neustart der Abläufe wird mit der Schaltfläche Deploy aktiviert.

Es gibt zwei grundlegende Fehlerbedingungen:

- **Node-RED antwortet nicht**
  Dieser Zustand tritt ein, wenn der Node-RED nicht mehr reagiert. Es werden keine festgelegten Automatisierungen durchgeführt. Dieses Problem kann durch verschiedene Faktoren verursacht werden, z. B. Systemüberlastung, Fehler in den Ablaufeinstellungen oder Konflikte zwischen importierten Modulen von Drittanbietern.
- **Node-RED ist instabil**
  Die Instabilität von Node-RED äußert sich durch wiederholte Neustarts der Plattform, was den Ablauf der Automatisierung stören und zu Datenverlusten führen kann. Ein wiederholter Neustart erfolgt normalerweise, wenn einer der Flows falsch konfiguriert ist und einen Neustart auslöst. Alle Streams werden für die Dauer des Neustarts ausgesetzt.

Installationsname

Der Name der spezifischen **Access Commander**-Installation wird in der Kopfzeile der Webschnittstelle angezeigt, und der Name wird allen angemeldeten Benutzern angezeigt. Der Standardname von **Access Commander** kann geändert werden, z. B. in die Adresse des Gebäudes, das eine bestimmte Anlage verwaltet.

Um den Namen zu ändern, gehen Sie zu **Einstellungen > Konfiguration > Registerkarte Installationsname**. Wenn eine Person mehrere Anlagen verwaltet, können Sie den Namen ändern, um einzelne Anlagen zu unterscheiden. Der Anlagenname wird auch in E-Mails an Unternehmen verwendet.

E-Mail-Funktion (SMTP) aktivieren und einrichten

Die E-Mail-Funktion ermöglicht den Versand von Benachrichtigungen oder den Versand von Login-Passwörtern an Benutzer. E-Mails werden über das SMTP-Protokoll versendet.

1. Die Einstellungen werden unter **Einstellungen > Konfiguration > E-Mail vorgenommen**.

2. Nach dem Einschalten der E-Mail-Funktion öffnet sich ein Dialogfenster, in dem Sie folgende Parameter einstellen können:
   - **SMTP-Serveradresse**, an die E-Mails gesendet werden.
   - **Server Port**, voreingestellt auf 25.
   - **Nutzername** Und **Passwort** auf das Konto auf dem SMTP-Server, wenn der SMTP-Server eine Autorisierung erfordert.
   - **Standard-Absenderadresse**, von dem aus E-Mails versendet werden.
3. Bei Bedarf einschalten:
   - **SSL** zur E-Mail-Verschlüsselung,
   - **Überprüfung des SSL-Serverzertifikats**,
   - **Kompatibilitätsmodus** bei Verbindung zu älteren SMTP-Servern, die keine neuen Funktionen unterstützen (GSSAPI).
4. Nach dem Speichern können Sie es im Reiter E-Mail einrichten **Basisadresse für E-Mail-Links**, das Teil der gesendeten E-Mail-Nachrichten sein wird und E-Mail-Empfänger auf den ausgewählten Teil der Schnittstelle verweisen kann **Access Commander**.
5. Sie können die vorgenommenen Einstellungen überprüfen, indem Sie eine Test-E-Mail senden.

Zwei-Faktoren-Authentifizierung

Die Zwei-Faktoren-Authentifizierung bietet ein höheres Maß an Sicherheit des Benutzerkontos in **Access Commander**. Um sich anzumelden, gibt der Benutzer seine Anmeldedaten ein und muss dann seine Anmeldung mit einer Authentifizierungsanwendung bestätigen. Sobald der Administrator die Notwendigkeit der Zwei-Faktoren-Authentifizierung aktiviert hat, wird der Benutzer bei der nächsten Anmeldung aufgefordert, sein Konto mit seiner eigenen Authentifizierungsanwendung zu verknüpfen.

Access Commander verlangt nicht, dass Sie Ihre Identität jedes Mal neu bestätigen, wenn Sie sich anmelden oder geschützte Aktionen durchführen. Sobald Sie die Überprüfung abgeschlossen haben, erinnert sich das System für eine begrenzte Zeit an Sie:

- 7 Tage für normale Anmeldungen
- 5 Minuten für Aktionen, die als sicherheitskritisch angesehen werden, wie das Ändern von API-Schlüsseln, das Aktualisieren Ihres eigenen Passworts oder das Ändern des Root-Passworts.

Das System kann sich bis zu zwei authentifizierte Geräte merken. Wenn Sie sich von einem neuen Gerät aus authentifizieren, wird das älteste gespeicherte Gerät entfernt. Wenn Sie versuchen, eine sicherheitskritische Aktion außerhalb des zulässigen Zeitfensters durchzuführen, fordert das System Sie einfach auf, sich erneut zu authentifizieren, bevor Sie fortfahren können.

1. Die Zwei-Faktoren-Authentifizierung wird vom Administrator auf der Seite **Einstellungen > Konfiguration > Registerkarte der Zwei-Faktoren-Authentifizierung** eingestellt.
2. Der Administrator kann auswählen, welche Benutzer eine Zwei-Faktoren-Authentifizierung benötigen.
   Möglichkeiten zur Anforderung einer zweistufigen Authentifizierung
   - **Optional**
     Die Zwei-Faktoren-Authentifizierung ist freiwillig Die Benutzer können sie in ihrem Profil selbst aktivieren.
   - **Obligatorisch für Benutzer mit einer Rolle**
     Jeder Benutzer, dem eine Rolle zugewiesen wurde, muss seine Anmeldung über eine Authentifizierungsanwendung bestätigen.
   - **Obligatorisch**
     Alle Benutzer müssen ihre Anmeldung über die Authentifizierungsanwendung bestätigen.

