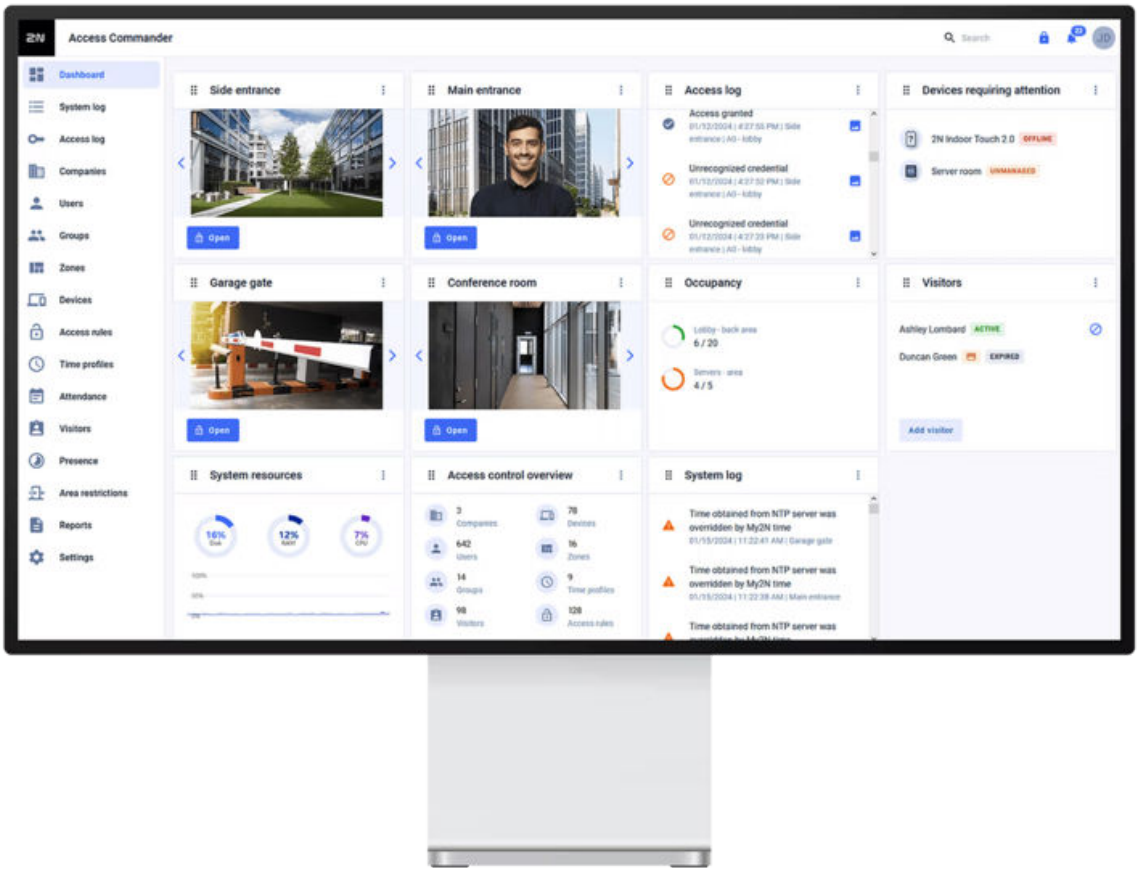
2N Access Commander

Manuale di installazione



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

2N.com

Indice

Simboli e termini utilizzati

Nel manuale vengono impiegati i seguenti simboli e pittogrammi.

PERICOLO
Rispettare sempre queste istruzioni al fine di evitare pericolo di infortuni.

AVVERTIMENTO
Rispettare sempre queste istruzioni al fine di evitare danni all'apparecchiatura.

ATTENZIONE
Avvertanza importante. La mancata osservanza delle istruzioni può causare l'errato funzionamento dell'apparecchiatura.

SUGGERIMENTO
Informazioni utili per semplificare e velocizzare l'impiego o la regolazione.

NOTA
Procedure e consigli per uno sfruttamento efficace delle proprietà dell'apparecchiatura.

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 il dispositivo all'Access Commander
. I dispositivi sono unità fisiche dell'edificio che controllano gli ingressi (2N citofoni, 2N unità di controllo degli ac

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.
- Gestire le appartenenze ai gruppi.
- Creare e gestire le visite.
- 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.

Amministratore dell'azienda

- Impostazione della lingua predefinita dell'azienda.
- Monitoraggio del registro di sistema (limitato agli eventi aziendali).
- La possibilità di impostare un widget per il Registro di sistema e la funzione di blocco di emergenza sui dispositivi utilizzati dall'azienda (compresi i dispositivi condivisi con altre aziende).

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 del firmware supportate di questi dispositivi sono elencate nel capitolo Firmware (p. 66).

Citofoni 2N

- 2N IP Style: supporta la lettura del codice QR
- 2N IP Verso 2.0: supporta la lettura del codice QR
- 2N IP Force 2.0: supporta la lettura del codice QR
- 2N IP Verso
- 2N LTE Verso
- 2N IP One
- 2N IP Force
- 2N IP Safety
- 2N IP Vario
- 2N IP Base
- 2N IP Solo
- 2N IP Uni
- 2N IP Video Kit
- 2N IP Audio Kit
- 2N IP Audio Kit Lite

Unità di accesso 2N

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

Serrature elettroniche 2N

- 2N Fortis Handle
- 2N Fortis Cylinder

Unità di risposta 2N

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

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

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

Licenza:	Trial	Basic	Advanced	Pro	Unlimited
Componente n.	n/a	n/a	91379031	91379032	91379033
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	✓	✓	✓	✓	✓
Gestione delle serrature elettroniche	✓	✓	✓	✓	✓
Importa utenti da CSV o da dispositivi	✓	×	✓	✓	✓
Gestione firmware in blocco	✓	×	✓	✓	✓
Autenticazione multipla	✓	×	✓	✓	✓
Autorizzazione dell'utente	✓	×	✓	✓	✓
Notifica	✓	×	✓	✓	✓
Presenza	✓	×	✓	✓	✓

Licenza:	Trial	Basic	Advanced	Pro	Unlimited
Componente n.	n/a	n/a	91379031	91379032	91379033
Chiavi di accesso API	✓	×	✓	✓	✓
Registri CAM	✓	×	✓	✓	✓
Controllo dell'ascensore	✓	×	✓	✓	✓
Pannello di controllo	✓	×	✓	✓	✓
Blocco di emergenza	✓	×	✓	✓	✓
Supporto credenziali mobili	✓	×	✓	✓	✓
Gestione delle visite	✓	×	✓	✓	✓
Automazione	✓	×	✓	✓	✓
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 per una macchina virtuale (p. 20)

Installazione

Access Commander può essere distribuito in due modi:

- Un piccolo computer desktop 2N Access Commander Box 2.0 (ordine n. 1120120xx)
- 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 2.0 (1120120xx, 03129-00) è un minicomputer desktop compatto con software preinstallato. Si tratta di una soluzione "plug and play" in cui è sufficiente collegare un alimentatore e un cavo Ethernet a questo minicomputer. Per una corretta e completa funzionalità del sistema, si raccomanda di collocare questo minicomputer in un luogo sicuro e di lasciarlo funzionare in modo permanente. Access Commander Box 2.0 funge da server per raccogliere dati, eventi e registri dall'intero sistema di controllo accessi.

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.

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

1. Collegare Access Commander Box alla rete utilizzando un cavo Ethernet.
2. Utilizzi 2N IP Network Scanner e Axis IP Utility per individuare Access Commander Box sulla 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 su Access Commander Box **collegandosi direttamente al computer**

1. Colleghi Access Commander Box direttamente al suo computer utilizzando un cavo di rete.
2. Dopo circa **15 secondi,** imposterà automaticamente l'indirizzo link-local.
3. Apra **accesscommander.local** nel suo browser.
   In alternativa, può utilizzare 2N IP Network Scannder o Axis IP Utility per localizzare il dispositivo anche se non ha ricevuto un indirizzo IP tramite DHCP.
4. Nell'interfaccia web, imposti un indirizzo statico come richiesto.

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. Acceda al sistema come «root» con la password «2n». Quando appare la schermata blu, cambi la password predefinita.

4. Nel menu Avanzate, selezioni «Networking» e poi «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.

SUGGERIMENTO
Collegarsi direttamente al computer e utilizzare l'indirizzo **accesscommander.local** è il modo più semplice e consigliato per impostare un indirizzo statico su Access Commander Box.

NOTA
Il numero di serie visualizzato in 2N Network Scanner o Axis IP Utility può essere diverso dal numero di serie indicato sull'etichetta di Access Commander Box.

Fortis Commander

Fortis Commander è un'applicazione indipendente che collega le serrature elettroniche **Fortis** al sistema **Access Commander**. L'applicazione imposta i blocchi in base al file di progetto creato in **Access Commander**u che contiene la configurazione dei blocchi. Il file è criptato e può essere utilizzato solo su un'installazione specifica.

Connettori e installazione

Fortis Commander è progettato per essere installato su un computer Windows con supporto Bluetooth Low Energy (BLE).

L'applicazione è disponibile sul sito web 2N Download Centre.

Procedura d'installazione

1. Scarichi il pacchetto di installazione dal link fornito.
2. Esegua il programma di installazione e completi l'installazione seguendo le istruzioni sullo schermo.

File di progetto

Il file di progetto viene creato in **Access Commander** e contiene la configurazione completa del progetto. Il file è crittografato e protetto da password.

Impostazione dei blocchi in Access Commander

Prima di caricare le chiavi su singole serrature, deve associare **Access Commander** con **Fortis Commander**.

Generazione della Master Encryption Key (MEK) e preparazione del progetto

1. Accedere ad Access Commander.
2. Accedere a **Impostazioni > Serrature elettroniche**.
3. Nella scheda **Initial Settings** fare clic su Generate Keys.

4. Creare la chiave di crittografia principale.

ATTENZIONE
La chiave di crittografia principale non può essere visualizzata o modificata in seguito .

NOTA
In base alla chiave di crittografia principale (MEK), **2N Access Commander** genera una serie di chiavi di crittografia. Pertanto, la chiave deve essere unica e sufficientemente sicura. Il set di chiavi si basa sulla chiave di crittografia master, quindi i progetti con la stessa chiave di crittografia master generano gli stessi set di chiavi. Se un progetto viene perso, è possibile creare un nuovo progetto con la stessa chiave di crittografia master e continuare la crittografia.

5. Dopo aver generato le chiavi e impostato la password per il file di progetto, può scaricare **il file di progetto**, che è un'immagine della configurazione della serratura elettronica nel sistema **Access Commander**.
6. Nella scheda **di Fortis Commander** clicchi su Download Application **,** da dove inizierà a scaricare **Fortis Commander** (applicazione per la configurazione di serrature elettroniche).

ATTENZIONE
Le informazioni sul progetto sono dati sensibili. Proteggeteli dagli abusi.

Configurazione della serratura elettronica con Fortis Commander

1. Installi **Fortis Commander** e lo apra.
2. Clicchi su Apri progetto e apra il file di progetto scaricato in Esplora file.
3. Nella finestra di dialogo che appare, inserisca la password per il file di progetto.
4. Dopo aver aperto il file di progetto, selezioni Collegare al dispositivo e colleghi la carta servizi alla serratura.
5. Clicchi su **Assign**, che assegna il blocco al progetto.
6. Scolleghi il dispositivo e clicchi su **File > Chiudi progetto**.
7. Una volta completata la configurazione, apra il sistema **Access Commander**. Vada alla scheda **Impostazioni > Serrature elettroniche** e clicchi nuovamente su Fortis Commander. Carichi il file di progetto.

NOTA
Quando sposta la serratura da un'installazione all'altra o quando effettua un reclamo, deve eseguire un reset di fabbrica . Questa operazione ripristina le impostazioni di fabbrica del lucchetto e rimuove tutte le configurazioni precedenti.

Procedura di aggiornamento della configurazione

1. Apportare modifiche in **Access Commander**.
2. Scarichi il nuovo file di progetto.

3. Carichi il file su **Fortis Commander** e apporti le modifiche necessarie ai lucchetti.
4. Se apporta altre modifiche a **Access Commander**u, scarichi sempre un nuovo file di progetto.

ATTENZIONE
Per ogni modifica della configurazione in **Access Commander**u deve scaricare un nuovo file di progetto - non può utilizzare un file più vecchio che è già stato caricato su **Fortis Commander**.

Blocco e sblocco permanente

L'app le consente di bloccare e sbloccare in modo permanente il lucchetto. La funzione viene utilizzata per gli interventi di assistenza o per il controllo di emergenza senza l'uso di una scheda.

Raccolta di eventi da serrature elettroniche che utilizzano carte / chip RFID

Impostazioni della raccolta eventi

1. Apra **Impostazioni > Serrature elettroniche > Eventi scheda**.
2. Selezioni il tipo di evento:
   - **Raccogliere gli eventi di accesso e di sistema** - Tutti gli eventi di accesso e di sistema vengono registrati sulla scheda/chip e scritti nel **Registro di sistema** e nel **Registro di accesso**.
   - **Raccogliere solo gli eventi di sistema** - vengono registrati solo gli eventi di sistema, gli eventi di accesso non vengono memorizzati sulle schede.
   - **Non raccolga eventi sulle schede** - nessun evento viene scritto nella scheda; è possibile accedervi solo attraverso **Fortis Commander**u.

SUGGERIMENTO
La selezione del set di eventi appropriato può ridurre il carico del sistema e l'utilizzo della memoria. Tuttavia, un protocollo dettagliato è importante per la diagnostica e gli audit di sicurezza.

Esportazione di eventi da una scheda

La scheda memorizza un massimo di **16 primi eventi**. Gli eventi possono essere letti in due modi:

- In **Access Commander**, faccia clic sull'icona nella casella di ricerca nell'intestazione e carichi la scheda.
- Utilizzando un dispositivo con **2N OS**, gli eventi vengono letti dalla carta e inviati a **Access Commander**u.

Caricare gli eventi sul lucchetto

1. Apra **Impostazioni > Serrature elettroniche > Fortis Commander** e clicchi su Download File.
2. Apra il file in **Fortis Commander**.
3. Nell'applicazione **Fortis Commander**, si colleghi alla serratura elettronica.
4. Carichi nuovamente il file aggiornato su **Access Commander**.
5. Una volta caricati, gli eventi vengono visualizzati in **Log di accesso** e **Log di sistema**.

Operazioni di servizio

Queste operazioni sono disponibili per **Fortis Cylinder**:

- **Smontaggio** - smontaggio di serrature a scopo di assistenza.

- **Sostituzione della batteria** - sostituzione della batteria nella serratura.

ATTENZIONE
Le operazioni di servizio non sono rilevanti per altri tipi di serrature.

NOTA
Dalla modalità di assistenza, la serratura torna alla modalità normale premendo il pulsante Lock per bloccare in modo permanente.

Distribuzione tramite macchina virtuale

Access Commander può 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. Scaricare l'ultima versione di VirtualBox da https://www.virtualbox.org/wiki/Downloads.
   Si consiglia di scaricare la versione che include il pacchetto di estensione VirtualBox.
2. Scaricare il software appropriato dalla sezione Supporto > Centro download > 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 Supporto > Centro download > 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 Supporto > Centro download > 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).
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.

Hyper-V

1. Scaricare il software appropriato dalla sezione Supporto > Centro download > 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 per una macchina virtuale

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.

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

Parametri tecnici

Opzioni del programma su Access Commander Box 2.0

Numero di dispositivi collegati	Numero di utenti	Numero di utenti nel gruppo
7 000	200 000	1 500

Parametri tecnici Access Commander Box

Prima generazione Ordine n. 91379030	Seconda generazione N. ordine 1120120E, 1120120GB, 1120120US
• dimensioni: 56,1 × 107,6 × 114,4 mm (2,21" × 4,24" × 4,50") • 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	• Dimensioni: 127,5 x 132 x 57,6 mm (5,02" x 5,20" x 2,27") • Intel® Processor N100, 6W TDP • SSD 980 NVMe M.2 – 250 GB • DDR4 SO-DIMM memory – 16 GB, 1,2 V, 3200 MHz • Supporto HDMI 2.1, DisplayPort 1.4 e VGA • Porta LAN 2.5G RJ45 per la connessione Ethernet • Temperatura di stoccaggio: da -40 °C a +85 °C • Temperatura di esercizio: da 0 °C a +50 °C

Hardware consigliato per una macchina virtuale

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.

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

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 fornire al distributore il numero di serie di uno dei dispositivi 2N collegati ad **Access Commander**. Il file di licenza viene generato in base al numero di serie di questo dispositivo con licenza. Questo deve essere il numero di serie dell'unità citofonica principale, dell'unità di accesso o dell'unità di risposta (non è possibile utilizzare il 2N Indoor Touch).

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 Commander**,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.

Rinnovo della licenza

Per ripristinare una licenza sospesa, è necessario collegare e attivare il dispositivo con licenza o far generare e caricare un nuovo file di licenza per un altro dispositivo. Se si carica una nuova licenza, è necessario attivare prima il dispositivo per il quale è stata generata la nuova licenza. Una volta attivato il dispositivo con licenza, è possibile attivare anche tutti gli altri dispositivi.

