2N Access Commander

Manuale d'uso

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

2N.com

Sommario

Firmware 3.1

Indice

Simboli e termini utilizzati

Nel manuale vengono utilizzati i seguenti simboli e pittogrammi:

PERICOLO
Rispetta sempre queste istruzioni per evitare il rischio di lesioni.

AVVERTIMENTO
Rispetta sempre queste istruzioni per evitare danni al dispositivo.

ATTENZIONE
Avvertimento importante. La mancata osservanza delle istruzioni potrebbe causare il malfunzionamento del dispositivo.

SUGGERIMENTO
Informazioni utili per un utilizzo o una configurazione più semplice e veloce.

NOTA
Procedure e consigli per un utilizzo efficace delle funzionalità del dispositivo.

informazioni generali

2N Access Commander è uno strumento software per la gestione del sistema di accesso collettivo. Interfaccia Access Commander è accessibile tramite un browser web.

Le impostazioni possono essere effettuate all'interno di un'unica installazione **Access Commander** dividi in **Società**, che sono gestiti separatamente. Questo metodo consente di suddividere l'amministrazione tra gli amministratori delle singole aziende. Un amministratore di un'azienda non ha accesso alle informazioni su un'altra azienda. Gli amministratori di un'azienda non vedranno gli utenti di un'altra azienda.

Per gestire gli accessi è necessario aggiungere a **Access Commander Dispositivo**. I dispositivi sono unità fisiche nell'edificio che controllano gli ingressi (citofoni 2N o unità di accesso 2N) o consentono la comunicazione (unità di risposta 2N). I dispositivi sono raggruppati in **Zona**. Ogni dispositivo può trovarsi solo in una zona.

È possibile condividere zone o strutture tra aziende, consentendo la gestione degli accessi aziendali alle aree comuni (ingressi, ristoranti, sale conferenze...).

Utenti sono singole persone di cui è necessario gestire i movimenti all'interno dell'edificio o che possono essere chiamate da dispositivi connessi. Gli utenti sono raggruppati in **Gruppi**, in cui viene effettuata la gestione di massa del loro accesso alle zone. L'utente esegue l'autenticazione sul dispositivo e il dispositivo valuta quindi se l'utente ha un accesso valido al dispositivo. La validità dell'accesso è regolata dall'art **Diritti di accesso**. Gli utenti selezionati possono anche avere autorizzazioni amministrative **Access Commander** o parti di esso.

Profili temporali impostano gli orari in cui il dispositivo consente l'accesso o in cui è possibile chiamare gli utenti.

Modulo presenze consente il monitoraggio delle presenze degli utenti.

Modulo presenza ti consente di tenere traccia delle zone in cui si trovano attualmente gli utenti.

Visite sono persone i cui diritti di accesso sono validi solo per un periodo limitato.

Autorizzazioni utente

Fai rapporto **Access Commander** può essere eseguito da più utenti a seconda delle autorizzazioni loro assegnate.

Gli account elevati vengono configurati tramite un ruolo nelle impostazioni utente. È possibile assegnare più ruoli a un utente.

NOTA
Le autorizzazioni utente si applicano alla gestione all'interno dell'azienda dell'utente. L'amministratore ha accesso alla gestione completa di tutte le aziende.

Amministratore

- Impostazione del sistema e dei singoli moduli in base alla licenza valida.
- Cambio licenza

- Tutte le autorizzazioni di altri ruoli applicabili a tutte le società.

Gestore degli accessi

- Creare e gestire gruppi.
- Aggiunta di utenti ai gruppi.
- Creazione e gestione di profili temporali.
- Impostazione delle regole di accesso.

Gestore utenti

- Creare e gestire gli utenti.
- Creare e gestire le visite.
- Gestire le appartenenze ai gruppi.
- Visualizzazione del registro di accesso e di sistema.

Responsabile visite

- Creare e gestire le visite.
- Gestire le appartenenze ai gruppi.
- Visualizzazione del registro accessi delle visite.

Responsabile della porta

- Monitoraggio della trasmissione della telecamera dai dispositivi assegnati.
- Apertura remota dei dispositivi assegnati.
- Blocco di emergenza dei dispositivi assegnati.
- Visualizzazione del registro degli accessi dei dispositivi assegnati.
- Monitoraggio degli stati e degli eventi di sicurezza nel registro di sistema.

Responsabile delle presenze

- Monitoraggio e gestione delle presenze dei gruppi assegnati.
- Visualizzazione del registro degli accessi degli utenti dei gruppi assegnati.

Dispositivi e applicazioni supportati

Questo capitolo elenca i dispositivi supportati, i browser Web supportati e le piattaforme di virtualizzazione compatibili tramite le quali è possibile installare Access Commander.

Dispositivi supportati

Di seguito è riportata una panoramica dei dispositivi supportati dal sistema di accesso Access Commander. Questi dispositivi possono essere gestiti nel sistema.

NOTA
Le versioni firmware supportate di questi dispositivi sono elencate nel capitolo Firmware (p. 41).

Citofoni 2N

- 2N IP Style: supporta la lettura del codice QR
- 2N IP Verso 2.0 – supporta la lettura del codice QR
- 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

Unità di accesso 2N

- Access Unit QR: supporta la lettura dei codici QR
- 2N Access Unit 2.0
- 2N Access Unit
- 2N IP Access Unit M

Unità di risposta 2N

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

Browser Web

Configurazione **Access Commander** avviene tramite l'interfaccia web. Il sistema è stato ottimizzato per il browser Google Chrome (versione 90 e successive).

Altri browser supportati:

- Mozilla Firefox (versione 78 e successive)
- Microsoft Edge (versione 91 e successive)
- Safari (versione 14 e successive)

Altri browser non sono stati testati, pertanto non è possibile garantirne la piena funzionalità.

Piattaforme di virtualizzazione

- Virtual Box
- VMware Player (versione 6.5 e successive)
- VMware vSphere (versione 6.5 e successive)
- Hyper-V

Porti utilizzati

Tabella 1. Elenco dei servizi e delle porte richieste

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

[a.] Viene utilizzato sia per la comunicazione con il cliente che per la comunicazione con i gatekeeper.

[b.] L'utente può nelle impostazioni **Access Commander** scegli una porta diversa per il servizio LDAP.

Panoramica delle licenze

Dopo l'installazione iniziale **Access Commander** è disponibile una licenza di prova. La licenza di prova permette di testare tutte le funzionalità sulla gestione di 1 dispositivo e 5 utenti. Per l'amministrazione completa è necessario attivare una delle quattro licenze: *Di base* (gratuito), *Avanzate*, *Per* O *Per illimitato*.

Licenza:	Trial	Basic	Advanced	Pro	Unlimited
Componente n.	n/a	n/a	91379031	91379032	91379033
Numero massimo di utenti	5	50	300	1000	Illimitato[a.]
Numero massimo di dispositivi (sia attivati che disattivati)	1	5	30	100	Illimitato
Numero massimo di amministratori/manager	5	1	5	1000	Illimitato
Registri di accesso e di sistema	✓	✓	✓	✓	✓
Regole di accesso	✓	✓	✓	✓	✓
Gestione dell'API	✓	✓	✓	✓	✓
Attivazione/disattivazione dell'account	✓	✓	✓	✓	✓
Limitazione del numero di accessi non riusciti	✓	✓	✓	✓	✓
Allarme silenzioso	✓	✓	✓	✓	✓
Codice della zona	✓	✓	✓	✓	✓
Monitoraggio del dispositivo	✓	✓	✓	✓	✓
Gestione del registro	✓	✓	✓	✓	✓
Importa utenti da CSV o da dispositivi	✓	×	✓	✓	✓
Gestione firmware in blocco	✓	×	✓	✓	✓
Autenticazione multipla	✓	×	✓	✓	✓
Autorizzazione dell'utente	✓	×	✓	✓	✓

Licenza:	Trial	Basic	Advanced	Pro	Unlimited
Componente n.	n/a	n/a	91379031	91379032	91379033
Notifica	✓	×	✓	✓	✓
Presenza	✓	×	✓	✓	✓
Chiavi di accesso API	✓	×	✓	✓	✓
Registri CAM	✓	×	✓	✓	✓
Controllo dell'ascensore	✓	×	✓	✓	✓
Pannello di controllo	✓	×	✓	✓	✓
Blocco di emergenza	✓	×	✓	✓	✓
Supporto credenziali mobili	✓	×	✓	✓	✓
Gestione delle visite	✓	×	✓	✓	✓
Gestione dell'occupazione	✓	×	×	✓	✓
Sincronizzazione (LDAP e CSV)	✓	×	×	✓	✓
Anti-passback	✓	×	×	✓	✓
Partecipazione	✓	Opzio-nale	Opzionale	Opzionale	Opzionale

[a.] Illimitato entro le massime capacità della piattaforma software, vale a dire Hardware consigliato (p. 15)

Installazione

Access Commander può essere distribuito in due modi:

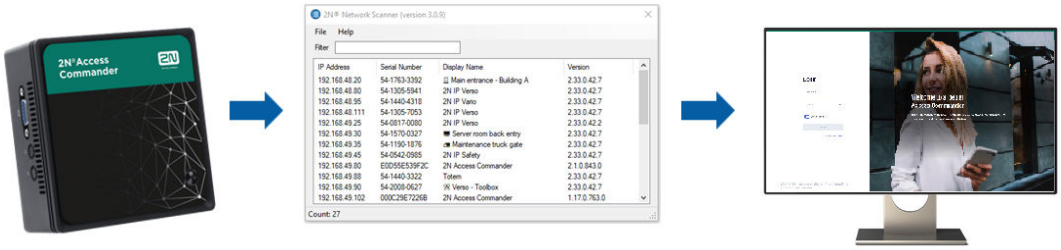
- Un piccolo computer desktop 2N Access Commander Box(ordine n. 91379030)
- Computer virtuale

Soluzione Access Commander Boxè limitato a 2000 dispositivi collegati. Altre funzionalità del software sono identiche per entrambe le soluzioni.

Distribuzione tramite Access Commander Box

Access Commander Box(ordine n. 91379030, AXIS ordine n. 01672-001) è un minicomputer desktop compatto con software preinstallato. Si tratta di una soluzione "plug and play", in cui è sufficiente collegare una fonte di alimentazione e un cavo Ethernet a questo minicomputer. Per una corretta e completa funzionalità del sistema, si consiglia di riporre questo minicomputer in un luogo sicuro e lasciarlo acceso permanentemente. Access Commander Box funge da server per la raccolta di dati, eventi e log dall'intero sistema di accesso.

Accedere Access Commander **con un indirizzo IP dinamico**



1. Collegare Access Commander Box alla rete utilizzando un cavo Ethernet.
2. Utilizzando l'app 2N IP Network Scanner individuare Access Commander Box nella rete.
3. Nel tuo browser web, vai all'indirizzo IP Access Commander Box e accedi a Access Commander.
   La password predefinita dell'utente Admin è 2n e deve essere modificata dopo l'accesso.

> **NOTA**
> In caso di distribuzione tramite Access Commander Box connettersi all'interfaccia web da un altro computer sulla rete. Sistema operativo Access Commander Box garantisce il funzionamento Access Commander e la sua configurazione Linux di base non consente l'esecuzione del browser web.

Impostazione di un indirizzo statico Access Commander **aiuto** Access Commander Box

1. Collegare Access Commander Box alla rete utilizzando un cavo Ethernet.
2. Connettiti a Access Commander Box tastiera e monitor. Viene visualizzata una schermata nera.
3. Accedi al sistema come «root» con password «2n». Una volta visualizzata la schermata blu, modificare la password predefinita.
4. Nel menu avanzato, seleziona «Networking» e successivamente «Static IP».
5. Imposta indirizzo IP statico, gateway e DNS.

6. Salva questa impostazione e utilizza il logout per uscire dal menu della console.
7. Connettersi all'indirizzo IP impostato tramite un browser web.

Parametri tecnici Access Commander Box

- Design ultra compatto: 0,69 L (56,1 x 107,6 x 114,4 mm)
- Processore Intel®Celeron®J3160 (cache da 2 MB; massimo 2,24 GHz)
- Disco rigido SSD SATA III da 2,5" (120 GB)
- Memoria DDR3 SODIMM (4 GB) – 1,35 V, 1600 MHz
- Supporto per doppio display tramite porta VGA e HDMI
- Porta LAN Gigabit per connessione Ethernet
- Telaio di montaggio VESA (75 x 75 mm + 100 x 100 mm)
- Temperatura di stoccaggio: da -20 °C a +60 °C
- Temperatura ambiente di funzionamento: da 0 °C a +35 °C

Distribuzione tramite macchina virtuale

Access Commanderpuò essere distribuito come macchina virtuale. Di seguito sono riportate le procedure di installazione sulle piattaforme di virtualizzazione supportate.

Virtual Box

SUGGERIMENTO
Si consiglia di abilitare la tecnologia di virtualizzazione VT-X nel BIOS.

1. DI https://www.virtualbox.org/wiki/Downloadsscarica l'ultima versione di VirtualBox.
   Si consiglia di scaricare la versione che include il pacchetto di estensione VirtualBox.
2. Scaricare il software appropriato dalla sezione Software e firmware su 2N.com. Dopo il download, decomprimere il file.
3. Apri VirtualBox e seleziona "File - Importa app...".
4. Modifica il titolo.
5. Controlla le impostazioni della CPU (minimo 2), le impostazioni della RAM (minimo 2048 MB) e la selezione della scheda di rete.
6. Conferma i termini della licenza.

Dopo l'installazione, si aprirà la console di configurazione Linux, dove è possibile eseguire le impostazioni di base del sistema. La configurazione completa viene eseguita nell'interfaccia web.

VMware Player

ATTENZIONE
La versione supportata di VMWare è 6.5 e successive.

1. Scaricare il software appropriato dalla sezione Software e firmware su 2N.com. Dopo il download, decomprimere il file.
2. In VMware Player "File – Apri..." seleziona il percorso del file OVA.
3. Rinominare secondo necessità e fare clic su "Importa".

4. Controlla le impostazioni della CPU (minimo 2), le impostazioni della RAM (minimo 2048 MB) e la selezione della scheda di rete.

Dopo l'installazione, si aprirà la console di configurazione Linux, dove è possibile eseguire le impostazioni di base del sistema. La configurazione completa viene eseguita nell'interfaccia web.

VMware vSphere

ATTENZIONE
La versione supportata di VMWare è 6.5 e successive.

1. Scaricare il software appropriato dalla sezione Software e firmware su 2N.com. Dopo il download, decomprimere il file.
2. In VMware vSphere, seleziona "File – Deploy OVF Template.." e segui la procedura guidata.
3. Dopo l'importazione, controlla le impostazioni "Modifica impostazioni..."
   Modifica il nome (nella scheda Opzioni).
   Controlla le impostazioni della CPU (minimo 2), le impostazioni della RAM (minimo 2048 MB) e la selezione della scheda di rete.

Dopo l'installazione, si aprirà la console di configurazione Linux, dove è possibile eseguire le impostazioni di base del sistema. La configurazione completa viene eseguita nell'interfaccia web.

Hyper-V

1. Scaricare il software appropriato dalla sezione Software e firmware su 2N.com. Dopo il download, decomprimere il file.
2. Avvia Hyper-V Manager e seleziona l'opzione per l'host desiderato Importa macchina virtuale.
3. Nella guida all'installazione verificare le informazioni visualizzate e confermarne la lettura con il pulsante Prossimo.
4. Selezionare il percorso della cartella dal passaggio 1.
5. Conferma la selezione della macchina virtuale.
6. Seleziona il tipo di importazione.
7. Seleziona la scheda NIC virtuale per la macchina virtuale.
8. Controllare il riepilogo delle impostazioni selezionate nei passaggi precedenti e confermare con il pulsante Fine.

Dopo l'installazione, si aprirà la console di configurazione Linux, dove è possibile eseguire le impostazioni di base del sistema. La configurazione completa viene eseguita nell'interfaccia web.

Hardware consigliato

Incide il numero di dispositivi collegati**Access Commander**. Pertanto, impostare la dimensione degli elementi hardware in base alle condizioni effettive. La tabella seguente mostra il numero minimo consigliato di core CPU e dimensioni della RAM per il diverso numero di dispositivi e utenti gestiti Access Commander.

ATTENZIONE
Si consiglia di mantenere una connessione continua tra **Access Commander** e dispositivi. Se disconnessi, i dispositivi archiviano i registri eventi offline e, quando ricollegati, i dati di registro vengono sincronizzati Access Commander. Durante il processo di sincronizzazione, l'applicazione continua a essere eseguita, ma con un numero maggiore di dispositivi l'intero processo potrebbe richiedere più tempo.

Tabella 2. Hardware della macchina virtuale

Numero di dispositivi	numero di utenti	Numero minimo di core della CPU	Dimensione minima della RAM	Allocazione minima dell'HDD
1 000	10 000	2	2GB	120 GB
2 000	100 000	2	4GB	120 GB
2 000	200 000	4	8GB	120 GB
7 000	200 000	4	16 GB	120 GB

Tabella 3. Access Commander Box

Numero di dispositivi collegati 2.0	Numero di utenti 2.0	Numero di utenti nel gruppo
2000	100000	1500

Si consiglia di non superare il numero di 1500 utenti nel gruppo. Se sono presenti restrizioni per aree, ad esempio anti-passback o controllo dell'occupazione per un numero elevato di utenti, l'applicazione potrebbe rallentare.

Attivazione della licenza

Per l'attivazione è necessario ottenere le licenze file di licenza e caricarlo su **Access Commander**. La licenza Basic può essere attivata direttamente in **Acces Commander** nella pagina Impostazioni > scheda Licenza.

Ottenere il file di licenza

Per ottenere una licenza è necessario comunicare al distributore il numero di serie di uno dei dispositivi 2N a cui è collegato **Acces Commander**. File di licenza viene generato in base al numero di serie di questo dispositivo con licenza.