Einschalten der Zwei-Phasen-Authentifizierung

Wenn der Administrator die optionale Zwei-Faktoren-Authentifizierung einrichtet, aktiviert der Benutzer die Zwei-Faktoren-Authentifizierung selbst wie folgt:

1. Mit einem Klick auf das Bild des Benutzers in der oberen rechten Ecke öffnet sich das Benutzermenü.

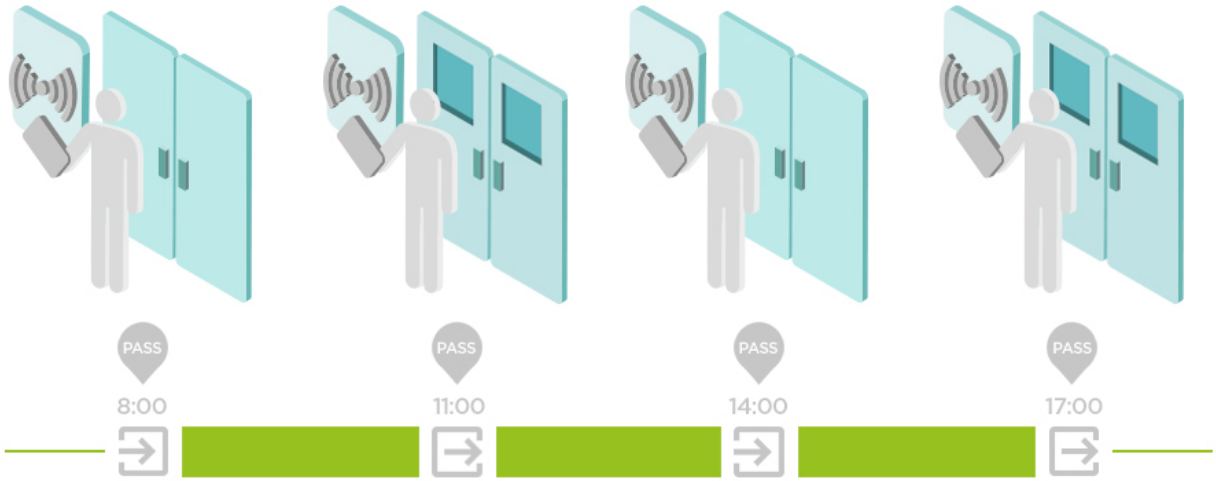
2. Verwenden Sie die Registerkarte Authentifizierungsanwendungen, um Ihr Konto mit der ausgewählten Authentifizierungsanwendung zu verknüpfen. Befolgen Sie die Anweisungen unter **Access Commander**.
3. Wählen Sie Profil anzeigen.

Anwesenheitseinstellungen

Access Commander ermöglicht die Überwachung der Benutzeranwesenheit. Im Anwesenheitsmodus werden die Ein- und Austrittszeiten der einzelnen Benutzer erfasst.

Anwesenheitsmodi

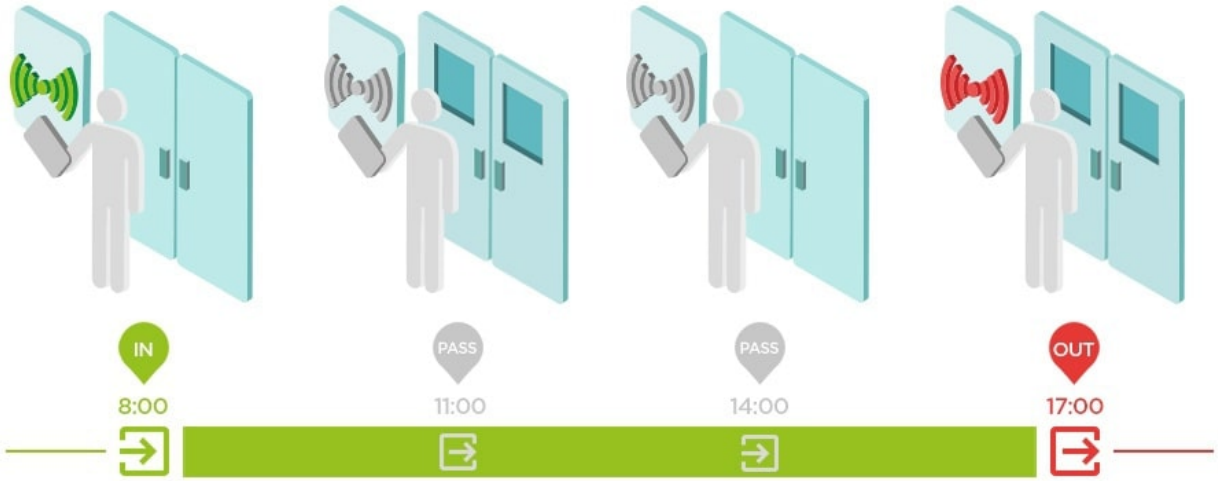
- **FREI**



Ankünfte und Abgänge werden ab der ersten und letzten Benutzerauthentifizierung auf einem beliebigen Gerät an einem Tag gezählt. Das Präsenzmodul funktioniert in diesem Modus nicht.

- **IN-OUT**

  Für einen ordnungsgemäßen Betrieb muss das Gerät so eingestellt sein, dass es den Bereich betreten und verlassen kann.



- **IN-OUT für alle Geräte**
  Dieser Modus ermöglicht die Anwesenheitsüberwachung. Ankünfte werden auf eingehenden Geräten erfasst, Abgänge werden auf ausgehenden Geräten erfasst. Bewegungen zwischen Zonen werden nicht als Ankunft/Abfahrt registriert.
- **IN-OUT für ausgewählte Geräte**
  Dieser Modus ermöglicht die Anwesenheitsüberwachung. An- und Abreisen werden auf ausgewählten Geräten erfasst, die als An- bzw. Abgänge eingestellt sind. An- und Abreisen werden nur auf diesen ausgewählten Geräten erfasst. Somit kann die Erfassung der Ankunft/Abfahrt beispielsweise nur am Haupteingang des Gebäudes eingestellt werden.

Einstellungen für den Gerätezugriffspunkt

Sie können jedes Gerät logisch in zwei Zugangspunkte unterteilen - Ankunft und Abfahrt. Jeder Zugangspunkt stellt einen Durchgang in eine Richtung dar und bestimmt, ob der Gerätebenutzer die Zone betritt oder verlässt. Ein Zugangspunkt kann von einem oder mehreren Gerätemodulen kontrolliert werden. Alle zugewiesenen Module verwalten dann die Durchgänge in der Richtung des spezifischen Zugangspunkts. Zugangspunkte werden vor allem in Situationen verwendet, in denen sich ein Gerät an der Grenze zwischen zwei Zonen befindet und die Bewegungsrichtung zwischen diesen Zonen genau erfasst werden muss (z.B. für Anti-Passback-Funktionen).

Zugangspunkte werden auch verwendet, um Benutzer im Modul zu verfolgen Gegenwart (S. 84). Access Points werden auch zur Überwachung des Ein- und Ausgangs verwendet Gebietsbeschränkungen (S. 86).

ANMERKUNG
In der Web-Konfigurationsoberfläche jedes Geräts werden die Zugangspunkte als **Ankunft** und **Abreise** bezeichnet. Um sie einzurichten, gehen Sie zu **Zutritt> Zutrittsregeln> Zutritt und Abreise tabs**.