La sospensione della licenza avviene se il dispositivo con licenza viene disconnesso da **Access Commander** per un periodo superiore al periodo di protezione della licenza. La durata del periodo di protezione dipende da quanto tempo il dispositivo con licenza è stato collegato a **Access Commander**. La durata dei periodi di protezione è indicata nella tabella seguente. Quando una licenza viene sospesa, tutti i dispositivi collegati vengono automaticamente rimossi dalla gestione e contrassegnati come non gestiti.

NOTA

La rimozione dei dispositivi dalla gestione significa che non è possibile apportare modifiche alla loro configurazione tramite **Access Commander**. Le modifiche apportate in **Access Commander** non vengono propagate al dispositivo. Tuttavia, i dispositivi continuano a funzionare in base ai dati dell'ultima configurazione trasferita da **Access Commander**. Ciò significa che gli accessi e le altre impostazioni dei dispositivi rimangono invariati rispetto a prima della sospensione della licenza.

È possibile modificare la configurazione di un dispositivo non gestito solo nell'interfaccia di configurazione web del singolo dispositivo. Quando il dispositivo viene ricollegato alla gestione di **Access Commander**, il dispositivo viene sincronizzato e le modifiche apportate direttamente nell'interfaccia di configurazione web del dispositivo vengono sovrascritte dalle impostazioni di **Access Commander**.

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

Serrature elettroniche

Il sistema **Access Commander** fornisce la gestione degli accessi tramite serrature elettroniche 2N Fortis, che vengono sbloccate da carte RFID con tecnologia MIFARE® DESFire®. Quando si configurano le serrature elettroniche, a ogni serratura viene assegnata una chiave di crittografia. Le chiavi della serratura vengono quindi memorizzate sulle carte RFID degli utenti autorizzati. Se le chiavi sulla scheda e nella serratura coincidono, il meccanismo di chiusura viene sbloccato.

Una carta di accesso RFID può essere utilizzata per accedere a un massimo di 90 porte con serrature 2N Fortis, a seconda del numero di profili orari applicati. Se la capacità di memoria della carta viene superata, la scrittura dei dati sulla carta fallirà. L'evento di mancata scrittura viene registrato nel registro degli accessi al sistema. Se si utilizzano i Gruppi di chiusura, è possibile scrivere più porte su una singola scheda rispetto all'assegnazione individuale. Se si utilizzano i Gruppi di chiusura, si possono registrare più porte per scheda rispetto all'assegnazione individuale.

Fortis Commander

Fortis Commander è un'applicazione indipendente che collega le serrature elettroniche **Fortis** al sistema **Access Commander**. L'applicazione imposta i blocchi in base al file di progetto creato in **Access Commander**u che contiene la configurazione dei blocchi. Il file è criptato e può essere utilizzato solo su un'installazione specifica.

Connettori e installazione

Fortis Commander è progettato per essere installato su un computer Windows con supporto Bluetooth Low Energy (BLE).

L'applicazione è disponibile sul sito web 2N Download Centre.

Procedura d'installazione

1. Scarichi il pacchetto di installazione dal link fornito.
2. Esegua il programma di installazione e completi l'installazione seguendo le istruzioni sullo schermo.

File di progetto

Il file di progetto viene creato in **Access Commander** e contiene la configurazione completa del progetto. Il file è crittografato e protetto da password.

Impostazione dei blocchi in Access Commander

Prima di caricare le chiavi su singole serrature, deve associare **Access Commander** con **Fortis Commander**.

Generazione della Master Encryption Key (MEK) e preparazione del progetto

1. Accedere ad Access Commander.
2. Accedere a **Impostazioni > Serrature elettroniche**.
3. Nella scheda **Initial Settings** fare clic su Generate Keys.
4. Creare la chiave di crittografia principale.

ATTENZIONE
La chiave di crittografia principale non può essere visualizzata o modificata in seguito .

NOTA
In base alla chiave di crittografia principale (MEK), **2N Access Commander** genera una serie di chiavi di crittografia. Pertanto, la chiave deve essere unica e sufficientemente sicura. Il set di chiavi si basa sulla chiave di crittografia master, quindi i progetti con la stessa chiave di crittografia master generano gli stessi set di chiavi. Se un progetto viene perso, è possibile creare un nuovo progetto con la stessa chiave di crittografia master e continuare la crittografia.

5. Dopo aver generato le chiavi e impostato la password per il file di progetto, può scaricare **il file di progetto**, che è un'immagine della configurazione della serratura elettronica nel sistema **Access Commander**.
6. Nella scheda **di Fortis Commander** clicchi su Download Application**,** da dove inizierà a scaricare **Fortis Commander** (applicazione per la configurazione di serrature elettroniche).

ATTENZIONE
Le informazioni sul progetto sono dati sensibili. Proteggeteli dagli abusi.

Configurazione della serratura elettronica con Fortis Commander

1. Installi **Fortis Commander** e lo apra.
2. Clicchi su Apri progetto e apra il file di progetto scaricato in Esplora file.
3. Nella finestra di dialogo che appare, inserisca la password per il file di progetto.
4. Dopo aver aperto il file di progetto, selezioni Collegare al dispositivo e colleghi la carta servizi alla serratura.
5. Clicchi su **Assign**, che assegna il blocco al progetto.
6. Scolleghi il dispositivo e clicchi su **File > Chiudi progetto**.
7. Una volta completata la configurazione, apra il sistema **Access Commander**. Vada alla scheda **Impostazioni > Serrature elettroniche** e clicchi nuovamente su Fortis Commander. Carichi il file di progetto.

NOTA
Quando sposta la serratura da un'installazione all'altra o quando effettua un reclamo, deve eseguire un reset di fabbrica . Questa operazione ripristina le impostazioni di fabbrica del lucchetto e rimuove tutte le configurazioni precedenti.

Procedura di aggiornamento della configurazione

1. Apportare modifiche in **Access Commander**.
2. Scarichi il nuovo file di progetto.
3. Carichi il file su **Fortis Commander** e apporti le modifiche necessarie ai lucchetti.
4. Se apporta altre modifiche a **Access Commander**u, scarichi sempre un nuovo file di progetto.

ATTENZIONE
Per ogni modifica della configurazione in **Access Commander**u deve scaricare un nuovo file di progetto - non può utilizzare un file più vecchio che è già stato caricato su **Fortis Commander**.

Blocco e sblocco permanente

L'app le consente di bloccare e sbloccare in modo permanente il lucchetto. La funzione viene utilizzata per gli interventi di assistenza o per il controllo di emergenza senza l'uso di una scheda.

Raccolta di eventi da serrature elettroniche che utilizzano carte / chip RFID

Impostazioni della raccolta eventi

1. Apra **Impostazioni > Serrature elettroniche > Eventi scheda**.
2. Selezioni il tipo di evento:
   - **Raccogliere gli eventi di accesso e di sistema** - Tutti gli eventi di accesso e di sistema vengono registrati sulla scheda/chip e scritti nel **Registro di sistema** e nel **Registro di accesso**.
   - **Raccogliere solo gli eventi di sistema** - vengono registrati solo gli eventi di sistema, gli eventi di accesso non vengono memorizzati sulle schede.
   - **Non raccolga eventi sulle schede** - nessun evento viene scritto nella scheda; è possibile accedervi solo attraverso **Fortis Commander**u.

SUGGERIMENTO
La selezione del set di eventi appropriato può ridurre il carico del sistema e l'utilizzo della memoria. Tuttavia, un protocollo dettagliato è importante per la diagnostica e gli audit di sicurezza.

Esportazione di eventi da una scheda

La scheda memorizza un massimo di **16 primi eventi**. Gli eventi possono essere letti in due modi:

- In **Access Commander**, faccia clic sull'icona nella casella di ricerca nell'intestazione e carichi la scheda.
- Utilizzando un dispositivo con **2N OS**, gli eventi vengono letti dalla carta e inviati a **Access Commander**u.

Caricare gli eventi sul lucchetto

1. Apra **Impostazioni > Serrature elettroniche > Fortis Commander** e clicchi su Download File.
2. Apra il file in **Fortis Commander**.
3. Nell'applicazione **Fortis Commander**, si colleghi alla serratura elettronica.
4. Carichi nuovamente il file aggiornato su **Access Commander**.
5. Una volta caricati, gli eventi vengono visualizzati in **Log di accesso** e **Log di sistema**.

Operazioni di servizio

Queste operazioni sono disponibili per **Fortis Cylinder**:

- **Smontaggio** - smontaggio di serrature a scopo di assistenza.
- **Sostituzione della batteria** - sostituzione della batteria nella serratura.

ATTENZIONE
Le operazioni di servizio non sono rilevanti per altri tipi di serrature.

NOTA
Dalla modalità di assistenza, la serratura torna alla modalità normale premendo il pulsante Lock per bloccare in modo permanente.

Aggiornare la scheda

Le carte di accesso degli utenti devono essere aggiornate regolarmente. L'utente aggiorna la scheda collegandola al dispositivo IP 2N sul quale dispone di diritti di accesso validi. La carta deve essere tenuta in mano dal lettore del dispositivo fino all'accensione dell'interruttore di apertura della porta. L'interruttore di apertura della porta si attiva solo dopo l'aggiornamento dell'accesso alle serrature

È possibile modificare la validità predefinita di dieci giorni delle tessere all'indirizzo **Impostazioni > Serrature elettroniche > scheda Parametri tessera**.

ATTENZIONE
Se si modificano i diritti di accesso ai lucchetti in **Access Commander**, le modifiche si rifletteranno sulla tessera di accesso dell'utente solo dopo che questa è stata aggiornata sul lettore di tessere del dispositivo 2N! Per motivi di sicurezza, si consiglia di impostare un periodo di validità più breve per le carte, in modo da garantire che vengano aggiornate regolarmente.

I lettori IP, i dispositivi che consentono l'aggiornamento delle schede e le relative impostazioni sono descritti nel capitolo Impostazioni del lettore del dispositivo IP (p. 29).

Schede compatibili

NOTA
Ai fini della presente documentazione, il termine **carta** qualsiasi identificatore compatibile che utilizzi la tecnologia MIFARE DESFire.

Per aprire le serrature elettroniche 2N Fortis Non è possibile utilizzare carte con ID casuale.

Le carte con tecnologia PICard non possono essere utilizzate per aprire le serrature elettroniche 2N Fortis.

Profili temporali sulle serrature elettroniche

Le serrature elettroniche supportano profili temporali con le seguenti limitazioni:

- I giorni festivi non sono validi.
- È possibile impostare fino a 4 intervalli di tempo diversi nell'arco di una giornata.
- All'interno di un profilo temporale è possibile definire 4 programmi di intervalli giornalieri.

SUGGERIMENTO
Ciò significa che, ad esempio, è possibile avere impostazioni diverse per lunedì, martedì, mercoledì e giovedì, ma per venerdì, sabato e domenica è necessario utilizzare una delle impostazioni esistenti.

ATTENZIONE
Se il profilo temporale viola le restrizioni specificate, la regola di accesso verrà ignorata e all'utente non verrà concesso l'accesso.

Fortis Commander

Fortis Commander è un'applicazione indipendente che collega le serrature elettroniche **Fortis** al sistema **Access Commander**. L'applicazione imposta i blocchi in base al file di progetto creato in **Access Commander**u che contiene la configurazione dei blocchi. Il file è criptato e può essere utilizzato solo su un'installazione specifica.

Connettori e installazione

Fortis Commander è progettato per essere installato su un computer Windows con supporto Bluetooth Low Energy (BLE).

L'applicazione è disponibile sul sito web 2N Download Centre.

Procedura d'installazione

1. Scarichi il pacchetto di installazione dal link fornito.
2. Esegua il programma di installazione e completi l'installazione seguendo le istruzioni sullo schermo.

File di progetto

Il file di progetto viene creato in **Access Commander** e contiene la configurazione completa del progetto. Il file è crittografato e protetto da password.

Impostazione dei blocchi in Access Commander

Prima di caricare le chiavi su singole serrature, deve associare **Access Commander** con **Fortis Commander**.

Generazione della Master Encryption Key (MEK) e preparazione del progetto

1. Accedere ad Access Commander.
2. Accedere a **Impostazioni > Serrature elettroniche**.
3. Nella scheda **Initial Settings** fare clic su Generate Keys.

4. Creare la chiave di crittografia principale.

ATTENZIONE
La chiave di crittografia principale non può essere visualizzata o modificata in seguito .

NOTA
In base alla chiave di crittografia principale (MEK), **2N Access Commander** genera una serie di chiavi di crittografia. Pertanto, la chiave deve essere unica e sufficientemente sicura. Il set di chiavi si basa sulla chiave di crittografia master, quindi i progetti con la stessa chiave di crittografia master generano gli stessi set di chiavi. Se un progetto viene perso, è possibile creare un nuovo progetto con la stessa chiave di crittografia master e continuare la crittografia.

5. Dopo aver generato le chiavi e impostato la password per il file di progetto, può scaricare **il file di progetto**, che è un'immagine della configurazione della serratura elettronica nel sistema **Access Commander**.
6. Nella scheda **di Fortis Commander** clicchi su Download Application**,** da dove inizierà a scaricare **Fortis Commander** (applicazione per la configurazione di serrature elettroniche).

ATTENZIONE
Le informazioni sul progetto sono dati sensibili. Proteggeteli dagli abusi.

Configurazione della serratura elettronica con Fortis Commander

1. Installi **Fortis Commander** e lo apra.
2. Clicchi su Apri progetto e apra il file di progetto scaricato in Esplora file.
3. Nella finestra di dialogo che appare, inserisca la password per il file di progetto.
4. Dopo aver aperto il file di progetto, selezioni Collegare al dispositivo e colleghi la carta servizi alla serratura.
5. Clicchi su **Assign**, che assegna il blocco al progetto.
6. Scolleghi il dispositivo e clicchi su **File > Chiudi progetto**.
7. Una volta completata la configurazione, apra il sistema **Access Commander**. Vada alla scheda **Impostazioni > Serrature elettroniche** e clicchi nuovamente su Fortis Commander. Carichi il file di progetto.

NOTA
Quando sposta la serratura da un'installazione all'altra o quando effettua un reclamo, deve eseguire un reset di fabbrica . Questa operazione ripristina le impostazioni di fabbrica del lucchetto e rimuove tutte le configurazioni precedenti.

Procedura di aggiornamento della configurazione

1. Apportare modifiche in **Access Commander**.
2. Scarichi il nuovo file di progetto.

3. Carichi il file su **Fortis Commander** e apporti le modifiche necessarie ai lucchetti.
4. Se apporta altre modifiche a **Access Commander**u, scarichi sempre un nuovo file di progetto.

ATTENZIONE
Per ogni modifica della configurazione in **Access Commander**u deve scaricare un nuovo file di progetto - non può utilizzare un file più vecchio che è già stato caricato su **Fortis Commander**.

Blocco e sblocco permanente

L'app le consente di bloccare e sbloccare in modo permanente il lucchetto. La funzione viene utilizzata per gli interventi di assistenza o per il controllo di emergenza senza l'uso di una scheda.

Raccolta di eventi da serrature elettroniche che utilizzano carte / chip RFID

Impostazioni della raccolta eventi

1. Apra **Impostazioni > Serrature elettroniche > Eventi scheda**.
2. Selezioni il tipo di evento:
   - **Raccogliere gli eventi di accesso e di sistema** - Tutti gli eventi di accesso e di sistema vengono registrati sulla scheda/chip e scritti nel **Registro di sistema** e nel **Registro di accesso**.
   - **Raccogliere solo gli eventi di sistema** - vengono registrati solo gli eventi di sistema, gli eventi di accesso non vengono memorizzati sulle schede.
   - **Non raccolga eventi sulle schede** - nessun evento viene scritto nella scheda; è possibile accedervi solo attraverso **Fortis Commander**u.

SUGGERIMENTO
La selezione del set di eventi appropriato può ridurre il carico del sistema e l'utilizzo della memoria. Tuttavia, un protocollo dettagliato è importante per la diagnostica e gli audit di sicurezza.

Esportazione di eventi da una scheda

La scheda memorizza un massimo di **16 primi eventi**. Gli eventi possono essere letti in due modi:

- In **Access Commander**, faccia clic sull'icona nella casella di ricerca nell'intestazione e carichi la scheda.
- Utilizzando un dispositivo con **2N OS**, gli eventi vengono letti dalla carta e inviati a **Access Commander**u.

Caricare gli eventi sul lucchetto

1. Apra **Impostazioni > Serrature elettroniche > Fortis Commander** e clicchi su Download File.
2. Apra il file in **Fortis Commander**.
3. Nell'applicazione **Fortis Commander**, si colleghi alla serratura elettronica.
4. Carichi nuovamente il file aggiornato su **Access Commander**.
5. Una volta caricati, gli eventi vengono visualizzati in **Log di accesso** e **Log di sistema**.