Connessione dispositivo con licenza garantisce la validità della licenza. In caso di disconnessione del dispositivo concesso in licenza, inizierà un periodo di protezione, trascorso il quale la licenza verrà sospesa.

Carica licenza

ATTENZIONE

- Dopo il passaggio dalla licenza di prova non è più possibile riattivare la licenza di prova.
- Le impostazioni delle funzionalità avanzate non supportate dalla nuova licenza non vengono salvate.

1. Vai a **Impostazioni** > **Scheda Licenza**.
2. Clicca su Carica licenza e nella finestra aperta caricare il file di licenza ottenuto dal repository.
3. Dopo aver caricato il file, fare clic su Attiva la licenza.
4. Assicurati che il dispositivo con licenza per il quale è stata generata la licenza sia attivato.

dispositivo di licenza	Dispositivo 2N selezionato collegato a **Access Commanderu**,che garantisce la validità della licenza. Il dispositivo di licenza funge da chiave hardware per la licenza.
file di licenza	Un file con una licenza, il caricamento che attiva la licenza. Il file di licenza viene generato dal distributore in base al numero di serie del dispositivo con licenza.

Sospensione della patente

La sospensione della licenza si verifica se il dispositivo con licenza viene disconnesso**Access Commander**per un periodo superiore al periodo di protezione della licenza. La durata del periodo di protezione dipende da quanto tempo è stato collegato il dispositivo con licenza **Access Commander**. La durata dei periodi di protezione è elencata in tabella che segue.

Quando una licenza viene sospesa, tutti i dispositivi connessi vengono automaticamente non gestiti e contrassegnati come non gestiti. Per riattivarli, è necessario connettersi e attivare il dispositivo con licenza oppure generare e caricare un nuovo file di licenza per un altro dispositivo.

Nel caso di caricamento di una nuova licenza, è necessario prima attivare il dispositivo con licenza per il quale viene generata la nuova licenza. Dopo aver attivato il dispositivo con licenza, sarà possibile attivare anche tutti gli altri dispositivi.

Il periodo di tempo a cui il dispositivo con licenza è stato connesso Access Commander	Il periodo di protezione per il quale sarà Access Commander in funzione senza dispositivo di licenza collegato
meno di 24 ore	1 giorno
1 giorno - 30 giorni	10 giorni
31 giorni - 180 giorni	1 mese
più di 180 giorni	3 mesi

Accesso di base all'interfaccia

*Questo capitolo descrive la messa in servizio e l'utilizzo di base **Access Commander**. L'installazione è descritta nel capitolo* *Installazione (p. 13)**.*

Interfaccia **Access Commander** è accessibile tramite un browser web. L'indirizzo IP dell'interfaccia web può essere cercato utilizzando il programma 2N Network Scanner.

NOTA
In caso di distribuzione tramite Access Commander Box connettersi all'interfaccia web da un altro computer sulla rete. Sistema operativo Access Commander Box garantisce il funzionamento Access Commander e la sua configurazione Linux di base non consente l'esecuzione del browser web.

Pannello di controllo

Dashboard è la visualizzazione di base dell'interfaccia web **Access Commander**. Si tratta di una bacheca configurabile che visualizza dati in tempo reale. **Access Commander** offre diversi widget che vengono aggiunti alla dashboard tramite un pulsante . I widget sulla Dashboard possono essere spostati, rinominati oppure le loro impostazioni di base possono essere eseguite in vari modi. La gestione e l'eliminazione dei widget avviene nel menu esteso nell'intestazione di ciascun widget.

Qualsiasi utente con un account su **Access Commander** puoi impostare la tua dashboard. La disponibilità dei widget è limitata a seconda del ruolo dell'utente e della licenza disponibile.

Cambio di lingua

Dopo il primo login se **Access Commander** viene visualizzato nella lingua impostata per l'azienda dell'utente loggato. Ogni utente può cambiare la lingua. Dopo il successivo accesso, l'interfaccia verrà visualizzata nella lingua appena impostata.

1. Fare clic sull'icona utente nell'angolo in alto a destra per aprire il menu utente.
2. Seleziona Cambia lingua.
3. Selezionare la lingua appropriata e confermare con Cambia lingua.

Cambia la password dell'account

1. Fare clic sull'icona utente nell'angolo in alto a destra per aprire il menu utente.
2. Seleziona Visualizza profilo.
3. Clicca su nel parametro Password.

4. Conferma la password esistente e inseriscine una nuova.

> **NOTA**
> Se la password per l'account 'admin' è la stessa password root dell'utente di sistema (per accedere alla console di installazione di Linux), quando la password per l'account 'admin' viene modificata, la password dell'account root verrà modificata. verranno modificati anche automaticamente.

Cambia la tua immagine di profilo

1. Fare clic sull'icona utente nell'angolo in alto a destra per aprire il menu utente.
2. Seleziona Visualizza profilo.
3. Clicca sull'immagine nell'intestazione dei dettagli dell'utente.
4. Nella finestra di dialogo aperta, imposta la foto.
   La risoluzione dell'immagine verrà regolata automaticamente a 432 × 432 px.

Loghi

Ecco una panoramica di ciò che troverai nel capitolo:

Registri di sistema

NOTA

- All'utente vengono mostrati i registri che può visualizzare in base alle autorizzazioni utente.
- I dati vengono scritti nei log in inglese.

La pagina Registri di sistema visualizza un elenco di eventi e notifiche che **Access Commander** generato.

Nell'elenco dei log di sistema, per ogni evento e notifica è indicato:

- gravità (informazioni, avviso, errore);
- l'ora in cui si è verificato l'evento;
- la categoria in cui rientra l'azione (Stato Dispositivo, Importazione, Sincronizzazione Utente, Sistema, Azioni Utente, Restrizioni Area);
- soggetto a cui si riferisce l'azione (dispositivo, utente, zona, visita...);
- una breve descrizione dell'evento;
- autore dell'evento.

Facendo clic su una riga si espandono le informazioni dettagliate sul record specificato.

L'elenco può essere filtrato utilizzando sopra l'elenco. In alternativa è possibile impostare filtri per singole colonne nel menu esteso che si apre cliccando su nell'intestazione di ogni colonna. Menù esteso di colonne consente inoltre di spostare le colonne, fissarle alla prima o all'ultima posizione o nasconderle.

Le colonne Gravità e Ora non possono essere nascoste.

Esportazione di loghi

I record possono essere scaricati in un file CSV o stampati facendo clic su un pulsante Esportare sopra l'elenco. Nel file CSV esportato l'ora è indicata in GMT+0.

Durata dei log

Una volta che l'utilizzo della capacità del disco raggiunge l'80%, verrà avviata l'eliminazione automatica del registro. La capacità del disco può essere monitorata nella pagina Impostazioni. I registri del primo tipo

vengono eliminati per primi in ordine, gli altri registri vengono eliminati gradualmente finché l'utilizzo dello spazio su disco non scende al 75% o finché rimangono solo i registri con un tempo di archiviazione minimo possibile incompleto del tipo di registro specificato.

Il tempo di archiviazione per un determinato tipo di registro viene impostato nella scheda Impostazioni > Conservazione registro. La conservazione delle registrazioni della telecamera non può essere più lunga della conservazione dei registri di sistema e di accesso.

SUGGERIMENTO
Se utilizzi costantemente il 70% della capacità del disco, ti consigliamo di ridurre il tempo massimo di archiviazione del registro.

Accedi ai log

NOTA

- All'utente vengono mostrati i registri che può visualizzare in base alle autorizzazioni utente.
- I dati vengono scritti nei log in inglese.

La pagina Registri di accesso visualizza i record dei tentativi di autenticazione riusciti e non riusciti e dei blocchi di emergenza.

L'elenco dei registri di accesso afferma:

- Categoria
  - concesso - accesso consentito
  - negato: accesso negato
  - pubblico – consentendo l'accesso gratuito
  - lockout - blocco del dispositivo
- L'ora in cui si è verificato l'evento
- L'utente che ha eseguito l'azione
- L'azienda dell'utente
- La zona in cui si è verificato l'evento
- Il dispositivo su cui si è verificata l'azione
- Autenticazione utilizzata per il tentativo (PIN, codice QR, ecc.)

Facendo clic su una riga si espandono le informazioni dettagliate sul record specificato.

L'elenco può essere filtrato utilizzando sopra l'elenco. In alternativa è possibile impostare filtri per singole colonne nel menu esteso che si apre cliccando su nell'intestazione di ogni colonna. Menù esteso di colonne consente inoltre di spostare le colonne, fissarle alla prima o all'ultima posizione o nasconderle.

Esportazione di loghi

I record possono essere scaricati in un file CSV o stampati facendo clic su un pulsante 

sopra l'elenco. Nel file CSV esportato l'ora è indicata in GMT+0.

Durata dei log

Una volta che l'utilizzo della capacità del disco raggiunge l'80%, verrà avviata l'eliminazione automatica del registro. La capacità del disco può essere monitorata nella pagina Impostazioni. I registri del primo tipo vengono eliminati per primi in ordine, gli altri registri vengono eliminati gradualmente finché l'utilizzo dello spazio su disco non scende al 75% o finché rimangono solo i registri con un tempo di archiviazione minimo possibile incompleto del tipo di registro specificato.

Il tempo di archiviazione per un determinato tipo di registro viene impostato nella scheda Impostazioni > Conservazione registro. La conservazione delle registrazioni della telecamera non può essere più lunga della conservazione dei registri di sistema e di accesso.

SUGGERIMENTO
Se utilizzi costantemente il 70% della capacità del disco, ti consigliamo di ridurre il tempo massimo di archiviazione del registro.

Notifica

Il modulo Notifiche consente di impostare il monitoraggio degli eventi selezionati e delle proprietà del sistema di cui è a conoscenza **Access Commander** informare tramite e-mail o notifica nella barra in alto accanto al menu utente.

Un elenco di notifiche viene visualizzato anche nella pagina Registri di sistema > Notifiche.

I record possono essere scaricati in un file CSV o stampati facendo clic su un pulsante 

sopra l'elenco. Nel file CSV esportato l'ora è indicata in GMT+0.

Impostazione di un nuovo tipo di notifica

1. Vai alla pagina **Impostazioni** > **Notifica**.
2. Fai clic sul pulsante Aggiungi nell'angolo in alto a destra della pagina.
3. Inserisci un nome per il nuovo tipo di notifica.

Dopo la creazione verrà visualizzato il dettaglio della notifica in cui è possibile selezionare i dispositivi per i quali monitorare la notifica; aggiungere gli utenti a cui inviare la notifica; scegliere il metodo di consegna della notifica.

Impostazioni di notifica

I tipi di notifica vengono impostati nei dettagli del tipo di notifica specificato. Il dettaglio del tipo di notifica si apre facendo clic sulla notifica selezionata nell'elenco nella pagina Impostazioni > Notifiche.

Metodo di notifica

In questa scheda vengono impostati i metodi di notifica delle notifiche e l'elenco dei destinatari delle notifiche tramite posta elettronica.

La notifica in **Access Commander** appaiono sotto l'icona nella barra in alto, accanto al menu utente o in Registro di sistema > Notifiche.

È possibile inviare e-mail di notifica agli utenti gestiti in **Access Commander** e destinatari esterni al sistema. Gli utenti possono essere selezionati dall'elenco. Gli indirizzi e-mail degli altri destinatari devono essere inseriti manualmente.

NOTA
Per il corretto funzionamento delle notifiche via email è necessario che il protocollo SMTP sia impostato correttamente, vedi Abilitazione e configurazione della funzione e-mail (SMTP) (p. 58).

Dispositivi monitorati

Il tipo di notifica indicato può essere generato sia per tutti i dispositivi che solo per alcuni dispositivi. Se Monitora tutti i dispositivi è abilitato, l'evento può verificarsi su qualsiasi dispositivo e verrà generata una notifica. Se Monitoraggio di tutti i dispositivi è disabilitato, verrà generata una notifica solo se l'evento si verifica sul dispositivo selezionato. La selezione dell'apparecchio avviene nel menu che si apre con .

Durata dei log

Una volta che l'utilizzo della capacità del disco raggiunge l'80%, verrà avviata l'eliminazione automatica del registro. La capacità del disco può essere monitorata nella pagina Impostazioni. I registri del primo tipo vengono eliminati per primi in ordine, gli altri registri vengono eliminati gradualmente finché l'utilizzo dello spazio su disco non scende al 75% o finché rimangono solo i registri con un tempo di archiviazione minimo possibile incompleto del tipo di registro specificato.

Il tempo di archiviazione per un determinato tipo di registro viene impostato nella scheda Impostazioni > Conservazione registro. La conservazione delle registrazioni della telecamera non può essere più lunga della conservazione dei registri di sistema e di accesso.

SUGGERIMENTO
Se utilizzi costantemente il 70% della capacità del disco, ti consigliamo di ridurre il tempo massimo di archiviazione del registro.

Aziende

Le impostazioni possono essere effettuate all'interno di un'unica installazione **Access Commander** dividi in **Società**, che sono gestiti separatamente. Questo metodo consente di suddividere l'amministrazione tra gli amministratori delle singole aziende. Un amministratore di un'azienda non ha accesso alle informazioni su un'altra azienda. Gli amministratori di un'azienda non vedranno gli utenti di un'altra azienda.

È possibile condividere zone o strutture tra aziende, consentendo la gestione degli accessi aziendali alle aree comuni (ingressi, ristoranti, sale conferenze...).

Creazione di una nuova società

1. Vai alla pagina **Aziende**.
2. Fai clic sul pulsante Aggiungi azienda nell'angolo in alto a destra.
3. Inserisci il nome dell'azienda.
4. Puoi avviare un'azienda facendo clic su Creare.

L'azienda appena creata apparirà nell'elenco. Nei dettagli dell'azienda è necessario effettuare le sue impostazioni. L'aggiunta di utenti all'azienda viene effettuata nelle impostazioni dei singoli utenti.

Impostazioni aziendali

Le informazioni sull'azienda possono essere visualizzate e modificate nei dettagli dell'azienda. I dettagli di un'azienda vengono aperti facendo clic su un'azienda selezionata nell'elenco nella pagina Aziende.

I dettagli dell'azienda sono suddivisi nelle schede Panoramica, E-mail e Sincronizzazione utente.

Il linguaggio della società

Nella scheda Generale è possibile selezionare la lingua aziendale in cui verrà utilizzata l'interfaccia **Access Commander** visualizzare agli utenti di tale azienda. Gli utenti possono modificare la lingua dell'interfaccia in un secondo momento. La scelta della lingua da parte dell'azienda influisce anche sui modelli di posta elettronica inviati agli Utenti. Il testo delle e-mail può essere modificato nella scheda E-mail.

Zone

L'assegnazione delle zone ad un'azienda definisce l'insieme delle strutture alle quali gli utenti aziendali avranno diritto di accesso (ad esempio, la zona delle aree comuni e la zona del 4° piano, che comprende la porta d'ingresso della reception e tutti gli ingressi del quarto piano). Le zone possono essere assegnate a più società contemporaneamente e più zone possono essere assegnate a una società.

Mobile Key

In azienda è possibile impostare i parametri di abbinamento con l'applicazione 2N Mobile Key, che abilita l'autenticazione Bluetooth. Vengono impostati sia i dispositivi su cui gli utenti potranno effettuare l'abbinamento sia il tempo di validità della chiave mobile necessaria per l'abbinamento. La chiave mobile stessa viene generata nelle impostazioni dell'utente.

Visite

In questa scheda vengono impostati i gruppi ai quali l'amministratore della visita potrà assegnare nuove visite. Uno dei gruppi può essere specificato come predefinito. La nuova visita verrà automaticamente assegnata al gruppo predefinito, se non diversamente impostato.

ATTENZIONE
Senza un gruppo predefinito impostato correttamente non è possibile fornire l'accesso ai visitatori nell'interfaccia utente semplificata.

E' possibile selezionare le modalità di autenticazione assegnabili alla visita. Il metodo di autenticazione viene quindi assegnato a una visita dal responsabile delle visite.

Ulteriori informazioni sull'impostazione delle visite in Visite (p. 50).

Fondo di lavoro

Il pool di lavoro e le ferie vengono utilizzati per calcolare il pool di lavoro mensile degli utenti nel modulo presenze. Selezionando i giorni è possibile determinare quali giorni della settimana verranno conteggiati come giorni lavorativi. Il giorno viene selezionato facendo clic. I giorni verdi identificano quali giorni sono considerati giorni lavorativi.

L'adeguamento dell'orario di lavoro definisce quanto tempo ha a disposizione un turno giornaliero.

Vacanze

Impostando le ferie, si determina quali giorni non sono inclusi nel calcolo del pool di lavoro mensile. Le ore lavorate nei giorni festivi vengono conteggiate allo stesso modo delle ore lavorate nei fine settimana: il tempo lavorato viene registrato in aggiunta al normale orario di lavoro.

Offerta estesa ti permette di copiare le vacanze da un'altra azienda. Le festività vengono copiate includendo date e nomi. La copia può essere utilizzata più volte, ma se il giorno festivo appena copiato è già impostato in azienda, il suo nome verrà sovrascritto.

E-mail inviate ai membri dell'azienda

Le impostazioni e-mail hanno una propria scheda nei dettagli dell'azienda. **Access Commander** consente di inviare email automatiche ai membri dell'azienda (compresi i visitatori) con informazioni sull'assegnazione di un metodo di autenticazione. All'utente o al visitatore viene inviata un'e-mail con l'indirizzo e-mail impostato.