Aktivieren von Access Points in Access Commander

1. Gehen Sie zur Seite Zonen v **Access Commander**.
2. Drücken Sie in der oberen rechten Ecke und ermöglichen die Nutzung von Access Points.

Modulzuweisung für Ankunft oder Abreise

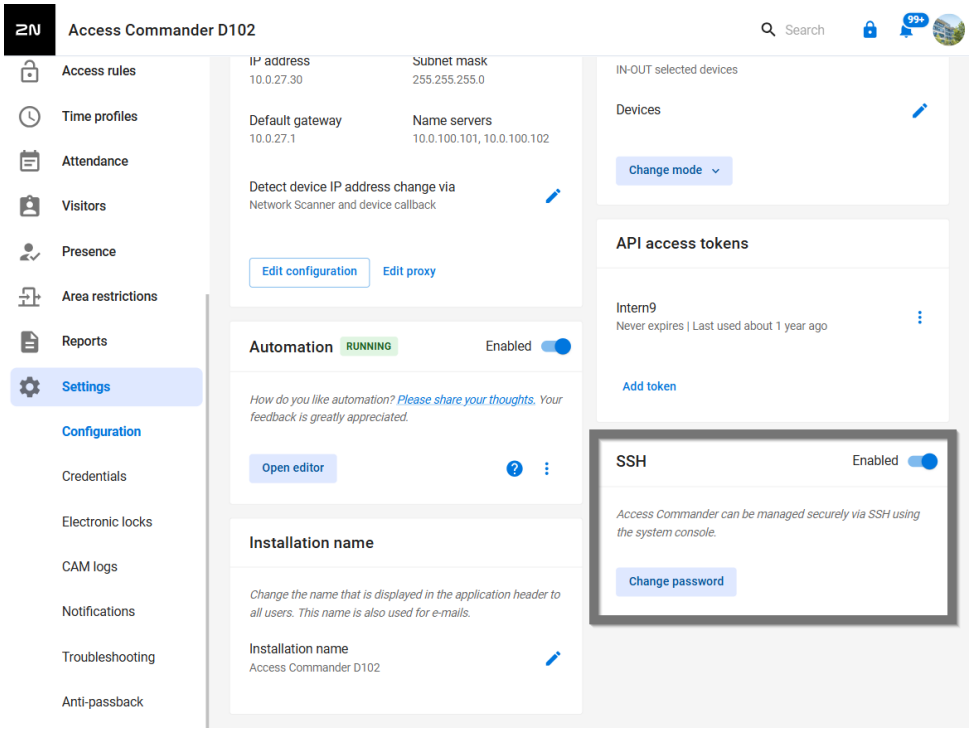
1. Geben Sie die Webkonfiguration des Geräts ein.

> **TIPP**
> Sie können auf die webbasierte Konfigurationsschnittstelle zugreifen, indem Sie in der Liste auf der Seite Geräte klicken .

2. Gehen Sie zu **Zugriff > Zugriffsregeln**.
3. Klicken Sie auf der Registerkarte **Ankunft** oder **Abreise** unter **Module** auf Verwalten.
4. Es öffnet sich ein Dialogfenster mit einer Liste der verfügbaren Zugangsverwaltungsmodule.
5. Ziehen Sie die Module per Drag & Drop in Gruppen entsprechend der Richtung, die sie bieten sollen.

> **TIPP**
> Klicken Sie auf , um ein bestimmtes Modul zu finden. Das Modul löst je nach seinen Fähigkeiten ein optisches oder akustisches Signal aus.

Erlauben Sie den SSH-Zugriff



> **WARNUNG**
> Die Aktivierung des SSH-Zugriffs wird nur fortgeschrittenen Benutzern empfohlen. Bei unsachgemäßer Verwendung besteht ein Sicherheitsrisiko.

Verwenden Sie die Registerkarte **Einstellungen > Konfiguration > SSH**, um Secure Shell zu aktivieren, das eine sichere Fernkommunikation mit der Systemkonsole ermöglicht. Wenn Sie SSH aktivieren, können Sie Ihr System sichern und wiederherstellen oder **Access Commander** vollständig neu starten.

Um sich mit einer Access Commander Box oder einer virtuellen Maschine zu verbinden, muss der SSH-Client die IP-Adresse von **Access Commander** und das System-Root-Passwort kennen. Das System-Root-Passwort kann unter **Einstellungen > Konfiguration > Registerkarte SSH** festgelegt werden.

ANMERKUNG
Das Ändern des Root-Passworts erfolgt in der Konfigurationskonsole, nicht in Access Commander.

Der SSH-Zugriff kann auch direkt in der Linux-Konfigurationskonsole aktiviert und verwaltet werden, siehe Linux-Einstellungen (S. 90).

Verschlüsselungsschlüssel für die My2N-Anwendung

Benutzer können die My2N App verwenden, um sich mit 2N Geräten zu verbinden. Die Kommunikation zwischen der My2N-Anwendung und dem Gerät ist immer verschlüsselt. **Access Commander** verwaltet automatisch die System-Kopplungsschlüssel, die an WaveKey-fähige Geräte verteilt werden, um ein sicheres, vertrauenswürdiges Pairing zu gewährleisten. Ohne den Verschlüsselungsschlüssel zu kennen, kann die Anwendung My2N den Benutzer nicht authentifizieren. Der primäre Verschlüsselungsschlüssel wird automatisch generiert, wenn die Gegensprechanlage zum ersten Mal gestartet wird oder, im Falle der **Access Commander** Verwaltung, als Teil der Konfiguration. Der Schlüssel kann jederzeit manuell neu generiert werden. Der primäre Kodierungsschlüssel wird bei der Kopplung zusammen mit der Auth-ID in das mobile Gerät übertragen.

ANMERKUNG
Im System werden zwei Arten von Schlüsseln verwendet: **passende Schlüssel** und **Zugangsschlüssel**. Kopplungsschlüssel werden verwendet, um die My2N App mobile Anwendung mit dem Gerät zu authentifizieren. Zugriffsschlüssel bestimmen die Berechtigungen für Funktionen innerhalb der mobilen App.

Neue Schlüssel erstellen

1. Gehen Sie zu **Einstellungen > Authentifizierung > Registerkarte Verschlüsselungsschlüssel für die Anwendung My2N**.
   Es können bis zu 4 Zugangsschlüssel erzeugt werden. Wenn Sie versuchen, einen fünften Schlüssel zu generieren, warnt **Access Commander** davor, dass bei der Generierung des Schlüssels der älteste Schlüssel gelöscht wird. Auf der Registerkarte sind die Generierungszeiten für jeden Schlüssel aufgeführt.
2. Neuen Schlüssel generieren

   TIPP
   Aus Sicherheitsgründen wird empfohlen, die Kopplungsschlüssel einmal in einem längeren Zeitraum (z.B. einmal im Jahr) zu erneuern.
3. Der neu generierte Schlüssel wird automatisch auf die My2N-App hochgeladen, wenn das Mobiltelefon zum ersten Mal mit einem zuvor gekoppelten Gerät verwendet wird.