Operazioni di servizio

Queste operazioni sono disponibili per **Fortis Cylinder**:

- **Smontaggio** - smontaggio di serrature a scopo di assistenza.

- **Sostituzione della batteria** - sostituzione della batteria nella serratura.

ATTENZIONE
Le operazioni di servizio non sono rilevanti per altri tipi di serrature.

NOTA
Dalla modalità di assistenza, la serratura torna alla modalità normale premendo il pulsante Lock per bloccare in modo permanente.

Impostazioni del lettore del dispositivo IP

Impostazioni nell'interfaccia web del dispositivo IP

ATTENZIONE
Se ha appena collegato un modulo di espansione del lettore di schede RFID al dispositivo 2N utilizzando un cavo VBUS, deve accoppiare questo modulo con il dispositivo. L'accoppiamento del modulo di espansione del lettore può essere effettuato tramite l'interfaccia web del dispositivo all'indirizzo **Access > Moduli**.

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

   SUGGERIMENTO
   Può accedere all'interfaccia di configurazione web cliccando su nell'elenco della pagina Dispositivi.

2. Vai su Hardware > Moduli di espansione.
3. Nella pagina, vai alle impostazioni del modulo lettore di schede RFID.
4. Fare clic su Modulo di coppia.
5. Dal menù **Tipi di carte consentiti** seleziona un'opzione «Serrature elettroniche 2N».

   ATTENZIONE
   Per una funzionalità ottimale, abilita solo i tipi di carta che utilizzi effettivamente.

6. Salva le modifiche.

Moduli compatibili

Sincronizzazione delle chiavi con le serrature elettroniche 2N Fortis Può essere eseguita su tutti i lettori RFID 2N immessi sul mercato a partire da febbraio 2023. La maggior parte dei lettori prodotti dopo tale data sono compatibili, ad eccezione dei modelli elencati di seguito.

I seguenti modelli **non sono compatibili**:

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

Per i seguenti moduli, la compatibilità è garantita solo per le unità prodotte a partire dall'autunno 2023:

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

Impostazione dei blocchi in Access Commander

Prima di caricare le chiavi su singole serrature, deve associare **Access Commander** con **Fortis Commander**.

Generazione della Master Encryption Key (MEK) e preparazione del progetto

1. Accedere ad Access Commander.
2. Accedere a **Impostazioni > Serrature elettroniche**.
3. Nella scheda **Initial Settings** fare clic su Generate Keys.
4. Creare la chiave di crittografia principale.

ATTENZIONE
La chiave di crittografia principale non può essere visualizzata o modificata in seguito .

NOTA
In base alla chiave di crittografia principale (MEK), **2N Access Commander** genera una serie di chiavi di crittografia. Pertanto, la chiave deve essere unica e sufficientemente sicura. Il set di chiavi si basa sulla chiave di crittografia master, quindi i progetti con la stessa chiave di crittografia master generano gli stessi set di chiavi. Se un progetto viene perso, è possibile creare un nuovo progetto con la stessa chiave di crittografia master e continuare la crittografia.

5. Dopo aver generato le chiavi e impostato la password per il file di progetto, può scaricare **il file di progetto**, che è un'immagine della configurazione della serratura elettronica nel sistema **Access Commander**.
6. Nella scheda **di Fortis Commander** clicchi su Download Application, da dove inizierà a scaricare **Fortis Commander** (applicazione per la configurazione di serrature elettroniche).

ATTENZIONE
Le informazioni sul progetto sono dati sensibili. Proteggeteli dagli abusi.

Configurazione della serratura elettronica con Fortis Commander

1. Installi **Fortis Commander** e lo apra.
2. Clicchi su Apri progetto e apra il file di progetto scaricato in Esplora file.
3. Nella finestra di dialogo che appare, inserisca la password per il file di progetto.

4. Dopo aver aperto il file di progetto, selezioni Collegare al dispositivo e colleghi la carta servizi alla serratura.
5. Clicchi su **Assign**, che assegna il blocco al progetto.
6. Scolleghi il dispositivo e clicchi su **File > Chiudi progetto**.
7. Una volta completata la configurazione, apra il sistema **Access Commander**. Vada alla scheda **Impostazioni > Serrature elettroniche** e clicchi nuovamente su Fortis Commander. Carichi il file di progetto.

NOTA
Quando sposta la serratura da un'installazione all'altra o quando effettua un reclamo, deve eseguire un reset di fabbrica . Questa operazione ripristina le impostazioni di fabbrica del lucchetto e rimuove tutte le configurazioni precedenti.

Procedura di aggiornamento della configurazione

1. Apportare modifiche in **Access Commander**.
2. Scarichi il nuovo file di progetto.
3. Carichi il file su **Fortis Commander** e apporti le modifiche necessarie ai lucchetti.
4. Se apporta altre modifiche a **Access Commander**u, scarichi sempre un nuovo file di progetto.

ATTENZIONE
Per ogni modifica della configurazione in **Access Commander**u deve scaricare un nuovo file di progetto - non può utilizzare un file più vecchio che è già stato caricato su **Fortis Commander**.

Blocco e sblocco permanente

L'app le consente di bloccare e sbloccare in modo permanente il lucchetto. La funzione viene utilizzata per gli interventi di assistenza o per il controllo di emergenza senza l'uso di una scheda.

Schede per la manutenzione

Le schede di manutenzione consentono l'accesso autorizzato alla serratura. Consentono di mettere in funzione la serratura, di cambiare la batteria, di smontare la serratura.

ATTENZIONE
La scheda di manutenzione non può essere utilizzata contemporaneamente come scheda di accesso utente.

Impostazioni della scheda Manutenzione

1. In **Access Commander** andate su **Impostazioni > Serrature elettroniche**.
2. Nella scheda **Manutenzione** fare clic su Creare.

3. Nella finestra di dialogo che si apre, selezionare il tipo di scheda che si desidera creare.
   - Impostazione di nuovi lucchetti - attiva in modalità di servizio i nuovi lucchetti precedentemente configurati nelle impostazioni di fabbrica.
   - Servizio - attiva la modalità di servizio per la serratura già impostata.
   - Smontaggio - per lo smontaggio della serratura a cilindro 2N Fortis già impostata, consultare il Manuale di installazione 2N Fortis.
   - Sostituzione della batteria - per la sostituzione della batteria della serratura a cilindro 2N Fortis già impostata, vedere il Manuale di installazione 2N Fortis.

   SUGGERIMENTO
   Una carta fisica può essere caricata contemporaneamente con **Setting New Locks** e qualsiasi altra carta servizi. Si consiglia una combinazione di **Setting New Locks** e **Service**.
4. Fare clic su Continuare a.
5. Collegare la scheda al lettore RFID USB collegato. Attendere che i dati vengano caricati sulla scheda.

La validità dei dati sulla scheda di manutenzione è di un anno. Dopo questo periodo di tempo, i dati dovranno essere cancellati e la scheda dovrà essere nuovamente impostata.

Supporto per schede DESFire di terze parti (creazione di app anonime)

Access Commander le permette di lavorare con le carte MIFARE DESFire. Supporta le carte già in uso in altri sistemi di controllo degli accessi e ne consente il riutilizzo senza la necessità di conoscere la chiave master (PICC Master Key).

Si tratta di una modalità speciale in cui la carta consente la creazione di una nuova applicazione indipendente senza la necessità di conoscere la sua chiave master (PICC Master Key).

Con questa funzionalità, gli amministratori possono:

- Riutilizzare le carte fisiche esistenti.
- Scriva l'applicazione OSO per **Access Commander** a loro.
- Evita di dover conoscere o gestire la chiave master PICC dei sistemi originali.

Per creare un'applicazione OSO su una scheda

1. Colleghi la carta DESfire esistente dell'utente a un lettore collegato a **Access Commander**.
2. Creare le credenziali utente.
3. Access Commander rileva automaticamente se la carta supporta la creazione di applicazioni anonime.
4. Se la modalità è supportata, **Access Commander** scrive una nuova applicazione anonima sulla carta senza influenzare i dati esistenti o le applicazioni di terze parti.

ATTENZIONE
Se la modalità è supportata, Access Commander scrive una nuova applicazione anonima senza la possibilità di formattare la scheda in un secondo momento, utilizzando una funzione nella sezione Impostazioni. Solo il contenuto dell'applicazione può essere eliminato, non lo spazio precedentemente occupato sulla scheda.

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)**.*

L'interfaccia **di Access Commander** è accessibile tramite un browser web. L'indirizzo IP dell'interfaccia web può essere ricercato utilizzando 2N Network Scanner o Axis IP Utility. L'interfaccia web è accessibile anche direttamente all'indirizzo **accesscommander.local**. Questa funzionalità è abilitata per impostazione predefinita.

NOTA

- Se sulla rete sono in esecuzione più istanze di Access Commander, il sistema assegna automaticamente nomi univoci: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local**, e altre istanze in base al numero di server presenti sulla rete.
- Per la distribuzione tramite Access Commander Box, si colleghi all'interfaccia web da un altro computer della rete. Il sistema operativo Access Commander Box esegue **Access Commander** e le sue impostazioni Linux di base, ma non consente di eseguire un browser web.

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.

Le credenziali predefinite sono:

Nome utente: **Admin**

Parola d'ordine: **2n**

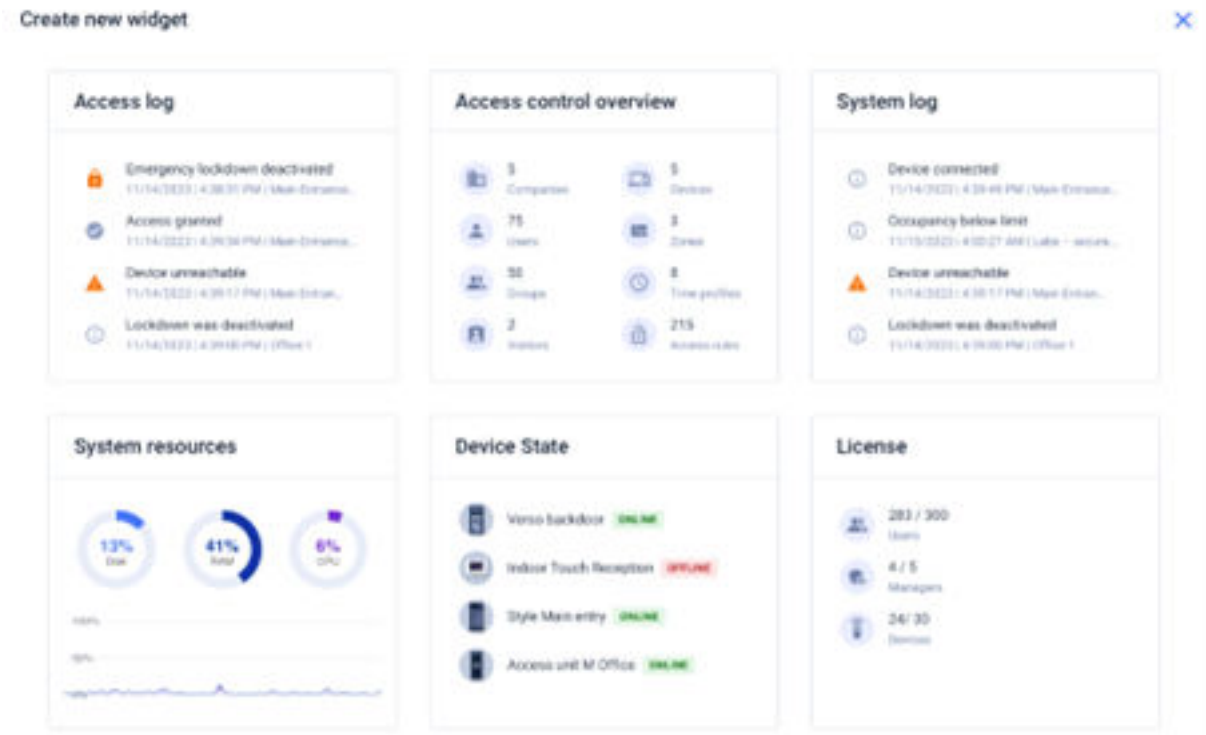
Dopo il primo accesso è necessario modificare immediatamente la password.

NOTA

Selezioni l'opzione **Non disconnetterti**, se vuole evitare di reinserire le sue credenziali di accesso al prossimo accesso. Il login è valido per un massimo di 7 giorni, dopodiché dovrà effettuare nuovamente il login.

Per accedere potrebbe essere necessaria Autenticazione a due fattori (p. 101).

Pannello di controllo



Il Dashboard è una vista di base dell'interfaccia web di **Access Commander**. È un cruscotto configurabile che visualizza i dati in tempo reale. **Access Commander** offre diversi Widget che vengono aggiunti alla Dashboard tramite il pulsante . I Widget della Dashboard possono essere spostati, rinominati o modificati nelle loro impostazioni di base in vari modi. La gestione e l'eliminazione dei widget si effettua 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'immagine dell'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.

Modificare la password dell'account

1. Fare clic sull'immagine dell'utente nell'angolo in alto a destra per aprire il menu utente.
2. Selezionare Mostra profilo.
3. Fare clic sul simbolo accanto a Password.

4. Confermare la password esistente e inserirne una nuova.

> **NOTA**
> Se la password dell'account 'admin' è la stessa dell'utente root (per l'accesso alla console di configurazione di Linux), quando la password dell'account 'admin' viene cambiata, viene cambiata automaticamente anche la password dell'account root.

Cambia la tua immagine di profilo

1. Fare clic sull'immagine dell'utente nell'angolo in alto a destra per aprire il menu utente.
2. Selezionare Mostra 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 ha generato.

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

- gravità (info, warning, error).
- l'ora in cui si è verificato l'evento.
- la categoria a cui appartiene l'azione (Stato del dispositivo, Importazione, Sincronizzazione utente, Sistema, Azioni dell'utente, Limitazioni dell'area).
- l'entità interessata dall'azione (struttura, utente, zona, visitatore...).
- 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 cliccando sul pulsante Export sopra l'elenco. Nel file CSV esportato l'ora è indicata in GMT+0.

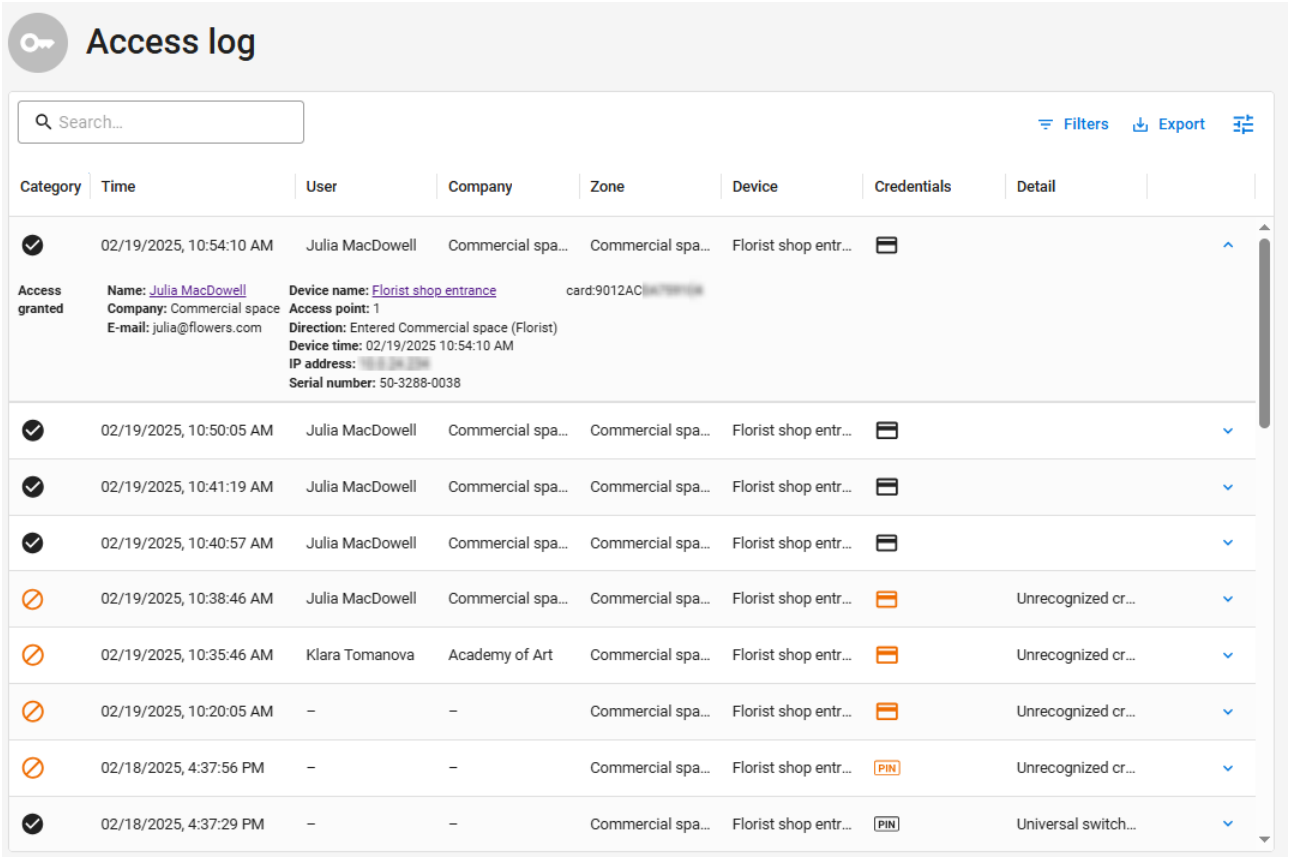
Durata dei log

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 conservazione per un determinato tipo di registro è impostato nella scheda **Impostazioni > Conservazione dei registri**. La conservazione dei registri delle telecamere non può essere più lunga di quella 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 cliccando sul pulsante Export 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 conservazione per un determinato tipo di registro è impostato nella scheda **Impostazioni > Conservazione dei registr**i. La conservazione dei registri delle telecamere non può essere più lunga di quella 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.

