2N Access Commander

Benutzerhandbuch

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

2N.com

Zusammenfassung

Firmware 3.1

Inhaltsverzeichnis

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 Zugriffe zu verwalten, ist es notwendig, hinzuzufügen **Access CommanderGerät**. Geräte sind physische Einheiten im Gebäude, die Eingänge steuern (2N-Sprechanlagen oder 2N-Zutrittseinheiten) oder die Kommunikation ermöglichen (2N-Antworteinheiten). Geräte werden gruppiert in **Zone**. Jedes Gerät kann sich nur in einer Zone befinden.

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.
- Zeitprofile erstellen und verwalten.
- Zeiterfassung festlegen.

Benutzer Manager

- Benutzer erstellen und verwalten.
- Besuche erstellen und verwalten.
- Verwalten Sie ihre Gruppenmitgliedschaften.
- Zugriffs- und Systemprotokoll einsehen.

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.

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. 42).

Gegensprechanlagen 2N

- 2N IP Style – unterstützt das Lesen von QR-Codes
- 2N IP Verso 2.0 – unterstützt das Lesen von QR-Codes
- 2N IP Verso
- 2N LTE Verso
- 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 IP Access Unit M

Reaktionseinheiten 2N

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

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

Tabelle 1. 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
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	✓	✓	✓	✓	✓
Importieren Sie Benutzer aus CSV oder von Geräten	✓	×	✓	✓	✓
Massen-Firmware-Verwaltung	✓	×	✓	✓	✓
Mehrfachauthentifizierung	✓	×	✓	✓	✓

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

[a.] Unbegrenzt im Rahmen der maximalen Möglichkeiten der Softwareplattform, nämlich Empfohlene Hardware (S. 15)

Installation

Access Commander kann auf zwei Arten verteilt werden:

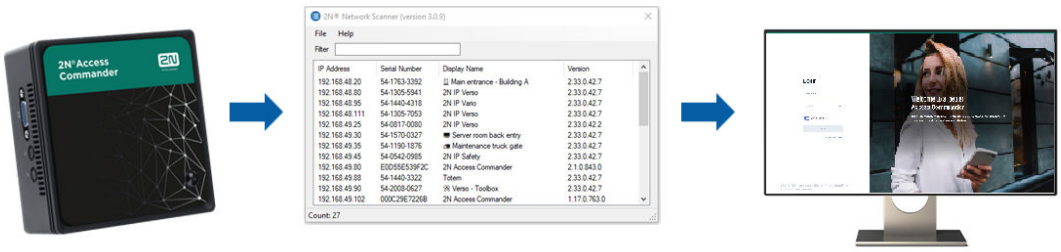
- Ein kleiner Desktop-Computer 2N Access Commander Box (Bestell-Nr. 91379030)
- Virtueller Computer

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 (Bestell-Nr. 91379030, Achsenteil. Also 01672-001) ist ein kompakter Desktop-Minicomputer mit vorinstallierter Software. Es handelt sich um eine „Plug-and-Play“-Lösung, bei der Sie lediglich eine Stromquelle und ein Ethernet-Kabel an diesen Minicomputer anschließen müssen. Für eine korrekte und vollständige Systemfunktionalität wird empfohlen, diesen Minicomputer an einem sicheren Ort aufzubewahren und ihn dauerhaft laufen zu lassen. Access Commander Box dient als Server zum Sammeln von Daten, Ereignissen und Protokollen aus dem gesamten Zugangssystem.

Einloggen in Access Commander mit einer dynamischen IP-Adresse



1. Verbinden Access Commander Box über ein Ethernet-Kabel mit dem Netzwerk verbinden.
2. Nutzung der App 2N IP-Network Scanner Lokalisieren Access Commander Box im Internet.
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.

Festlegen einer statischen Adresse Access Commander helfen 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 an als „root“ mit Passwort „2n“. Sobald der blaue Bildschirm erscheint, ändern Sie das Standardkennwort.

4. Wählen Sie im erweiterten Menü aus „Networking“ und folglich „Static 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.

Technische Parameter Access Commander Box

- 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

Verteilung über virtuelle Maschine

Access Commanderkann als virtuelle Maschine verteilt werden. Nachfolgend finden Sie die Installationsverfahren auf unterstützten Virtualisierungsplattformen.

Virtual Box

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

1. VON https://www.virtualbox.org/wiki/DownloadsLaden Sie die neueste Version von VirtualBox herunter. Es wird empfohlen, die Version inklusive VirtualBox Extension Pack herunterzuladen.
2. Laden Sie die entsprechende Software aus dem Abschnitt 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 Abschnitt 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 Abschnitt 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“).
   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 Abschnitt 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

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.

Tabelle 2. 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

Tabelle 3. Access Commander Box

Anzahl angeschlossener Geräte 2,0	Anzahl der Benutzer 2,0	Anzahl der Benutzer in der Gruppe
2000	100000	1500

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.

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 Händler die Seriennummer eines der angeschlossenen 2N-Geräte mitteilen **Access Commander**. Lizenzdatei wird basierend auf der Seriennummer generiert lizenziertes Gerät.

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.

Lizenzsperre

Die Lizenzsperre tritt ein, wenn die Verbindung zum lizenzierten Gerät getrennt wird**Access Commander**für einen längeren Zeitraum als die Schutzdauer der Lizenz. Die Dauer der Schutzdauer hängt davon ab, wie lange das lizenzierte Gerät angeschlossen war **Access Commander**. Die Dauer der Schutzfristen ist in aufgeführt Tabelle unten.

Wenn eine Lizenz ausgesetzt wird, werden alle angeschlossenen Geräte automatisch nicht verwaltet und als nicht verwaltet markiert. Um sie wieder zu aktivieren, müssen Sie das lizenzierte Gerät anschließen und aktivieren oder eine neue Lizenzdatei für ein anderes Gerät erstellen und hochladen lassen.

Beim Hochladen einer neuen Lizenz müssen Sie zunächst das Lizenzgerät aktivieren, für das die neue Lizenz generiert wird. Nach der Aktivierung des lizenzierten Geräts ist es möglich, auch alle anderen Geräte zu aktivieren.

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

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)**.*

Schnittstelle **Access Commander** ist über einen Webbrowser zugänglich. Mit dem Programm kann die IP-Adresse des Webinterfaces gesucht werden 2N Network Scanner.

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.