Der erzeugte Schlüssel kann durch Anklicken von gelöscht werden.

TIPP
Für ein höheres Maß an Sicherheit ist es besser, den **QR-Code** zu verwenden, der den öffentlichen Schlüssel enthält. Wenn der QR-Code nicht verfügbar ist, können Sie die **PIN-Kopplung** verwenden.

ACHTUNG
Die QR-Code-Kopplung wird nur von Geräten mit der HIP-Firmware 2.50.0 und höher (einschließlich der 3.0-Serie) unterstützt. In einer Umgebung mit Access Commander kann der **QR-Code** angezeigt werden, aber bei älteren Versionen von HIP ist die Kopplung nur mit **PIN** erfolgreich.

ANMERKUNG

- Wenn die My2N App keinen Zugriff auf gültige Verschlüsselungscodes hat, kann sie nicht zur Benutzerauthentifizierung verwendet werden. Um die Funktionalität der Anwendung wiederherzustellen, muss die Anwendung erneut mit dem Gerät gekoppelt werden, das mit Access Commander verbunden ist. Dadurch werden die gültigen Verschlüsselungsschlüssel in die My2N App hochgeladen.
- Die Gewährung des Zugriffs auf das Gerät hängt von den eingestellten Zugriffsrechten des Benutzers ab.

RFID-Karten-Kompatibilitätsmodus

Wenn **Access Commander** meldet, dass die soeben hinzugefügte Karte bereits im System verwendet wird, kann dies daran liegen, dass der RFID-Kartenkompatibilitätsmodus aktiviert ist. Dieser Modus wird vom Administrator auf der **Registerkarte Einstellungen > Authentifizierung > Kompatibilitätsmoduseinstellungen** aktiviert.

ACHTUNG

- Der Kompatibilitätsmodus sollte nur aktiviert werden, wenn Probleme beim Laden zuvor registrierter Karten auftreten. Die Verwendung des Kompatibilitätsmodus kann sich auf die Authentifizierungsmechanismen auswirken
- Es wird nicht empfohlen, den Kompatibilitätsmodus mit der Verwendung von Karten zu kombinieren, die durch PiCard-Technologien gesichert sind.

PICard-Schlüssel

Unter **Einstellungen > Zugriff > Registerkarte PICard-Schlüssel** werden die Verschlüsselungsschlüssel der 2N PICard Commander-Anwendung gespeichert. Wenn die Verschlüsselungsschlüssel in **Access Commander** geladen werden, zeigt die Registerkarte den Namen des PICard Commander-Projekts und die numerische Kennung für den Schlüsselexport an. Auf der Registerkarte können Sie die hochgeladenen Schlüssel aus **Access Commander** löschen

ACHTUNG
Wenn Sie die PICard-Schlüssel entfernen, funktionieren alle Karten, die mit diesen Schlüsseln verschlüsselt wurden, nicht mehr.

Importieren Sie PICard-Verschlüsselungsschlüssel

1. Gehen Sie zu **Einstellungen > Zugriff > Registerkarte PICard-Tasten**.
2. Nach dem Klicken auf Importieren Laden Sie die Verschlüsselungsschlüsseldatei aus Ihrem Repository hoch.
3. Geben Sie ein Passwort ein, um die Datei zu schützen, wenn Sie beim Exportieren aus der Anwendung eines festgelegt haben PICard Commander.

2N PICard Commander ist eine Softwareanwendung zum Verschlüsseln von Zugangsdaten auf Zugangskarten. Die Anwendung erstellt Projekte, die eine Reihe von Verschlüsselungs- und Leseschlüsseln generieren. Projektleserschlüssel können in 2N-Geräte oder in importiert werden **Access Commander**, der anschließend die Verteilung der Leseschlüssel an die angeschlossenen 2N-Geräte gewährleistet.

Aktivierte USB-Lesegeräte

Um die Aufzeichnung einiger Benutzerauthentifizierungsmethoden zu erleichtern, können Sie USB-Lesegeräte verwenden, die an den Computer angeschlossen sind, auf den der **Access Commander** zugreift. Die Lesegeräte müssen in **Access Commander** unter **Einstellungen > Zugriff > Registerkarte Erlaubte USB-Lesegeräte** aktiviert werden.

1. Gehen Sie zu **Einstellungen > Zugriff > Registerkarte USB-Lesegerät aktiviert.**
2. Klicken Sie auf Enable Readers, um das Dialogfeld zu öffnen.
3. Das Aktivieren/Deaktivieren der Verwendung eines externen USB-Geräts erfolgt in einem Dialogfeld.
4. Anschließend wird ihre Leserfreigabe durch Klicken auf Ändern geändert.

Access Commander ermöglicht die Verwendung folgender USB-Geräte:

- 125-kHz-RFID-Kartenleser – Bestell-Nr. 9137420E
- 13,56 MHz und 125 kHz RFID-Kartenleser – Bestell-Nr. 9137421E
- Fingerabdruckleser - Bestell-Nr. 9137423E

CAM-Protokolle

CAM-Protokolle werden verwendet, um automatisch mehrere Bilder vor und nach einem ausgewählten Ereignis aufzuzeichnen. Unter **Einstellungen > CAM-Protokolle** können Sie die verschiedenen Arten von Ereignissen verwalten, für die CAM-Protokolle erstellt werden sollen.

Beispielsweise können bei jedem Karteneinschub CAM-Protokolle erstellt werden. Wenn jemand die Karte durchzieht, werden 5 Bilder vor dem Durchzug und 3 Bilder nach dem Durchzug in den Zugriffsprotokollen aufgezeichnet. Frames werden nach 1 Sekunde aufgezeichnet. Für die Bilder wird ein Speicherplatz von 1, 3 oder 5 GB angelegt. Wenn der Speicher voll ist, werden die ältesten Bilder gelöscht. Die Zugriffsprotokolle selbst werden nicht gelöscht.