Registro delle chiamate

La pagina Registro chiamate registra tutte le attività di chiamata dai citofoni collegati e da altri dispositivi SIP (ad esempio, le segreterie telefoniche o i comunicatori per ascensori).

NOTA
Il registro delle chiamate è disponibile solo per l'autorizzazione dell'utente Amministratore.

L'elenco del registro delle chiamate per ogni evento dichiara:

- tipo di chiamata
- l'ora in cui è avvenuta la chiamata
- se la porta è aperta
- tipo di apparecchio
- controparte
- durata della chiamata
- motivo della fine della chiamata

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

Durata dei log

Il tempo di conservazione per un determinato tipo di registro è impostato nella scheda Impostazioni > *Conservazione dei registri*.

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

ATTENZIONE
Si raccomanda di utilizzare l'ultima versione del firmware sui suoi dispositivi affinché tutte le funzionalità del Registro chiamate funzionino correttamente. Alcune informazioni e colonne potrebbero non essere disponibili o non essere visualizzate correttamente sui dispositivi con versioni firmware precedenti.

- **Durata della chiamata:** La colonna Lunghezza chiamata non è supportata dalle versioni precedenti del firmware. Queste informazioni sono disponibili a partire dalla versione firmware 2.49.
- **Identificazione della controparte:** Per identificare correttamente la controparte dalla directory del dispositivo, è necessaria la versione del firmware 2.50 o superiore. Nelle versioni precedenti, la ricerca della directory del dispositivo potrebbe non comportarsi correttamente.

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.

L'elenco delle notifiche è visualizzato anche nella pagina **Registri di sistema > Notifiche**.

I record possono essere scaricati in un file CSV cliccando sul pulsante Export 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 > Notifiche**.
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 sono impostati nei dettagli del tipo di notifica. Per aprire i dettagli del tipo di notifica, fare clic sulla notifica selezionata nell'elenco della 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.

Le notifiche appaiono in **Access Commander** sotto l'icona nella barra superiore, 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. 101).

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 conservazione per un determinato tipo di registro è impostato nella scheda **Impostazioni > Conservazione dei registri**. La conservazione dei registri delle telecamere non può essere più lunga di quella 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.

Nell'intestazione del dettaglio dell'azienda è presente un pulsante Blocco che attiva il Blocco di emergenza (p. 62) per tutti i dispositivi nelle zone di questa azienda.

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.

My2N app

In azienda è possibile impostare i parametri di abbinamento con Applicazione My2N, che abilita l'autenticazione Bluetooth. Vengono impostati sia i dispositivi su cui gli utenti potranno effettuare l'abbinamento sia il periodo di validità dell'accesso mobile richiesto per l'abbinamento. L'accesso mobile stesso viene generato 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. 79).

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
- My2N app per impostare l'autenticazione Bluetooth per l'utente

In dettaglio **aziende > scheda E-mail > scheda Modelli** per le 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 a **Aziende > dettaglio dell'azienda selezionata > scheda Sincronizzazione utenti**.
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.

   L'attivazione di TLS consente di attivare il Transport Layer Security (TLS) per la connessione FTP. TLS cripta i dati trasmessi tra **Access Commander** e il server.
   Abilitare l'autenticazione del certificato TLS per abilitare l'autenticazione TLS dei certificati forniti dal server. Una volta abilitato, **Access Commander** verificherà che sta comunicando con un server affidabile, aumentando così la sicurezza della connessione.
3. 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.
4. La scheda Opzioni di **di** consente di gestire le modalità di sincronizzazione dei dati.

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

SUGGERIMENTO
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.

Impostazioni di sincronizzazione dei dati LDAP

Attributi importati - La modifica dello schema imposta l'assegnazione degli attributi dal server LDAP ai parametri di **Access Commander**.

NOTA
Gli attributi dei numeri di telefono sono estesi con un filtro che converte i numeri nel formato desiderato, compatibile con l'elenco degli utenti dell'azienda in **Access Commander**. Sono disponibili due filtri:

- `toPhoneNumber` - rimuove i caratteri non necessari (spazi, trattini, ecc.) dai numeri di telefono.
- `skipExtension` - rimuove l'interno dai numeri di telefono.

Esempio di utilizzo: Se si inserisce l'attributo `{telephoneNumber|toPhoneNumber|skipExtension}`, il valore originale del numero di telefono in Active Directory «+420 123 456 789 x2222» viene convertito in «+420123456789».

Utenti rimossi da LDAP - definisce cosa deve accadere agli utenti che sono stati cancellati da LDAP. Gli utenti eliminati da LDAP possono essere mantenuti in **Access Commander** oppure eliminati. Se gli utenti devono essere disattivati, dopo la loro cancellazione da LDAP i loro dati rimarranno in **Access Commander**, ma non si sincronizzeranno con i dispositivi. Gli utenti disattivati non hanno diritti di accesso, non sono raggiungibili, ecc.

Active Directory Banned Users - Imposta cosa succede agli utenti che sono stati banditi da Active Directory. Questa modifica di Active Directory può essere ignorata da **Access Commander** oppure può disattivare l'utente. Gli utenti disattivati non hanno diritti di accesso, non possono essere raggiunti, ecc. Dopo la riattivazione in Active Directory, anche gli utenti disattivati vengono riattivati **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 un DN di base e un filtro personalizzati per sincronizzare i gruppi. Nelle impostazioni dello schema, è possibile attivare la sincronizzazione degli utenti dei gruppi annidati.

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 annidata - consente all'utente di sincronizzare l'intera struttura. Quando è disattivata, vengono ricercati e sincronizzati solo i dati della 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.

Importazione utenti in azienda

Il menu esteso ⋮ nell'intestazione dei dettagli dell'azienda consente di importare una volta nuovi utenti nell'azienda, da un file CSV o da un altro dispositivo 2N.

Importa utenti da un file CSV

SUGGERIMENTO
È possibile scaricare un file CSV di esempio per l'importazione degli utenti utilizzando questo link.

Access Commander consente di caricare in blocco gli utenti dell'azienda. Le informazioni di base sugli utenti possono essere preparate in un file esterno e poi l'utente può essere importato facilmente. Gli utenti possono essere caricati in una sola azienda alla volta in un unico file.

Questa funzionalità non consente l'eliminazione degli utenti.

NOTA
Gli utenti con il ruolo di amministratore possono eseguire una sincronizzazione completa e ripetibile dell'elenco utenti tra aziende, ad es Sincronizzazione degli utenti con FTP (p. 92).

Importa dal dispositivo 2N

È possibile trasferire un elenco di utenti da un dispositivo 2N ad **Access Commander**. È possibile importare solo da un dispositivo non ancora aggiunto ad **Access Commander**. Un dispositivo non può contenere utenti già presenti in **Access Commander** (cioè con lo stesso UUID). Tutti gli utenti possono essere importati in blocco solo in un'azienda specifica.

1. Si consiglia di eseguire il backup della configurazione prima di importarla. Il backup del sistema **Access Commander** viene eseguito nella scheda **Impostazioni > Backup del sistema**. Il backup della configurazione del dispositivo si esegue nell'interfaccia di configurazione web, in **Sistema > Manutenzione**.
2. Aggiungere il dispositivo da cui si vuole importare l'elenco utenti come dispositivo **Access Commander**.

   ATTENZIONE
   Non aggiungere ancora dispositivi alle zone! Il dispositivo erediterebbe le regole di accesso e l'elenco degli utenti verrebbe sovrascritto sul dispositivo.

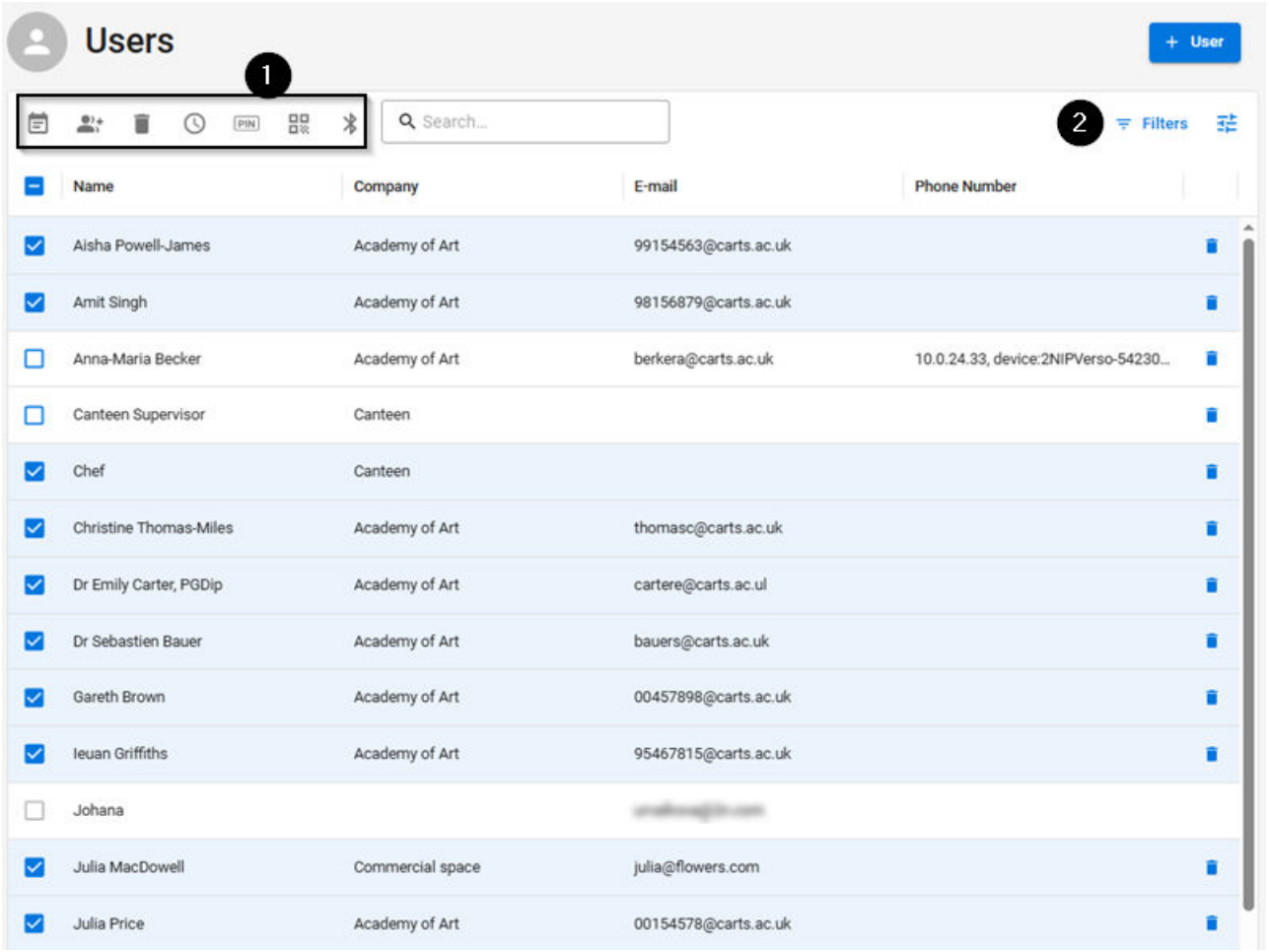
3. Andare al dettaglio dell'azienda in cui si desidera importare l'utente. Nel menu avanzato ⋮, selezionare Importa da dispositivo.
4. Si aprirà una finestra di dialogo. Dall'elenco a discesa dei dispositivi disponibili, seleziona il dispositivo da cui desideri importare l'elenco degli utenti.
5. Fare clic su Importa per avviare l'importazione in background. Il completamento del processo viene registrato nel Registro di sistema.
6. Una volta importata con successo, il dispositivo può essere aggiunto alle zone e incluso nelle regole di accesso.

ATTENZIONE
La procedura di importazione funziona solo per utenti specifici (UUID) sul dispositivo e importa tutti gli utenti dal dispositivo contemporaneamente in un'unica azienda.

Utenti

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

L'elenco degli utenti mostra tutti gli utenti creati. Sopra l'elenco è possibile filtrare gli utenti (numero 2 nell'immagine) o cercare un utente specifico per nome, e-mail o numero di telefono.



Azioni di massa

È possibile selezionare più utenti contrassegnandoli e applicare le seguenti azioni di massa (numero 1 nella figura):

- 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 l'accesso mobile agli utenti nella selezione a cui non è stato ancora assegnato l'accesso mobile.

NOTA
Per assegnare un codice PIN/QR o un accesso 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.

NOTA
Access Commander consente di caricare in blocco gli utenti dell'azienda. Le informazioni di base sugli utenti possono essere preparate in un file esterno e poi l'utente può essere importato facilmente. Gli utenti possono essere caricati in una sola azienda alla volta in un unico file.

L'importazione all'ingrosso viene effettuata nei dettagli dell'azienda, vale a dire Importazione utenti in azienda (p. 45).

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, Presenze e Registro modifiche. La scheda Presenze viene visualizzata solo per gli utenti per i quali è stato abilitato il monitoraggio, vedere Monitoraggio delle presenze degli utenti (p. 55). Il modulo presenze 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 avanzato nell'intestazione del dettaglio 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 caricato avvicinando la carta ad un lettore USB 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.

Una carta di accesso RFID può essere utilizzata per accedere a un massimo di 90 porte con serrature 2N Fortis, a seconda del numero di profili orari applicati. Se la capacità di memoria della carta viene superata, la scrittura dei dati sulla carta fallirà. L'evento di mancata scrittura viene registrato nel registro degli accessi al sistema. Se si utilizzano i Gruppi di chiusura, è possibile scrivere più porte su una singola scheda rispetto all'assegnazione individuale. Se si utilizzano i Gruppi di chiusura, si possono registrare più porte per scheda rispetto all'assegnazione individuale.

SUGGERIMENTO
Il gestore utenti e l'amministratore possono visualizzare l'identificatore della tessera nel registro di accesso. È così possibile caricare un'auto nuova/non assegnata su un dispositivo accessibile e poi copiarne l'identificativo dal log. Dopo aver inserito l'identificatore tra le carte RFID, l'utente può iniziare a utilizzare la carta. È necessario abilitare la visualizzazione degli identificatori nel registro accessi **Impostazioni > Autenticazione**.

NOTA
Se **Access Commander** segnala che la nuova tessera appena aggiunta è già in uso nel sistema, il motivo potrebbe essere che la modalità di compatibilità della tessera RFID è abilitata. Questa modalità viene attivata dall'amministratore in **Impostazioni > Autenticazione > scheda Impostazioni modalità compatibilità**.

My2N app – utilizzato per connettersi all'applicazione My2N che consente l'autenticazione via Bluetooth, vedi capitolo Autenticazione Bluetooth (p. 52).

Codice PIN – genera automaticamente un PIN di 5 cifre.

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

Codice QR – genera automaticamente un codice QR. I dispositivi in grado di leggere i 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. 52).

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 l'impostazione 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 unica, è possibile concedere a un utente l'accesso all'interfaccia di **Access Commander**. Una volta effettuato l'accesso, l'utente può monitorare le proprie presenze (se disponibili), cambiare l'e-mail o l'immagine del profilo. La prima volta che l'utente accede, gli verrà chiesto di cambiare la password. Se per l'utente è richiesta l'autenticazione a due fattori, gli verrà chiesto di collegarsi a un'applicazione di autenticazione personalizzata, vedere Autenticazione a due fattori (p. 101). In questa scheda è possibile rimuovere il collegamento all'applicazione di autenticazione.

Nella scheda Account, è possibile concedere le autorizzazioni agli utenti con credenziali di accesso per amministrare **Access Commander** utilizzando i ruoli utente. Le autorizzazioni di ciascun ruolo sono descritte nel capitolo Autorizzazioni utente (p. 7).