Armaturenbrett

Das Dashboard ist die Grundansicht der Weboberfläche **Access Commander**. Es handelt sich um ein konfigurierbares Schwarzes Brett, das Echtzeitdaten anzeigt. **Access Commander** bietet mehrere Widgets, die über eine Schaltfläche zum Dashboard hinzugefügt werden . Widgets im Dashboard können verschoben, umbenannt oder ihre Grundeinstellungen auf verschiedene Weise vorgenommen werden. Das Verwalten und Löschen von Widgets erfolgt im erweiterten 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

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 „Systemprotokolle“ wird eine Liste der Ereignisse und Benachrichtigungen angezeigt **Access Commander** generiert.

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

- Schweregrad (Info, Warnung, Fehler);
- der Zeitpunkt, zu dem das Ereignis eingetreten ist;
- die Kategorie, zu der die Aktion gehört (Gerätestatus, Import, Benutzersynchronisierung, System, Benutzeraktionen, Bereichseinschränkungen);
- Gegenstand der Aktion (Gerät, Benutzer, Zone, Besuch...);
- eine kurze Beschreibung der Veranstaltung;
- 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 Aufzeichnungen können in einer CSV-Datei heruntergeladen oder ausgedruckt werden, indem Sie auf die Taste Export oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 aufgeführt.

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.

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 Aufzeichnungen können in einer CSV-Datei heruntergeladen oder ausgedruckt werden, indem Sie auf die Taste Export oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 aufgeführt.

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.

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.

Eine Liste der Benachrichtigungen wird auch auf der Seite Systemprotokolle > Benachrichtigungen angezeigt.

Die Aufzeichnungen können in einer CSV-Datei heruntergeladen oder ausgedruckt werden, indem Sie auf die Taste Export oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 aufgeführt.

Einrichten eines neuen Benachrichtigungstyps

1. Gehen Sie zur Seite **Einstellungen** > **Notifikation**.
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

Benachrichtigungstypen werden im Detail des jeweiligen Benachrichtigungstyps festgelegt. Das Detail des Benachrichtigungstyps wird geöffnet, indem Sie auf der Seite Einstellungen > Notifikation auf die ausgewählte Benachrichtigung in der Liste klicken.

Art der Benachrichtigung

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

Die Benachrichtigung in **Access Commander** erscheinen unter dem Symbol in der oberen Leiste, neben dem Benutzermenü oder in Systemlog > Notifikation.

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. 61).

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.

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.

Mobile Key

Im Unternehmen besteht die Möglichkeit, die Pairing-Parameter mit der Anwendung festzulegen 2N Mobile Key, was die Bluetooth-Authentifizierung ermöglicht. Es werden sowohl die Geräte festgelegt, mit denen Benutzer eine Kopplung durchführen können, als auch die Gültigkeitsdauer des für die Kopplung erforderlichen Mobilfunkschlüssels. Der mobile Schlüssel 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. 52).

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
- Mobile Key zum Einrichten der Bluetooth-Authentifizierung für den Benutzer

In den Unternehmensdetails > Registerkarte „E-Mails“ > Registerkarte „E-Mail-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.

   Es öffnet sich das Detail der eingestellten LDAP-Verbindung. Verbindungseinstellungen können getestet werden. Mit der Taste Jetzt synchronisieren Sie starten eine einmalige Synchronisierung.
3. 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.
4. Auf Karte **Optionen** Sie können Benutzerdaten Attributen auf dem LDAP-Server zuweisen.

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

LDAP-Synchronisierungsoptionen

Importierte Attribute – Durch Bearbeiten des Schemas erfolgt die Zuordnung von Daten aus **Access Commander** zu den Attributen auf dem LDAP-Server.

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.

Benutzer in Active Directory deaktiviert – legt fest, was mit Benutzern geschieht, die in Active Directory gesperrt wurden. Das Deaktivieren im Active Directory kann **Access Commander** Sie können den Benutzer ignorieren oder löschen (verbieten). Nach der Reaktivierung im Active Directory werden gelöschte Benutzer erneut hochgeladen **Access Commander.**

Synchronisierung von Gruppen – ermöglicht das Hochladen von Gruppenmitgliedschaften von LDAP nach **Access Commander**. Mithilfe der Einstellungen des Synchronisierungsschemas ist es möglich, Ihren eigenen Basis-DN und den Filter zu definieren, nach dem die Gruppen synchronisiert werden. Schema ermöglicht die Synchronisierung verschachtelter Gruppen.

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 Suche im gesamten Baum, ansonsten wird nur die Wurzel durchsucht.

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

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

Alle angelegten Benutzer werden in der Benutzerliste angezeigt. Benutzer können oberhalb der Liste gefiltert werden oder Sie können direkt nach einem bestimmten Benutzer anhand seines Namens, seiner E-Mail-Adresse oder seiner Telefonnummer suchen.

Massenaktionen

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

- 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, denen noch kein Mobile Key zugewiesen wurde, einen Mobile Key zu

ANMERKUNG
Um einem Benutzer einen PIN/QR-Code oder einen mobilen Schlüssel zuweisen zu können, 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.

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. 34). 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. Die Kennung kann gelesen werden, indem man die Karte an das Lesegerät hält oder den Ausweis über die Tastatur eingibt. Der Bezeichner muss eine hexadezimale Zahl mit mindestens 6 Zeichen Länge sein. Einem Benutzer können bis zu 2 Zutrittskarten zugewiesen werden.

Mobile Key – Wird für die Verbindung mit der Anwendung verwendet 2N Mobile Key Aktivieren der Authentifizierung über Bluetooth, siehe Kapitel Bluetooth-Authentifizierung (S. 33).

PIN-Code – generiert automatisch eine 6-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. 32).

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. 67). 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. 25). 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** – spezifischer Identifikator, erforderlich für die Massensynchronisation mit einer CSV-Datei (siehe Synchronisierung von Benutzern mit FTP (S. 64));

- **Eine Notiz**.

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 .

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.

Über die virtuelle Telefonnummer kann der Benutzer über die Zifferntastatur des Geräts angerufen werden. Eine virtuelle Nummer kann zwei bis vier Ziffern haben. Virtuelle Nummern sind nicht mit den eigenen Telefonnummern des Benutzers verknüpft, sodass Benutzer ihre eigenen Telefonnummern auf dem Gerät verbergen können. In der Registerkarte besteht auch die Möglichkeit, einen Vertreter festzulegen, an den der Anruf weitergeleitet wird, falls dieser Benutzer nicht erreichbar ist. Der Vertreter kann aus anderen Benutzern im Unternehmen 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. Stellen Sie sicher, dass es drin ist **Einstellungen** > **Ansätze** aktivierter USB-Fingerabdruckleser.