Erstellen eines CAM-Protokolltyps

1. Gehen Sie zur Seite **Einstellungen > CAM-Protokolle**.
2. Klicken Sie oben rechts auf der Seite auf die Schaltfläche „Hinzufügen“.
3. Geben Sie einen Namen für den CAM-Protokollereignistyp ein.
   Der neu erstellte CAM-Protokollereignistyp wird in der Liste angezeigt und die Details im CAM-Protokoll werden geöffnet. Im Detail des CAM-Protokolls muss eingestellt werden, für welche Ereignisse und auf welchen Geräten die Bilder der Kameras generiert werden.

CAM-Logos einstellen

Informationen zum CAM-Protokolltyp können im CAM-Protokolldetail verwaltet werden. Die Details des CAM-Protokolls werden durch Klicken auf das ausgewählte CAM-Protokoll in der Liste oder nach dem Erstellen eines neuen CAM-Protokolls geöffnet.

Ereignisse beobachtet

Auf der Registerkarte können Sie eine Liste von Ereignissen auswählen, bei denen Bilder von den Kameras erfasst werden.

Verfolgte Ereignisse können die folgenden sein:

- **Ansätze**
  - Benutzer akzeptiert
  - Autokennzeichen erkannt
  - Benutzer abgelehnt
  - Drücken Sie die REX-Taste
- **Sicherheit**
  - Schutzschalter aktiviert
  - Unbefugtes Öffnen der Tür
  - Ferngesteuerte Türöffnung
  - Zugriff verweigert – wiederholte Fehleingabe
  - Stiller Alarm aktiviert
- **Aufruf**
  - Anruf eingeleitet

Überwachte Geräte

Es wird empfohlen, die Aufzeichnung von CAM-Protokollen nur von Geräten einzustellen, die mit einer Kamera ausgestattet sind. Die Auswahl des Gerätes erfolgt in einem sich öffnenden Dialogfenster  . Gleichzeitig ermöglicht die Karte die Aufzeichnung von CAM-Protokollen aller Geräte.

Elektronische Schlösser

Das System **Access Commander** ermöglicht die Zugangsverwaltung über elektronische Schlösser 2N Fortis, die durch RFID-Karten mit MIFARE-Technologie® DESFire® entriegelt werden. Bei der Konfiguration von elektronischen Schlössern wird jedem Schloss ein Verschlüsselungscode zugewiesen. Die Schlossschlüssel werden dann auf den RFID-Karten der berechtigten Benutzer gespeichert. Wenn die Schlüssel auf der Karte und im Schloss übereinstimmen, wird der Schließmechanismus entriegelt.

Eine RFID-Zugangskarte kann für den Zugang zu bis zu 90 Türen mit Schlössern 2N Fortis verwendet werden, abhängig von der Anzahl der angewendeten Zeitprofile. Wenn die Speicherkapazität der Karte überschritten wird, schlägt das Schreiben von Daten auf die Karte fehl. Das Ereignis des Schreibfehlers wird im Zugriffsprotokoll des Systems aufgezeichnet. Wenn Schlossgruppen verwendet werden, können mehr Türen auf eine einzelne Karte geschrieben werden als bei einer individuellen Zuweisung. Wenn Schlossgruppen verwendet werden, können mehr Türen pro Karte registriert werden als bei einer individuellen Zuweisung.

Fortis Commander

Fortis Commander ist eine eigenständige Anwendung, die die elektronischen Schlösser **Fortis** mit dem System **Access Commander** verbindet. Die Anwendung setzt Sperren entsprechend der in **Access Commander**u erstellten Projektdatei, die die Sperrkonfiguration enthält. Die Datei ist verschlüsselt und kann nur auf einer bestimmten Installation verwendet werden.

Stecker und Installation

Fortis Commander ist für die Installation auf einem Windows-Computer mit Bluetooth Low Energy (BLE) Unterstützung konzipiert.

Die App finden Sie auf der Website 2N Download Centre.

Verlauf der Installierung

1. Laden Sie das Installationspaket über den angegebenen Link herunter.
2. Starten Sie das Installationsprogramm und schließen Sie die Installation ab, indem Sie den Anweisungen auf dem Bildschirm folgen.

Projektdatei

Die Projektdatei wird in **Access Commander** erstellt und enthält die vollständige Projektkonfiguration. Die Datei ist verschlüsselt und passwortgeschützt.

Sperren in Access Commander einstellen

Bevor Sie Schlüssel zu einzelnen Schlössern hochladen können, müssen Sie **Access Commander** mit **Fortis Commander** koppeln.

Generierung des Master Encryption Key (MEK) und Projektvorbereitung

1. Melden Sie sich bei Access Commander an.
2. Gehen Sie zu **Einstellungen > Elektronische Schlösser**.
3. Auf der Registerkarte **Ersteinstellungen** klicken Sie auf Schlüssel generieren.
4. Erstellen Sie den Hauptverschlüsselungscode.

ACHTUNG
Der Hauptverschlüsselungscode kann später weder eingesehen noch geändert werden .

ANMERKUNG
Anhand des Hauptchiffrierschlüssels (MEK) generiert **2N Access Commander** eine Reihe von Chiffrierschlüsseln. Der Schlüssel sollte also eindeutig und ausreichend sicher sein. Der Schlüsselsatz basiert auf dem Hauptchiffrierschlüssel, so dass Projekte mit demselben Hauptchiffrierschlüssel dieselben Schlüsselsätze erzeugen. Wenn ein Projekt verloren geht, kann ein neues Projekt mit demselben Hauptschlüssel erstellt werden und die Verschlüsselung fortsetzen.

5. Nachdem Sie die Schlüssel erzeugt und das Passwort für die Projektdatei festgelegt haben, können Sie **die Projektdatei** herunterladen, die ein Abbild der Konfiguration des elektronischen Schlosses im System **Access Commander** ist.
6. Klicken Sie auf der Registerkarte **von Fortis Commander** auf Anwendung herunterladen**,** von wo aus das Herunterladen von **Fortis Commander** (Anwendung zur Konfiguration von elektronischen Schlössern) gestartet wird.

ACHTUNG
Projektinformationen sind sensible Daten. Schützen Sie sie vor Missbrauch.

Konfigurieren des elektronischen Schlosses mit Fortis Commander

1. Installieren Sie **Fortis Commander** und öffnen Sie es.
2. Klicken Sie auf Projekt öffnen und öffnen Sie die heruntergeladene Projektdatei im Datei-Explorer.