Interfaccia semplificata

È possibile lanciare un'interfaccia utente semplificata per il responsabile delle visite di una singola azienda. L'interfaccia semplificata consente al responsabile delle visite di aggiungere, rimuovere e gestire le visite. I registri e le presenze non possono essere visualizzati nell'interfaccia semplificata. Lo scopo dell'interfaccia semplificata è principalmente quello di facilitare agli utenti degli appartamenti l'accesso ai propri visitatori. Tutte le visite create nell'interfaccia semplificata sono sempre assegnate *al gruppo predefinito per le nuove visite*. Il gestore delle visite non ha la possibilità di modificare questo gruppo. Il gruppo predefinito per le nuove visite deve essere selezionato in anticipo nelle impostazioni dell'azienda e il gruppo deve essere impostato con regole di accesso valide per l'accesso all'appartamento, compreso il percorso per raggiungerlo. L'utente dell'appartamento può quindi gestire i metodi di autenticazione e la durata delle visite in un'interfaccia semplificata.

ATTENZIONE
Prima di abilitare l'interfaccia semplificata, **l'amministratore del sistema deve impostare il gruppo predefinito per le nuove visite** in Impostazioni aziendali (p. 42). Al gruppo predefinito devono essere assegnate regole di accesso tali da consentire al visitatore di accedere alle aree visitate. Senza un gruppo predefinito correttamente impostato, 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:

- **Email** - l'indirizzo a cui l'utente riceverà le informazioni relative al suo account in **Access Commander.**
- **Numero utente** - un identificatore specifico necessario per la sincronizzazione in blocco con un file CSV (vedere Sincronizzazione degli utenti con FTP (p. 92)).
- **Nota a**

Si avvicina

La scheda Accessi viene utilizzata per assegnare un utente ad un gruppo e per impostare l'intervallo di tempo durante il quale le credenziali di accesso dell'utente saranno valide. L'intervallo di tempo viene impostato nel menu avanzato della scheda, che si apre cliccando su . L'impostazione dell'ora di inizio validità si applica solo agli accessi ai dispositivi IP. L'accesso alle serrature elettroniche 2N Fortis è valido dal momento in cui la carta di accesso viene assegnata all'utente.

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.

Numero virtuale

Il numero di telefono virtuale può essere utilizzato per chiamare gli utenti tramite la tastiera numerica del dispositivo. I numeri virtuali non sono collegati ai numeri di telefono personali degli utenti, consentendo così di nascondere i numeri di telefono personali degli utenti sul dispositivo. I numeri virtuali possono essere impostati, ad esempio, in base ai numeri degli appartamenti. I numeri virtuali possono quindi essere utilizzati in installazioni in cui il numero di tasti di selezione rapida è insufficiente.

Il numero virtuale può avere da 1 a 7 cifre. La prima e l'ultima posizione possono essere costituite da una cifra o da una lettera, mentre il resto deve essere composto esclusivamente da cifre (ad esempio A123, 456B, C12E).

Deputy

Nella scheda è anche possibile impostare un sostituto a cui inoltrare la chiamata nel caso in cui l'utente non sia disponibile. Il rappresentante può essere scelto tra gli 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. Per caricarle, utilizzi un lettore di impronte digitali esterno. Si assicuri di aver installato il driver USB 2N. Il driver può essere scaricato 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. Assicurarsi che il lettore di impronte digitali USB sia abilitato in **Impostazioni > Accesso**.
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 My2N, che l'utente deve aver scaricato sul proprio cellulare.

Questo processo è protetto dal meccanismo di **accoppiamento Bluetooth fidato** . Il processo di accoppiamento varia a seconda della versione del firmware del dispositivo collegato.

GET IT ON Google Play Download on the App Store

La connessione dell'app sul telefono dell'utente ai dispositivi 2N avviene inserendo il codice di accoppiamento nell'app My2N.

Il codice di accoppiamento può essere ottenuto in due modi:

- collegandosi al dispositivo **2N OS**
- tramite un lettore USB Bluetooth collegato al suo computer

ATTENZIONE
Per un accoppiamento fidato di successo, il dispositivo deve avere la versione firmware 2.50 (o 3.0) o superiore. Se il dispositivo ha un firmware più vecchio, l'accoppiamento avverrà con il meccanismo più vecchio, utilizzando **PIN** senza **codice QR**.

SUGGERIMENTO
Per un livello di sicurezza più elevato, è preferibile effettuare l'associazione utilizzando il **codice QR** . Se **codice QR** non è disponibile o non è supportato dal suo dispositivo, utilizzi **PIN**.

Creazione di un codice di abbinamento tramite computer

1. Scarica sul tuo computer 2N Driver USB IP e installarlo.
2. Assicurarsi che il lettore USB Bluetooth sia abilitato in **Impostazioni > Autenticazione > scheda Lettori USB abilitati**.
3. Collegare il lettore Bluetooth USB al computer.
4. Nelle impostazioni utente v **Scheda Autenticazione** scegli l'autenticazione My2N.
5. Nella finestra di dialogo che si apre, seleziona Accoppiamento utilizzando un lettore.
   Nella finestra di dialogo verrà visualizzato un codice di abbinamento.
6. Segua la procedura seguente (Associazione nell'app mobile My2N (p. 53)) per accoppiarsi nell'app.

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. 72);
   - viene impostato un tempo adeguato per l'accoppiamento, vale a dire???.
2. Nelle impostazioni utente v **Scheda Autenticazione** scegli l'autenticazione My2N.
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. Segua la procedura seguente (Associazione nell'app mobile My2N (p. 53)) per accoppiarsi nell'app.

Associazione nell'app mobile My2N

1. Scaricalo Applicazione My2N al tuo cellulare. L'applicazione è disponibile all'indirizzo App Store E Google Play.
2. Apra l'app My2N e inserisca il PIN di accoppiamento.

> **NOTA**
> Se l'app visualizza **il codice QR**, ma il dispositivo ha un firmware precedente a 2.50.0, l'associazione avrà successo solo inserendo **il PIN**.

3. Abiliti tutti i permessi importanti per garantire che l'applicazione My2N funzioni correttamente.
4. Seguire le istruzioni sul cellulare: avvicinarsi al dispositivo in modalità abbinamento e cliccare su Inizia l'accoppiamento. Il telefono cellulare cercherà quindi un dispositivo da accoppiare.
5. Concedi l'accesso al telefono cellulare selezionato. Potrai quindi aprire le porte in tutta la sede.

AVVERTIMENTO
Per i cellulari con sistemi operativi più vecchi (Android 9/iOS 17 e precedenti) sarà necessario utilizzare un'applicazione per l'abbinamento Mobile Key.

Associazione nell'app mobile Mobile Key

1. Scarica l'applicazione Mobile Key al tuo cellulare. L'applicazione è disponibile all'indirizzo App Store E 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.

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.
- Gestire le appartenenze ai gruppi.
- Creare e gestire le visite.
- 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.

Amministratore dell'azienda

- Impostazione della lingua predefinita dell'azienda.
- Monitoraggio del registro di sistema (limitato agli eventi aziendali).
- La possibilità di impostare un widget per il Registro di sistema e la funzione di blocco di emergenza sui dispositivi utilizzati dall'azienda (compresi i dispositivi condivisi con altre aziende).

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. 76).

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. 77).

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. My2N app
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.

Gruppi di serrature

La scheda mostra una panoramica del gruppo di chiusura. Può aggiungere un altro gruppo in questa scheda.

Per ogni gruppo di chiusura, può visualizzare i dettagli del gruppo.

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 cliccando sul pulsante Export 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

L'icona sulla barra del dispositivo reindirizza all'interfaccia di configurazione web del dispositivo.

Stati del dispositivo

- Online
- Non gestito
- Incompatibile
- Non configurato: è necessario caricare la configurazione delle serrature elettroniche da un programma di terze parti.
- 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 IP

NOTA
L'aggiunta di serrature elettroniche 2N Fortis è descritta in Serrature elettroniche (p. 22).

1. Vai alla pagina **Dispositivo**.
2. Fai clic sul pulsante Aggiungi dispositivo nell'angolo in alto a destra.
3. Per aggiungere un citofono 2N, un'unità di accesso 2N o una segreteria telefonica 2N, selezionare «2N IP devices».
4. Nella finestra di dialogo che si apre, individuare il dispositivo sulla rete locale o digitare l'indirizzo IP e la porta nel formato: «Indirizzo IP:porta».
   Dopo aver inserito l'indirizzo IP del dispositivo è possibile premere INVIO sulla tastiera per inserire un altro dispositivo.

5. 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.
6. Applicazione del modello (opzionale): Per applicare un modello al dispositivo che sta aggiungendo, attivi l'interruttore **Dopo aver aggiunto il dispositivo, utilizzi il modello di configurazione**.
   - Il principio della selezione e dell'applicazione di una configurazione da un modello è lo stesso dell'applicazione manuale di un modello a un dispositivo esistente, come descritto in dettaglio in Modelli di dispositivi (p. 69).
7. Assegna un nome al dispositivo prima di crearlo.
8. I dispositivi appena aggiunti vengono visualizzati nell'elenco. Effettuare ulteriori impostazioni del dispositivo nei dettagli del dispositivo.

Gruppi di serrature

I gruppi di blocco le consentono di raggruppare i singoli blocchi in unità logiche che possono essere utilizzate per definire le regole di accesso, monitorare o gestire i dispositivi.

Visualizza i gruppi

Apra **Dispositivi > Gruppi di blocco**.

NOTA
L'elenco mostra tutti i gruppi di chiusura che sono stati creati. Utilizzi la casella di ricerca per filtrare i record in base al nome.

Creare un nuovo gruppo di chiusura

1. Apra **Dispositivi > Gruppi di blocco**.
2. Clicchi su + Gruppo Serrature.
3. Inserisca il nome di un gruppo e selezioni la scheda Crea.
4. Nel modulo **Serrature** faccia clic su Aggiungi serrature. Selezioni i lucchetti che devono far parte del gruppo.
5. Nel modulo **Zone** faccia clic su Aggiungi zone. Selezioni le zone che devono far parte del gruppo.
6. Selezioni ⋮ per aggiungere, rinominare o eliminare un gruppo di chiusura.

AVVERTIMENTO
La modifica dell'assegnazione del lucchetto a un gruppo diverso richiede una riconfigurazione. Si assicuri che tutte le modifiche del sistema siano state completate prima di esportare il file di configurazione.

Impostazione dei blocchi in Access Commander

Prima di caricare le chiavi su singole serrature, deve associare **Access Commander** con **Fortis Commander**.

Generazione della Master Encryption Key (MEK) e preparazione del progetto

1. Accedere ad Access Commander.
2. Accedere a **Impostazioni > Serrature elettroniche**.

3. Nella scheda **Initial Settings** fare clic su Generate Keys.
4. Creare la chiave di crittografia principale.

ATTENZIONE
La chiave di crittografia principale non può essere visualizzata o modificata in seguito .

NOTA
In base alla chiave di crittografia principale (MEK), **2N Access Commander** genera una serie di chiavi di crittografia. Pertanto, la chiave deve essere unica e sufficientemente sicura. Il set di chiavi si basa sulla chiave di crittografia master, quindi i progetti con la stessa chiave di crittografia master generano gli stessi set di chiavi. Se un progetto viene perso, è possibile creare un nuovo progetto con la stessa chiave di crittografia master e continuare la crittografia.

5. Dopo aver generato le chiavi e impostato la password per il file di progetto, può scaricare **il file di progetto**, che è un'immagine della configurazione della serratura elettronica nel sistema **Access Commander**.
6. Nella scheda **di Fortis Commander** clicchi su Download Application, da dove inizierà a scaricare **Fortis Commander** (applicazione per la configurazione di serrature elettroniche).

ATTENZIONE
Le informazioni sul progetto sono dati sensibili. Proteggeteli dagli abusi.

Configurazione della serratura elettronica con Fortis Commander

1. Installi **Fortis Commander** e lo apra.
2. Clicchi su Apri progetto e apra il file di progetto scaricato in Esplora file.
3. Nella finestra di dialogo che appare, inserisca la password per il file di progetto.
4. Dopo aver aperto il file di progetto, selezioni Collegare al dispositivo e colleghi la carta servizi alla serratura.
5. Clicchi su **Assign**, che assegna il blocco al progetto.
6. Scolleghi il dispositivo e clicchi su **File > Chiudi progetto**.
7. Una volta completata la configurazione, apra il sistema **Access Commander**. Vada alla scheda **Impostazioni > Serrature elettroniche** e clicchi nuovamente su Fortis Commander. Carichi il file di progetto.

NOTA
Quando sposta la serratura da un'installazione all'altra o quando effettua un reclamo, deve eseguire un reset di fabbrica . Questa operazione ripristina le impostazioni di fabbrica del lucchetto e rimuove tutte le configurazioni precedenti.

Procedura di aggiornamento della configurazione

1. Apportare modifiche in **Access Commander**.

2. Scarichi il nuovo file di progetto.
3. Carichi il file su **Fortis Commander** e apporti le modifiche necessarie ai lucchetti.
4. Se apporta altre modifiche a **Access Commander**u, scarichi sempre un nuovo file di progetto.

ATTENZIONE
Per ogni modifica della configurazione in **Access Commander**u deve scaricare un nuovo file di progetto - non può utilizzare un file più vecchio che è già stato caricato su **Fortis Commander**.

Blocco e sblocco permanente

L'app le consente di bloccare e sbloccare in modo permanente il lucchetto. La funzione viene utilizzata per gli interventi di assistenza o per il controllo di emergenza senza l'uso di una scheda.

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 di creazione delle connessioni con i dispositivi. I dispositivi online sono quelli con cui dispone **Access Commander** connessioni stabilite e su cui viene caricato il firmware accettato. Grazie alla connessione stabilita con il dispositivo, può avvenire la sincronizzazione dei dati. Il firmware incompatibile può essere abilitato **Pagina del 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 impostato 2 punti di accesso e se il rilevamento dei punti di accesso è abilitato (vedere Impostazioni del punto di accesso del dispositivo (p. 77)), viene visualizzata l'opzione di assegnazione di 2 zone. Un punto di accesso del dispositivo può trovarsi in una sola 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.

Nella scheda è possibile modificare l'indirizzo IP in cui si trova il dispositivo, consentendo ad **Access Commander** di puntare a un dispositivo che è stato scollegato e ricollegato alla rete con un indirizzo IP diverso.

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 Apri.

Viene utilizzato per bloccare le porte anche per i gruppi con accesso valido Blocco di emergenza (p. 62).

Backup

Questa scheda consente di eseguire il backup della configurazione dell'interfono in un file xml. Il backup viene avviato con Avviare un backup. Quando un backup viene salvato nella memoria locale, verrà archiviato in una memoria delimitata **Access Commander**. Quando si salva in un file, si apre una finestra di dialogo in cui è possibile crittografare il file di backup utilizzando una password. Il file contiene informazioni sensibili, pertanto si consiglia di proteggere il file. La crittografia del backup è disponibile sui dispositivi con firmware 2.45 e versioni successive

Ogni ultimo backup verrà visualizzato nella scheda. È possibile sincronizzare automaticamente il dispositivo con l'ultimo backup utilizzando il menu Ripristina. Nel menu a discesa di questo menu, puoi anche scegliere di eseguire il ripristino da un backup di un altro dispositivo connesso o da un file esterno

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

Chiama

scheda telefonica viene visualizzata se sul dispositivo è disponibile e abilitata una connessione di telecomunicazione. La scheda mostra tutti gli account abilitati che proteggono la connessione e ne mostra lo stato. La connessione di telecomunicazione viene impostata direttamente nell'interfaccia di configurazione del dispositivo in questione, nella sezione Chiamate. L'interfaccia di configurazione è accessibile tramite un pulsante Configurazione hardware nell'intestazione dei dettagli del dispositivo.

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. Accedere a **Dispositivo > Dettagli 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

Collegando il modulo relè AXIS A9188 a un citofono 2N o a un'unità di controllo accessi 2N, è possibile controllare l'accesso ai singoli piani dell'edificio. Un massimo di 8 di questi moduli relè possono essere collegati a un citofono 2N o a un'unità di accesso 2N, ognuno dei quali può controllare 8 piani, per un totale di 64 piani. Per utilizzare questa funzione, è necessario disporre di una licenza attiva: per i citofoni IP (codice d'ordine 9137916) o per le unità di accesso (codice d'ordine 9160401).

Impostazioni di controllo dell'ascensore

1. Prima di eseguire la configurazione in **Access Commander**, assicurarsi che il modulo relè AXIS A9188 sia collegato al dispositivo 2N che fornirà l'autorizzazione di accesso al piano. Assicurarsi inoltre che sul modulo sia impostato HTTPS e che la password di root sia stata modificata.
2. 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**.
3. Nell'intestazione dei dettagli del dispositivo, navighi su configurazione hardware dispositivo. Si sposti su **Integrazione > Controllo accessi > scheda Ascensore**. Abiliti tutti i moduli relè che devono controllare l'accesso dall'ascensore. Se i moduli richiedono l'autenticazione, inserisca il nome utente e la password. Salvi le impostazioni. Esca dalla configurazione hardware utilizzando la croce nella barra blu superiore.
4. Vai alla scheda Ascensore nei dettagli del dispositivo.
5. 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 .
6. 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 mostra tutti i moduli AXIS A9188 collegati e il loro stato attuale. I singoli moduli sono abilitati nella configurazione del dispositivo, in **Hardware > Controllo ascensori**.