Access Commander consente di inviare email con le seguenti informazioni:

- Codice PIN per la visita
- Codice QR per la visita
- Codice PIN per l'utente
- Codice QR per gli utenti
- Mobile Key per impostare l'autenticazione Bluetooth per l'utente

Nei dettagli dell'azienda > scheda E-mail > scheda Modelli e-mail, è possibile impostare l'aspetto di queste e-mail e modificarne il testo. La modifica del testo di un'e-mail avviene in una finestra di dialogo che si apre facendo clic sul tipo di e-mail selezionato. Nella finestra di dialogo è possibile modificare:

- oggetto: l'oggetto dell'e-mail
- intestazione: visualizzata nel campo colorato del corpo dell'e-mail
- introduzione: il testo fornito prima dei dati generati automaticamente da **Access Commander**
- messaggio successivo: il testo che segue i dati generati da **Access Commander**
- firma - la firma apposta alla fine dell'e-mail

Sincronizzazione aziendale (LDAP)

La sincronizzazione con LDAP viene utilizzata per scaricare gli utenti e le relative modifiche da un sistema LDAP esterno. I dati dell'utente includono nome utente, ID, identificatori della carta, codice PIN/QR, immagine, indirizzo e-mail, numero di telefono, password e login, targhe di immatricolazione del veicolo.

NOTA
Ulteriori informazioni su LDAP sono disponibili all'indirizzo www.ldap.com.

1. Vai su Aziende > dettagli dell'azienda selezionata > scheda Sincronizzazione utente.
2. Se non è impostata alcuna connessione, creane una.
   Compilare:

   - **il nome del server** – se il DNS è impostato correttamente basta inserire il nome del server («WIN-9ABEB4AUOHD»). Se il DNS non è impostato, nel nome del server viene inserito l'indirizzo IP del server su cui viene eseguito il servizio LDAP.
   - **Porta** – l'impostazione predefinita è la porta LDAP 389 (senza SSL). Se desideri utilizzare una connessione crittografata nella tua azienda, inserisci il numero di porta 636. Il supporto SSL deve essere abilitato anche sul lato server LDAP. Se l'amministratore imposta un numero di porta diverso, è necessario modificarlo anche nella v **Access Commanderal**.
   - **Nome di login** – il nome di accesso dell'utente che ha i diritti corrispondenti per la radice data o per l'intero albero. Il nome di accesso deve essere inserito nel formato: "administrator@domain.com"
   - **Parola d'ordine** – la password dell'utente specificato sul server LDAP.
   - **Sicurezza della comunicazione (SSL)** – quando SSL è disabilitato, non è necessario riscrivere il numero di porta. Quando si abilita SSL, il numero di porta deve essere modificato in 636.
   - **DN base** – il punto radice da cui inizia la ricerca nella directory. Può essere un'estensione o la radice di una directory, ad esempio: CN=amministratore, CN=utenti, DC=dominio, DC=com.

   Si apriranno i dettagli della connessione LDAP impostata. È possibile testare le impostazioni di connessione. Utilizzando il pulsante Sincronizza ora si avvia una sincronizzazione una tantum.
3. Sulla scheda è impostata la sincronizzazione automatica **Importare**. Quando si abilita la sincronizzazione automatica, inserire gli intervalli in cui deve avvenire la sincronizzazione. In base alla frequenza, scegli in quale minuto o ora verranno sincronizzati i dati.
4. Sulla carta **Opzioni** è possibile assegnare i dati utente agli attributi sul server LDAP.

È possibile eliminare la connessione impostata nel menu esteso carte **Importare**. Sulla carta **Opzioni** vengono impostati altri parametri di sincronizzazione.

Opzioni di sincronizzazione LDAP

Attributi importati – modificando lo schema, l'assegnazione dei dati da **Access Commander** agli attributi sul server LDAP.

Utenti rimossi da LDAP – definisce cosa dovrebbe accadere agli utenti che sono stati eliminati in LDAP. Gli utenti eliminati da LDAP possono essere **Access Commander** conservarli o eliminarli. Se gli utenti devono essere disabilitati, dopo averli eliminati da LDAP, i loro dati rimarranno **Access Commander**, ma non si sincronizzerà con i dispositivi.

Utenti disabilitati in Active Directory – imposta cosa succede agli utenti che sono stati bannati in Active Directory. La disabilitazione in Active Directory può **Access Commander** ignorare o poter eliminare (bannare) l'utente. Dopo la riattivazione in Active Directory, gli utenti eliminati vengono nuovamente caricati in **Access Commander.**

Sincronizzazione dei gruppi – consente di caricare le appartenenze ai gruppi da LDAP a **Access Commander**. Utilizzando le impostazioni dello schema di sincronizzazione è possibile definire il proprio DN di Base ed il filtro in base al quale i gruppi verranno sincronizzati. Lo schema consente la sincronizzazione di gruppi nidificati.

Sincronizzazione dell'avatar – imposta il download delle foto dell'utente dal sistema LDAP.

Monitoraggio dei collegamenti – imposta se sincronizzare i dati dai collegamenti LDAP.

Ricerca nidificata – permette di effettuare la ricerca su tutto l'albero, altrimenti viene ricercata solo la radice.

Cercapersone abilitato – l'impaginazione utilizza l'estensione LDAP Simple Paged Results Control. Ciò consente di suddividere i risultati in più pagine, il che è essenziale per i servizi di directory di grandi dimensioni. Parametro **Dimensioni della pagina** determina quanti record conterrà una pagina.

Utenti

Aiuto **Access Commander** può essere gestito **Utenti**, modificare il loro accesso, gestire le loro informazioni di contatto, ecc.

Tutti gli utenti creati vengono visualizzati nell'elenco degli utenti. Gli utenti possono essere filtrati sopra l'elenco oppure è possibile cercare direttamente un utente specifico in base al nome, all'e-mail o al numero di telefono.

Azioni di massa

Tramite il tagging è possibile selezionare più utenti e applicare loro le seguenti azioni collettive:

- Attiva il monitoraggio delle presenze per gli utenti
- Aggiungi utente al gruppo
- Elimina utente
- Imposta l'intervallo di tempo di validità dell'accesso
- Assegnare un codice PIN di accesso agli utenti a cui non è ancora stato assegnato un PIN o un codice QR
- Assegnare un codice QR di accesso agli utenti a cui non è stato ancora assegnato un PIN o un codice QR
- Assegna una chiave mobile agli utenti della selezione a cui non è ancora stata assegnata una chiave mobile

NOTA
Per assegnare un codice PIN/QR o una chiave mobile a un utente, è necessario che l'utente disponga di un indirizzo e-mail valido.

Crea un nuovo utente

1. Vai alla pagina **Utenti**.
2. Fare clic sul pulsante Aggiungi utente nell'angolo in alto a destra.
3. Compila le informazioni richieste: nome utente e azienda di appartenenza.

L'utente appena creato apparirà nell'elenco e si apriranno i dettagli dell'utente. Ulteriori impostazioni utente vengono effettuate in dettaglio, come l'assegnazione di un numero di telefono, l'impostazione dei metodi di autenticazione, l'assegnazione a gruppi, ecc.

Impostazioni utente

Le informazioni sull'utente possono essere visualizzate e gestite nei dettagli dell'utente. Il dettaglio dell'utente si apre cliccando sull'utente selezionato nell'elenco della pagina Utenti.

I dettagli dell'utente sono suddivisi nelle schede Panoramica, Partecipazione e Registro modifiche. La scheda presenze viene visualizzata solo per quegli utenti che hanno abilitato il monitoraggio, vedere Monitoraggio delle presenze degli utenti (p. 33). Il modulo presenza è disponibile a seconda della licenza.

Modifica del nome e della foto dell'utente

Le opzioni per rinominare l'utente e impostare la foto si trovano nel menu esteso nell'intestazione dei dettagli dell'utente.

La risoluzione dell'immagine verrà regolata automaticamente a 432 × 432 px.

Autenticazione

Questa scheda viene utilizzata per impostare i metodi di autenticazione dell'utente sui dispositivi. L'utente deve autenticarsi sul dispositivo e, se dispone di un accesso valido, gli verrà concesso l'accesso al dispositivo.

Carta RFID – aggiunge una carta RFID esistente all'utente. Si aprirà una finestra di dialogo in cui è necessario inserire l'identificatore della carta. L'identificatore può essere letto avvicinando la carta al lettore o inserendo la carta d'identità utilizzando la tastiera. L'identificatore deve essere un numero esadecimale lungo almeno 6 caratteri. Ad un utente possono essere assegnate fino a 2 tessere di accesso.

Mobile Key – utilizzato per connettersi all'applicazione 2N Mobile Key abilitare l'autenticazione tramite Bluetooth, vedere il capitolo Autenticazione Bluetooth (p. 32).

Codice PIN – genera automaticamente un PIN di 6 cifre.

All'utente può essere assegnato un PIN o un codice QR per l'accesso, ma non è possibile averli entrambi contemporaneamente.

QR Code – genererà automaticamente un codice QR. I dispositivi che consentono la lettura dei codici QR sono elencati in Dispositivi e applicazioni supportati (p. 8).

All'utente può essere assegnato un PIN o un codice QR per l'accesso, ma non è possibile averli entrambi contemporaneamente.

Impronta digitale – apre una finestra di dialogo per il caricamento di un'impronta digitale, che l'utente può utilizzare per autenticarsi sui dispositivi che supportano la lettura delle stesse. Ogni utente può caricare fino a 2 impronte digitali. La procedura è descritta nel capitolo Caricamento dell'impronta digitale (p. 31).

Targa – imposta la targa del veicolo dell'utente, che il dispositivo può scansionare e utilizzare per autenticare l'utente.

Carta virtuale – consente di impostare l'ID della tessera di accesso virtuale dell'utente. Ad ogni utente può essere assegnata esattamente una carta virtuale. L'ID della carta virtuale è una sequenza di 6-32 caratteri dal set 0-9, A-F. Il numero della carta virtuale viene utilizzato per identificare l'utente nei dispositivi collegati tramite l'interfaccia Wiegand.

Cambia codice – permette di impostare fino a 4 codici per l'attivazione di interruttori (es. serratura). Il codice interruttore viene utilizzato per aprire la serratura utilizzando la tastiera del dispositivo e un codice DTMF.

ATTENZIONE
Con l'autenticazione a più fattori è necessario seguire l'ordine dei metodi di autenticazione.

SUGGERIMENTO
Durante la compilazione dell'indirizzo e-mail è possibile inviare all'indirizzo indicato il codice PIN/QR di accesso generato.

Account

Impostando un nome di accesso e una password monouso, è possibile garantire all'utente l'accesso all'interfaccia **Access Commander**. Una volta effettuato l'accesso, l'utente può monitorare la propria presenza (se disponibile), modificare la propria e-mail o modificare la propria immagine del profilo. Al primo accesso verrà richiesto all'utente di modificare la password. Se per un utente è richiesta l'autenticazione a due fattori, all'utente verrà richiesto di collegarsi a un'applicazione di autenticazione personalizzata, vedere Autenticazione a due fattori (p. 64). In questa scheda è anche possibile rimuovere la connessione con l'applicazione di autenticazione.

Nella scheda Account è possibile concedere permessi amministrativi agli utenti con dati di accesso **Access Commander** utilizzando i ruoli utente. Le autorizzazioni dei singoli ruoli sono descritte nel capitolo Autorizzazioni utente (p. 7).

Interfaccia semplificata

È possibile lanciare un'interfaccia utente semplificata per un singolo responsabile delle visite aziendali. Un'interfaccia semplificata consente al gestore dei visitatori di aggiungere, rimuovere e gestire i visitatori. I registri e le presenze non possono essere visualizzati nell'interfaccia semplificata. Lo scopo dell'interfaccia semplificata è principalmente quello di rendere più semplice per gli utenti degli appartamenti concedere l'accesso ai propri visitatori. Tutte le visite create nell'interfaccia semplificata vengono sempre assegnate a *gruppo predefinito per le nuove visite*. Il responsabile delle visite non ha la possibilità di modificare questo gruppo. Il gruppo predefinito per i nuovi visitatori deve essere selezionato in anticipo nelle impostazioni dell'azienda e per il gruppo devono essere impostate regole di accesso valide per l'accesso all'appartamento, compreso il percorso per raggiungerlo. L'utente dell'appartamento potrà poi gestire le modalità di autenticazione e la durata delle visite in un'interfaccia semplificata.

ATTENZIONE
Prima di abilitare l'interfaccia semplificata **l'amministratore di sistema dovrà impostare il gruppo predefinito per le nuove visite** In Impostazioni aziendali (p. 24). Tali regole di accesso devono essere assegnate al gruppo predefinito affinché il visitatore abbia accesso alle aree visitate. Senza un gruppo predefinito impostato correttamente non è possibile fornire l'accesso ai visitatori nell'interfaccia semplificata.

Dati personali

Utilizzato per aggiungere informazioni di base sull'utente. Consente di aggiungere l'indirizzo email dell'utente al quale verranno inviate le informazioni relative all'account dell'utente e di aggiungere un numero di telefono per contattare l'utente.

E' possibile scrivere sulla tessera:

- **E-mail**– l'indirizzo al quale verranno inviate all'utente le informazioni relative al suo account **Access Commander**;
- **Numero utente** – identificatore specifico, richiesto per la sincronizzazione di massa con un file CSV (vedi Sincronizzazione degli utenti con FTP (p. 60));
- **Una nota**.

Si avvicina

La scheda accessi serve per assegnare l'utente ad un gruppo e per impostare l'intervallo di tempo in cui saranno validi i dati di accesso dell'utente. L'intervallo di tempo viene impostato nel menu esteso della scheda, che si apre cliccando su .

SUGGERIMENTO
I limiti temporali di accesso al dispositivo vengono impostati tramite i profili temporali.

Se l'utente è membro di un gruppo, la scheda visualizza quel gruppo. Se l'utente non è assegnato a un gruppo, può essere aggiunto nella scheda. Il gruppo può essere modificato o eliminato nel menu avanzato .

Numeri di telefono

Questa carta viene utilizzata per stabilire la connessione con l'utente. Il numero di telefono è la destinazione della chiamata del dispositivo appartenente a questo utente.

Il numero di telefono virtuale può essere utilizzato per chiamare l'utente utilizzando il tastierino numerico del dispositivo. Un numero virtuale può avere da due a quattro cifre. I numeri virtuali non sono correlati ai numeri di telefono dell'utente, consentendo agli utenti di nascondere i propri numeri di telefono sul dispositivo. Nella scheda è anche possibile impostare un interlocutore al quale verrà inoltrata la chiamata in caso di irreperibilità di tale utente. Il rappresentante può essere scelto tra altri utenti dell'azienda.

Registro degli accessi

Il registro degli accessi visualizza la cronologia degli accessi.

Modifica registro

Tutte le modifiche alle impostazioni utente possono essere visualizzate nella scheda Registro modifiche. L'ordinamento di base avviene in base all'ora del cambio. Nel log è possibile scoprire chi ha apportato la modifica. Dopo aver cliccato sulla riga è possibile conoscere il dettaglio della modifica apportata.

Caricamento dell'impronta digitale

Ogni utente può caricare fino a 2 impronte digitali. Utilizza un lettore di impronte digitali esterno per caricarli. Controlla se hai il driver installato2N Driver USB. Il driver è disponibile per il download Qui.

L'impronta digitale caricata di un utente può essere utilizzata per le seguenti azioni:

- Apri la porta;
- Avvia un allarme silenzioso - impostabile solo se è attiva la funzione Apertura Porta;
- Automazione F1 e F2: genera l'evento FingerEntered in Automazione. F1 e F2 vengono utilizzati per distinguere il dito attaccato in Automazione.

Caricamento dell'impronta digitale

1. Assicurati che sia inserito **Impostazioni** > **Si avvicina** lettore di impronte digitali USB abilitato.
2. Nelle impostazioni utente v **Scheda Autenticazione** scegli l'autenticazione Impronta digitale.
3. Seleziona il dito per il quale desideri caricare l'impronta digitale.
   Apparirà una finestra intitolata "Caricamento impronta digitale".
4. Posizionare il dito selezionato sul lettore. Ripeti questo passaggio 3 volte, ogni volta quando richiesto.
   Dopo l'ultima scansione verrai informato dell'avvenuta scansione dell'impronta digitale.

5. Premendo il pulsante**Creare**il processo è completo.

Autenticazione Bluetooth

L'autenticazione dell'utente tramite Bluetooth avviene tramite l'app Mobile Key, che l'utente deve aver scaricato sul proprio cellulare.

Connessione dell'applicazione sul telefono dell'utente con dispositivi v **Access Commander** viene effettuato inserendo il codice di abbinamento nell'applicazione Mobile Key.

Il codice di abbinamento può essere ottenuto in due modi:

- tramite un lettore USB Bluetooth collegato a un computer
- connessione al dispositivo.

Creazione di un codice di abbinamento tramite computer

1. Scarica sul tuo computer 2N Driver USB IP e installarlo.
2. Assicurati che il lettore Bluetooth USB sia abilitato nel **Impostazioni** > **Si avvicina** > **la scheda Lettori USB abilitati**.
3. Collegare il lettore Bluetooth USB al computer.
4. Nelle impostazioni utente v **Scheda Autenticazione** scegli l'autenticazione Mobile Key.
5. Nella finestra di dialogo che si apre, seleziona Accoppiamento utilizzando un lettore.
   Nella finestra di dialogo verrà visualizzato un codice di abbinamento.
6. Seguire la procedura seguente per associare l'app sotto (p. 32).

Crea un codice di accoppiamento sul dispositivo

1. Assicurati di questo
   - il dispositivo di accoppiamento è impostato per l'azienda dell'utente specificato, vedere???;
   - il dispositivo di accoppiamento si trova in una zona alla quale l'utente ha accesso valido, vale a dire Regole di accesso (p. 44);
   - viene impostato un tempo adeguato per l'accoppiamento, vale a dire???.
2. Nelle impostazioni utente v **Scheda Autenticazione** scegli l'autenticazione Mobile Key.
3. Nella finestra di dialogo che si apre, seleziona Accoppia utilizzando il tuo dispositivo.
4. Il codice di abbinamento generato viene visualizzato sulla carta insieme al tempo di abbinamento rimanente. Passare il codice di abbinamento all'utente. Se l'utente ha un indirizzo e-mail completo, è possibile inviare la chiave mobile all'e-mail facendo clic su .
5. Seguire la procedura seguente per associare l'app sotto (p. 32).