3. Geben Sie in dem daraufhin angezeigten Dialogfeld das Passwort für die Projektdatei ein.
4. Nachdem Sie die Projektdatei geöffnet haben, wählen Sie Mit Gerät verbinden und verbinden Sie die Servicekarte mit dem Schloss.
5. Klicken Sie auf **Zuweisen**, wodurch die Sperre dem Projekt zugewiesen wird.
6. Trennen Sie die Verbindung zum Gerät und klicken Sie auf **Datei > Projekt schließen**.
7. Wenn die Konfiguration abgeschlossen ist, öffnen Sie das System **Access Commander**. Gehen Sie auf die Registerkarte **Einstellungen > Elektronische Schlösser** und klicken Sie erneut auf Fortis Commander. Laden Sie die Projektdatei hoch.

ANMERKUNG
Wenn Sie das Schloss zwischen Installationen verschieben oder einen Anspruch geltend machen, müssen Sie einen **Factory Reset** durchführen. Dieser Vorgang setzt das Schloss auf die Werkseinstellungen zurück und löscht alle vorherigen Konfigurationen.

Verfahren zur Aktualisierung der Konfiguration

1. Nehmen Sie Änderungen in **Access Commander** vor.
2. Laden Sie die neue Projektdatei herunter.
3. Laden Sie die Datei auf **Fortis Commander** hoch und nehmen Sie die erforderlichen Änderungen an den Schlössern vor.
4. Wenn Sie andere Änderungen an **Access Commander**u vornehmen, laden Sie immer eine neue Projektdatei herunter.

ACHTUNG
Für jede Konfigurationsänderung in **Access Commander**u müssen Sie eine neue Projektdatei herunterladen - Sie können keine ältere Datei verwenden, die bereits auf **Fortis Commander** hochgeladen wurde.

Dauerhaftes Ver- und Entriegeln

Die App ermöglicht es Ihnen, das Schloss dauerhaft zu sperren und zu entsperren. Die Funktion wird für Service-Einsätze oder Notfallkontrollen ohne Verwendung einer Karte verwendet.

Erfassung von Ereignissen aus elektronischen Schlössern mit RFID-Karten/Chips

Einstellungen für die Ereignissammlung

1. Öffnen Sie **Einstellungen > Elektronische Schlösser > Registerkarte Ereignisse**.

2. Wählen Sie den Ereignistyp:
   - **Sammeln von Zugangs- und Systemereignissen** - Alle Zugangs- und Systemereignisse werden auf der Karte/dem Chip aufgezeichnet und in das **System Log** und **Access Log** geschrieben.
   - **Nur Systemereignisse sammeln** - nur Systemereignisse werden protokolliert, Zugriffsereignisse werden nicht auf Karten gespeichert.
   - **Sammeln Sie keine Ereignisse auf** Registerkarten - es werden keine Ereignisse auf die Registerkarte geschrieben; sie können nur über **Fortis Commander**u aufgerufen werden.

TIPP
Wenn Sie geeigneten Ereignissatzes auswählen, können Sie die Systemlast und die Nutzung des Speicherplatzes verringern. Eine detaillierte Protokollierung ist jedoch für Diagnosen und Sicherheitsaudits wichtig.

Ereignisse von einer Karte exportieren

Die Karte speichert maximal **16 erste Ereignisse**. Ereignisse können auf zwei Arten gelesen werden:

- Klicken Sie in **Access Commander** auf das Symbol im Suchfeld in der Kopfzeile und laden Sie die Registerkarte.
- Wenn Sie ein Gerät mit **2N OS** verwenden, werden Ereignisse von der Karte gelesen und an **Access Commander**u gesendet.

Hochladen von Ereignissen auf das Schloss

1. Öffnen Sie **Einstellungen > Elektronische Schlösser > Fortis Commander** und klicken Sie auf Datei herunterladen.
2. Öffnen Sie die Datei in **Fortis Commander**.
3. Verbinden Sie sich über die App **Fortis Commander** mit dem elektronischen Schloss.
4. Laden Sie die aktualisierte Datei wieder auf **Access Commander** hoch.
5. Nach dem Hochladen werden die Ereignisse in **Zugriffsprotokolle** und **Systemprotokolle** angezeigt.

Serviceleistungen

Diese Funktionen sind verfügbar für **Fortis Cylinder**:

- **Demontage** - Demontage von Schlössern zu Servicezwecken.
- **Auswechseln der Batterie** - Auswechseln der Batterie im Schloss.

ACHTUNG
Servicevorgänge sind für andere Arten von Sperren nicht relevant.

ANMERKUNG
Aus dem Servicemodus kehrt das Schloss in den normalen Modus zurück, indem Sie die Taste Lock drücken, um es dauerhaft zu sperren.

Aktualisieren Sie die Karte

Benutzerzugangskarten müssen regelmäßig aktualisiert werden. Der Benutzer aktualisiert die Karte, indem er die Karte an das 2N IP-Gerät anschließt, für das er gültige Zugriffsrechte besitzt. Die Karte muss so lange

am Gerätelesegerät gehalten werden, bis der Türöffnungsschalter eingeschaltet wird. Der Türöffnungsschalter wird erst aktiviert, nachdem der Zugang zu den Schlössern aktualisiert wurde

Sie können die standardmäßige zehntägige Gültigkeit der Karten unter **Einstellungen > Elektronische Schlösser > Registerkarte Kartenparameter** ändern.

ACHTUNG
Wenn Sie die Zutrittsrechte zu den Schlössern in **Access Commander** ändern, werden die Änderungen auf der Zutrittskarte des Benutzers erst nach der Aktualisierung auf dem Kartenleser des 2N Geräts sichtbar! Aus Sicherheitsgründen empfiehlt es sich, die Gültigkeitsdauer der Karten zu verkürzen, damit sie regelmäßig aktualisiert werden.

IP-Lesegeräte, Geräte, die Kartenaktualisierungen ermöglichen, und deren Einstellungen werden im Kapitel IP-Gerätelesereinstellungen (S. 30).

Kompatible Karten

ANMERKUNG
Für die Zwecke dieser Dokumentation bezeichnet der Begriff **Karte** jeder kompatible Identifikator mit MIFARE DESFire-Technologie.

Zum Öffnen elektronischer Schlösser 2N Fortis Karten mit Zufalls-ID können nicht verwendet werden.

Karten mit PICard-Technologie können nicht zum Öffnen elektronischer Schlösser verwendet werden 2N Fortis.

Zeitprofile auf elektronischen Schlössern

Elektronische Schlösser unterstützen Zeitprofile mit den folgenden Einschränkungen:

- Feiertage gelten nicht.
- Innerhalb eines Tages können bis zu 4 verschiedene Zeitintervalle eingestellt werden.
- Innerhalb eines Zeitprofils können 4 tägliche Intervallpläne definiert werden.

TIPP
Dies bedeutet, dass Sie beispielsweise für Montag, Dienstag, Mittwoch und Donnerstag unterschiedliche Einstellungen haben können, für Freitag, Samstag und Sonntag jedoch eine der vorhandenen Einstellungen verwenden müssen.