Monitoraggio

La pagina serve per reperire informazioni sui dispositivi IP connessi (citofoni, unità di accesso, unità di risposta). Ogni amministratore può impostare la tabella in base alle proprie esigenze utilizzando Le impostazioni sono uniche per ogni account e si effettuano selezionando le colonne da visualizzare.

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.

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.

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.

Ottenere le versioni del firmware da 2N update server può richiedere alcuni minuti.

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

Esclusione del dispositivo

I dispositivi possono essere esclusi dalla gestione di massa del firmware aggiungendoli alla versione v **Dispositivi > Firmware > scheda 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

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

Sicurezza

Il metodo di sicurezza della comunicazione tra Access Commander e i dispositivi è impostato in **Dispositivi > Sicurezza > scheda Verifica certificato dispositivo**.

Access Commander consente tre livelli di sicurezza della comunicazione con i dispositivi:

1. **Comunicazione criptata senza verifica del certificato** - **Access Commander** utilizza un certificato autofirmato per la comunicazione HTTPS. Questo certificato è considerato non attendibile dai browser web.
2. **Verifica dell'impronta del certificato** — la comunicazione è assicurata controllando il certificato registrato sul dispositivo. Durante la comunicazione, viene verificata l'impronta di questo certificato
   Quando l'autenticazione tramite impronta digitale è attivata, l'amministratore del dispositivo deve confermare la validità dell'impronta del certificato quando aggiunge un nuovo dispositivo. All'amministratore del dispositivo verrà richiesto di verificare l'impronta digitale anche se il certificato di un dispositivo già aggiunto viene modificato
3. **Verifica completa del certificato** - la comunicazione è protetta da un certificato firmato da una cosiddetta autorità di certificazione. Durante la comunicazione, l'intera catena di certificazione viene verificata in base ai requisiti della PKI.

ATTENZIONE
Sul dispositivo 2N Indoor Touch non è possibile caricare certificati SSL propri. Dopo l'attivazione dell'autenticazione dei certificati il collegamento con essi andrà perso.

Come gestire i certificati

Il metodo di sicurezza della comunicazione tra Access Commander e i dispositivi è impostato in **Dispositivi > Sicurezza > scheda Verifica certificato dispositivo**.

Quando l'autenticazione del certificato SSL è attivata, la sincronizzazione avviene solo sui dispositivi che dispongono di un certificato SSL con un'autorità attendibile firmata. La sincronizzazione dei dispositivi senza tali certificati SSL verrà disattivata. I dispositivi passeranno allo stato offline

Il certificato dell'autorità sottoscrivente deve essere riconosciuto come idoneo sul server in cui è in funzione **2N Access Commander**.

SUGGERIMENTO
Il processo di caricamento dei certificati sul server è descritto in Domande frequenti.

Per una corretta autenticazione, i certificati del dispositivo devono essere firmati dall'autorità di certificazione e includere l'indirizzo IP o il nome di dominio del dispositivo.

Carica un certificato del dispositivo

1. Accedere all'interfaccia di configurazione web del dispositivo.
2. Vada su **Sistema > Certificati > scheda Certificati utente**.
3. Carica il certificato preparato.
4. Acceda a **Sistema > Connessione di rete > scheda Server web**.
5. Nel parametro **Certificato del server HTTPS**, selezioni il certificato che ha caricato.
6. Salva le modifiche.

Impostazioni del punto di accesso del dispositivo

È possibile dividere logicamente ogni dispositivo in due punti di accesso - arrivo e partenza. Ogni punto di accesso rappresenta un passaggio in una direzione e determina se l'utente del dispositivo entra o esce dalla zona. Un punto di accesso può essere controllato da uno o più moduli del dispositivo. Tutti i moduli assegnati gestiscono quindi i passaggi in direzione del punto di accesso specifico. I punti di accesso sono utilizzati soprattutto nelle situazioni in cui un dispositivo si trova al confine di due zone e la direzione del movimento tra di esse deve essere registrata con precisione (ad esempio, per le funzioni anti-passback).

I punti di accesso sono utilizzati anche per tracciare gli utenti nel modulo Presenza (p. 82). I punti di accesso sono utilizzati anche per tracciare l'ingresso e l'uscita nel modulo Restrizioni di zona (p. 84).

NOTA
Nell'interfaccia di configurazione web di ogni dispositivo, i punti di accesso sono indicati come **Entrata** e **Uscita**. Per configurarle, accedere a **Accesso > Regole di accesso > selezionare la scheda « Accesso e uscita »**.

Abilitazione dei punti di accesso in Access Commander

1. Vai alla pagina Zone v **Access Commander**.
2. Nell'angolo in alto a destra, premi e abilitare l'uso dei punti di accesso.

Assegnazione del modulo per l'arrivo o la partenza

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

   SUGGERIMENTO
   Può accedere all'interfaccia di configurazione web cliccando su nell'elenco della pagina Dispositivi.

2. Vada su **Accesso > Regole di accesso**.
3. Nella scheda **Arrivo** o **Partenza** sotto **Moduli** faccia clic su Gestione.
4. Si apre una finestra di dialogo con un elenco dei moduli di gestione degli accessi disponibili.
5. Trascini i moduli in gruppi in base alla direzione che devono fornire.

   SUGGERIMENTO
   Clicchi su per individuare un modulo specifico. Il modulo emette un segnale visivo o acustico, a seconda delle sue capacità.

Modelli di dispositivi

La funzione Modelli di dispositivo le consente di configurare più dispositivi. I modelli semplificano l'installazione iniziale del sistema e unificano le impostazioni tra i vari progetti.

I modelli funzionano in base al principio del modello. I modelli le consentono di salvare l'intera configurazione di qualsiasi dispositivo con **2N OS** o solo parti selezionate della configurazione, per poi applicarla ad altri dispositivi. La configurazione può basarsi su un dispositivo già configurato, su un backup del dispositivo o su un modello precedentemente esportato.

Quando crea un modello, può scegliere quali parti della configurazione includere. Le singole parti differiscono a seconda del tipo di dispositivo (ad esempio, impostazioni dei relè, uscite audio, automazione). Questa selezione fa parte del processo di creazione del modello e non può essere modificata una volta salvato il modello.

NOTA
L'utilizzo di modelli può ridurre significativamente il tempo necessario per la messa in funzione iniziale.

Creare e gestire i modelli

Per accedere alla funzione dei modelli, vada in Dispositivi > Modelli.

1. Clicchi su + Crea modello da.
2. Si apre la finestra di dialogo **Crea modello**.
3. Dal menu a discesa **Dispositivi***, selezioni un dispositivo esistente che servirà come dispositivo di base per il suo modello. Verranno visualizzati solo i dispositivi compatibili con i modelli.
4. Clicchi su Avanti per continuare a configurare il modello.

ATTENZIONE
Alcune configurazioni possono visualizzare degli avvertimenti. Queste informano che le configurazioni selezionate possono avere limitazioni o rischi potenziali. La selezione è ancora attiva, ma si consiglia di controllare la notifica.

Importa un modello o un backup da un file

Se ha già un modello o un backup del dispositivo salvato in un file, può importarlo facilmente:

1. Vada a Dispositivi > Modelli.
2. Clicchi su Importa da in alto a destra.
3. Selezioni il modello o il file di backup dal suo computer e clicchi su Importa.

NOTA
Durante l'importazione, alcune sezioni possono apparire disattivate. Si tratta di parti della configurazione che potrebbero causare modifiche indesiderate o interferire con il funzionamento del dispositivo. Queste sezioni vengono rimosse automaticamente al momento dell'importazione e l'utente può vederle brevemente al momento del caricamento.

Modificare il modello

Il modello può essere ulteriormente modificato dopo la creazione. L'interfaccia visualizza solo le parti della configurazione che sono state incluse al momento della creazione del modello.

1. Vada a Dispositivi > Modelli.
2. Selezioni un modello dall'elenco.
3. Clicchi su Modifica modello.

Verrà visualizzata una finestra di dialogo con le sezioni di configurazione.

Regolazione dei valori

- Il valore viene regolato facendo doppio clic.
- L'elemento modificato viene immediatamente contrassegnato come modificato.
- L'icona di avvertimento indica i valori che potrebbero non superare la convalida completa sul dispositivo.

ATTENZIONE
La convalida eseguita durante la modifica di un modello è solo indicativa e viene effettuata **a livello di articolo**. Il controllo non cattura tutti i conflitti tra i dispositivi e le versioni del firmware e non corrisponde alla convalida completa che avviene su **2N OS**.

Un articolo contrassegnato da un'avvertenza può essere ancora utilizzabile sul dispositivo, mentre un articolo senza avvertenza può essere rifiutato al momento dell'applicazione. La valutazione vera e propria avviene sul dispositivo.

Applicazione di un modello a un dispositivo

Il modello può essere applicato a uno o più dispositivi. Può anche essere applicato utilizzando azioni massicce nell'elenco dei dispositivi o direttamente dai dettagli del dispositivo.

1. Vada a Dispositivi > Modelli.
2. Selezioni il modello che desidera applicare al dispositivo.
3. Clicchi su Applica al dispositivo.
4. Selezionare il dispositivo e confermare.
5. Viene visualizzata la panoramica della configurazione. Queste sezioni corrispondono alle selezioni effettuate al momento della creazione del modello, ma possono essere modificate.
6. Clicchi su Utilizza.

ATTENZIONE
Se durante l'applicazione del modello viene rilevata una mancata corrispondenza tra la versione del firmware o il tipo di dispositivo per cui è stato creato il modello e la versione o il tipo del dispositivo di destinazione, viene visualizzato un messaggio di avviso. La discrepanza deve essere confermata prima di procedere.

NOTA

- Lo stato conferma solo il successo dell'avvio del processo. Non informa sull'effettivo progresso o completamento della domanda.
- Per le istruzioni su come utilizzare il modello quando aggiunge un dispositivo, consulti Aggiungere un nuovo dispositivo (p. 59).

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.

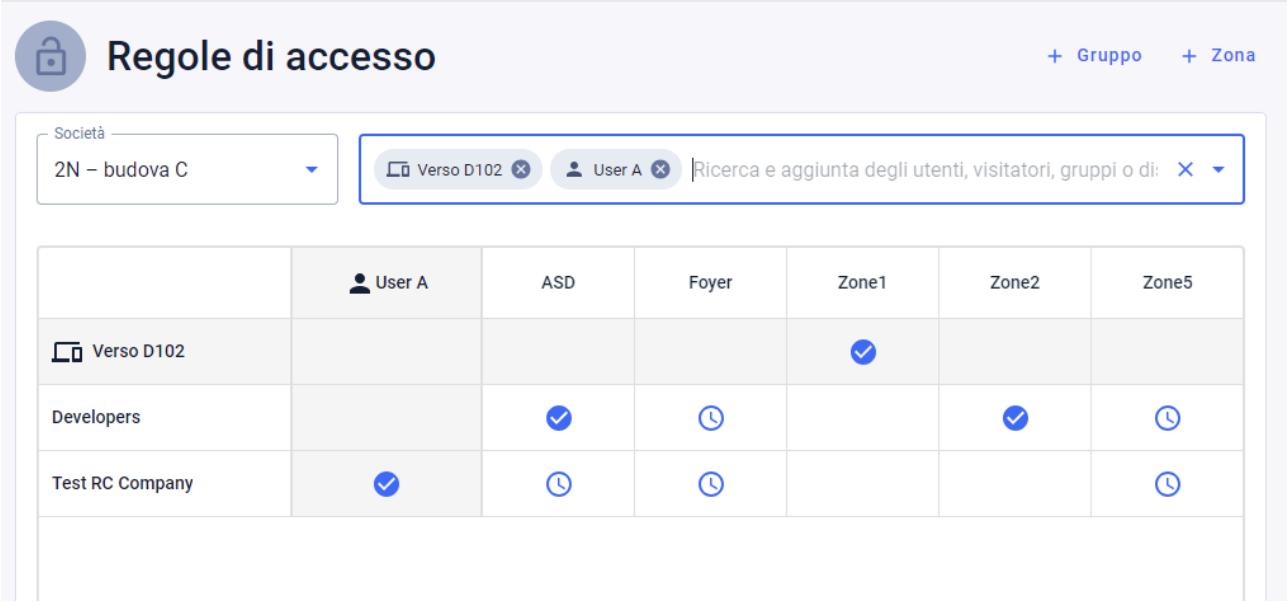
Visualizzazione a matrice

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. 74). 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.

Profili temporali sulle serrature elettroniche

Le serrature elettroniche supportano profili temporali con le seguenti limitazioni:

- I giorni festivi non sono validi.
- È possibile impostare fino a 4 intervalli di tempo diversi nell'arco di una giornata.
- All'interno di un profilo temporale è possibile definire 4 programmi di intervalli giornalieri.

SUGGERIMENTO
Ciò significa che, ad esempio, è possibile avere impostazioni diverse per lunedì, martedì, mercoledì e giovedì, ma per venerdì, sabato e domenica è necessario utilizzare una delle impostazioni esistenti.

ATTENZIONE
Se il profilo temporale viola le restrizioni specificate, la regola di accesso verrà ignorata e all'utente non verrà concesso l'accesso.

Creazione di un profilo temporale

1. Vada a **Profili orari**.
2. Clicchi su + Profilo orario nell'angolo in alto a destra.
3. Nella finestra di dialogo aperta, impostare il nome del profilo temporale.

4. Selezioni Aggiungi fasce orarie per selezionare una restrizione oraria. I giorni evidenziati in blu identificano i giorni che rientrano nel profilo orario. Per selezionare un giorno, clicchi su di esso. Può impostare un intervallo di tempo all'interno dei giorni per determinare la validità del profilo orario.

> **NOTA**
> Può impostare un intervallo di tempo entro i giorni per determinare la validità del profilo orario.

> **ATTENZIONE**
> Dopo la creazione del profilo orario, è possibile impostare orari diversi per ogni giorno.

5. 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.

> **NOTA**
> I profili globali possono influenzare l'accesso in tutte le aziende. Solo l'amministratore può modificarli.
>
> Un amministratore degli accessi può correggere solo i profili orari della sua azienda.

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 delle presenze e delle modalità di presenza si effettua in **Impostazioni > Configurazione > scheda Presenze**, vedereImpostazioni di partecipazione (p. 76).

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. 47).

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

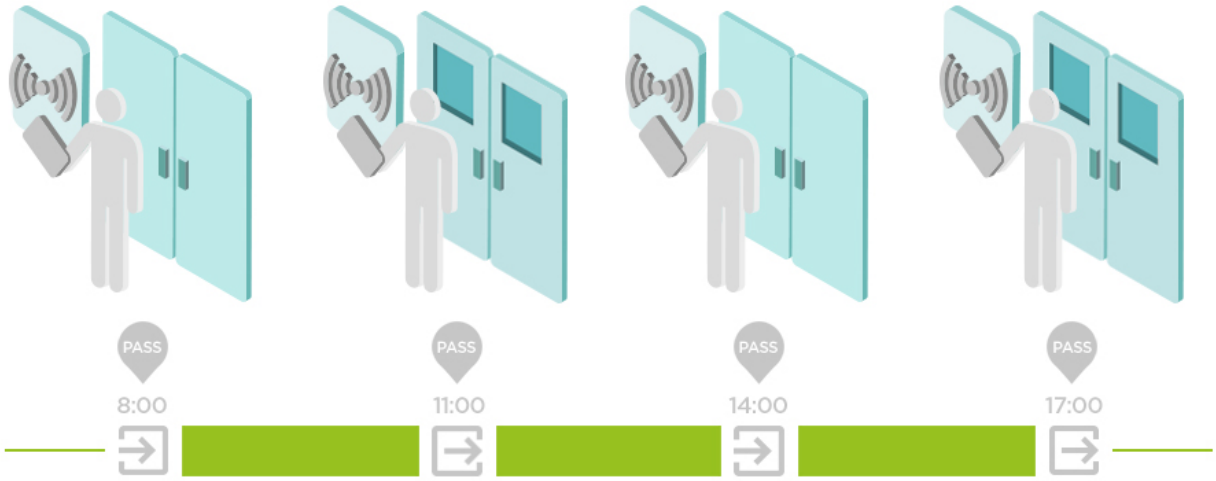
Il responsabile delle presenze può modificare i dati sulle presenze degli utenti. La modifica viene effettuata facendo clic sull'intervallo di tempo da modificare. Una volta aperti, è possibile modificare i tempi limite e aggiungere una nota all'intervallo.