Associazione nell'app mobile Mobile Key

1. Scarica l'applicazione Mobile Key al tuo cellulare. L'applicazione è disponibile all'indirizzo App Store a Google Play.
2. Apri l'app e abilita l'app Mobile Key accesso al Bluetooth.
3. A seconda del tipo di chiavetta mobile, avvicinare il lettore USB o il dispositivo di abbinamento al telefono cellulare.
4. Nell'app Mobile Key fare clic sul dispositivo offerto da accoppiare.

5. L'applicazione richiede di inserire un codice PIN. Inserisci il codice di abbinamento e confermane l'inserimento.

Monitoraggio delle presenze degli utenti

Access Commander consente il monitoraggio delle presenze degli utenti. Nella modalità presenza vengono registrati gli orari di ingresso e di uscita dei singoli utenti.

La registrazione delle presenze degli utenti deve essere attivata. L'attivazione avviene nel menu esteso  nell'intestazione dei dettagli dell'utente. L'attivazione della registrazione delle presenze per più utenti contemporaneamente può essere effettuata selezionando gli utenti nell'elenco nella pagina Utenti e utilizzando un'azione in blocco  .

Il responsabile delle presenze può modificare i dati sulle presenze degli utenti. La modifica viene effettuata facendo clic sull'intervallo di tempo da modificare. Una volta aperti, è possibile modificare i tempi limite e aggiungere una nota all'intervallo.

ATTENZIONE
Per il corretto funzionamento delle presenze è necessario avere **Access Commander**licenza attiva disponibile per monitorare la presenza dell'utente. Il rilevamento delle presenze deve essere attivato nelle impostazioni del singolo utente.

Il monitoraggio e l'adeguamento delle presenze sono descritti nel capitolo Partecipazione (p. 47).

Gruppi

Il gruppo viene utilizzato per raggruppare gli utenti e per impostare più facilmente i diritti dei suoi membri per accedere alla zona. Non è necessario impostare i diritti a livello di singoli utenti e visite, ma il gruppo sarà associato alla zona.

L'elenco può essere filtrato utilizzando sopra l'elenco. In alternativa è possibile impostare filtri per singole colonne nel menu esteso che si apre cliccando su nell'intestazione di ogni colonna. Menù esteso di colonne consente inoltre di spostare le colonne, fissarle alla prima o all'ultima posizione o nasconderle.

Crea un nuovo gruppo

1. Vai alla pagina **Gruppi**.
2. Fare clic sul pulsante per aggiungere un gruppo nell'angolo in alto a destra.
3. Nella finestra di dialogo che si apre, è necessario inserire il nome del gruppo e selezionare a quale azienda appartiene.

> **ATTENZIONE**
> Una volta creato un gruppo, la società madre non può essere modificata.

Il gruppo appena creato apparirà nell'elenco e si aprirà il suo dettaglio. Nei dettagli del gruppo, devi aggiungere membri e impostare le loro regole di accesso.

Impostazioni del gruppo

Le informazioni sul gruppo possono essere visualizzate e modificate nei dettagli del gruppo. I dettagli del gruppo vengono aperti facendo clic sul gruppo selezionato nell'elenco dei gruppi. Nel dettaglio, è presente una panoramica dei membri del gruppo e una panoramica delle loro regole di accesso.

Membri

La scheda visualizza tutti gli utenti che appartengono al gruppo. È possibile aggiungere al gruppo solo gli utenti o le carte visitatore che appartengono alla stessa azienda del gruppo.

Regole di accesso

Visualizza una panoramica di tutte le regole di accesso già create e offre la possibilità di modificarle o crearle. Creando una regola di accesso, a un gruppo specifico viene consentito l'accesso alla zona. Quando si crea una regola, è necessario inserire un gruppo e un profilo temporale in cui il gruppo dovrà avere accesso alla zona.

Zone

Le zone vengono utilizzate per una gestione più semplice dell'accesso ai singoli dispositivi. Le zone combinano i dispositivi in unità logiche. Nella pagina viene visualizzato un elenco di tutte le zone.

L'elenco può essere filtrato utilizzando sopra l'elenco. In alternativa è possibile impostare filtri per singole colonne nel menu esteso che si apre cliccando su nell'intestazione di ogni colonna. Menù esteso di colonne consente inoltre di spostare le colonne, fissarle alla prima o all'ultima posizione o nasconderle.

Abilitazione dei punti di accesso

Aiuto si aprirà una finestra di dialogo in cui viene avviato il supporto del punto di accesso, altro v Impostazioni del punto di accesso del dispositivo (p. 48).

Creazione di una nuova zona

1. Vai alla pagina **Zone**.
2. Fare clic sul pulsante per aggiungere una zona nell'angolo in alto a destra.
3. Nella finestra di dialogo che si apre, devi inserire il nome della zona e selezionare a quali aziende appartiene.

La zona appena creata viene visualizzata nell'elenco. I dispositivi possono essere aggiunti ad una zona nei dettagli della zona o nei dettagli del dispositivo. Ulteriori impostazioni possono essere effettuate nei dettagli della zona.

Impostazioni della zona

Le informazioni sulla zona possono essere visualizzate e modificate nei dettagli della zona. I dettagli della zona vengono aperti facendo clic sulla zona selezionata nell'elenco.

Autenticazione a più fattori

È possibile impostare la necessità di autenticazione in diversi modi per tutti i dispositivi della zona. È possibile selezionare solo alcune modalità di autenticazione, ma nel loro utilizzo occorre rispettare rigorosamente il seguente ordine:

1. Mobile Key
2. Carta RFID
3. Impronta digitale
4. Codice PIN

ATTENZIONE
Con l'autenticazione a più fattori è necessario seguire l'ordine dei metodi di autenticazione.

La necessità di autenticazione a più fattori può essere limitata da un profilo temporale. Quando l'autenticazione a più fattori è attivata, verrà visualizzata un'opzione **Utilizza l'autenticazione a più fattori**, in cui

è possibile utilizzare  selezionare un profilo temporale. Quando si sceglie la modalità In qualsiasi momento, sarà sempre richiesta l'autenticazione a più fattori.

L'autenticazione a più fattori può essere richiesta solo per accedere alla zona. Questa impostazione è valida solo quando si utilizzano punti di accesso.

Accedi alle impostazioni

È possibile impostare un volume nella scheda **Codice PIN per accedere alla zona** oppure visualizzarlo se è già stato creato un codice PIN.

Inoltre, nelle impostazioni di accesso è possibile abilitare e disabilitare le seguenti funzioni:

Allarme silenzioso – utilizzando un codice speciale viene attivata un'azione silenziosa che invia un messaggio di allarme; il dispositivo non emette suoni di allarme durante un allarme silenzioso. L'impostazione del codice speciale per l'allarme silenzioso e la sua esatta funzione vengono effettuate nella configurazione del dispositivo.

Blocca l'accesso – dopo cinque tentativi falliti, il successivo tentativo di accesso sarà consentito solo dopo 30 secondi.

Verifica targa – i veicoli avranno accesso alla zona in base alla verifica della targa su tutti i dispositivi che supportano questa funzione.

Dispositivo

La scheda visualizza una panoramica dei dispositivi aggiunti alla zona specifica. In questa scheda è possibile aggiungere ulteriori dispositivi.

Se vengono utilizzati punti di accesso, i singoli punti di accesso vengono aggiunti alla zona. Il tipo di punto di accesso del dispositivo in questione è descritto come Ingresso di zona.

I metodi di autenticazione disponibili vengono visualizzati per ciascun dispositivo/punto di accesso.

Aziende

La carta gestisce a quali aziende appartiene la zona specificata. Una zona può appartenere a più aziende.

Regole di accesso

Visualizza una panoramica di tutte le regole di accesso già create e offre la possibilità di modificarle o crearle. Creando una regola di accesso, a un gruppo specifico viene consentito l'accesso alla zona. Quando si crea una regola, è necessario inserire un gruppo e un profilo temporale in cui il gruppo dovrà avere accesso alla zona.

La modifica di una regola di accesso può essere effettuata facendo clic sulla regola specifica.

Dispositivo

La pagina Dispositivi mostra tutti i dispositivi aggiunti al suo interno **Access Commander**.

L'elenco può essere filtrato utilizzando sopra l'elenco. In alternativa è possibile impostare filtri per singole colonne nel menu esteso che si apre cliccando su nell'intestazione di ogni colonna. Menù esteso di colonne consente inoltre di spostare le colonne, fissarle alla prima o all'ultima posizione o nasconderle.

I record possono essere scaricati in un file CSV o stampati facendo clic su un pulsante Esportare sopra l'elenco. Nel file CSV esportato l'ora è indicata in GMT+0.

Tramite il tagging è possibile selezionare più dispositivi e applicare ad essi le seguenti azioni collettive:

- Gestisci i dispositivi selezionati
- Rimuovi i dispositivi selezionati dalla gestione
- Esegui il backup dei dispositivi selezionati

Icona sulla linea del dispositivo reindirizza all'interfaccia di configurazione web del dispositivo specificato.

Stati del dispositivo

- Online
- Non gestito
- Incompatibile
- Offline
  - Login failed – In **Access Commander** sono state inserite credenziali di accesso errate per la configurazione web del dispositivo.
  - Non raggiungibile – **Access Commander** non riesce a stabilire una connessione con il dispositivo.
  - Certificato non valido - È richiesta l'autenticazione del certificato SSL e il dispositivo non dispone di un certificato SSL valido.

Aggiunta di un nuovo dispositivo

1. Vai alla pagina **Dispositivo**.
2. Fai clic sul pulsante Aggiungi dispositivo nell'angolo in alto a destra.
3. Nella finestra di dialogo che si apre, cerca il dispositivo nella rete locale o scrivi il suo indirizzo IP e la porta corrispondente nel formato:«Indirizzo: porto»
   Dopo aver inserito l'indirizzo IP del dispositivo è possibile premere INVIO sulla tastiera per inserire un altro dispositivo.
4. Dopo aver inserito tutti i dispositivi che desideri aggiungere, inserisci la password per accedere alla configurazione web di questi dispositivi. È possibile aggiungere solo i dispositivi a cui si accede contemporaneamente con la stessa password.
5. Assegna un nome al dispositivo prima di crearlo.

I dispositivi appena aggiunti vengono visualizzati nell'elenco. Effettuare ulteriori impostazioni del dispositivo nei dettagli del dispositivo.

Blocco di emergenza

Il bloccaggio di emergenza viene utilizzato per bloccare completamente la porta controllata dal dispositivo in questione. Durante il bloccaggio di emergenza non è possibile aprire la porta utilizzando gli accessi utente impostati, anche se l'utente o il visitatore utilizza un accesso valido con un profilo temporale valido.

Il bloccaggio di emergenza può essere attivato/disattivato:

- nel dettaglio del dispositivo – blocca il dispositivo in questione;
- nei dettagli della zona: blocca tutti i dispositivi nella zona;
- nei dettagli dell'azienda: blocca tutti i dispositivi dell'azienda;
- utilizzando l'azione globale nella barra superiore premendo il pulsante  – blocca tutti i dispositivi **Access Commander**;
- nel widget della dashboard.

Nel widget Blocco di emergenza è possibile predefinire un gruppo specifico di dispositivi che potranno essere bloccati in caso di emergenza.

ATTENZIONE
I dispositivi offline, i dispositivi inattivi, i dispositivi con firmware incompatibile e i dispositivi con firmware precedente alla versione 2.32 non verranno bloccati dopo una richiesta di blocco di emergenza. Il dispositivo offline verrà bloccato non appena sarà nuovamente disponibile.

Impostazioni del dispositivo

Le informazioni sul dispositivo possono essere visualizzate e gestite nei dettagli del dispositivo. I dettagli del dispositivo vengono aperti facendo clic sull'elemento del dispositivo selezionato nel loro elenco. A seconda del tipo di dispositivo, i dettagli possono essere suddivisi nelle schede Panoramica, Chiamata e Ascensore.

Dai dettagli del dispositivo è possibile accedere alla configurazione web del dispositivo utilizzando il pulsante **Configurazione hardware** nella parte in alto a destra del dettaglio del dispositivo. La configurazione dei singoli dispositivi è descritta nel relativo manuale di configurazione. È possibile ritornare dall'interfaccia web di configurazione chiudendo la configurazione con una croce nella barra blu superiore.

Panoramica

Stato

Questa scheda mostra lo stato della creazione di connessioni con i dispositivi. I dispositivi online sono quelli con cui ha **Access Commander** connessione stabilita e su cui è caricato il firmware accettato. Grazie alla connessione stabilita con il dispositivo è possibile la sincronizzazione dei dati. Nella pagina è possibile abilitare firmware incompatibile **Dispositivo** > **Firmware**.

La sincronizzazione automatica viene attivata dopo ogni modifica per riflettersi nella configurazione dei dispositivi finali. La sincronizzazione avviene solo sui dispositivi interessati. Solo le richieste innescate da modifiche che possono influenzare i dispositivi finali vengono accodate per la sincronizzazione. Tali modifiche riguardano solitamente i diritti di accesso, i numeri di telefono, i profili temporali utilizzati, ecc. Ad esempio, la modifica del nome di un utente che non è assegnato a nessun gruppo non attiverà la sincronizzazione automatica. La durata della sincronizzazione stessa (proiezione di tutte le modifiche sui dispositivi finali) dipende dal numero di dispositivi da sincronizzare e dalla quantità di dati caricati sul dispositivo.

Controllo di accesso

Imposta la zona a cui appartiene il dispositivo.

Se il dispositivo ha 2 punti di accesso impostati e se il rilevamento del punto di accesso è abilitato (vedi Impostazioni del punto di accesso del dispositivo (p. 48)), viene visualizzata l'opzione per assegnare 2 zone. Un punto di accesso del dispositivo può trovarsi solo in una zona.

Configurazione

La scheda visualizza la versione corrente del firmware, l'indirizzo MAC e l'indirizzo IP e consente di modificare la password per accedere alla sua configurazione web.

Controllo della porta

Questa scheda visualizza le riprese delle telecamere del dispositivo e consente l'apertura remota dell'interruttore della porta controllato dal dispositivo. L'apertura della porta per un certo tempo può essere impostata nel menu esteso, che si apre cliccando su .

Lo stato attuale dell'interruttore della porta viene visualizzato accanto al pulsante Aprire.

Viene utilizzato per bloccare le porte anche per i gruppi con accesso valido Blocco di emergenza (p. 38).

Backup

Permette il backup della configurazione dell'interfono in un file xml. Il backup viene avviato utilizzando Avvia il backup. L'ultimo backup viene visualizzato nella scheda da cui è possibile scaricare il file di backup. Il dispositivo può essere sincronizzato automaticamente con l'ultimo backup utilizzando il menu v Ristabilire. In questo menu è possibile sincronizzare il dispositivo secondo un backup memorizzato su un altro dispositivo.

NOTA
È possibile eseguire il backup di tutti i dispositivi disponibili (dispositivi online e dispositivi collegati con firmware incompatibile).

Chiamata

Questa scheda viene visualizzata nel dettaglio del dispositivo da cui è possibile effettuare le chiamate.

Visualizzazione della rubrica

La scheda Contatti gestisce la visualizzazione della rubrica sui dispositivi dotati di display. La scheda visualizza l'albero dei contatti così come appare nella rubrica del dispositivo. Cliccando su Alterare si aprirà una finestra di dialogo per la modifica dell'albero dei contatti. Nella parte sinistra della finestra di dialogo aperta viene visualizzato l'ordinamento delle cartelle dei contatti. Nella parte destra vengono impostati i contatti all'interno della cartella selezionata. La cartella principale è la prima pagina che appare quando apri la directory sul tuo dispositivo. I contatti verranno visualizzati tutti in una pagina della rubrica se sono tutti archiviati in questa cartella principale. I contatti possono essere ulteriormente raggruppati in cartelle e ordinati nella cartella principale.

Aggiunta di contatti al display del dispositivo

1. Vai a **Dispositivo** > dettaglio dispositivo > **Scheda Chiamate** > **Scheda Contatti**.
2. Aprire la gestione dello schermo facendo clic su Alterare.

3. Nella parte destra della finestra di dialogo aperta, seleziona la cartella a cui desideri aggiungere i contatti.
   Puoi aggiungere alla cartella:

   1. **Utenti**
      È possibile selezionare più utenti contemporaneamente.
   2. **Gruppi**
      Gli utenti possono essere aggiunti alla cartella in massa per gruppo. Ogni utente del gruppo verrà visualizzato sotto il suo nome nella directory. È possibile selezionare più gruppi contemporaneamente.
   3. **Chiamare i gruppi**
      I gruppi di chiamata sono gruppi di contatti che verranno chiamati contemporaneamente. Quando si crea un gruppo di chiamata è necessario inserire il suo nome, con il quale il gruppo di chiamata verrà visualizzato nella rubrica. I contatti dell'utente vengono aggiunti a un gruppo di chiamata proprio come i contatti vengono aggiunti alle cartelle.
      Puoi rinominare il gruppo di chiamata nel menu esteso accanto alla cartella, che si apre facendo clic su .

4. Puoi rinominare la cartella nel menu avanzato della cartella, che puoi aprire facendo clic su . Nel menu esteso è possibile aggiungere alla cartella specificata un'immagine che verrà poi visualizzata sul dispositivo per questa cartella.

5. Appunta le cartelle o i gruppi di chiamata che vuoi che appaiano ai primi posti nel menù esteso per la cartella specificata utilizzando  .

Altri numeri virtuali

Su un dispositivo dotato di tastierino numerico è possibile avviare una chiamata in uscita inserendo un numero virtuale. In questa scheda è possibile aggiungere utenti che potranno chiamare numeri virtuali, anche se questi utenti non hanno accesso al dispositivo. Le chiamate verso numeri virtuali di utenti che hanno accesso al dispositivo sono consentite automaticamente.