ACHTUNG
Verstößt das Zeitprofil gegen die festgelegten Einschränkungen, wird die Zutrittsregel ignoriert und dem Benutzer der Zutritt verweigert.

Karten für die Wartung

Wartungskarten ermöglichen den autorisierten Zugang zum Schloss. Sie ermöglichen es, das Schloss in Betrieb zu nehmen, die Batterie zu wechseln und das Schloss zu demontieren.

ACHTUNG
Die Wartungskarte kann nicht gleichzeitig als Benutzerzugangskarte verwendet werden.

Einstellungen auf der Registerkarte Wartung

1. Gehen Sie in **Access Commander** zu **Einstellungen > Elektronische Schlösser**.
2. Klicken Sie auf der Registerkarte **Wartung** auf Erstellen.
3. Wählen Sie in dem sich öffnenden Dialogfeld die Art der Karte aus, die Sie erstellen möchten.
   - Einstellung neuer Schlösser - aktiviert zuvor konfigurierte neue Schlösser in den Werkseinstellungen im Servicemodus.
   - Service - aktiviert den Servicemodus für das bereits eingestellte Schloss.
   - Demontage - gibt das bereits eingestellte 2N Fortis Zylinderschloss zur Demontage frei, siehe 2N Fortis Installationshandbuch.
   - Batteriewechsel - gibt das bereits eingestellte 2N Fortis Zylinderschloss zum Batteriewechsel frei, siehe 2N Fortis Installationshandbuch.

   TIPP
   Eine physische Karte kann gleichzeitig mit **Setting New Locks** und einer anderen Servicekarte geladen werden. Wir empfehlen eine Kombination aus **Einstellung neuer Schlösser** und **Service**.
4. Klicken Sie auf . Weiter zu.
5. Schließen Sie die Karte an das angeschlossene USB-RFID-Lesegerät an. Warten Sie, bis die Daten auf die Karte geladen sind.

Die Gültigkeit der Daten auf der Wartungskarte beträgt ein Jahr. Nach Ablauf dieser Zeit müssen die Daten gelöscht und die Karte neu eingerichtet werden.

Fehlerbehebung

Diagnoseprotokolle

Diagnoseprotokolle werden vom technischen Support verwendet, um gemeldete Probleme zu identifizieren und zu lösen. Protokolle enthalten Informationen über durchgeführte Aktionen, Fehler, Statusänderungen und andere relevante Ereignisse.

Laden Sie Diagnoseprotokolle herunter

1. Gehe zu **Einstellungen > Fehlerbehebung > Registerkarte Diagnoseprotokolle**.
2. Klicke auf Protokolle erstellen.
   Das Generieren des Protokollpakets dauert einige Minuten.
3. Sobald das Deck fertig ist, erscheint es auf der Karte und ist verfügbar Herunterladen.

Nutzungsstatistiken

Wenn die Funktion eingeschaltet ist, wird gesendet **Access Commander** einmal täglich anonyme Daten über die genutzten Funktionen an einen sicheren 2N-Server. Jede Sendung erfolgt unter einer eindeutigen Kennung, die bei jeder neuen Sendung automatisch neu generiert wird. Dadurch wird verhindert, dass die

2N-Partei die jeweilige Installation identifiziert **Access Commander**. Die gewonnenen Informationen werden verwendet, um die Produktentwicklung zu verbessern, Funktionen zu entwickeln und das Benutzererlebnis zu verbessern.

Benachrichtigung

Mit dem Benachrichtigungsmodul können Sie die Überwachung ausgewählter Ereignisse und Systemeigenschaften einrichten, die ihm bekannt sind **Access Commander** Informieren Sie per E-Mail oder Benachrichtigung in der oberen Leiste neben dem Benutzermenü.

Die Liste der Benachrichtigungen wird auch auf der **Seite Systemprotokolle > Benachrichtigungen angezeigt**.

Die Datensätze können in eine CSV-Datei heruntergeladen werden, indem Sie auf die Schaltfläche Export oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 angegeben.

Einrichten eines neuen Benachrichtigungstyps

1. Gehen Sie zur Seite **Einstellungen > Benachrichtigungen**.
2. Klicken Sie oben rechts auf der Seite auf die Schaltfläche „Hinzufügen“.
3. Geben Sie einen Namen für den neuen Benachrichtigungstyp ein.
   Nach der Erstellung werden die Details der Benachrichtigung angezeigt, in der die Geräte ausgewählt werden können, für die die Benachrichtigung überwacht werden soll; Benutzer hinzufügen, an die die Benachrichtigung gesendet werden soll; Wählen Sie die Zustellungsmethode für die Benachrichtigung.

Benachrichtigungseinstellungen

Die Benachrichtigungsarten werden in den Details der Benachrichtigungsart festgelegt. Um die Details der Benachrichtigungsart zu öffnen, klicken Sie auf die ausgewählte Benachrichtigung in der Liste auf der Seite **Einstellungen > Benachrichtigungen**.

Art der Benachrichtigung

Auf dieser Registerkarte werden die Benachrichtigungsmethoden und die Liste der E-Mail-Benachrichtigungsempfänger festgelegt.

In **Access Commander** erscheinen die Benachrichtigungen unter dem in der oberen Leiste, neben dem Benutzermenü oder unter **Systemprotokoll > Benachrichtigungen**.

Benachrichtigungs-E-Mails können an die in verwalteten Benutzer gesendet werden **Access Commander** und Empfänger außerhalb des Systems. Benutzer können aus der Liste ausgewählt werden. Die E-Mail-Adressen der anderen Empfänger müssen manuell eingegeben werden.

ANMERKUNG
Für die korrekte Funktion von E-Mail-Benachrichtigungen ist die korrekte Einstellung von SMTP erforderlich, siehe E-Mail-Funktion (SMTP) aktivieren und einrichten (S. 103).

Überwachte Geräte

Der angegebene Benachrichtigungstyp kann sowohl für alle Geräte als auch nur für einige Geräte generiert werden. Wenn „Alle Geräte überwachen“ aktiviert ist, kann das Ereignis auf jedem Gerät auftreten und es wird eine Benachrichtigung generiert. Wenn die Überwachung aller Geräte deaktiviert ist, wird nur dann eine Benachrichtigung generiert, wenn das Ereignis auf dem ausgewählten Gerät auftritt. Die Auswahl des Gerätes erfolgt im Menü, das mit geöffnet wird .