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

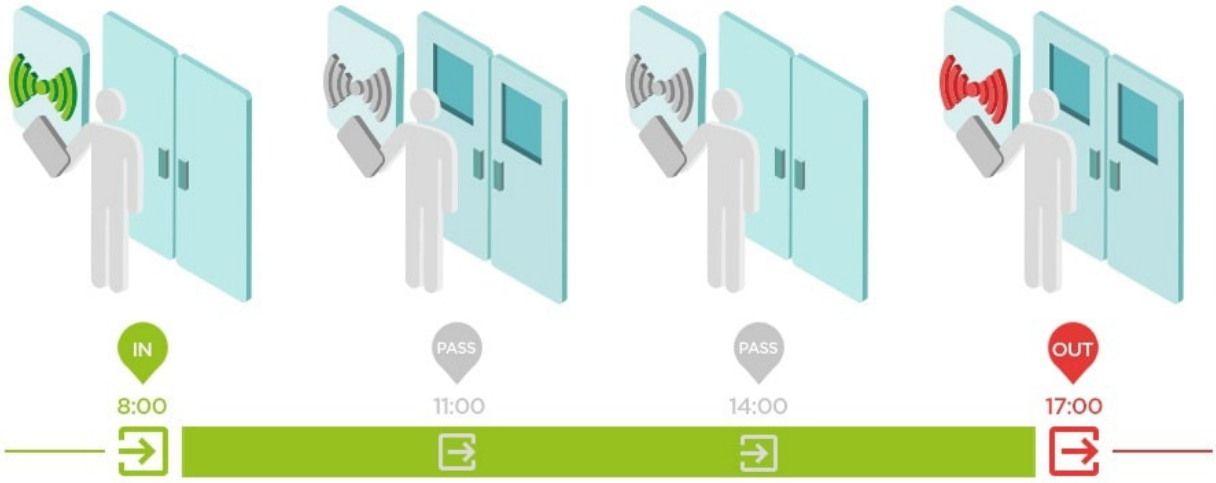
- **FREE**



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**

Per un funzionamento corretto, il dispositivo deve essere impostato per entrare e uscire dall'area.



- **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

È possibile dividere logicamente ogni dispositivo in due punti di accesso - arrivo e partenza. Ogni punto di accesso rappresenta un passaggio in una direzione e determina se l'utente del dispositivo entra o esce dalla zona. Un punto di accesso può essere controllato da uno o più moduli del dispositivo. Tutti i moduli assegnati gestiscono quindi i passaggi in direzione del punto di accesso specifico. I punti di accesso sono utilizzati soprattutto nelle situazioni in cui un dispositivo si trova al confine di due zone e la direzione del movimento tra di esse deve essere registrata con precisione (ad esempio, per le funzioni anti-passback).

I punti di accesso sono utilizzati anche per tracciare gli utenti nel modulo Presenza (p. 82). I punti di accesso sono utilizzati anche per tracciare l'ingresso e l'uscita nel modulo Restrizioni di zona (p. 84).

NOTA
Nell'interfaccia di configurazione web di ogni dispositivo, i punti di accesso sono indicati come **Entrata** e **Uscita**. Per configurarle, accedere a **Accesso > Regole di accesso > selezionare la scheda « Accesso e uscita »**.

Abilitazione dei punti di accesso in Access Commander

1. Vai alla pagina Zone v **Access Commander**.
2. Nell'angolo in alto a destra, premi e abilitare l'uso dei punti di accesso.

Assegnazione del modulo per l'arrivo o la partenza

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

SUGGERIMENTO
Può accedere all'interfaccia di configurazione web cliccando su nell'elenco della pagina Dispositivi.

2. Vada su **Accesso > Regole di accesso**.
3. Nella scheda **Arrivo** o **Partenza** sotto **Moduli** faccia clic su Gestione.
4. Si apre una finestra di dialogo con un elenco dei moduli di gestione degli accessi disponibili.
5. Trascini i moduli in gruppi in base alla direzione che devono fornire.

SUGGERIMENTO
Clicchi su per individuare un modulo specifico. Il modulo emette un segnale visivo o acustico, a seconda delle sue capacità.

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 di tempo per le visite di accesso non deve superare i 90 giorni.
4. Prima di creare una visita, è possibile impostare i metodi 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. 79).

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. 80).

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 pagina Schede è utilizzata per gestire le tessere di accesso per i visitatori che sono disponibili per aggiungere una visita. Una nuova tessera 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.

NOTA
Se **Access Commander** segnala che la nuova tessera appena aggiunta è già in uso nel sistema, il motivo potrebbe essere che la modalità di compatibilità della tessera RFID è abilitata. Questa modalità viene attivata dall'amministratore in **Impostazioni > Autenticazione > scheda Impostazioni modalità compatibilità**.

Gestione di una carta sicura con un lettore USB

Il lettore USB può essere utilizzato per diagnosticare e gestire la carta protetta nel campo di ricerca dell'intestazione.

SUGGERIMENTO
Prima di utilizzare il lettore USB, deve essere abilitato in **Access Commander**. Per maggiori informazioni, veda Lettori USB abilitati (p. 107).

1. Colleghi il lettore USB al computer.
2. Clicchi sull'icona nella casella di ricerca nell'intestazione.
3. Si attacchi al lettore.

Operazioni disponibili

- Recupero dei dati dalla carta
- Cerca un utente per scheda
- Per visualizzare gli eventi memorizzati nella scheda
- Aggiornamento dei dati di accesso
- Cancellare o formattare un'applicazione
- Estensione della carta servizi

Presenza

Il modulo **Presence** consente di monitorare l'attività degli utenti in tempo reale. Funziona indipendentemente dal modulo **Presenza**, che ha una licenza separata. Le presenze possono essere monitorate anche senza una licenza Presence attiva.

Le due funzioni sono visualizzate insieme nelle schede **Controllo presenze e presenza persone** nell'interfaccia di Access Commander, ma ognuna ha un proprio scopo e funziona in modo indipendente.

Affinché il modulo funzioni, deve impostare la modalità di presenza IN-OUT in **Impostazioni > Configurazione > scheda Presenze**, veda Impostazioni di partecipazione (p. 76).

- Se l'ultimo evento dell'utente in un determinato giorno è un arrivo (**IN** evento), è considerato presente.
- Se un utente passa attraverso un lettore impostato su una direzione non specificata, la zona dell'utente cambierà. Lo stesso accade se passa attraverso un lettore in modalità **IN**.
- Se l'ultimo evento dell'utente in un determinato giorno è un logout (evento**OUT**), viene trattato come 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 foglio elettronico utilizzano delimitatori diversi e il file CSV potrebbe non essere visualizzato correttamente quando viene aperto in essi. In questi casi, si consiglia di importare i dati dal file CSV in una cartella di lavoro aperta.

- **My2N app** – Utenti associati e non associati con tempo di associazione rimanente
  Il rapporto elenca i dati sullo stato dell'associazione dell'utente tramite l'applicazione My2N app o 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. 92).

  ATTENZIONE
  Il file contiene dati sensibili!

Restrizioni di zona

Utilizza le restrizioni di area per definire le aree in cui è possibile utilizzare le funzioni Occupancy e Anti-Passback.

NOTA
Il modulo Restrizioni di area e il modulo Presenza (inclusa la partecipazione) sono indipendenti l'uno dall'altro. L'occupazione e l'anti-passback non possono essere utilizzati per i moduli Presenza e Presenza. L'occupazione e l'anti-passback funzionano solo nel modello Restrizioni

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 schede indicano quali dispositivi sono elencati come ingresso o uscita nell'area. Può utilizzare il menu avanzato alla voce ⋮ per spostare i dispositivi tra le schede o rimuoverli da un'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. 77). Le proprietà del punto di accesso vengono espanse facendo clic sulla freccia.

Occupazione

Per un funzionamento corretto, il dispositivo deve essere impostato per entrare e uscire dall'area.

La scheda Occupazione fornisce una panoramica del numero di persone nell'area e consente di impostare limiti di occupazione. Se viene raggiunto il limite di occupazione, è possibile negare gli input aggiuntivi o registrare solo questi input nel registro di sistema. La funzione di occupazione non tiene traccia della presenza di persone nell'area. Un modulo Presence separato è progettato per monitorare la presenza di singole persone

ATTENZIONE
Quando autorizza ripetutamente un utente, ogni autorizzazione conta come un ingresso. Ciò significa che se un utente viene registrato tre volte consecutivamente sul dispositivo di ingresso, questo verrà conteggiato come tre persone presenti nell'area. Pertanto, se l'installazione fisica del dispositivo consente il recupero ripetuto di una singola tessera utente, è consigliabile combinare la funzione di occupazione con la funzione anti-passback.

Anti-passback

Per un funzionamento corretto, il dispositivo deve essere impostato per entrare e uscire dall'area.

È possibile attivare la funzione anti-passback sull'area, che garantisce l'estensione del controllo degli accessi monitorando e prevenendo il mancato utilizzo dei diritti per il rientro nelle aree riservate. Le aree monitorate sono definite da dispositivi di confine che conducono a o consentono di abbandonare tali aree. In questi dispositivi, le persone sono sottoposte a controlli delle autorizzazioni in base alle regole definite per quell'area specifica. Dopo aver lasciato l'area attraverso un dispositivo di confine, l'utente può tornare nell'area solo dopo un timeout, se è stato impostato un timeout. Se l'utente tenta di tornare nell'area prima, il sistema nega l'accesso o semplicemente registra l'evento.

AVVERTIMENTO

- L'area anti-passback diventa priva di significato e potenzialmente pericolosa se nell'area è presente un dispositivo con un pulsante REX attivo collegato che consente un accesso non autorizzato.

Impostazione di un'eccezione

A volte può essere auspicabile che le condizioni anti-passback non si applichino a determinati utenti. 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 devono essere soggetti alle condizioni di 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 quelli che hanno tentato di accedere all'area anti-passback prima della scadenza del timeout. Utilizzando ✕, gli utenti possono essere esclusi dall'elenco e autorizzati ad accedere nuovamente all'area.

SUGGERIMENTO

Quando a un utente viene negato l'accesso a causa di un anti-passback attivo, può essere inviata all'utente un'e-mail informativa automatica. Per attivare l'invio dell'e-mail, andare su **Impostazioni > Anti-passback > scheda Notifica** e-mail utente bloccato.

Reimpostazione delle restrizioni

La scheda **Impostazioni > Anti-passback > Ripristino delle restrizioni dell'area** stabilisce i giorni e gli orari in cui il record dell'area verrà cancellato, ovvero tutti gli utenti potranno passare di nuovo, indipendentemente dalle precedenti violazioni delle regole.

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.

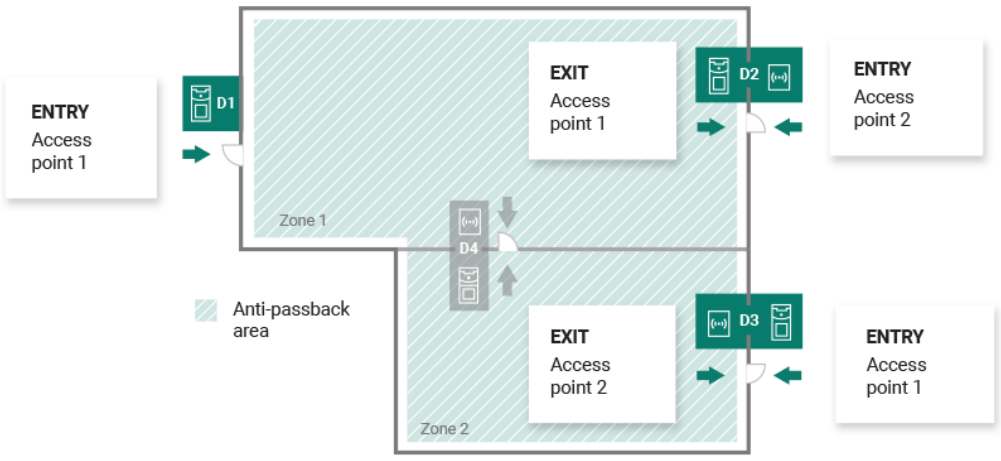
Gli errori di configurazione più comuni

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.
- Un dispositivo di input di quest'area è già utilizzato come input di un'altra area. Per un corretto funzionamento, è necessario modificare l'assegnazione.
- 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.

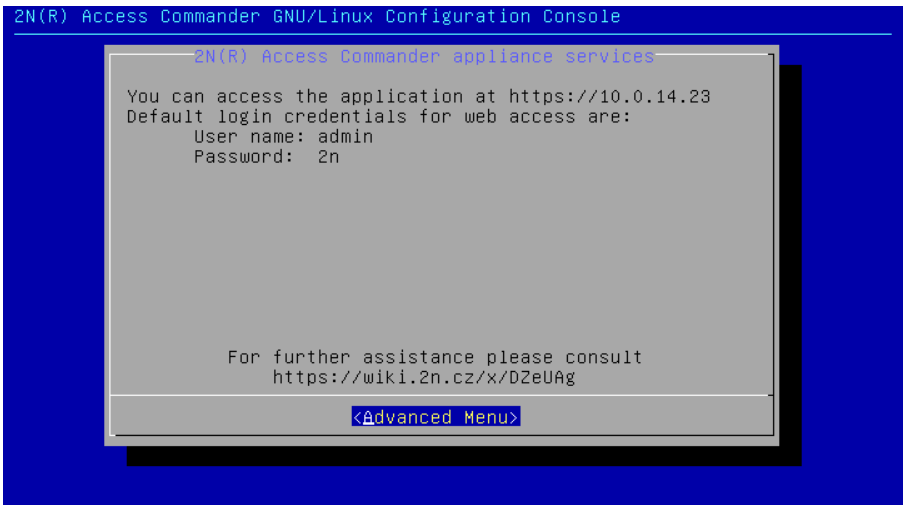
Impostazioni di sistema

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 password root viene modificata nella console di configurazione, non in Access Commander.
- **Backup e ripristino**
  Utilizzato per importare dati e configurazione, impostare backup ripetuti, ripristinare da backup precedenti.

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. In **Impostazioni > scheda Aggiornamento del sistema** il controllo automatico degli aggiornamenti può essere disattivato.

Installa l'aggiornamento Access Commander

AVVERTIMENTO
Si consiglia di eseguire questa operazione prima di installare l'aggiornamento backup del sistema (p. 91). 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.

Domini richiesti per gli aggiornamenti del sistema

ATTENZIONE
La connessione di 2N Access Commander ai server elencati di seguito è essenziale per la riuscita dell'aggiornamento del sistema. Senza l'accesso a questi domini abilitati, il processo di aggiornamento fallirà e il sistema non si aggiornerà.

Questo accesso è fondamentale per scaricare le ultime versioni delle applicazioni, i pacchetti di sistema, le patch di sicurezza e altri componenti che mantengono il suo sistema in uno stato ottimale e sicuro.

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

Downgrade

Non è possibile ripristinare una versione precedente del firmware.

Beta test

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

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

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.
5. 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.
5. 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**. È possibile scaricare un file CSV di esempio dalla scheda (nel menu esteso ⋮).

SUGGERIMENTO
L'elenco degli utenti attuali, che corrisponde alla struttura del file CSV di esempio, può essere scaricato da Rapporti (p. 83).

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 consente di collegare **Access Commander** a un repository FTP che contiene un file CSV con un elenco di utenti. La scheda visualizza quindi le informazioni relative a questo repository FTP.

1. Accedere a **Impostazioni > scheda Sincronizzazione utente**.
2. Clicca su ✎ nel parametro Archiviazione.
3. Nella finestra di dialogo aperta, imposta l'indirizzo del server FTP in cui è archiviato il file CSV.
4. L'attivazione di TLS consente di attivare il Transport Layer Security (TLS) per la connessione FTP. TLS cripta i dati trasmessi tra **Access Commander** e il server.
   Abilitare l'autenticazione del certificato TLS per abilitare l'autenticazione TLS dei certificati forniti dal server. Una volta abilitato, **Access Commander** verificherà che sta comunicando con un server affidabile, aumentando così la sicurezza della connessione.

   ATTENZIONE
   Il proxy per FTP con autenticazione TLS non è supportato.
5. Immettere le credenziali per accedere al server FTP.

File CSV

NOTA
Alcuni programmi di foglio elettronico utilizzano delimitatori diversi e il file CSV potrebbe non essere visualizzato correttamente quando viene aperto in essi. 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.

Data e ora

Per modificare il metodo di recupero dell'ora, accedere a **Impostazioni > Configurazione > scheda Data e ora**.

La data e l'ora di **Access Commander** possono essere sincronizzate con Internet o impostate manualmente. Se **Access Commander** non è collegato a Internet, è necessario impostare manualmente la data, l'ora e il fuso orario. Altrimenti, è possibile passare all'NTP e ottenere l'ora dal 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 dei dispositivi collegati può essere sincronizzata con quella di **Access Commander**. La condivisione dell'ora con i dispositivi si attiva attivando il parametro Sincronizzazione dispositivo in **Impostazioni > Configurazione > scheda Data e oraNastavení > Konfigurace > karta Datum a čas.**.

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**.

  SUGGERIMENTO
  L'ora del server NTP fornisce la migliore precisione dell'ora sul dispositivo.

- **I dispositivi utilizzano Access Commander come server NTP** – controlla l'ora sui dispositivi in base all'ora impostata**Access Commander**.