Quando si selezionano gli utenti, vengono visualizzati solo gli utenti che hanno un numero virtuale compilato.

Pulsanti

Questa scheda viene visualizzata nel dettaglio dei dispositivi dotati di pulsanti che possono essere utilizzati per comporre i numeri di telefono degli utenti. Nella scheda Pulsanti, i singoli utenti vengono assegnati ai singoli pulsanti sul dispositivo. Premendo un pulsante sul dispositivo si avvia una chiamata in uscita verso la destinazione dell'utente assegnato. L'utente viene assegnato al pulsante facendo clic su  e selezionando l'utente.

Sollevare

Utilizzando la connessione del modulo relè Axis A9188 A Citofono IP 2N (2N Verso IP,2N Force IP,2N IP Safety IP, 2N IP Vario) o a Access Unit l'accesso ai singoli piani dell'edificio può essere controllato tramite un ascensore. A uno Citofono IP 2N di chi Unità di accesso è possibile collegare un massimo di questi 5 moduli relè, mentre ciascuno dei moduli può controllare 8 piani, ovvero un massimo di 40 piani in totale. Per utilizzare questa funzione è necessario disporre di una licenza attiva per Citofoni IP 2N (codice ordine 9137916) e licenza Access Unit (ordine n. 9160401).

Impostazioni di controllo dell'ascensore

1. Vai ai dettagli del dispositivo che dovrebbe controllare l'accesso ai singoli piani. Nel menu esteso nell'intestazione, attiva il controllo dell'ascensore. Verrà visualizzata una scheda nei dettagli del dispositivo **Sollevare**.

2. Nell'intestazione dei dettagli del dispositivo, vai a configurazione hardware dispositivo. Nella sezione Hardware > Controllo ascensore, accendi i moduli che dovrebbero controllare l'accesso dall'ascensore. Se i moduli richiedono l'autenticazione, inserire un nome utente e una password. Salva le impostazioni. Uscire dalla configurazione hardware utilizzando la croce nella barra blu superiore.
3. Vai alla scheda Ascensore nei dettagli del dispositivo.
4. Nella scheda Piano ascensore, seleziona l'uscita relè per il piano a cui vuoi impostare l'accesso. L'etichettatura delle uscite è nel formato: *output io_module_relay*. Clicca su .
5. Nella finestra di dialogo aperta, assegnare un nome al piano e selezionare la zona inserita in quel piano. Solo gli utenti autorizzati ad accedere alla zona secondo le regole di accesso definite potranno accedere a questo piano. Se l'ingresso al piano non è regolamentato dalle regole della zona, spuntare la casella **consentito l'accesso del pubblico**. Selezionando un profilo temporale, si limita l'accesso pubblico solo all'orario definito dal profilo temporale selezionato. Al di fuori di tale fascia oraria l'ingresso sarà nuovamente consentito solo agli utenti con accesso valido in base alle regole di accesso.

ATTENZIONE
Se l'accesso è impostato secondo le regole di accesso della zona, il dispositivo dell'ascensore non assume nessun'altra impostazione di questa zona (codice PIN, autenticazione multipla, allarme silenzioso, ...).

Pavimento
Una volta abilitata, questa scheda visualizza un elenco di tutti i piani configurabili. Ogni piano ha la propria designazione nell'ordine del modulo e dell'uscita relè. Ad ogni piano può quindi essere assegnato il proprio nome.

Moduli
Questa scheda visualizza tutti i moduli AXIS A9188 collegati e i relativi stati correnti.

Monitoraggio
La pagina viene utilizzata per trovare informazioni sui dispositivi collegati. Ogni amministratore può impostare la tabella in base alle proprie esigenze utilizzando . L'impostazione è unica per ciascun account. Le impostazioni vengono effettuate selezionando le colonne visualizzate.

Cliccando sulla riga si accede al dettaglio del dispositivo in questione.

Firmware
La pagina Firmware garantisce un aggiornamento di massa del firmware dei singoli tipi di dispositivi collegati e aiuta quindi a mantenerli in condizioni ottimali. La gestione in blocco dei dispositivi può essere sospesa. Facoltativamente, alcuni dispositivi possono essere esclusi dalla gestione del firmware in blocco.

La versione attuale del firmware è disponibile online tramite il 2N Update Server, opzionalmente è anche possibile caricare manualmente il file di aggiornamento. La distribuzione di una nuova versione è sempre soggetta all'approvazione dell'amministratore, che ha quindi il pieno controllo sul processo di aggiornamento.

La versione con gestione di massa visualizza un elenco dei tipi collegati di citofoni IP 2N, unità di risposta 2N e unità di accesso 2N.

SUGGERIMENTO
La nuova versione del firmware può essere prima implementata su uno o più dispositivi selezionati in modalità test e solo successivamente consentire l'aggiornamento di altri dispositivi.

Esclusione del dispositivo

I dispositivi possono essere esclusi dalla gestione in blocco del firmware aggiungendoli all'elenco nella scheda Dispositivi > Firmware > Dispositivi esclusi.

Versione firmware incompatibile

Quando aggiungi o aggiorni un dispositivo che non dispone di firmware compatibile, quel dispositivo entrerà in uno stato incompatibile. Uno stato incompatibile significa che i nuovi utenti non vengono memorizzati sul dispositivo. Inoltre vengono scaricati gli eventi dal dispositivo ed è possibile utilizzare la configurazione o il backup del dispositivo. Viene creata una nuova voce nella tabella e l'amministratore ha la possibilità di consentire l'utilizzo di firmware incompatibile.

Access Commander disabilita automaticamente i dispositivi con firmware non supportato dalla versione corrente. La scheda visualizza queste versioni firmware non supportate sui dispositivi collegati. Di seguito è riportato l'elenco delle versioni firmware supportate.

Access Commander può controllare tutti i dispositivi utilizzando una versione firmware non supportata se tale versione è approvata. L'approvazione viene effettuata nella scheda Dispositivo > Firmware > Versione firmware incompatibile utilizzando l'icona .

ATTENZIONE
L'approvazione di una versione non supportata può causare problemi come la perdita di dati o impedire in altro modo il corretto funzionamento.

Versioni firmware supportate

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

Sicurezza

Dopo aver abilitato la verifica del certificato SSL, la sincronizzazione avverrà solo sui dispositivi dotati di un certificato SSL firmato da un'autorità attendibile. La sincronizzazione del dispositivo senza tali certificati SSL verrà disabilitata.

Affinché l'autenticazione abbia esito positivo, i certificati del dispositivo devono essere firmati da una CA e contenere l'indirizzo IP o il nome di dominio del dispositivo. Il certificato dell'autorità di firma deve essere considerato attendibile dal server su cui è in esecuzione**Access Commander**. I certificati del dispositivo devono essere caricati tramite l'interfaccia web del dispositivo (Sistema > Certificati > Certificati personali) e impostati come certificato server HTTPS in Servizi > Server Web > Impostazioni avanzate.

ATTENZIONE
Sul dispositivo 2N Indoor Touchnon può caricare i propri certificati SSL, dopo aver abilitato la verifica del certificato la connessione con essi verrà persa.

Impostazioni del punto di accesso del dispositivo

Dispositivo (Citofono 2N O Unità di accesso 2N) può avere fino a due punti di accesso. Ogni punto di accesso consente il passaggio in una direzione. I punti di accesso distinguono la direzione del passaggio attraverso il dispositivo. Ad ogni punto di accesso possono essere assegnati uno o più lettori che sono collegati al dispositivo e funzionano in direzione del punto. I punti di accesso vengono utilizzati per registrare l'ingresso o l'uscita da una zona. Il loro utilizzo è necessario se il dispositivo si trova all'interfaccia tra due zone.

I punti di accesso vengono utilizzati anche per tenere traccia degli utenti nel modulo Presenza (p. 52). I punti di accesso vengono utilizzati anche per monitorare l'ingresso e l'uscita Restrizioni di zona (p. 54).

NOTA
Impostazione dei singoli punti di accesso in **Access Commander** è prescritto nell'interfaccia web del dispositivo nella sezione Servizi > Controllo accessi:

- Punto di accesso 1 = Regole di arrivo
- Punto di accesso 2 = Regole di uscita

Configurazione dei punti di accesso

1. Accedere all'interfaccia di configurazione web del dispositivo.

   SUGGERIMENTO

   È possibile accedere all'interfaccia di configurazione web facendo clic su nell'elenco nella pagina Dispositivi.

2. Vai alla sezione Hardware > menu Moduli di espansione.
3. Individuare il modulo di accesso da utilizzare come Punto di accesso 1 (Arrivo) o Punto di accesso 2 (In uscita).
4. Nel parametro Porta, impostare la direzione desiderata e salvare le impostazioni.
5. Vai alla pagina Zone v **Access Commander**.
6. Nell'angolo in alto a destra, premi e abilitare l'uso dei punti di accesso.

Regole di accesso

Le regole di accesso sono uno strumento per gestire in modo chiaro l'accesso dei gruppi di utenti alle zone. L'accesso può essere concesso in base ai profili temporali.

Le regole di accesso determinano CHI ha accesso, DOVE e QUANDO.

- **CHI** è determinato dal gruppo e dagli utenti ad esso assegnati (un utente può far parte contemporaneamente di più gruppi appartenenti a una società).
- **DOVE** è determinato dalla zona o dai dispositivi (un dispositivo può trovarsi solo in una zona alla volta).
- **QUANDO**è determinato dal profilo temporale assegnato. Questo articolo è facoltativo. Un profilo temporale non compilato significa accesso illimitato (24 ore su 24, 7 giorni su 7).

NOTA
Un gruppo può avere accesso a più zone, così come più gruppi possono avere accesso a una zona.

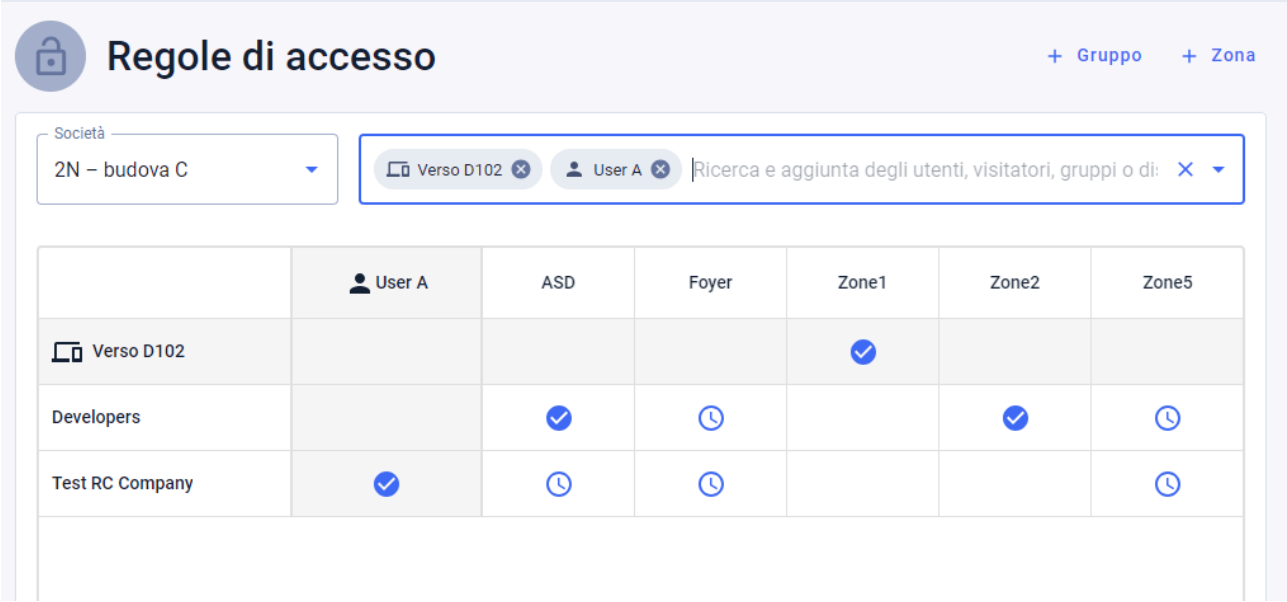
Visualizzazione a matrice

La visualizzazione a matrice delle regole nella pagina Regole di accesso mostra una panoramica degli accessi e ne consente l'impostazione. La matrice è disponibile per ogni azienda esistente e mostra tutti i gruppi e le zone ad essa assegnati. L'amministratore può cambiare azienda nel menu sopra la matrice.

Facendo clic sulla cella corrispondente alla zona e al gruppo selezionati si imposta l'accesso del gruppo alla zona. Apparirà un menu in cui potrai scegliere tra l'accesso illimitato o l'accesso limitato da un profilo temporale. I profili temporali devono essere preimpostati nella pagina Profili temporali (p. 46). Se necessario è possibile aggiungere un nuovo gruppo o zona alla matrice aziendale.

Nel campo di ricerca sopra la matrice è possibile aggiungere utenti o dispositivi alla matrice. Gli utenti possono essere aggiunti a un gruppo attraverso l'intersezione di utente e gruppo. Intersecando un dispositivo e una zona, i dispositivi vengono aggiunti alla zona.

Un esempio di visualizzazione a matrice



L'immagine offre una panoramica della matrice per l'azienda 2N Telekomunikace as. Dalla panoramica risulta chiaro che:

- Il dispositivo filtrato Verso 2.0 D102 fa parte della Zona1.
- L'utente filtrato Utente A fa parte del gruppo Test RC Company.
- Gli utenti del gruppo Sviluppatori hanno accesso illimitato alle zone ASD e Zona2, accesso limitato alle zone Foyer e Zona5 (secondo il profilo orario impostato) e non hanno accesso alla zona Zona1.
- Gli utenti del gruppo Azienda RC Prova hanno accesso limitato alle zone ASD, Foyer e Zona5 (secondo il profilo orario impostato) e non hanno accesso alle zone Zona1 e Zona2.

Elenco delle regole

La pagina Elenco regole visualizza un elenco di tutte le regole di accesso attualmente valide. Fare clic sulla regola per modificarla. È possibile aggiungere una nuova regola di accesso facendo clic sul pulsante Aggiungi nell'angolo in alto a destra. Prima di creare, è necessario impostare i parametri della regola.

Sia l'elenco delle regole che la matrice visualizzano le stesse regole di accesso. Una modifica in una vista viene automaticamente copiata nell'altra vista. Le regole di accesso vengono regolate anche nelle impostazioni di zona e di gruppo.

Profili temporali

Le funzioni intercom selezionate possono essere limitate nel tempo. Alle funzioni menzionate può essere assegnato un cosiddetto profilo temporale, che determina quando la determinata funzione è disponibile.

I profili temporali possono soddisfare i seguenti requisiti:

- bloccare completamente le chiamate all'utente selezionato al di fuori dell'orario riservato
- bloccare le chiamate verso i numeri telefonici selezionati dell'utente al di fuori dell'orario riservato
- bloccare l'accesso degli utenti al di fuori del tempo assegnato

Ogni profilo orario definisce la disponibilità della funzione a cui è associato tramite un calendario settimanale. Puoi facilmente impostare l'ora da-a ed eventualmente giorni della settimana in cui la funzionalità dovrebbe essere disponibile. La determinazione dell'accesso utilizzando il profilo temporale è impostata dalle regole di accesso. La limitazione della disponibilità dell'utente al di fuori del profilo temporale viene impostata insieme al numero di telefono dell'utente.

Opzionalmente si possono creare fino a 20 profili temporali generali che, oltre al controllo degli accessi, possono essere utilizzati anche per casi particolari di configurazione locale. Questi profili temporali vengono caricati su tutti i dispositivi sincronizzati.

Creazione di un profilo temporale

1. Vai alla pagina **Profili temporali**.
2. Fare clic sul pulsante per aggiungere un profilo temporale nell'angolo in alto a destra.
3. Nella finestra di dialogo aperta, impostare il nome del profilo temporale.
4. Seleziona un'opzione per scegliere un limite di tempo Aggiungi fasce orarie. I giorni verdi identificano i giorni che rientrano nel profilo temporale. Il giorno viene selezionato facendo clic. Entro giorni è possibile impostare un intervallo temporale che determina la validità del profilo temporale.
   È possibile impostare orari diversi per ogni giorno solo al momento della creazione del profilo temporale.

Il profilo temporale appena creato viene aggiunto all'elenco e i suoi dettagli vengono aperti, in cui è possibile effettuare ulteriori impostazioni. Nel dettaglio del profilo orario è possibile impostare la posizione del profilo sui dispositivi.

Impostazione del profilo temporale

La suddivisione dei giorni e degli orari viene visualizzata nel dettaglio del profilo orario. Gli intervalli blu mostrano quando il profilo è attivo. È possibile impostare qualsiasi numero di intervalli entro un giorno.

L'intervallo viene aggiunto facendo clic sulla fascia oraria e impostando l'ora esatta in cui il profilo dovrebbe essere attivo. Il tempo di un singolo intervallo può essere modificato facendo clic sull'intervallo. Se si vuole che il profilo sia attivo tutto il giorno è necessario creare un intervallo che copra l'intera giornata cioè 00:00-23:59.

Nel menu esteso che si apre cliccando su ⋮ è possibile impostare la posizione sul dispositivo. La posizione sul dispositivo definisce la posizione nell'elenco dei profili temporali che viene caricato su tutti i dispositivi a cui è assegnato il profilo temporale.

La limitazione della disponibilità dell'utente al di fuori del profilo temporale viene impostata insieme al numero di telefono nelle impostazioni dell'utente.

Partecipazione

Access Commander consente il monitoraggio delle presenze degli utenti. Nella modalità presenza vengono registrati gli orari di ingresso e di uscita dei singoli utenti.