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 Mobile Key app, die der Nutzer auf sein Mobiltelefon heruntergeladen haben muss.

GET IT ON Google Play Download on the App Store

Verbindung der Anwendung auf dem Telefon des Benutzers mit Geräten v **Access Commander** erfolgt durch Eingabe des Pairing-Codes in der Anwendung Mobile Key.

Der Pairing-Code kann auf zwei Arten erhalten werden:

- über ein USB-Bluetooth-Lesegerät, das an einen Computer angeschlossen ist
- Verbindung zum Gerät herstellen.

Erstellen eines Pairing-Codes per Computer

1. Auf Ihren Computer herunterladen 2N IP USB Driver und installieren Sie es.
2. Stellen Sie sicher, dass der USB-Bluetooth-Leser im aktiviert ist **Einstellungen** > **Authentifizierung** > **Klicken Sie auf die Registerkarte „Erlaubte USB-Lesegeräte“.**.
3. Verbinden Sie den USB-Bluetooth-Leser mit dem Computer.
4. In den Benutzereinstellungen v **Registerkarte „Authentifizierung“.** Wählen Sie Authentifizierung Mobile Key.
5. Wählen Sie im sich öffnenden Dialogfeld aus Koppeln Sie mit einem Lesegerät.
   Im Dialogfeld wird ein Kopplungscode angezeigt.
6. Befolgen Sie die nachstehenden Schritte zum Koppeln in der App unten (S. 34).

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. 46);
   - Eine angemessene Zeit für das Pairing eingestellt ist, siehe ???.
2. In den Benutzereinstellungen v **Registerkarte „Authentifizierung“.** Wählen Sie Authentifizierung Mobile Key.
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. Befolgen Sie die nachstehenden Schritte zum Koppeln in der App unten (S. 34).

Pairing in der mobilen App Mobile Key

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 Mobile Key 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 Mobile Key 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.

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. 49).

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. 50).

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. Mobile Key
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.

Unternehmen

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

Zugriffsregeln

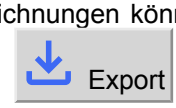
Es zeigt eine Übersicht aller bereits erstellten Zugriffsregeln und bietet die Möglichkeit, diese zu ändern oder zu erstellen. Durch das Erstellen einer Zugriffsregel wird einer bestimmten Gruppe Zugriff auf die Zone gewährt. Beim Erstellen einer Regel müssen Sie eine Gruppe und ein Zeitprofil angeben, 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 Aufzeichnungen können in einer CSV-Datei heruntergeladen oder ausgedruckt werden, indem Sie auf die Taste 

oberhalb der Liste klicken. In der exportierten CSV-Datei ist die Zeit in GMT+0 aufgeführt.

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
- Unvereinbar
- 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.

Ein neues Gerät hinzufügen

1. Gehen Sie zur Seite **Gerät**.
2. Klicken Sie oben rechts auf die Schaltfläche „Gerät hinzufügen“.
3. Suchen Sie im geöffneten Dialogfenster nach dem Gerät im lokalen Netzwerk oder geben Sie dessen IP-Adresse und den entsprechenden Port im Format ein:„IAdresse:Port“
   Nach Eingabe der IP-Adresse des Geräts ist es möglich, durch Drücken der EINGABETASTE auf der Tastatur ein anderes Gerät einzugeben.
4. 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.
5. Benennen Sie das Gerät, bevor Sie es erstellen.

Neu hinzugefügte Geräte erscheinen in der Liste. Weitere Geräteeinstellungen nehmen Sie in den Gerätedetails vor.

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 jeweiligen 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 des Verbindungsaufbaus mit Geräten angezeigt. Online-Geräte sind diejenigen, mit denen er hat **Access Commander** hergestellte Verbindung und auf die die akzeptierte Firmware hochgeladen wird. Dank der hergestellten Verbindung mit dem Gerät kann eine Datensynchronisierung erfolgen. Auf der Seite kann inkompatible Firmware aktiviert werden **Gerät** > **Firmware**.

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 auf dem Gerät 2 Access Points eingestellt sind und die Access Point-Erkennung aktiviert ist (siehe Einstellungen für den Gerätezugriffspunkt (S. 50)), wird die Option zur Zuweisung von 2 Zonen angezeigt. Ein Gerätezugriffspunkt kann sich nur in einer Zone befinden.

Aufbau

Die Karte zeigt die aktuelle Firmware-Version, MAC-Adresse und IP-Adresse an und ermöglicht die Änderung des Passworts für den Zugriff auf ihre Webkonfiguration.

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 .

Neben der Schaltfläche wird der aktuelle Status des Türschalters angezeigt Offen.

Es dient zum Verriegeln von Türen auch für Gruppen mit gültigem Zutritt Notabschaltung (S. 39).

Sicherung

Ermöglicht die Sicherung der Intercom-Konfiguration in einer XML-Datei. Die Sicherung wird mit gestartet Sicherung starten. Das letzte Backup wird auf der Registerkarte angezeigt, von der aus Sie die Back-up-Datei herunterladen können. Über das v-Menü kann das Gerät automatisch mit dem letzten Backup synchronisiert werden Wiederherstellen. In diesem Menü ist es möglich, das Gerät anhand eines auf einem anderen Gerät gespeicherten Backups zu synchronisieren.

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

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. Gehe 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

Verwendung der Relaismodulverbindung Axis A9188 Zu 2N IP-Gegensprechanlage (2N IP Verso, 2N IP Force, 2N IP-Sicherheit, 2N IP Vario) oder zu Zugriffseinheit Der Zugang zu den einzelnen Etagen des Gebäudes kann über einen Aufzug gesteuert werden. Zu einem 2N IP-Gegensprechanlage wessen Zugriffseinheit Es ist möglich, maximal diese 8 Relaismodule anzuschließen, wobei jedes der Module 8 Etagen, also insgesamt maximal 64 Etagen, steuern kann. Um diese Funktion nutzen zu können, müssen Sie über eine aktive Lizenz verfügen 2N IP-Gegensprechanlagen (Bestellnr. 9137916) und Lizenz Zugriffseinheit (Bestell-Nr. 9160401).

Einstellungen zur Aufzugssteuerung

1. 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**.
2. Gehen Sie in der Kopfzeile der Gerätedetails zu Hardwarekonfiguration Gerät. Aktivieren Sie im Abschnitt Hardware > Aufzugssteuerung die Module, die den Zugang vom Aufzug aus steuern sollen. Wenn Module eine Authentifizierung erfordern, geben Sie einen Benutzernamen und ein Passwort ein. Speichern Sie die Einstellungen. Verlassen Sie die Hardware-Konfiguration über das Kreuz in der oberen blauen Leiste.
3. Gehen Sie in den Gerätedetails zur Registerkarte Aufzug.
4. 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 .
5. 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 deren aktueller Status angezeigt.