Netzwerkeinstellungen

Um eine Netzwerkverbindung einzurichten, gehen Sie zu **Einstellungen > Konfiguration > Registerkarte Netzwerk**. Auf dieser Registerkarte werden die aktuellen Netzwerkparameter des **Access Commander** angezeigt, und Sie können sie einstellen. Die Einstellung einzelner Parameter kann nach Aktivierung der manuellen Konfigurationsmethode erfolgen.

Mit der Konfigurationsmethode können Sie die Netzwerkeinstellungsparameter automatisch vom DHCP-Server oder manuell festlegen. Beim Ändern der automatisch eingestellten IP-Adresse vom DHCP-Server auf eine manuell eingegebene Adresse wird der Webbrowser auf die ausgefüllte IP-Adresse umgeleitet. Nach der Umleitung erfolgt ein Neustart**Access Commander** und ist erforderlich, um sich erneut am System anzumelden.

ACHTUNG

- Wenn Sie die Konfigurationsmethode auf DHCP ändern, ändern Sie die IP-Adresse des Servers und können dazu führen, dass die Verbindung unterbrochen wird.
- Wenn Sie den HTTP-Proxyserver ändern,**Access Commander**wird automatisch neu gestartet.

Erkennung einer Änderung der Geräte-IP-Adresse

Access Commander stellt über ihre IP-Adressen eine Verbindung zu Geräten her. Um zu verhindern, dass die Verbindung zu einem Gerät mit einer dynamischen IP-Adresse unterbrochen wird, stehen zwei Methoden zur Verfügung, um die IP-Adressen des Geräts zu erkennen

- **Network Scanner**
  Access Commander scannt das lokale Netzwerksegment regelmäßig mit dem integrierten 2N Network Scanner, um angeschlossene Geräte und deren aktuelle IP-Adressen zu identifizieren.
- **Device callback**
  Mit dieser Methode werden IP-Adressen von Geräten außerhalb des lokalen Netzwerksegments erkannt. Die Geräte werden beim Start, bei Änderung der IP-Adresse und in regelmäßigen Abständen (einmal pro Stunde) gemeldet. Damit diese Methode ordnungsgemäß funktioniert, müssen Sie das Ziel angeben, an das die Geräte gemeldet werden sollen (normalerweise die IP-Adresse des **Access Commander**).

Network Discovery

Netzwerkerkennung ermöglicht es anderen Diensten, wie **2N IP Utility** oder **2N Network Scanner**, die Installation von **Access Commander** im lokalen Netzwerk zu finden.

Sie können **Network Scanner** und **Axis Utility** gleichzeitig verwenden. Aus Sicherheitsgründen können jedoch beide Erkennungen **Access Commander** in den Systemeinstellungen vollständig deaktiviert werden.

TIPP
Access Commander kann in den Anwendungen **2N Network Scanner** und **2N Axis Utility** ein- oder ausgeblendet werden. Dasselbe gilt für den Zugriff auf die Weboberfläche über **accesscommander.local**. Wenn mehrere Access Commander-Instanzen im Netzwerk ausgeführt werden, vergibt das System automatisch eindeutige Namen: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local** und andere Instanzen auf der Grundlage der Anzahl der Server im Netzwerk.

Proxy Einstellung

Der Proxy wird unter anderem für folgende Dienste genutzt: HTTP-Anfragen, FTP-Synchronisierung, Upgrades usw.

ANMERKUNG
Proxy für FTP mit TLS-Authentifizierung wird nicht unterstützt.

1. Gehen Sie zu **Einstellungen > Konfiguration > Registerkarte Netzwerk**.
2. Wählen Sie Proxy bearbeiten.
3. Geben Sie in dem sich öffnenden Dialogfeld die Proxy-Server-Adressen für die gewünschten Protokolle ein.
4. Im letzten Feld können Sie Adressen eintragen, für die der Proxyserver nicht gelten soll.
   Verbindungen zu localhost und zu IP-Adressen im Bereich 127.0.0.1/8 werden niemals über einen Proxyserver geleitet.
5. Nachdem Sie die Einstellungen geändert haben, wird **2N Access Commander** automatisch neu gestartet.

Verwendung von NodeRED

Die NodeRED-Anwendung ignoriert die Proxy-Einstellungen des Systems. Damit der Proxyserver richtig funktioniert, muss er auf jedem NodeRED-Knoten, der seine Verwendung erfordert, explizit konfiguriert werden.

Weitere Informationen

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

HTTP API

Die URL für die Access Commander API lautet: **https://acom_ip_address/api/v3/**.

Die Liste der API-Endpunkte wird unter http(s)://acom_ip_address/support/api veröffentlicht. Außerhalb der **Access-Commander**-Benutzeroberfläche ist eine Liste der Endpunkte zur Ansicht verfügbar.

Sie können Antworten auf Anfragen mit Query filtern. Die Erstellung von **query** wird im Dokument Data Query Customization beschrieben (nur auf Englisch).

Authentifizierung

Die HTTP-API-Befehle werden unter den Benutzeranmeldedaten oder mithilfe einer Token-Authentifizierung gesendet. Das Authentifizierungstoken wird vom Administrator in**Einstellungen > Konfiguration > API-Zugriffsschlüssel**. Der API-Zugriffsschlüssel hat die Bearer-Token-Funktion. Beim Erstellen eines neuen API-Zugriffsschlüssels kann der Administrator die Gültigkeit des Schlüssels auf das Lesen beschränken, damit nur die GET-Befehle authentifiziert werden können. Der Schlüssel kann auf folgende Werte beschränkt werden: 1 Monat, 6 Monate, 1 Jahr.

ACHTUNG
Kopieren Sie nach der Erstellung des Zugangsschlüssels den Schlüssel in Ihre Zwischenablage und verwenden Sie ihn. Später lässt sich der Schlüssel nicht mehr anzeigen.

SignalR

SignalR ist ein Tool, das die Echtzeitkommunikation zwischen dem Server und dem Client ermöglicht. Dies bedeutet, dass der Server Inhalte an verbundene Clients senden kann, sobald diese verfügbar sind, und nicht auf eine Anfrage des Clients warten muss. Die Grundprinzipien von SignalR werden im Dokument beschrieben SignalR integration manual (nur auf Englisch). Liste der verfügbaren SignalR-Themen zur Verwendung mit **Access Commander** sind im Dokument beschrieben SignalR topics reference manual (nur auf Englisch).

Lizenzen Dritter

Eine vollständige Liste der verwendeten Bibliothekslizenzen von Drittanbietern finden Sie im Benutzermenü rechts in der oberen Leiste im Abschnitt „Info“.

2N Access Commander – Installationshandbuch

2N.com