L'impostazione della presenza e la sua modalità viene effettuata in **Impostazioni** > **Configurazione** > **la scheda Partecipazioni**, Vedere Impostazioni di partecipazione (p. 47).

ATTENZIONE
Per il corretto funzionamento delle presenze è necessario avere **Access Commander**licenza attiva disponibile per monitorare la presenza dell'utente. Il rilevamento delle presenze deve essere attivato nelle impostazioni del singolo utente.

La pagina delle presenze offre un elenco di utenti con presenze monitorate. C'è un'icona nell'angolo in alto a destra , con il quale è possibile scaricare un file CSV con i dati riepilogativi sulle presenze di tutti gli utenti. Durante lo scarico dei dati è necessario inserire il periodo temporale per il quale si vogliono generare le presenze.

Partecipazione di un utente specifico

È possibile selezionare un utente specifico dall'elenco di utenti nella pagina Partecipazione e visualizzare informazioni più dettagliate solo sulla sua partecipazione. L'elenco mostra solo gli utenti per i quali è abilitato il rilevamento delle presenze, vedere Utenti (p. 28).

Nella parte superiore dell'estratto conto è possibile selezionare il mese per il quale si desidera visualizzare le presenze. Accanto alla selezione del mese vengono visualizzati il fondo di lavoro impostato per il mese in questione, il saldo e le ore lavorate.

C'è un menu di espansione accanto al nome dell'utente consentendo il download dei dati sulle presenze dell'utente visualizzato in un file CSV o PDF. Entrambi i file contengono registrazioni di singoli giorni.

SUGGERIMENTO
E' possibile inoltre visualizzare le presenze dell'utente nell'anagrafica dell'utente, a cui si accede selezionandolo dall'elenco degli utenti presente nella pagina **Utenti**.

Modifica la presenza dell'utente

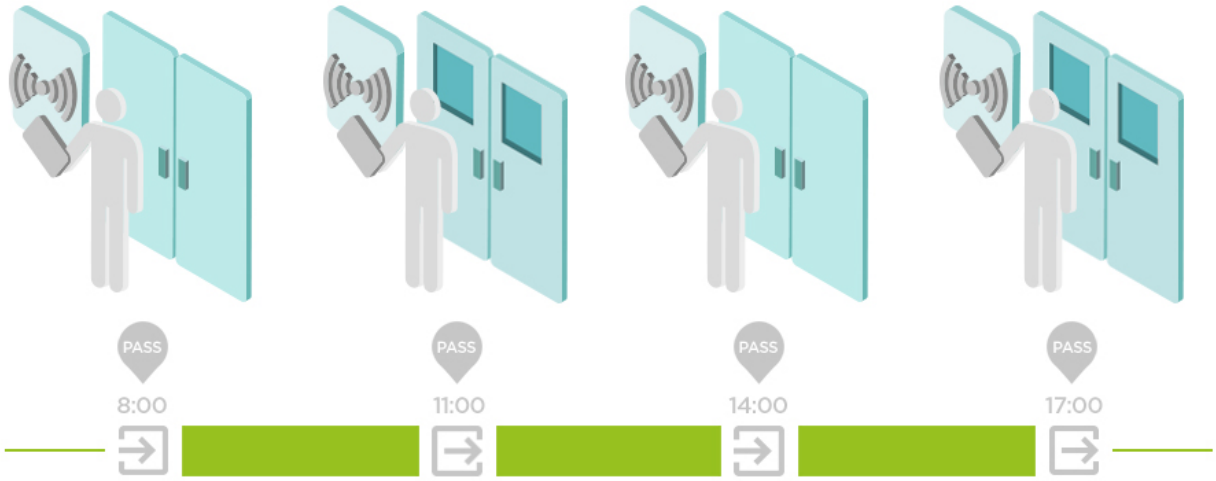
Il responsabile delle presenze può modificare i dati sulle presenze degli utenti. La modifica viene effettuata facendo clic sull'intervallo di tempo da modificare. Una volta aperti, è possibile modificare i tempi limite e aggiungere una nota all'intervallo.

Impostazioni di partecipazione

Access Commander consente il monitoraggio delle presenze degli utenti. Nella modalità presenza vengono registrati gli orari di ingresso e di uscita dei singoli utenti.

Modalità di partecipazione

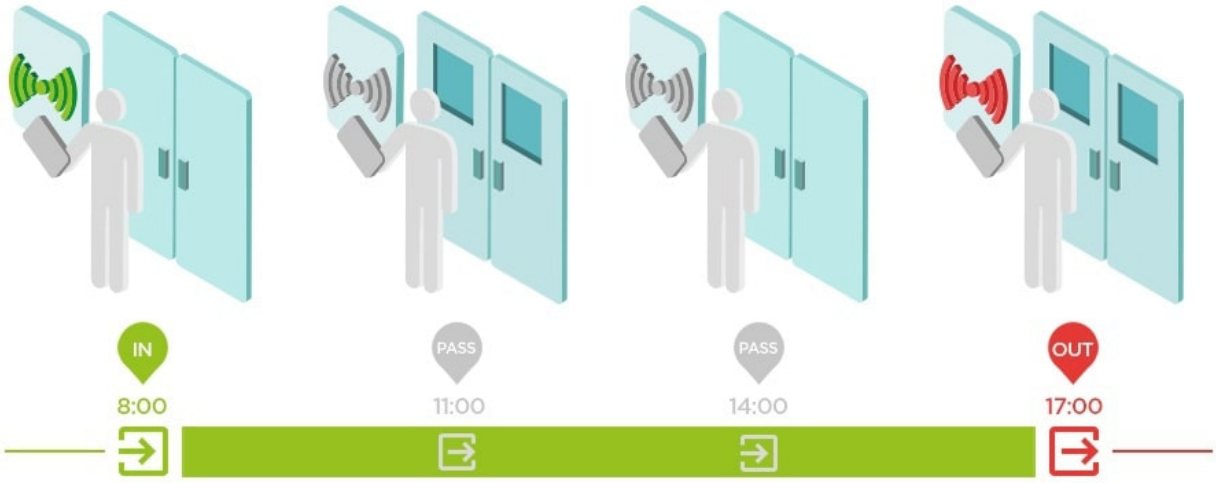
- **FREE**



Gli arrivi e le partenze vengono conteggiati dalla prima e dall'ultima autenticazione dell'utente su qualsiasi dispositivo in un giorno. Il modulo presenza non funziona in questa modalità.

- **IN-OUT**

I dispositivi in entrata e in uscita devono essere impostati per il corretto funzionamento.



- **IN-OUT per tutti i dispositivi**
  Questa modalità consente il monitoraggio della presenza. Gli arrivi vengono registrati sui dispositivi in entrata, le partenze vengono registrate sui dispositivi in uscita. Il movimento tra le zone non viene registrato come arrivo/partenza.
- **IN-OUT per i dispositivi selezionati**
  Questa modalità consente il monitoraggio della presenza. Gli arrivi e le partenze vengono registrati sui dispositivi selezionati impostati come arrivi o partenze. Arrivi e partenze vengono registrati solo su questi dispositivi selezionati. In questo modo è possibile impostare la registrazione dell'arrivo/partenza solo all'ingresso principale dell'edificio.

Impostazioni del punto di accesso del dispositivo

Dispositivo (Citofono 2N O Unità di accesso 2N) può avere fino a due punti di accesso. Ogni punto di accesso consente il passaggio in una direzione. I punti di accesso distinguono la direzione del passaggio attraverso il dispositivo. Ad ogni punto di accesso possono essere assegnati uno o più lettori che sono collegati al dispositivo e funzionano in direzione del punto. I punti di accesso vengono utilizzati per registrare l'ingresso o l'uscita da una zona. Il loro utilizzo è necessario se il dispositivo si trova all'interfaccia tra due zone.

I punti di accesso vengono utilizzati anche per tenere traccia degli utenti nel modulo Presenza (p. 52). I punti di accesso vengono utilizzati anche per monitorare l'ingresso e l'uscita Restrizioni di zona (p. 54).

NOTA
Impostazione dei singoli punti di accesso in **Access Commander** è prescritto nell'interfaccia web del dispositivo nella sezione Servizi > Controllo accessi:

- Punto di accesso 1 = Regole di arrivo
- Punto di accesso 2 = Regole di uscita

Configurazione dei punti di accesso

1. Accedere all'interfaccia di configurazione web del dispositivo.

   SUGGERIMENTO

   È possibile accedere all'interfaccia di configurazione web facendo clic su nell'elenco nella pagina Dispositivi.

2. Vai alla sezione Hardware > menu Moduli di espansione.
3. Individuare il modulo di accesso da utilizzare come Punto di accesso 1 (Arrivo) o Punto di accesso 2 (In uscita).
4. Nel parametro Porta, impostare la direzione desiderata e salvare le impostazioni.
5. Vai alla pagina Zone v **Access Commander**.
6. Nell'angolo in alto a destra, premi e abilitare l'uso dei punti di accesso.

Visite

In **Access Commander**è possibile creare profili di visitatori che hanno privilegi di accesso per un tempo limitato. Durante la visita è possibile aggiungere la tessera di accesso, il codice di accesso e compilare la targa del veicolo. Per la visita non verranno conteggiate le presenze. Il numero di visite non è limitato da alcuna licenza.

Impostazione della conservazione dei dati dei visitatori

L'amministratore può impostare il periodo di conservazione dei dati dei visitatori. Il periodo di conservazione dei dati dei visitatori è impostato in giorni facendo clic sull'icona  accanto al pulsante per creare una nuova visita.

Una volta scaduto l'intervallo di tempo della visita e il periodo di conservazione dei dati impostato, le visite vengono automaticamente cancellate ogni mezzanotte. Le visite a cui sono ancora assegnate le carte visitatore non verranno cancellate.

NOTA
Le impostazioni possono essere utilizzate per conformarsi alle normative locali sulla protezione dei dati. Il nome della visita e la nota verranno conservati nel registro degli accessi in base alle impostazioni di durata nella gestione del registro.

Creazione di una nuova visita

1. Vai alla pagina **Visite**.
2. Fai clic sul pulsante Aggiungi visita nell'angolo in alto a destra.
3. Nella finestra di dialogo che si apre, è necessario inserire il nome della visita, selezionare il gruppo visitato e impostare l'inizio e la fine della visita. Se non imposti l'inizio e la fine della visita, l'intervallo di tempo per l'accesso alla visita inizierà immediatamente e terminerà a fine giornata.

   ATTENZIONE
   L'intervallo temporale per l'accesso alla visita non deve superare il mese.
4. Prima di creare una visita è possibile impostare le modalità di autenticazione che la visita utilizzerà per l'accesso.

La visita appena creata viene visualizzata nell'elenco. Nei dettagli della visita è possibile aggiungere modalità di autenticazione alla visita e gestirne l'accesso.

Fine della visita

Trascorso l'intervallo di tempo scade l'accesso per la visita.

Se l'amministratore o l'amministratore termina la visita utilizzando il pulsante FINE nella scheda Accesso nelle impostazioni della visita, l'accesso a questa visita verrà immediatamente bloccato. Un pulsante Interrompi è disponibile per un visitatore la cui visita è stata interrotta automaticamente perché il fuso orario potrebbe essere diverso sui dispositivi. Può succedere che mentre un visitatore non abbia un accesso valido

su un dispositivo, lo abbia comunque su un altro. Ciò accade se per il dispositivo sono impostati fusi orari diversi.

Se ad una visita è stata assegnata una tessera visitatore, la tessera verrà svincolata e potrà essere utilizzata per un'altra visita.

Visita le impostazioni

Le informazioni sulla visita possono essere visualizzate e modificate nei dettagli della visita. I dettagli della visita si aprono facendo clic sulla visita selezionata nell'elenco.

Si avvicina

La scheda accessi visualizza il gruppo di accesso e l'intervallo di tempo durante il quale la visita ha un accesso valido. L'intervallo di tempo per l'accesso alla visita può essere reimpostato scegliendo Reimposta visita nel menu esteso .

In questa scheda è possibile terminare la visita, vedi Fine della visita (p. 50).

Visita

La scheda mostra la persona visitata e l'azienda visitata. È possibile cambiare la persona visitata.

In questa scheda è possibile aggiungere una nota alla visita.

Dati personali

La scheda visualizza i dettagli di contatto della visita e consente di modificarli. L'e-mail impostata abilita l'invio dei codici di autenticazione.

Autenticazione

Durante la visita è possibile aggiungere la tessera di accesso, il PIN o il QR code di accesso e compilare la targa del veicolo. È possibile inserire una sola targa per visita. È possibile assegnare una tessera di accesso visitatore alla visita, vedi Carte (p. 51).

Durante la compilazione dell'indirizzo e-mail è possibile inviare all'indirizzo indicato il codice PIN/QR di accesso generato.

La tessera visitatore assegnata può essere restituita qui.

Registro degli accessi

Il registro degli accessi visualizza la cronologia degli accessi.

Carte

La sottopagina Carte viene utilizzata per gestire le carte di accesso dei visitatori disponibili per l'aggiunta a una visita. Una nuova carta viene aggiunta utilizzando il pulsante Aggiungi nell'angolo in alto a destra.

Le carte devono sempre essere assegnate a un'azienda. La carta può essere utilizzata solo per le visite che visiteranno questa azienda.

Una tessera esistente può essere sovrascritta o eliminata selezionandola nel menu esteso .

ATTENZIONE
Non è possibile eliminare una tessera assegnata ad una visita attiva.

Presenza

Il modulo presenza è un'estensione del modulo presenza e viene utilizzato per visualizzare un elenco di utenti che si trovano attualmente nell'edificio. Per il funzionamento del modulo è necessario impostare la modalità presenza IN-OUT v **Impostazioni** > **Configurazione** > **la scheda Partecipazioni**, Vedere Impostazioni di partecipazione (p. 47).

- Se l'ultimo evento dell'utente in un determinato giorno è un arrivo (**IN** evento), è considerato presente.
- Se l'utente attraversa un lettore che ha una direzione impostata non specificata, la zona in cui si trova l'utente cambierà. La stessa cosa accade se passa attraverso il lettore nella modalità**IN**.
- Se l'ultimo Evento del giorno indicato è una partenza (**FUORI** evento), è considerato assente.

ATTENZIONE
Il modulo presenze non funziona se viene utilizzata la modalità FREE all'interno del sistema di rilevazione presenze. È possibile utilizzare solo le impostazioni IN-OUT.

Scadenza della presenza dell'utente

Fare clic sull'icona in alto a destra è impostata la Scadenza presenza utente. La scadenza della presenza dell'utente imposta la cancellazione automatica della scheda di presenza dell'utente nel caso in cui l'utente dimentichi di contrassegnare la sua partenza. Questo limite temporale è espresso in ore e determina quanto tempo dopo l'ultimo passaggio dell'utente presente, la sua registrazione di presenza verrà automaticamente cancellata. L'impostazione di questo limite di tempo consente di definire per quanto tempo un record di presenza può rimanere nel sistema se l'utente non viene contrassegnato come assente. Ciò garantisce che l'elenco degli utenti presenti rimanga aggiornato e non contenga record di utenti che hanno già lasciato l'edificio e hanno dimenticato di disconnettersi.

Rapporti

È possibile scaricare i dati di riepilogo sugli utenti aggiunti dalla pagina Report. I file scaricati sono in formato CSV (Comma-Separated Values). Il nome del file indica sempre la data e l'ora in cui è stato generato il report.

NOTA
Alcuni programmi di fogli di calcolo utilizzano separatori diversi e il file CSV potrebbe non essere visualizzato correttamente quando viene aperto al loro interno. In questi casi, si consiglia di importare i dati dal file CSV in una cartella di lavoro aperta.

- **Mobile Key** – Utenti associati e non associati con tempo di associazione rimanente
  Il rapporto elenca i dati sullo stato dell'associazione dell'utente tramite l'applicazione Mobile Keyo dati sul periodo di validità del codice di abbinamento attivo.
- **Utenti** – Regole di accesso con gruppi, zone, dispositivi e profili orari
  Il report elenca i dati sull'assegnazione degli utenti ai gruppi, il loro accesso alle zone e ai dispositivi nelle zone e i profili temporali in cui agli utenti è consentito l'accesso. Ogni combinazione è elencata esattamente su una riga della tabella.
- **Utenti** – Esportazione dettagliata
  Il report elenca tutte le informazioni sugli utenti inserite nei loro profili, compresi i dati personali e di accesso.

  ATTENZIONE
  Il file contiene dati sensibili!
- **Utenti** – Esportazione della sincronizzazione globale
  Il report elenca i dati sull'assegnazione degli utenti ai gruppi, il loro accesso alle zone e ai dispositivi nelle zone e i profili temporali in cui agli utenti è consentito l'accesso. Ogni combinazione è elencata esattamente su una riga della tabella.
  Questo report può fungere da file CSV per la sincronizzazione degli utenti, vedere Sincronizzazione degli utenti con FTP (p. 60).

  ATTENZIONE
  Il file contiene dati sensibili!

Restrizioni di zona

Le restrizioni di area vengono utilizzate per definire le aree in cui è possibile utilizzare le funzioni Anti-passback e Occupazione.

Queste misure migliorano il livello di protezione e prevengono potenziali minacce alla sicurezza. Più specificamente, aiutano a prevenire l'ingresso non autorizzato in luoghi selezionati, consentono di tracciare i movimenti delle persone all'interno di un determinato spazio e registrano le entrate e le uscite, il che può essere utile per monitorare e analizzare gli eventi di sicurezza.

L'elenco mostra le aree create nel sistema. In questa scheda è possibile creare, eliminare aree e accedere ai loro dettagli. Allo stesso tempo permette di disattivare l'area e visualizzarne lo stato.