Überwachung

Die Seite dient dazu, Informationen über angeschlossene Geräte herauszufinden. Jeder Administrator kann die Tabelle nach seinen eigenen Bedürfnissen anpassen . Die Einstellung ist für jedes Konto einzigartig. Einstellungen werden durch Auswahl der angezeigten 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.

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.

Die Massenverwaltungsversion zeigt eine Liste der angeschlossenen Typen von 2N IP-Gegensprechanlagen, 2N-Antwort- und 2N-Zugangseinheiten an.

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.

Geräteausschluss

Geräte können von der Massenverwaltung der Firmware ausgeschlossen werden, indem Sie sie zur Liste auf der Registerkarte Geräte > Firmware > 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 steuern, die eine nicht unterstützte Firmware-Version verwenden, sofern diese Version genehmigt ist. Die Genehmigung erfolgt auf der Registerkarte Gerät > Firmware > Inkompatible Firmware-Version über das 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

- 2.43
- 2.42
- 2.41
- 2.40
- 2.39
- 2.38

Sicherheit

Nach der Aktivierung der SSL-Zertifikatsüberprüfung erfolgt die Synchronisierung nur auf Geräten, die über ein von einer vertrauenswürdigen Stelle signiertes SSL-Zertifikat verfügen. Die Gerätesynchronisierung ohne solche SSL-Zertifikate wird deaktiviert.

Für eine erfolgreiche Authentifizierung müssen Gerätezertifikate von einer Zertifizierungsstelle signiert sein und die IP-Adresse oder den Domänennamen des Geräts enthalten. Der Server, auf dem es ausgeführt wird, muss dem Zertifikat der signierenden Stelle vertrauen**Access Commander**. Gerätezertifikate müssen über die Weboberfläche des Geräts hochgeladen werden (System > Zertifikate > Persönliche Zertifikate) und unter Dienste > Webserver > Erweiterte Einstellungen als HTTPS-Serverzertifikat festgelegt werden.

ACHTUNG
Auf dem Gerät 2N Indoor-TouchSie können keine eigenen SSL-Zertifikate hochladen. Nach der Aktivierung der Zertifikatsüberprüfung geht die Verbindung zu ihnen verloren.

Einstellungen für den Gerätezugriffspunkt

Gerät (2N-Gegensprechanlage oder 2N-Zugangseinheit) kann bis zu zwei Zugangspunkte haben. Jeder Zugangspunkt ermöglicht den Durchgang in eine Richtung. Access Points unterscheiden die Durchgangsrichtung durch das Gerät. Jedem Zugangspunkt können ein oder mehrere Leser zugeordnet werden, die an das Gerät angeschlossen werden und in Richtung des Zugangspunkts arbeiten. Zugangspunkte werden verwendet, um das Betreten oder Verlassen einer Zone aufzuzeichnen. Ihr Einsatz ist erforderlich, wenn sich das Gerät an der Schnittstelle zwischen zwei Zonen befindet.

Zugangspunkte werden auch verwendet, um Benutzer im Modul zu verfolgen Gegenwart (S. 55). Access Points werden auch zur Überwachung des Ein- und Ausgangs verwendet Gebietsbeschränkungen (S. 57).

ANMERKUNG
Einrichten einzelner Access Points **Access Commander** ist im Webinterface des Geräts im Bereich Dienste > Zugriffskontrolle vorgeschrieben:

- Zugangspunkt 1 = Ankunftsregeln
- Zugangspunkt 2 = Ausgangsregeln

Zugangspunkte einrichten

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 zum Abschnitt Hardware > Menü Erweiterungsmodule.
3. Suchen Sie das Zugangsmodul, das als Zugangspunkt 1 (Ankunft) oder Zugangspunkt 2 (Ausgehend) verwendet werden soll.
4. Stellen Sie im Parameter Tür die gewünschte Richtung ein und speichern Sie die Einstellungen.

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

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.

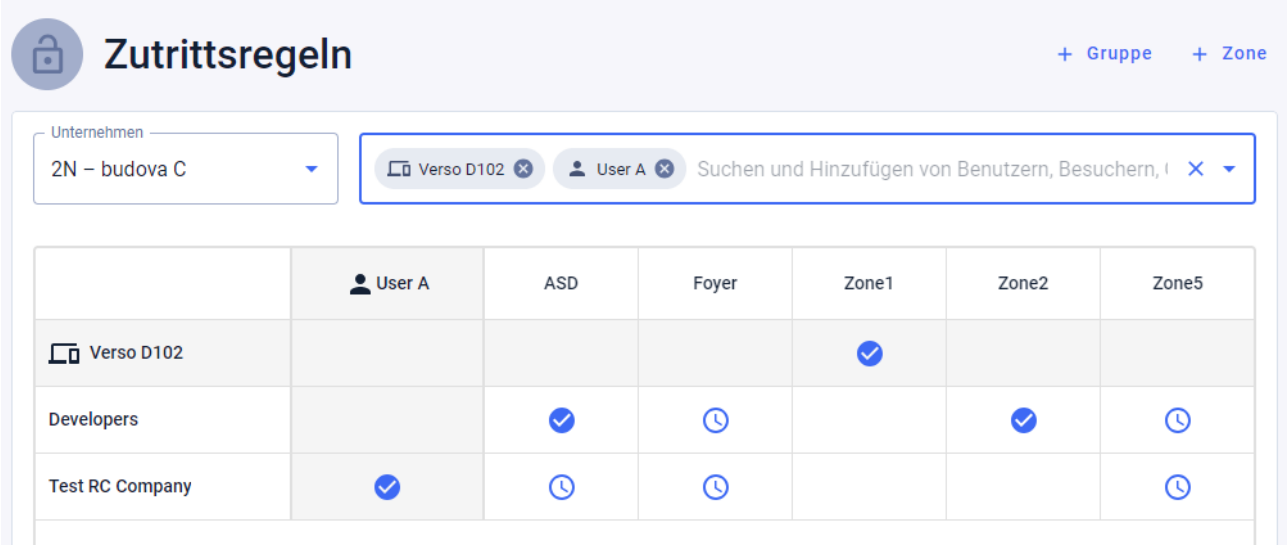
Matrixanzeige

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. 48). 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.