Crea un'area riservata

1. Vai alla pagina **Restrizioni di zona**.
2. Fare clic sul pulsante per aggiungere una regione nell'angolo in alto a destra.
3. Nella finestra di dialogo aperta, assegnare un nome all'area.
4. Nel dettaglio dell'area aperta, aggiungi un dispositivo all'area. I dispositivi vengono aggiunti utilizzando il pulsante nell'intestazione dei dettagli dell'area.
   L'area appena creata apparirà nell'elenco. Nel dettaglio è possibile impostare i dispositivi di ingresso e uscita, impostare l'occupazione consentita, attivare la funzione anti-passback e bloccare l'accesso all'area per gli utenti selezionati.

Impostazione delle restrizioni di zona

Un nuovo dispositivo viene aggiunto all'area utilizzando il pulsante nell'intestazione dei dettagli dell'area.

Ingresso e uscita

Queste carte indicano quali dispositivi vengono instradati come ingresso o uscita in una determinata area.

Utilizzando il menu esteso sotto i dispositivi possono essere spostati tra le schede o rimossi dall'area.

Autenticando l'utente al dispositivo di ingresso viene registrato l'ingresso nell'area. Autenticandosi al dispositivo di uscita, l'utente esce dall'area. In questo modo è possibile monitorare se l'utente è ancora nell'area e se desidera rientrarvi.

Se il dispositivo aggiunto ha due punti di accesso impostati, ciascun punto può essere utilizzato per una direzione diversa (Ingresso/Uscita). Le impostazioni del punto di accesso sono descritte nel capitolo Impostazioni del punto di accesso del dispositivo (p. 48). Le proprietà del punto di accesso vengono espanse facendo clic sulla freccia.

Occupazione

I dispositivi in entrata e in uscita devono essere impostati per il corretto funzionamento.

La scheda Occupazione consente di monitorare e controllare il numero di persone in un'area. Le restrizioni sull'occupazione aiutano a gestire il numero di persone in un'area. In caso di raggiungimento del limite di occupazione è possibile negare ulteriori accessi oppure registrare solo il superamento del limite. Per questa funzione è necessario un dispositivo di input e output.

Anti-passback

È possibile attivare nell'area la funzione Anti-passback, che garantisce l'estensione del controllo degli accessi attraverso il monitoraggio e l'abuso dei diritti per il rientro nelle aree riservate. Le aree monitorate sono

delimitate da dispositivi di frontiera che immettono o consentono di uscire dai locali. Su questi dispositivi, al passaggio delle persone, l'autorizzazione viene verificata secondo le regole definite per la zona interessata. Dopo aver lasciato l'area attraverso il dispositivo di confine, l'utente può rientrare nell'area solo allo scadere del timeout, se il timeout è impostato. Se l'utente tenta di ritornare nell'area prima, il sistema gli negherà l'accesso o registrerà solo questo evento nel log.

AVVERTIMENTO
Un'area anti-passback perde il suo significato e può essere potenzialmente pericolosa se nell'area è presente un dispositivo con collegato un pulsante REX attivo che consente l'accesso non autorizzato.

Impostazione di un'eccezione

A volte potrebbe essere auspicabile che i termini anti-passback non si applichino a utenti selezionati. In genere si tratta di utenti come l'amministratore dell'edificio, l'amministratore delegato, gli utenti VIP, ecc. Gli utenti o interi gruppi che non dovrebbero essere soggetti alle condizioni anti-passback sono impostati in Impostazioni > Anti-passback > Eccezioni.

NOTA
La sezione Impostazioni è disponibile solo per gli utenti con il ruolo di amministratore.

Elenco degli utenti bloccati

Gli utenti bloccati sono quegli utenti che hanno tentato di accedere all'area Anti-passback prima della scadenza del timeout. Aiuto  è possibile escludere gli utenti dalla lista consentendo loro nuovamente l'accesso all'area.

SUGGERIMENTO
Quando a un utente viene negato l'accesso a causa di un anti-passback attivo, è possibile che all'utente venga inviata un'e-mail informativa automatica. È possibile abilitare l'invio di e-mail in Impostazioni > Anti-passback > Notifica all'utente bloccato tramite la scheda e-mail.

Reimpostazione delle restrizioni

Nella scheda Impostazioni > Anti-passback > Reimposta restrizioni area, vengono impostati i giorni e gli orari in cui il record dell'area verrà eliminato, ad es. tutti gli utenti potranno ripassare indipendentemente dalle precedenti violazioni.

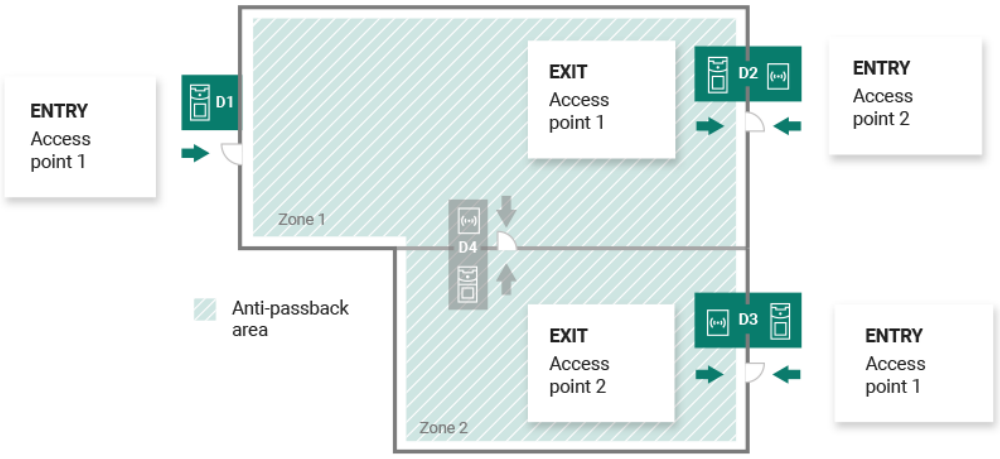
Gli errori di configurazione più comuni

ATTENZIONE
Se si verifica un errore in un'area, l'intera area verrà disabilitata. Verrà riattivato dopo la rimozione degli errori.

I seguenti casi possono impedire il corretto funzionamento delle restrizioni regionali

- Nessun dispositivo viene aggiunto all'area. È necessario assegnare almeno un dispositivo.
- Alcuni dispositivi di input/output non sono configurati correttamente o non contengono un lettore.
- Alcuni dispositivi di ingresso in quest'area sono già utilizzati come ingresso in un'altra area. Per un corretto funzionamento, l'assegnazione deve essere modificata.
- Alcune apparecchiature non sono dotate della necessaria licenza.
- Alcuni dispositivi sono stati disabilitati.
- Alcuni dispositivi sono stati disconnessi.
- Alcuni dispositivi non dispongono di una versione firmware compatibile.
  Alcuni dispositivi sono dotati di un pulsante REX che permette di uscire dall'area APB senza l'autorizzazione dell'utente. Per un corretto funzionamento il pulsante REX deve essere disattivato.

Un esempio di impostazione delle restrizioni



La figura mostra un'area Anti-passback con tre dispositivi di frontiera D1, D2 e D3. Per impostare la funzione Anti-passback vengono utilizzati solo i dispositivi di frontiera. Il dispositivo D4 all'interno dell'area Anti-passback non viene utilizzato per controllare l'ingresso/uscita dall'area. I dispositivi D2 e D3 hanno le direzioni di ingresso e di uscita impostate.

Dispositivo D1 serve solo per entrare nell'area Anti-passback. Il dispositivo è impostato come input.

Dispositivo D2 serve sia per l'input che per l'output. Il dispositivo è dotato di un modulo di espansione predisposto per entrare nell'area e di un'unità principale predisposta per uscire.

Dispositivo D3 serve sia per l'input che per l'output. Il dispositivo è dotato di un'unità principale predisposta per entrare nell'area e di un modulo di espansione predisposto per uscire.

Impostazioni di sistema

Data e ora

Data e ora in **Access Commander** può essere sincronizzato con Internet o impostato manualmente. La modifica del metodo di acquisizione dell'ora può essere effettuata in Impostazioni > Configurazione > scheda Data e ora. Nel caso non lo fosse **Access Commander** connesso a Internet, è necessario impostare manualmente la data, l'ora e il fuso orario. Altrimenti è possibile passare a NTP e ottenere l'ora da un server NTP. In questo caso è sufficiente impostare il fuso orario. Il server NTP aggiorna automaticamente la data e l'ora.

ATTENZIONE
Dopo aver salvato l'ora, modificare se **Access Commander**si riavvia automaticamente.

Sincronizzazione dell'ora con i dispositivi

L'ora sui dispositivi collegati può essere unificata con l'ora **Access Commander**. La condivisione del tempo con i dispositivi viene attivata attivando il parametro Sincronizza con il dispositivo in Impostazioni > Configurazione > scheda Data e ora.

Se la sincronizzazione dell'ora con il dispositivo è attivata, è possibile scegliere tra i seguenti metodi di sincronizzazione:

- **I dispositivi utilizzano lo stesso server NTP** – l'ora sui dispositivi è regolata dal server NTP impostato **Access Commander**.
- **I dispositivi utilizzano Access Commander come server NTP** – controlla l'ora sui dispositivi in base all'ora impostata**Access Commander**.

Impostazioni di rete

Le impostazioni della connessione di rete vengono effettuate in Impostazioni > Configurazione > scheda Rete. La scheda visualizza i parametri di rete correnti **Access Commander** e ne consente l'impostazione. È possibile impostare parametri individuali dopo aver abilitato il metodo di configurazione manuale.

Il metodo di configurazione consente di impostare i parametri di impostazione della rete automaticamente dal server DHCP o manualmente. Quando si modifica l'indirizzo IP impostato automaticamente dal server DHCP in un indirizzo inserito manualmente, il browser web verrà reindirizzato all'indirizzo IP inserito. Verrà eseguito un riavvio dopo il reindirizzamento**Access Commander** ed è necessario accedere nuovamente al sistema.

ATTENZIONE

- Se si modifica il metodo di configurazione in DHCP, si modificherà l'indirizzo IP del server e si potrebbe causare l'interruzione della connessione.
- Se cambi il server proxy HTTP,**Access Commander**si riavvierà automaticamente.

Abilitazione e configurazione della funzione e-mail (SMTP)

La funzione E-mail prevede l'invio di notifiche o l'invio delle password di accesso agli utenti. Le e-mail vengono inviate tramite il protocollo SMTP.

Le impostazioni vengono effettuate in Impostazioni > Configurazione > E-mail.

1. Dopo aver attivato la funzione E-mail, si apre una finestra di dialogo in cui è possibile impostare i seguenti parametri:
   - **Indirizzo del server SMTP**, a cui verranno inviate le email.
   - **Porta del server**, preimpostato su 25.
   - **Nome utente** E **parola d'ordine** all'account sul server SMTP se il server SMTP richiede l'autorizzazione.
   - **Indirizzo mittente predefinito**, da cui verranno inviate le email.
2. Attiva secondo necessità:
   - **SSL** per la crittografia della posta elettronica,
   - **Verifica del certificato del server SSL**,
   - **Modalità di compatibilità** in caso di connessione a server SMTP più vecchi che non supportano le nuove funzioni (GSSAPI).
3. Dopo il salvataggio, puoi configurarlo nella scheda E-mail **Indirizzo di base per i collegamenti e-mail**, che farà parte dei messaggi di posta elettronica inviati e potrà indirizzare i destinatari della posta elettronica alla parte selezionata dell'interfaccia **Access Commander**.
4. Puoi verificare le impostazioni effettuate inviando una email di prova.

Aggiornamento del sistema

Sistema **Access Commander** controlla regolarmente il server di aggiornamento e informa sugli aggiornamenti disponibili e sulle nuove versioni firmware disponibili dei dispositivi collegati. Il controllo automatico degli aggiornamenti può essere disattivato in Impostazioni > scheda Aggiornamenti di sistema.

Installa l'aggiornamento Access Commander

AVVERTIMENTO

Si consiglia di eseguire questa operazione prima di installare l'aggiornamento backup del sistema (p. 59). Eseguire il backup al di fuori dell'orario lavorativo per evitare l'indisponibilità temporanea del sistema per gli utenti.

1. Vai a **Impostazioni** > **Scheda Aggiornamento del sistema**.
2. Se il controllo automatico degli aggiornamenti è disattivato, fare clic su Controlla gli aggiornamenti.
3. Clicca su Scaricamento nel messaggio di informazioni sull'aggiornamento disponibile e confermare il download.
   La scheda informa che l'aggiornamento è pronto per l'installazione.

4. Clicca su Installare nel messaggio informativo e nella finestra di dialogo aperta, confermare l'installazione.
   Dopo aver avviato l'installazione, verrai reindirizzato alla pagina di manutenzione. La pagina di manutenzione informa l'amministratore che ha avviato l'installazione sullo stato in corso dell'installazione. Visualizza le informazioni ad altri utenti che è in corso un aggiornamento. Durante l'installazione non è possibile**Access Commander**iscrizione.
5. Una volta completata l'installazione, fare clic su Vai al login, che ti reindirizzerà alla pagina di accesso.

Beta test

Gli utenti possono scegliere di partecipare al beta testing degli aggiornamenti software **Access Commander** prima del rilascio ufficiale degli aggiornamenti. L'abilitazione viene effettuata in Impostazioni > scheda Aggiornamento sistema > Parametro server di aggiornamento.

AVVERTIMENTO
La versione di prova non è garantita e l'azienda non la fornisce 2N TELEKOMUNIKACE as non è responsabile per limitazioni funzionali e possibili danni derivanti da limitazioni funzionali della versione beta. Le versioni beta vengono fornite solo a scopo di test. La versione beta non è progettata per lavorare con dati importanti.

Una volta abilitate, le versioni beta verranno visualizzate negli aggiornamenti disponibili nella scheda Aggiornamenti di sistema.

AVVERTIMENTO
Dopo l'aggiornamento **Access Commander** non è possibile eseguire il downgrade dell'ultima versione beta a una versione precedente.

Backup del sistema

Nella pagina Impostazioni > scheda Backup del sistema, è possibile eseguire, configurare e controllare il backup e il ripristino dei dati**Access Commander**. I dati possono essere archiviati su storage locale o su Server Message Block (SMB). SMB è adatto per l'archiviazione a lungo termine dei backup.

È possibile eseguire il backup dei dati una volta o automaticamente a intervalli regolari e preimpostati.

Ogni backup può essere ripristinato, scaricato o eliminato nel menu che si espande dopo aver cliccato su ⋮ per un elemento nell'elenco di backup.

Backup dei dati una tantum

1. Vai a **Impostazioni** > **Scheda Backup del sistema**.
2. Nella parte inferiore della scheda, fare clic su Esegui il backup adesso.
3. Selezionare se crittografare i dati del file. In tal caso, inserisci la password che ti sarà richiesta per ripristinare il backup.

Impostazioni di backup automatico dei dati

1. Vai a **Impostazioni** > **Scheda Backup del sistema**.

2. Clicca su nel parametro Backup regolare.
3. Imposta i parametri di backup richiesti:
   - frequenza: l'intervallo che specifica la frequenza con cui verrà eseguito il backup
   - ora: il backup verrà effettuato nel giorno rilevante a quest'ora
   - giorno – giorno della settimana o del mese in cui verrà eseguito il backup
4. Selezionare se crittografare i dati del file. In tal caso, inserisci la password che ti sarà richiesta per ripristinare il backup.

Salvando, i backup verranno eseguiti automaticamente in base alle impostazioni selezionate.

Impostazioni di backup dei dati su SMB

1. Vai a **Impostazioni** > **Scheda Backup del sistema**.
2. Clicca su nel parametro Archiviazione.
3. Seleziona il tipo di archiviazione: SMB.
4. Inserisci l'indirizzo del server, le informazioni di accesso e la versione del protocollo.

Salvando, tutti i backup verranno inviati al Server Message Block impostato.

Ripristina dai dati di backup

1. Vai a **Impostazioni** > **Scheda Backup del sistema**.
2. Apri il menu esteso al backup selezionato e selezionare Ristabilire.

Ripristina da un file di backup

1. Vai a **Impostazioni** > **Scheda Backup del sistema**.
2. Nella parte inferiore della scheda, fare clic su Ripristina da file.
3. Seleziona il file di backup dal tuo archivio e fai clic su Ristabilire.

Trasferisci i dati da un altro Access Commander

1. Vai a **Impostazioni** > **Scheda Backup del sistema**.
2. Nella parte inferiore della scheda, fare clic su Migrare.
3. Immettere l'indirizzo IP dell'Access Commander da cui si desidera trasferire i dati.
4. Compila le credenziali dell'account amministratore di Access Commander da cui desideri trasferire i dati.

ATTENZIONE
Per importare dati da un altro Access Commander, è necessario abilitare il servizio SSH sul server da cui verranno scaricati i dati.

Sincronizzazione degli utenti con FTP

L'elenco degli utenti e le loro impostazioni di base, comprese le assegnazioni ad aziende e gruppi, possono essere sincronizzati utilizzando un file CSV gestito esternamente.

La sincronizzazione viene eseguita in **Impostazioni** > **Scheda Sincronizzazione utente**. Puoi scaricare un file CSV di esempio dalla scheda.

SUGGERIMENTO
L'elenco degli utenti attuali, che corrisponde alla struttura del file CSV di esempio, può essere scaricato dalla pagina Rapporti (p. 53).

Il file CSV preparato può essere importato direttamente sulla carta. Dati dal file con s **Access Commander** inizieranno a sincronizzarsi automaticamente.

Informazioni dettagliate sul risultato di ciascuna sincronizzazione vengono archiviate nel registro di sistema. Il registro stesso contiene informazioni di base sull'esito positivo o negativo della sincronizzazione. Le informazioni dettagliate sono memorizzate in un file che può essere scaricato utilizzando l'icona alla fine della riga.

Sincronizzazione automatica degli utenti con FTP

La scheda Sincronizzazione utente in Impostazioni ti consente di effettuare il collegamento **Access Commander** con l'archivio FTP dove si trova il file CSV con l'elenco degli utenti. La scheda visualizza quindi le informazioni su questo archivio FTP.

1. Clicca su nel parametro Archiviazione.
2. Nella finestra di dialogo aperta, imposta l'indirizzo del server FTP in cui è archiviato il file CSV.
3. Immettere le credenziali per accedere al server FTP.

File CSV

SCARICAMENTO
È possibile scaricare un file CSV di esempio per la sincronizzazione degli utenti utilizzando questo link.

NOTA
Alcuni programmi di fogli di calcolo utilizzano separatori diversi e il file CSV potrebbe non essere visualizzato correttamente quando viene aperto al loro interno. In questi casi, si consiglia di importare i dati dal file CSV in una cartella di lavoro aperta.

Un file CSV ha una determinata struttura che deve essere seguita. Tutti i valori sono separati da una virgola, solo l'elenco dei gruppi è separato da un punto e virgola. Il file CSV ha la seguente struttura:

- EmployeeID: chiave primaria che deve essere compilata. Questo è un identificatore utente univoco.
- User Name – il nome dell'utente creato in Access Commander.
- Company – il nome dell'azienda sotto la quale verrà incorporato l'utente. L'azienda deve essere creata in Access Commander. Le lettere minuscole e maiuscole utilizzate nei nomi di società o gruppi non sono intercambiabili.
- User Mail – indirizzo e-mail dell'utente.
- Card Numbers – il numero della carta dell'utente. È possibile impostare fino a due carte per un utente. I numeri delle singole carte devono essere separati da un punto e virgola (;).
- Switch Code – un codice interruttore, viene sempre creato un codice sotto il primo interruttore.

- Phone Number 1 – numero di telefono in prima posizione.
- Group Call – chiamata di gruppo al numero di telefono impostato sopra. Assume i valori True/False. Se impostato su True, vengono attivate le chiamate di gruppo. Se impostato su False, le chiamate di gruppo sono disabilitate.
- Phone Number 2 – numero di telefono in seconda posizione.
- Group Call – chiamata di gruppo al numero di telefono impostato sopra. Assume i valori True/False. Se impostato su True, vengono attivate le chiamate di gruppo. Se impostato su False, le chiamate di gruppo sono disabilitate.
- Phone Number 3 – numero di telefono in terza posizione.
- Virtual Number – numero virtuale dell'utente.
- Groups – elenco dei gruppi a cui aggiungere l'utente. Tutti i gruppi devono essere stabiliti in Access Commander. L'elenco dei gruppi è separato da un punto e virgola. Le lettere minuscole e maiuscole utilizzate nei nomi di società o gruppi non sono intercambiabili.
- Is Deleted – contrassegna se l'utente deve essere eliminato. Se impostato su FALSE, l'utente viene creato e solo i suoi dati vengono aggiornati durante la successiva sincronizzazione. Se impostato su TRUE, l'utente verrà eliminato alla successiva sincronizzazione. Se impostato su FALSE, l'utente verrà creato nuovamente.
- License Plates – marchi di registrazione. È possibile impostare più targhe, che devono essere separate da un punto e virgola.

Lettori USB abilitati

Per facilitare la registrazione di alcune modalità di autenticazione dell'utente, è possibile utilizzare lettori USB collegati al computer su cui è installato il **Access Commander**. I lettori sono richiesti in **Access Commander** abilitare in Impostazioni > Accesso > scheda Lettori USB consentiti.

L'abilitazione/disabilitazione dell'uso di un dispositivo USB esterno avviene in una finestra di dialogo che si apre facendo clic su Abilita i lettori. Successivamente si modifica il loro permesso cliccando su Alterare.

Access Commander consente l'utilizzo dei seguenti dispositivi USB:

- Lettore di carte RFID 125kHz – Ordine n. 9137420E
- Lettore di carte RFID 13,56 MHz e 125 kHz – Ordine n. 9137421E
- Lettore di impronte digitali - Ordine n. 9137423E
- Lettore Bluetooth USB esterno (dongle) – Ordine n. 9137422E

Chiavi PICard

Le chiavi di crittografia dell'applicazione sono archiviate in Impostazioni > Accesso > scheda Chiavi PICard 2N PICard Commander. Se le chiavi di crittografia sono presenti **Access Commander** caricato, il nome del progetto viene visualizzato nella scheda PICard Commander e un identificatore di esportazione con chiave numerica. La carta consente il caricamento delle chiavi da **Access Commander** eliminare.

ATTENZIONE
Se rimuovi le chiavi PICard, tutte le carte crittografate con tali chiavi smetteranno di funzionare.

Importa chiavi di crittografia PICard

1. Dopo aver cliccato su Importare carica il file della chiave di crittografia dal tuo repository.
2. Inserisci una password per proteggere il file se ne imposti una durante l'esportazione dall'applicazione PICard Commander.

2N PICard Commander è un'applicazione software per crittografare le credenziali sulle carte di accesso. L'applicazione crea progetti che generano un set di chiavi di crittografia e lettura. Le chiavi del lettore

di progetto possono essere importate nei dispositivi 2N o in **Access Command**er, che successivamente garantisce la distribuzione delle chiavi di lettura ai dispositivi 2N collegati.

Chiavi di crittografia per la chiave mobile

Gli utenti possono utilizzare l'app per connettersi con i dispositivi 2N Mobile Key. Comunicazione tra applicazioni Mobile Keyed è sempre crittografato dal dispositivo. Senza la conoscenza della chiave di crittografia, l'applicazione non puòMobile Keyautenticare l'utente. La chiave di crittografia primaria viene generata automaticamente al primo avvio dell'interfono e può essere rigenerata manualmente in qualsiasi momento successivo. La chiave di crittografia primaria viene trasferita insieme all'ID di autenticazione al dispositivo mobile durante l'accoppiamento.

Comunicazione tra applicazioni Mobile Keyed è sempre crittografato dal dispositivo. Senza la conoscenza della chiave di crittografia, l'applicazione non puòMobile Keyautenticare l'utente. La chiave di crittografia primaria viene generata automaticamente al primo avvio dell'interfono e può essere rigenerata manualmente in qualsiasi momento successivo. La chiave di crittografia primaria viene trasferita insieme all'ID di autenticazione al dispositivo mobile durante l'accoppiamento.

IN **Impostazioni > Accesso > scheda Chiavi di crittografia per Mobile Key** è possibile generare fino a 4 chiavi di crittografia. La chiave appena generata viene caricata automaticamente nell'applicazione Mobile Key la prima volta che si utilizza un telefono cellulare con un dispositivo precedentemente associato. Quando si tenta di generare la quinta chiave **Access Commander** avverte che generandola si cancellerà la chiave più vecchia. Sulla tessera sono riportati gli orari di generazione delle singole chiavi.

Se non ha un'applicazione Mobile Key accedere ad una qualsiasi delle chiavi di crittografia valide, non sarà possibile utilizzarla per autenticare l'utente. Per ripristinare la funzionalità dell'applicazione è necessario riassociare l'applicazione al dispositivo connesso **Access Commander**, che caricherà chiavi di crittografia valide nell'applicazione Mobile Key.

NOTA
Consentire l'accesso al dispositivo dipende dai diritti di accesso impostati dell'utente.

Registri CAM

I registri CAM vengono utilizzati per registrare automaticamente diverse immagini precedenti e successive all'evento selezionato. In Impostazioni > Registri CAM, puoi gestire diversi tipi di eventi per i quali devono essere generati i registri CAM.

Ad esempio, i registri CAM possono essere generati ad ogni inserimento della carta. Se qualcuno striscia la tessera, nei log degli accessi verranno registrate 5 immagini prima dello scorrimento e 3 immagini dopo lo scorrimento. I fotogrammi vengono registrati dopo 1 secondo. Per le immagini viene creata una memoria di 1, 3 o 5 GB. Se la memoria è piena, le immagini più vecchie verranno eliminate. I registri di accesso stessi non vengono cancellati.

Creazione di un tipo di registro CAM

1. Vai alla pagina **Impostazioni** > **Registri CAM**.
2. Fai clic sul pulsante Aggiungi nell'angolo in alto a destra della pagina.
3. Immettere un nome per il tipo di evento del registro CAM.

Il tipo di evento del registro CAM appena creato viene visualizzato nell'elenco e si aprono i dettagli nel registro CAM. Nel dettaglio del CAM log è necessario impostare per quali eventi e su quali dispositivi verranno generate le immagini provenienti dalle telecamere.

Impostazione dei loghi CAM

Le informazioni sul tipo di registro CAM possono essere gestite nei dettagli del registro CAM. Il dettaglio del registro CAM si apre cliccando sul registro CAM selezionato nell'elenco o dopo aver creato un nuovo registro CAM.

Eventi guardati

La scheda consente di selezionare un elenco di eventi durante i quali verranno catturate le immagini dalle telecamere.

Gli eventi tracciati possono essere i seguenti:

- **Si avvicina**
  - Utente accettato
  - Targa auto riconosciuta
  - Utente rifiutato
  - Premere il pulsante REX
- **Sicurezza**
  - Interruttore di protezione attivato
  - Apertura porta non autorizzata
  - Apertura porta a distanza
  - Accesso negato - ripetuta immissione errata
  - Allarme silenzioso attivato

Dispositivi monitorati

Si consiglia di impostare la registrazione dei log CAM solo da dispositivi dotati di telecamera. La selezione del dispositivo avviene in una finestra di dialogo che si apre con  . Allo stesso tempo, la scheda consente la registrazione dei log CAM di tutti i dispositivi.

Autenticazione a due fattori

L'autenticazione a due fattori fornisce un livello più elevato di sicurezza dell'account utente in **Accedi al comandante**. Per effettuare il login l'utente inserisce i dati di login e dovrà poi confermare il proprio login tramite l'applicazione di autenticazione. Una volta che l'amministratore attiva la necessità dell'autenticazione a due fattori, all'utente verrà richiesto di collegare il proprio account con la propria applicazione di autenticazione al successivo accesso.

L'autenticazione a due fattori viene impostata dall'amministratore nella scheda Impostazioni > Configurazione > Autenticazione a due fattori. L'amministratore può scegliere a quali utenti verrà richiesta l'autenticazione a due fattori.

Opzioni per richiedere la verifica in due passaggi

- **Opzionale**
  L'autenticazione a due fattori è facoltativa. Gli utenti possono attivarlo da soli sul proprio profilo, vedere Attiva la verifica in due passaggi (p. 64).
- **Obbligatorio per gli utenti con un ruolo**
  Ogni utente a cui è stato assegnato un ruolo deve confermare il proprio accesso utilizzando le applicazioni di autenticazione.
- **Obbligatorio**
  Tutti gli utenti devono confermare il proprio accesso utilizzando un'applicazione di autenticazione.

Attiva la verifica in due passaggi

Se l'amministratore imposta la verifica in due passaggi opzionale, l'utente stesso attiva la verifica in due passaggi come segue:

1. Fare clic sull'icona utente nell'angolo in alto a destra per aprire il menu utente.
2. Seleziona Visualizza profilo.
3. Nella scheda Verifica in due passaggi, colleghi l'account all'applicazione di verifica. Seguire le istruzioni.

Consenti l'accesso SSH

AVVERTIMENTO
L'abilitazione dell'accesso SSH è consigliata solo agli utenti esperti. L'uso improprio costituisce un pericolo per la sicurezza.

In Impostazioni > Configurazione > la scheda SSH viene utilizzata per abilitare Secure Shell, che fornisce una comunicazione remota sicura con la console di sistema. Con il servizio SSH abilitato, puoi eseguire il backup e ripristinare il sistema o eseguire un riavvio completo**Access Commander**.

Per connettere Access Commander Box o una macchina virtuale, il client SSH deve conoscere l'indirizzo IP **Access Commander** e la password di root del sistema. La password root del sistema può essere impostata in Impostazioni > Configurazione > scheda SSH.

NOTA
La modifica della password di root viene eseguita nella console di configurazione, non in Access Commander.

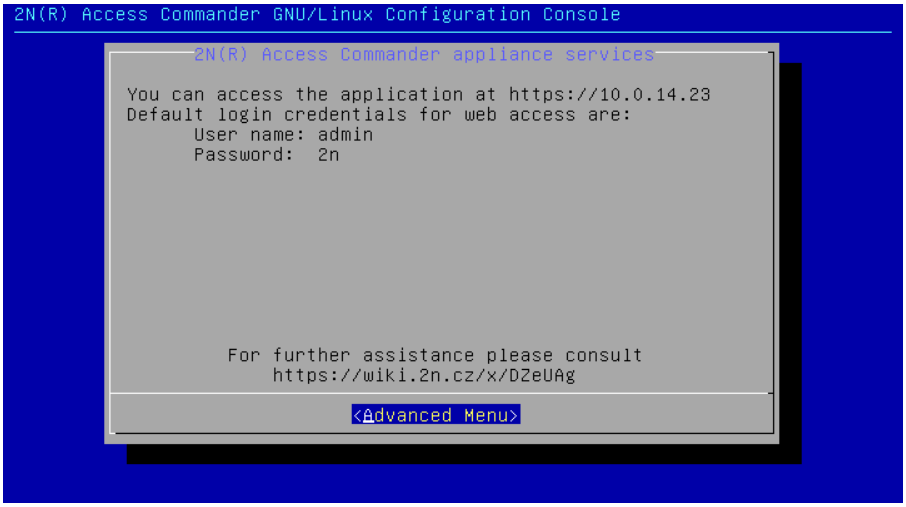
L'accesso SSH può anche essere abilitato e gestito direttamente nella console di configurazione Linux, vedere Impostazioni di Linux (p. 65).

Impostazioni di Linux

Le impostazioni di sistema di base possono essere effettuate nella console di configurazione Linux.

NOTA
se è **Access Commander** distribuito tramite una macchina virtuale, è possibile connettersi alla versione Linux da remoto tramite una connessione SSH.

La console di configurazione si apre effettuando l'accesso a **Access Commander** utilizzando l'account root. La home page visualizza le informazioni di base sull'accesso dell'amministratore all'interfaccia web e reindirizza al menu avanzato.



Nel Menù Avanzato è possibile impostare:

- **Rete**
  Impostazioni del server proxy, proprietà di rete, opzioni di sincronizzazione con il server DHCP.
- **Tim**
  Impostazione manuale dell'ora, server NTP e impostazioni del fuso orario
- **SSH**
  Imposta una connessione remota a **Access Commander** tramite SSH. Per abilitare SSH, è necessario impostare una password diversa da quella predefinita che soddisfi i requisiti per la sua difficoltà.
- **PMI**
  Avvia la procedura guidata per la configurazione delle connessioni alle cartelle condivise. Imposta l'indirizzo IP o il nome di dominio e il percorso della cartella. Per esempio. "192.168.1.1/condivisione". Per le impostazioni è necessario specificare il nome utente dell'utente che avrà accesso alla cartella specificata e il diritto di scrittura. È necessario inserire la password dell'utente e selezionare la versione del protocollo Samba. Dopo aver completato tutti i passaggi obbligatori, la connessione al server verrà verificata e verranno visualizzate le informazioni se la configurazione ha avuto successo o meno.
- **Parola d'ordine**
  Consente di modificare la password dell'utente root del sistema per accedere alla console o per accedere tramite SSH.

  > **NOTA**
  > La modifica della password di root viene eseguita nella console di configurazione, non in Access Commander.

- **Backup e ripristino**
  Utilizzato per importare dati e configurazione, impostare backup ripetuti, ripristinare da backup precedenti.

Risoluzione dei problemi

Log diagnostici

I registri diagnostici vengono utilizzati dal supporto tecnico per identificare e risolvere i problemi segnalati. I registri contengono informazioni su azioni eseguite, errori, modifiche di stato e altri eventi rilevanti.

Scarica i log diagnostici

1. Vai a **Impostazioni** > **Risoluzione dei problemi** > **Scheda Log di diagnostica**.
2. Clicca su Genera log.
   Sono necessari alcuni minuti per generare il pacchetto di log.
3. Una volta che il mazzo sarà pronto, apparirà sulla carta e sarà disponibile Scaricamento.

Statistiche sull'utilizzo

Se la funzione è attiva, invia **Access Commander** una volta al giorno dati anonimi sulle funzioni utilizzate su un server sicuro 2N. Ogni spedizione viene effettuata con un identificatore univoco, che viene generato nuovamente automaticamente ad ogni nuova spedizione. In questo modo al partner 2N viene impedito di identificare l'impianto in questione **Access Commander**. Le informazioni ottenute vengono utilizzate per migliorare lo sviluppo del prodotto, sviluppare funzionalità e migliorare l'esperienza dell'utente.

Informazioni aggiuntive

HTTP API

L'URL dell'API **Accedi al comandante** è: https://acom_indirizzo_ip/api/v3/.

Un elenco di endpoint API è pubblicato all'indirizzo http(s)://acom_ip_address/support/api. Fuori dai limiti **Access Commander** è disponibile per la visione elenco degli endpoint rilasciato con la versione firmware 2.7.

Autenticazione

I comandi API HTTP vengono inviati con le credenziali dell'utente o utilizzando l'autenticazione token. Il token di autenticazione viene creato dall'amministratore in Impostazioni > Configurazione > scheda Chiave di accesso API. La chiave di accesso API ha la funzione di Bearer Token. Quando crea una nuova chiave di accesso API, l'amministratore può limitare la validità della chiave alla sola lettura, quindi la chiave verrà autenticata solo tramite comandi GET. Le chiavi possono essere limitate a: 1 mese, 6 mesi, 1 anno.

ATTENZIONE
Dopo aver creato la chiave di accesso, copiala negli appunti e usala. Successivamente la chiave non sarà più visibile.

Licenze di terze parti

Un elenco completo delle licenze delle librerie di terze parti utilizzate è reperibile nel menu utente situato a destra della barra in alto, nella sezione Informazioni.

wiki.2n.com

2N Access Commander – Manuale d'uso

2N.com