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 eine Option aus, um ein Zeitlimit festzulegen Zeitfenster hinzufügen. Grüne Tage kennzeichnen Tage, die in das Zeitprofil fallen. Durch Anklicken wird der Tag ausgewählt. Innerhalb von Tagen ist es möglich, ein Zeitintervall festzulegen, das die Gültigkeit des Zeitprofils bestimmt.
   Erst beim Erstellen des Zeitprofils können für jeden Tag unterschiedliche Zeiten eingestellt werden.

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.

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 ihres Modus erfolgt in **Einstellungen** > **Aufbau** > **die Registerkarte Anwesenheit**, sehen Anwesenheitseinstellungen (S. 50).

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. 29).

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

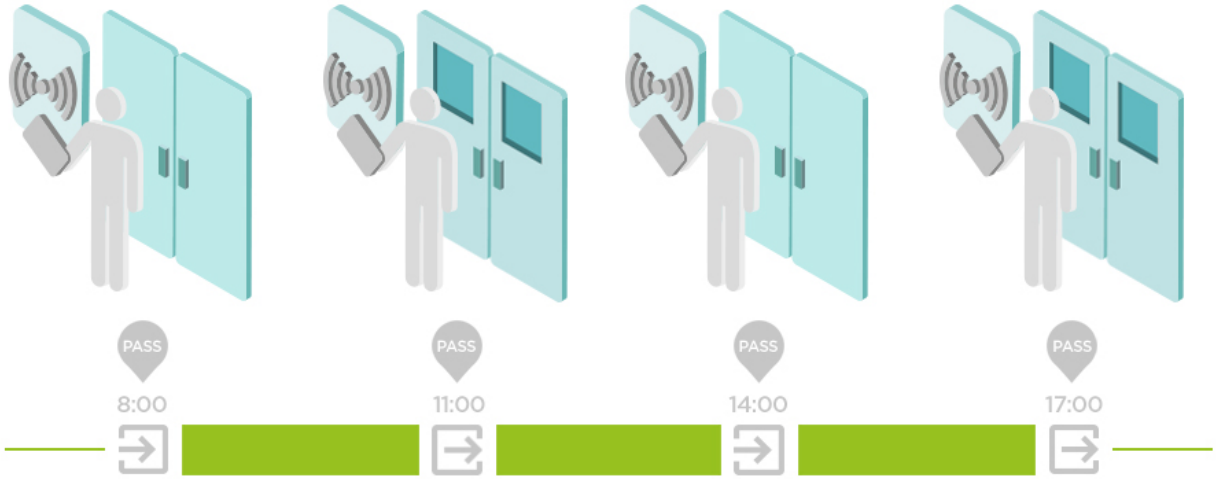
Der Anwesenheitsmanager kann die Anwesenheitsdaten der Benutzer bearbeiten. Die Bearbeitung erfolgt durch Anklicken des zu ändernden Zeitintervalls. Nach dem Öffnen können die Cut-off-Zeiten bearbeitet und dem Intervall eine Notiz hinzugefügt werden.

Anwesenheitseinstellungen

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

Anwesenheitsmodi

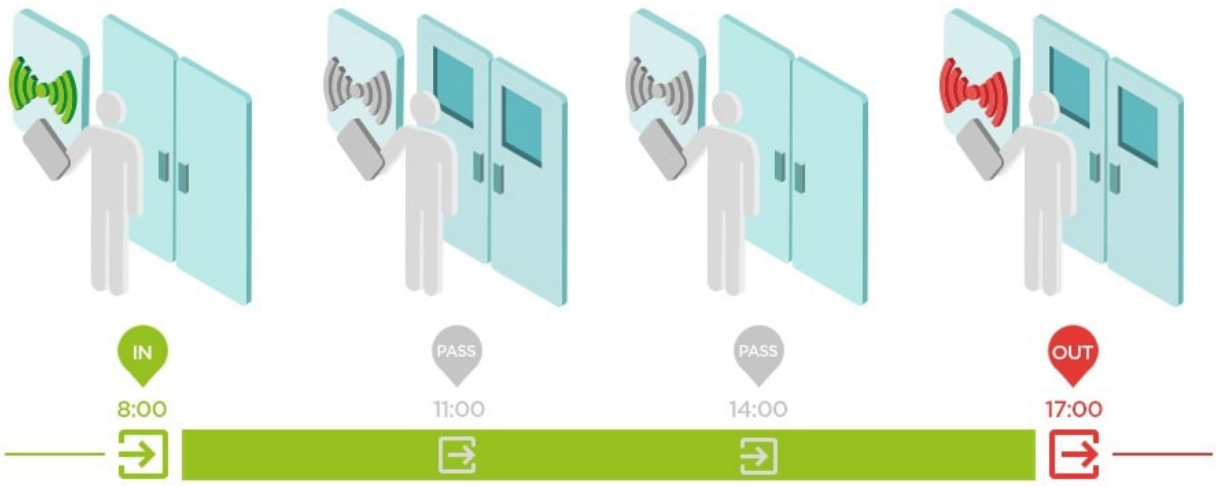
- **FREI**



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**

Eingehende und ausgehende Geräte müssen für den ordnungsgemäßen Betrieb eingestellt sein.



- **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

Gerät (2N-Gegensprechanlage oder 2N-Zugangseinheit) kann bis zu zwei Zugangspunkte haben. Jeder Zugangspunkt ermöglicht den Durchgang in eine Richtung. Access Points unterscheiden die Durchgangs-

richtung durch das Gerät. Jedem Zugangspunkt können ein oder mehrere Leser zugeordnet werden, die an das Gerät angeschlossen werden und in Richtung des Zugangspunkts arbeiten. Zugangspunkte werden verwendet, um das Betreten oder Verlassen einer Zone aufzuzeichnen. Ihr Einsatz ist erforderlich, wenn sich das Gerät an der Schnittstelle zwischen zwei Zonen befindet.

Zugangspunkte werden auch verwendet, um Benutzer im Modul zu verfolgen Gegenwart (S. 55). Access Points werden auch zur Überwachung des Ein- und Ausgangs verwendet Gebietsbeschränkungen (S. 57).

ANMERKUNG
Einrichten einzelner Access Points **Access Commander** ist im Webinterface des Geräts im Bereich Dienste > Zugriffskontrolle vorgeschrieben:

- Zugangspunkt 1 = Ankunftsregeln
- Zugangspunkt 2 = Ausgangsregeln

Zugangspunkte einrichten

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 zum Abschnitt Hardware > Menü Erweiterungsmodule.
3. Suchen Sie das Zugangsmodul, das als Zugangspunkt 1 (Ankunft) oder Zugangspunkt 2 (Ausgehend) verwendet werden soll.
4. Stellen Sie im Parameter Tür die gewünschte Richtung ein und speichern Sie die Einstellungen.
5. Gehen Sie zur Seite Zonen v **Access Commander**.
6. Drücken Sie in der oberen rechten Ecke und ermöglichen die Nutzung von Access Points.

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 einen Monat 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. 52).

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. 53).

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 Unterseite „Karten“ werden Besucherzugangskarten verwaltet, die einem Besuch hinzugefügt werden können. Über die Schaltfläche „Hinzufügen“ in der oberen rechten Ecke wird eine neue Karte 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.

Gegenwart

Das Anwesenheitsmodul ist eine Erweiterung des Anwesenheitsmoduls und dient der Anzeige einer Liste der Benutzer, die sich aktuell im Gebäude aufhalten. Für die Funktion des Moduls ist es notwendig, den Anwesenheitsmodus IN-OUT v einzustellen **Einstellungen** > **Aufbau** > **die Registerkarte Anwesenheit**, sehen Anwesenheitseinstellungen (S. 50).

- Wenn das letzte Ereignis des Benutzers an einem bestimmten Tag eine Ankunft ist (**IN** Ereignis) wird als vorhanden angesehen.
- Wenn der Benutzer ein Lesegerät passiert, dessen Richtung nicht festgelegt ist, ändert sich die Zone, in der sich der Benutzer befindet. Das Gleiche passiert, wenn es im Modus durch das Lesegerät geht**IN**.
- Wenn das letzte Ereignis am angegebenen Tag eine Abreise ist (**AUS** Ereignis) gilt als abwesend.

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.

- **Mobile Key** – Gekoppelte und nicht gekoppelte Benutzer mit verbleibender Kopplungszeit
  Der Bericht listet Daten zum Status der Benutzer-Kopplung über die Anwendung auf Mobile Key, 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. 64).

  ACHTUNG
  Die Datei enthält sensible Daten!

Gebietsbeschränkungen

Mit Bereichsbeschränkungen werden die Bereiche definiert, in denen die Anti-Passback- und Occupancy-Funktionen genutzt werden können.

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.

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 für das hinzugefügte Gerät zwei Zugangspunkte festgelegt sind, kann jeder Punkt für eine andere Richtung (Eingabe/Ausgabe) verwendet werden. Die Einstellungen des Zugangspunkts werden im Kapitel beschrieben Einstellungen für den Gerätezugriffspunkt (S. 50). Die Eigenschaften des Zugangspunkts werden durch Klicken auf den Pfeil erweitert.

Belegung

Eingehende und ausgehende Geräte müssen für den ordnungsgemäßen Betrieb eingestellt sein.

Auf der Registerkarte „Belegung“ können Sie die Anzahl der Personen in einem Bereich überwachen und steuern. Belegungsbeschränkungen helfen dabei, die Anzahl der Personen in einem Bereich zu verwalten. Bei Erreichen der Belegungsgrenze besteht die Möglichkeit, weitere Zutritte zu verweigern oder nur die Überschreitung der Grenze zu erfassen. Für diese Funktion ist ein Ein- und Ausgabegerät erforderlich.

Anti-Passback

Es besteht die Möglichkeit, die Anti-Passback-Funktion im Bereich zu aktivieren, die eine Erweiterung der Zugangskontrolle durch Überwachung und Missbrauch von Rechten beim Wiedereintritt in reservierte Berei-

che gewährleistet. Überwachte Bereiche werden durch Grenzvorrichtungen definiert, die in das Gelände führen oder es verlassen. Bei diesen Geräten wird beim Durchgang von Personen die Berechtigung nach den für den jeweiligen Bereich definierten Regeln überprüft. Nach Verlassen des Bereichs durch das Grenzgerät kann der Benutzer erst nach Ablauf des Timeouts in den Bereich zurückkehren, wenn der Timeout gesetzt ist. Sollte der Benutzer früher versuchen, in den Bereich zurückzukehren, verweigert ihm das System den Zutritt oder zeichnet dieses Ereignis nur im Protokoll auf.

WARNUNG
Ein Anti-Passback-Bereich verliert seine Bedeutung und kann potenziell gefährlich sein, wenn sich in dem Bereich ein Gerät mit angeschlossener aktiver REX-Taste befindet, das unbefugten Zutritt ermöglicht.

Eine Ausnahme festlegen

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

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

Liste der blockierten Benutzer

Blockierte Benutzer sind Benutzer, die vor Ablauf der Zeitüberschreitung versucht haben, auf den Anti-Passback-Bereich zuzugreifen. Helfen  Benutzer können aus der Liste ausgeschlossen werden, sodass sie wieder Zugriff auf den Bereich haben.

TIPP
Wenn einem Benutzer der Zutritt aufgrund einer aktiven Anti-Passback-Funktion verweigert wird, kann eine automatische Informations-E-Mail an den Benutzer gesendet werden. Sie können den E-Mail-Versand auf der Registerkarte „Einstellungen“ > „Anti-Passback“ > „Gesperrten Benutzer per E-Mail benachrichtigen“ aktivieren.

Beschränkungen zurücksetzen

Auf der Registerkarte Einstellungen > Anti-Passback > Bereichsbeschränkungen zurücksetzen werden die Tage und Zeiten festgelegt, an denen der Bereichsdatensatz gelöscht wird, d. h. Alle Benutzer können unabhängig von früheren Verstößen erneut passieren.

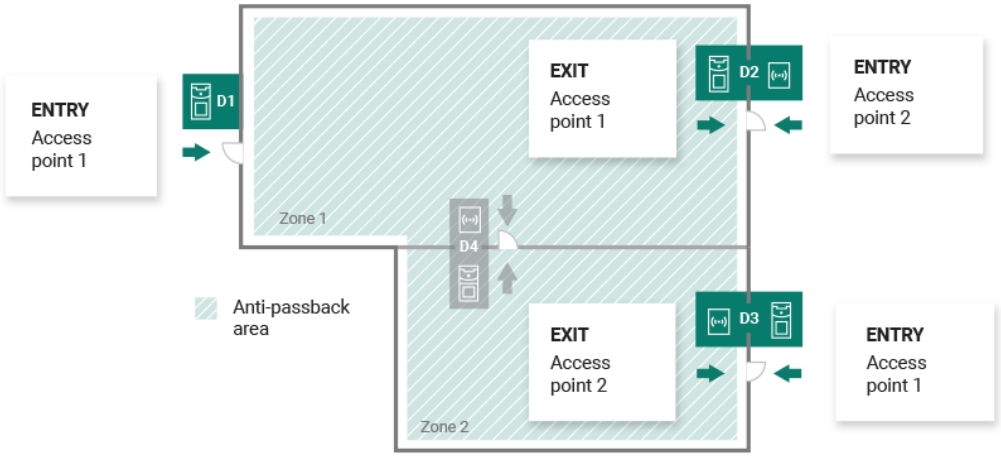
Die häufigsten Einrichtungsfehler

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 Eingang für einen anderen Bereich verwendet. Für eine korrekte Funktion muss die Zuordnung 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

Datum und Uhrzeit in **Access Commander** kann mit dem Internet synchronisiert oder manuell eingestellt werden. Das Ändern der Zeiterfassungsmethode erfolgt auf der Registerkarte „Einstellungen“ > „Konfiguration“ > „Datum und Uhrzeit“. Falls das nicht der Fall ist **Access Commander** Wenn Sie mit dem Internet verbunden sind, müssen Sie Datum, Uhrzeit und Zeitzone manuell einstellen. Andernfalls ist es möglich, auf NTP umzusteigen und die Zeit von einem NTP-Server zu beziehen. In diesem Fall müssen Sie nur die Zeitzone einstellen. Der NTP-Server aktualisiert Datum und Uhrzeit automatisch.

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

Zeitsynchronisierung mit Geräten

Die Uhrzeit der angeschlossenen Geräte kann mit der Uhrzeit vereinheitlicht werden **Access Commander**. Die Zeitfreigabe mit Geräten wird durch Umschalten des Parameters „Mit Gerät synchronisieren“ auf der Registerkarte „Einstellungen“ > „Konfiguration“ > „Datum und Uhrzeit“ aktiviert.

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

Netzwerkeinstellungen

Einstellungen für die Netzwerkverbindung werden auf der Registerkarte „Einstellungen“ > „Konfiguration“ > „Netzwerk“ vorgenommen. Auf der Registerkarte werden die aktuellen Netzwerkparameter angezeigt **Access Commander** und ermöglicht deren Einstellung. Nach Aktivierung der manuellen Konfigurationsmethode ist es möglich, einzelne Parameter einzustellen.

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.

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.

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

1. 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.
2. 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).
3. 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**.
4. Sie können die vorgenommenen Einstellungen überprüfen, indem Sie eine Test-E-Mail senden.

Systemupdate

System **Access Commander** prüft regelmäßig den Update-Server und informiert über verfügbare Updates und verfügbare neue Firmware-Versionen angeschlossener Geräte. Die automatische Update-Prüfung kann auf der Registerkarte „Einstellungen“ > „Systemupdates“ deaktiviert werden.

Installieren Sie das Update Access Commander

WARNUNG
Es wird empfohlen, dies vor der Installation des Updates zu tun Systemsicherung (S. 62). 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.

Beta-test

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

WARNUNG
Für die Testversion besteht keine Garantie und das Unternehmen stellt sie nicht zur Verfügung 2N TELEKOMUNIKACE as 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 Seite „Einstellungen“ > Registerkarte „Systemsicherung“ ist es möglich, Datensicherung und -wiederherstellung durchzuführen, zu konfigurieren und zu steuern**Access Commander**. Daten können im lokalen Speicher oder im Server Message Block (SMB) gespeichert werden. 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.

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.

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 in **Einstellungen** > **Registerkarte „Benutzersynchronisierung“.**. Sie können eine Beispiel-CSV-Datei von der Karte herunterladen.

TIPP
Die Liste der aktuellen Benutzer, die der Struktur der Beispiel-CSV-Datei entspricht, kann von der Seite heruntergeladen werden Berichte (S. 56).

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. Klicke auf im Speicherparameter.
2. Legen Sie im geöffneten Dialogfeld die Adresse des FTP-Servers fest, auf dem die CSV-Datei gespeichert ist.
3. Geben Sie die Anmeldeinformationen ein, um auf den FTP-Server zuzugreifen.

CSV-Datei

ZUM DOWNLOADEN
Über diesen Link können Sie eine Muster-CSV-Datei für die Benutzersynchronisierung herunterladen.

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.

Aktivierte USB-Lesegeräte

Um die Aufzeichnung einiger Benutzerauthentifizierungsmethoden zu erleichtern, ist es möglich, USB-Lesegeräte zu verwenden, die an den Computer angeschlossen sind, auf dem die **Access Commander**. Leser sind erforderlich in **Access Commander** Aktivieren Sie die Option unter Einstellungen > Zugriff > Registerkarte Zulässige USB-Lesegeräte.

Das Aktivieren/Deaktivieren der Verwendung eines externen USB-Geräts erfolgt in einem Dialogfeld, das sich durch Klicken auf öffnet Leser aktivieren. Anschließend wird ihre Berechtigung durch Klicken auf geändert Ändern.

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
- Externer USB-Bluetooth-Leser (Dongle) – Bestell-Nr. 9137422E

PICard-Schlüssel

Anwendungsverschlüsselungsschlüssel werden auf der Registerkarte Einstellungen > Zugriff > PICard-Schlüssel gespeichert 2N PICard Commander. Wenn die Verschlüsselungsschlüssel vorhanden sind **Access Commander** Wenn das Projekt hochgeladen wurde, wird der Projektname auf der Registerkarte angezeigt PICard Commander und eine numerische Schlüssel-Exportkennung. Die Karte ermöglicht das Hochladen von Schlüsseln **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. Nach dem Klicken auf Importieren Laden Sie die Verschlüsselungsschlüsseldatei aus Ihrem Repository hoch.
2. 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.

Verschlüsselungsschlüssel für den mobilen Schlüssel

Benutzer können die App verwenden, um eine Verbindung mit 2N-Geräten herzustellen Mobile Key. Kommunikation zwischen Anwendungen Mobile Keyund wird immer vom Gerät verschlüsselt. Ohne Kenntnis des Verschlüsselungsschlüssels kann die Anwendung nicht ausgeführt werdenMobile Keyauthentifizieren Sie den Benutzer. Der primäre Verschlüsselungsschlüssel wird beim ersten Start der Gegensprechanlage automatisch generiert und kann später jederzeit manuell neu generiert werden. Der primäre Verschlüsselungsschlüssel wird beim Pairing zusammen mit der Auth-ID an das Mobilgerät übertragen.

Kommunikation zwischen Anwendungen Mobile Keyund wird immer vom Gerät verschlüsselt. Ohne Kenntnis des Verschlüsselungsschlüssels kann die Anwendung nicht ausgeführt werdenMobile Keyauthentifizieren Sie den Benutzer. Der primäre Verschlüsselungsschlüssel wird beim ersten Start der Gegensprechanlage automatisch generiert und kann später jederzeit manuell neu generiert werden. Der primäre Verschlüsselungsschlüssel wird beim Pairing zusammen mit der Auth-ID an das Mobilgerät übertragen.

IN **Einstellungen > Zugriff > Registerkarte Verschlüsselungsschlüssel für Mobile Key** Es ist möglich, bis zu 4 Verschlüsselungsschlüssel zu generieren. Der neu generierte Schlüssel wird automatisch in die Anwendung hochgeladen Mobile Key wenn Sie zum ersten Mal ein Mobiltelefon mit einem zuvor gekoppelten Gerät verwenden. Beim Versuch, den fünften Schlüssel zu generieren **Access Commander** warnt, dass beim Generieren der älteste Schlüssel gelöscht wird. Die Karte zeigt die Zeitpunkte der Generierung einzelner Schlüssel.

Wenn es keine Anwendung gibt Mobile Key Wenn Sie keinen Zugriff auf einen der gültigen Verschlüsselungsschlüssel haben, ist es nicht möglich, ihn zur Authentifizierung des Benutzers zu verwenden. Um die Funktionalität der Anwendung wiederherzustellen, ist es notwendig, die Anwendung erneut mit dem verbundenen Gerät zu koppeln **Access Commander**, wodurch gültige Verschlüsselungsschlüssel in die Anwendung hochgeladen werden Mobile Key.

ANMERKUNG
Die Gewährung des Zugriffs auf das Gerät hängt von den eingestellten Zugriffsrechten des Benutzers ab.

CAM-Protokolle

CAM-Protokolle werden verwendet, um automatisch mehrere Bilder vor und nach dem ausgewählten Ereignis aufzuzeichnen. Unter Einstellungen > CAM-Protokolle können Sie verschiedene Arten von Ereignissen verwalten, für die CAM-Protokolle generiert 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

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.

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 Notwen-

digkeit der Zwei-Faktoren-Authentifizierung aktiviert hat, wird der Benutzer bei der nächsten Anmeldung aufgefordert, sein Konto mit seiner eigenen Authentifizierungsanwendung zu verknüpfen.

Die Zwei-Faktoren-Authentifizierung wird vom Administrator auf der Seite Einstellungen > Konfiguration > Registerkarte der Zwei-Faktoren-Authentifizierung eingestellt. 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, siehe Einschalten der Zwei-Phasen-Authentifizierung (S. 68).
- **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. Wählen Sie Profil anzeigen.
3. Verwenden Sie die Registerkarte Zwei-Faktoren-Authentifizierung, um das Konto mit der Authentifizierungsanwendung zu verknüpfen. Folgen Sie den Anweisungen.

Erlauben Sie den SSH-Zugriff

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

Unter Einstellungen > Konfiguration > wird die Registerkarte SSH verwendet, um Secure Shell zu aktivieren, das eine sichere Remote-Kommunikation mit der Systemkonsole ermöglicht. Wenn der SSH-Dienst aktiviert ist, können Sie Ihr System sichern und wiederherstellen oder einen vollständigen Neustart durchführen**Access Commander**.

Verbinden Access Commander Box oder einer virtuellen Maschine muss der SSH-Client die IP-Adresse kennen **Access Commander** und das System-Root-Passwort. 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.

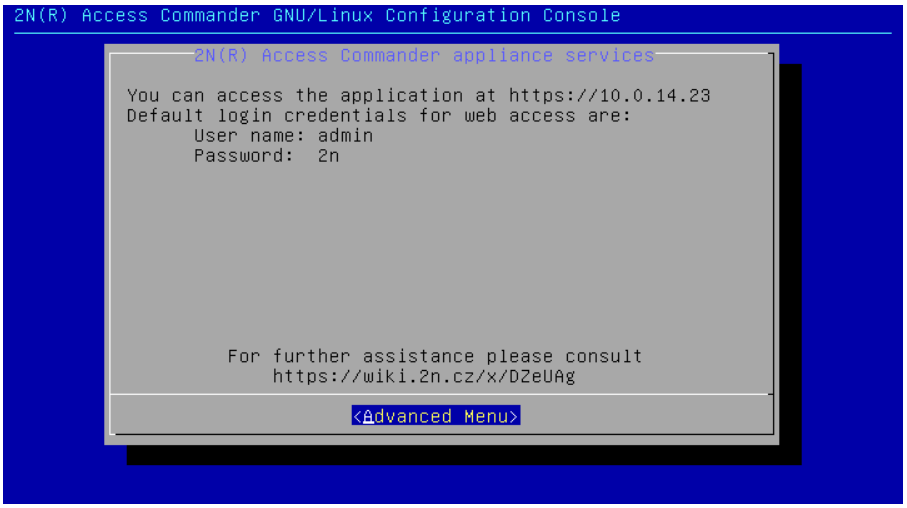
Der SSH-Zugriff kann auch direkt in der Linux-Konfigurationskonsole aktiviert und verwaltet werden, siehe Linux-Einstellungen (S. 69).

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.

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.

Weitere Informationen

HTTP API

Die URL-Adresse für den API **Access Commander** ist: 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**-Schnittstelle können Sie die Liste der mit Firmware-Version 2.7 freigegebenen Endpunkte sehen.

Authentifizierung

HTTP-API-Befehle werden mit den Anmeldedaten des Benutzers oder mit Token-Authentifizierung gesendet. Das Authentifizierungstoken wird vom Administrator unter Einstellungen > Konfiguration > Registerkarte API-Zugangsschlüssel erstellt. Der API-Zugangsschlüssel hat die Funktion eines Bearer Token. Bei der Erstellung eines neuen API-Zugangsschlüssels kann der Administrator den Schlüssel auf schreibgeschützt beschränken, so dass der Schlüssel nur GET-Befehle authentifiziert. Die Gültigkeit des Schlüssels kann begrenzt werden auf: 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.

Lizenzen Dritter

Eine vollständige Liste der verwendeten Bibliothekslizenzen von Drittanbietern finden Sie im Benutzermenü rechts in der oberen Leiste im Abschnitt „Info“.

wiki.2n.com

2N Access Commander – Benutzerhandbuch

2N.com