Automazione

La funzione Automation è disponibile in **2N Access Commander** dalla versione firmware 3.2 con le licenze Advanced, Pro e Unlimited. Costruita sulla piattaforma Node-RED, questa aggiunta offre direttamente ad **Access Commander** ampie capacità di programmazione basate sul flusso. Consente agli utenti di collegare **Access Commander** con vari sistemi di terze parti e di automatizzare flussi di lavoro personalizzati basati su eventi all'interno della piattaforma.

ATTENZIONE
Per sfruttare appieno questo versatile strumento di automazione, è necessario tenere presente quanto segue:

- **Responsabilità del cliente per la sicurezza**: Gli utenti sono responsabili di garantire che le loro configurazioni e flussi di lavoro di automazione siano sicuri e in linea con le best practice di sicurezza informatica. Ciò include la protezione dell'ambiente Node-RED, la gestione appropriata delle autorizzazioni e la salvaguardia dei dati sensibili all'interno delle loro automazioni.
- **Utilizzo del nodo REST API**: Se non utilizzato correttamente, questo nodo potrebbe causare perdite di dati o modifiche indesiderate. È responsabilità dell'utente assicurarsi che il nodo sia configurato e implementato correttamente. Si prega di prestare attenzione e di ricontrollare le impostazioni per evitare potenziali rischi per i dati.
- **Nodi e componenti aggiuntivi di terze parti**: 2N Telekomunikace non è responsabile per l'uso o l'integrazione di nodi di terze parti, componenti aggiuntivi o modifiche personalizzate a Node-RED all'interno della funzionalità di automazione. I clienti devono valutare attentamente e garantire la sicurezza e la stabilità di tutti i componenti aggiuntivi che scelgono di installare. Eventuali problemi derivanti da estensioni di terze parti dovranno essere risolti dal cliente o dal rispettivo fornitore terzo.
- **Limitazioni del supporto tecnico**: Sebbene il nostro team di supporto fornirà assistenza per i problemi relativi alla funzionalità di base della funzionalità di automazione all'interno di 2N Access Commander, inclusi i nostri nodi Access Commander personalizzati, non sarà in grado di fornire assistenza per la progettazione, lo sviluppo o il debug di flussi Node-RED personalizzati. Gli utenti che desiderano creare automazioni complesse potrebbero dover cercare ulteriore supporto da esperti qualificati di Node-RED o consultare le risorse disponibili.

Per iniziare a usare Node-RED, è consigliabile esplorare le funzionalità disponibili risorse online, come manuali dettagliati e numerosi tutorial su YouTube su Node-RED, che forniscono indicazioni sulla creazione e la gestione dei flussi.

Per ulteriori informazioni sui nodi personalizzati di **Access Commander** e sull'uso della funzione Automazione in **Access Commander**, consultare il presente manuale.

Questa funzione migliora le capacità di **Access Commander**. Si consiglia di esplorarne il potenziale garantendo la sicurezza delle configurazioni.

Creare automazioni

Le attività automatizzate vengono create in un editor esterno. Si accede all'editor da una scheda nella pagina **Impostazioni > Configurazione > scheda Automazione**. Le modifiche apportate nell'editor avranno effetto solo dopo essere state distribuite al server, operazione che viene eseguita tramite un pulsante Deploy nell'angolo in alto a destra dell'editor.

La creazione di attività automatizzate si basa sulla compilazione di flussi. I flussi vengono ricavati da singoli nodi collegati tra loro. Nel pannello di sinistra viene visualizzato un menu di nodi. Nel pannello di sinistra è possibile cercare i nodi in base al nome. È anche possibile aggiungere un nuovo nodo dopo aver creato una nuova connessione da un nodo esistente.

I dati trasmessi tra i nodi vengono definiti messaggi. La loro descrizione e il lavoro con loro sono dettagliati Qui. Questo stand descrive anche i nodi di base (nodi) che elaborano il formato dei singoli messaggi o le loro sequenze, come i nodi Cambia, Dividi, Unisci,... L'automazione può funzionare non solo con i dati ottenuti in questo compito unico (msg.), ma può anche funzionare con valori dinamici nel contesto dell'intera cronologia del flusso (flow.) o anche di tutti i flussi nell'installazione (global.).

ATTENZIONE
Pulsante Deploy invia i flussi impostati al server. Solo inviando al server i nuovi flussi avranno effetto!

Modalità provvisoria (safe mode)

La modalità provvisoria è uno strumento chiave per risolvere i problemi di automazione. L'esecuzione dell'editor in modalità provvisoria ti consente di apportare modifiche ai flussi senza che tali flussi vengano eseguiti in background. Ciò significa che puoi accedere all'editor, modificare ciò di cui hai bisogno e quindi ridistribuire le modifiche con un pulsante Deploy. Questa modalità è particolarmente utile se uno qualsiasi dei flussi causa il malfunzionamento o l'arresto anomalo di Node-RED, ad esempio a causa di un errore nel flusso o di un nodo di terze parti, oppure se il flusso deve essere interrotto immediatamente.

Nodi (nodes) Access Commander

REST API

Il nodo REST API invia una richiesta API HTTP definita. I dati di input contenuti nella proprietà **body** sono utilizzati come punti di richiesta di questa applicazione. L'output del nodo è costituito dai dati di risposta alla richiesta. La selezione e l'ordinamento dei dati di output possono essere specificati nel parametro **Query**.

Parametri del nodo

- **Method** – offre una scelta di metodi di richiesta API.
- **Endpoint** – è usato per specificare l'intero endpoint a cui verrà indirizzata la richiesta. Il percorso dell'endpoint può essere completato con il parametro points.
  L'utilizzo delle richieste HTTP è descritto in HTTP API (p. 117).
- **Query** – è usato per specificare quali parametri di dati devono essere trattati nell'endpoint e come devono essere restituiti nell'output. Questo parametro può essere specificato da un valore di input, la proprietà **query**. Una descrizione della costruzione delle **query** è contenuta nel documento Data Query Customization (solo in inglese).
- **Only send non-2xx responses to Catch node** – questa opzione influisce sul tipo di risposte HTTP che verranno catturate nel nodo Catch.
- **Name** – consente di rinominare il nodo per orientarsi meglio quando si lavora con il flusso.

Access log

Il nodo legge i record del Registro accessi e ne consente l'ulteriore elaborazione.

L'amministratore può impostare attività automatiche da eseguire quando **Access Commader** vede una voce di registro definita. La definizione dell'azione avviene nelle impostazioni del nodo. L'output è costituito da dati specifici sull'evento registrato. Una funzione basata su SignalR viene eseguita in background.

Parametri del nodo

- **Filter** – è usato per specificare quali record il nodo deve elaborare. I record che non corrispondono a questo filtro saranno ignorati dal flusso. Il formato del filtro è un oggetto JSON. Questo parametro può essere sovrascritto dal valore di input.
- **Name** – consente di rinominare il nodo per orientarsi meglio quando si lavora con il flusso.

System Log

Il nodo carica i record nel registro di sistema e consente l'ulteriore elaborazione di questi record.

L'amministratore può impostare attività automatiche da eseguire quando **Access Commader** vede una voce di registro definita. La definizione dell'azione avviene nelle impostazioni del nodo. L'output è costituito da dati specifici sull'evento registrato. Una funzione basata su SignalR viene eseguita in background.

Parametri del nodo

- **Filter** – è usato per specificare quali record il nodo deve elaborare. I record che non corrispondono a questo filtro saranno ignorati dal flusso. Il formato del filtro è un oggetto JSON. Questo parametro può essere sovrascritto dal valore di input.
- **Name** – consente di rinominare il nodo per orientarsi meglio quando si lavora con il flusso.

SignalR

Il nodo SignalR legge i dati nell'argomento da rimuovere. Il nodo recupera i dati in tempo reale, quindi è adatto a scenari in cui l'attività automatizzata consiste nel recuperare informazioni da Access Commander senza la necessità di un polling costante.

Parametri del nodo

- **Topic** – offre argomenti disponibili per la sottoscrizione.
- **Filter** – è usato per specificare quali record il nodo deve elaborare. I record che non corrispondono a questo filtro saranno ignorati dal flusso. Il formato del filtro è un oggetto JSON. Questo parametro può essere sovrascritto dal valore di input.
- **Name** – consente di rinominare il nodo per orientarsi meglio quando si lavora con il flusso.

Ulteriori informazioni sulla funzionalità di SignalR sono fornite nel capitoloSignalR (p. 117).

Dynamic SignalR

Il nodo Dynamic SignalR rispetto al nodo SignalR consente di modificare dinamicamente il campionamento dei dati. Ciò può includere la modifica dell'argomento o del metodo di campionamento in base ai valori di ingresso. I valori di uscita del nodo sono sia i dati recuperati dall'argomento (Data) sia le informazioni sul successo o il fallimento dell'azione del nodo.

Parametri del nodo

- **Topic** – definisce l'argomento per il quale deve avvenire la modifica del recupero dei dati.
- **Filter** – è usato per specificare quali record il nodo deve elaborare. I record che non corrispondono a questo filtro saranno ignorati dal flusso. Il formato del filtro è un oggetto JSON. Questo parametro può essere sovrascritto dal valore di input.
- **Records** – definisce il numero di record da leggere quando si usa il tipo di lettura fetch.
- **Fetch When Ready** – imposta se i valori devono essere recuperati quando viene attivato il comando fetch.
- **Name** – consente di rinominare il nodo per orientarsi meglio quando si lavora con il flusso.

Valori di input validi

Il nodo accetta le seguenti proprietà come valori di input. I valori di input validi sovrascrivono temporaneamente i parametri impostati nella configurazione del nodo.

- **topic** – una stringa che specifica l'argomento da rimuovere.
- **filter** – concatenati in formato JSON, che specificano i record da recuperare.
- **fetchWhenReady** – bootlean che specifica il parametro del nodo Fetch When Ready.
- **action** – una stringa che specifica l'azione da eseguire. Può essere sottoscrivere, annullare l'iscrizione...
- **update** – può contenere timestamp (stringa) e timeWindow (oggetto) che indicano quando l'azione da eseguire è stata modificata.

Ulteriori informazioni sulla funzionalità SignalR sono fornite nel capitolo SignalR (p. 117).

Write system log

Il nodo Write system log crea una voce di registro di sistema di Access Commander. La voce di registro contiene la gravità specificata, la descrizione dell'evento e altri dettagli. Se durante il processo si verifica un errore, questo viene registrato e lo stato del nodo viene aggiornato di conseguenza. Il nodo non ha valori di uscita.

Parametri del nodo

- **Severity** – determina la gravità del record. Questo parametro può essere specificato dal valore di input della query.
- **Filter** – è usato per specificare quali record il nodo deve elaborare. I record che non corrispondono a questo filtro saranno ignorati dal flusso. Il formato del filtro è un oggetto JSON. Questo parametro può essere sovrascritto dal valore di input.
- **Detail** – è utilizzato per una descrizione più dettagliata del record, che viene visualizzata nel log di sistema. Questo parametro può essere sovrascritto da un valore di input.
- **Name** – consente di rinominare il nodo per orientarsi meglio quando si lavora con il flusso.

Valori di input validi

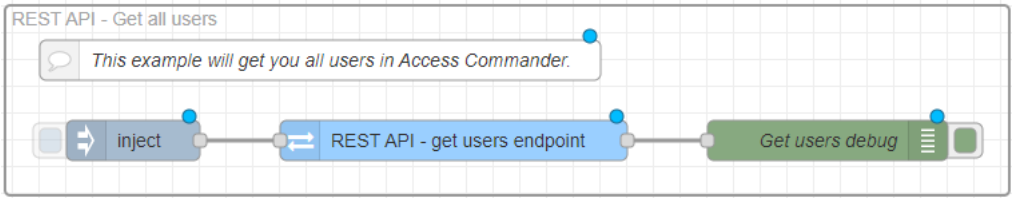
Il nodo accetta le seguenti proprietà come valori di input. I valori di input validi sovrascrivono temporaneamente i parametri impostati nella configurazione del nodo.

- **severity** – une chaîne de caractères spécifiant la gravité de l'enregistrement.
- **event** – una stringa che descrive brevemente l'azione registrata.
- **detail** – stringa che compila la descrizione dettagliata del record che verrà visualizzata nel registro di sistema.

Esempi di flussi (flows)

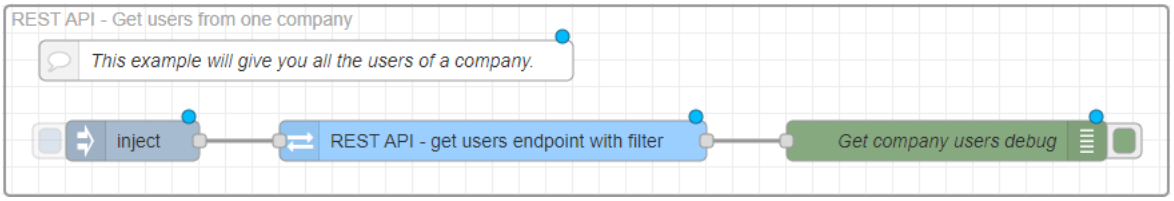
Access Commander offre diversi compiti automatizzati di base che rappresentano le possibilità di utilizzo dell'automazione. I flussi di questi compiti possono essere installati quando si avvia per la prima volta la funzione Automazione in **Access Commander**, ma possono anche essere importati in seguito, vedi Esporta/Importa flussi (p. 100). Questi flussi predefiniti possono essere facilmente modificati per i propri scopi.

Get all users



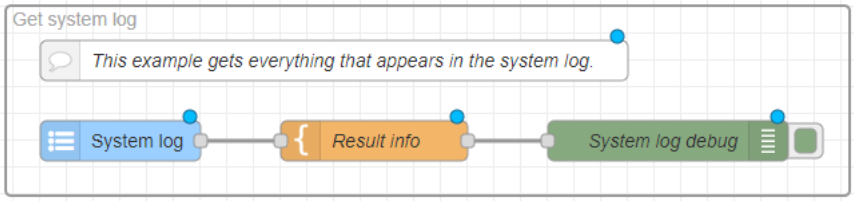
Questo flusso genera un elenco di tutti gli utenti, comprese le loro informazioni. L'attività viene avviata attivando il nodo Inject. È possibile applicare un filtro al nodo endpoint **REST API – get users endpoint** per specificare quali utenti il processo deve restituire. In questo modo, l'output del processo può essere adattato alle esigenze dell'amministratore.

Get users from one company



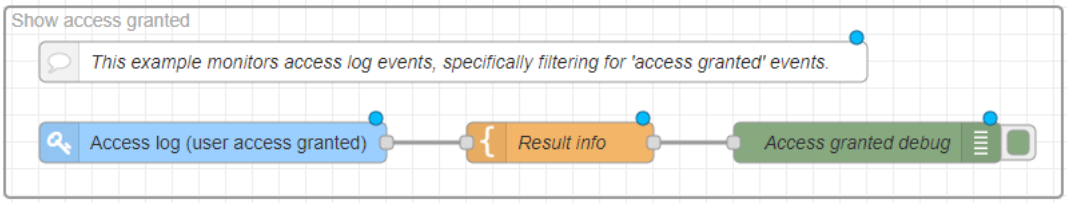
Questo flusso genera un elenco di tutti gli utenti di una singola azienda, con le relative informazioni. L'attività viene avviata attivando il nodo Inject. La selezione dell'azienda è impostata nel nodo **REST API – get users endpoint with filter** specificando il suo id.

Get system log



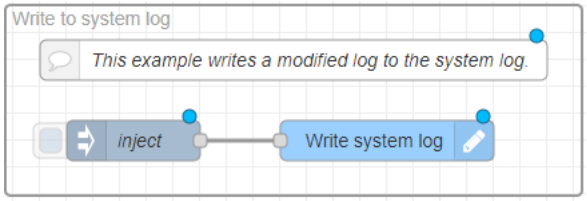
Questo flusso recupera tutte le nuove voci nel registro di sistema. La selezione degli eventi può essere affinata specificando un filtro nel nodo **System log**.

Show access granted



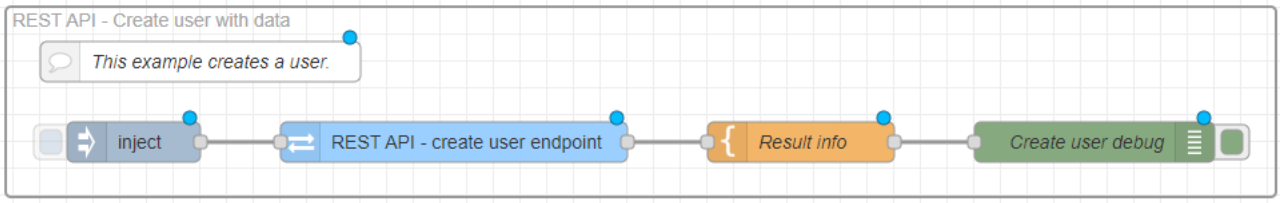
Questo flusso recupera tutte le nuove voci nel registro di accesso. Lo stream è impostato per caricare solo l'accesso concesso. Nel nodo **Access log** è possibile modificare questa restrizione.

Write to system log



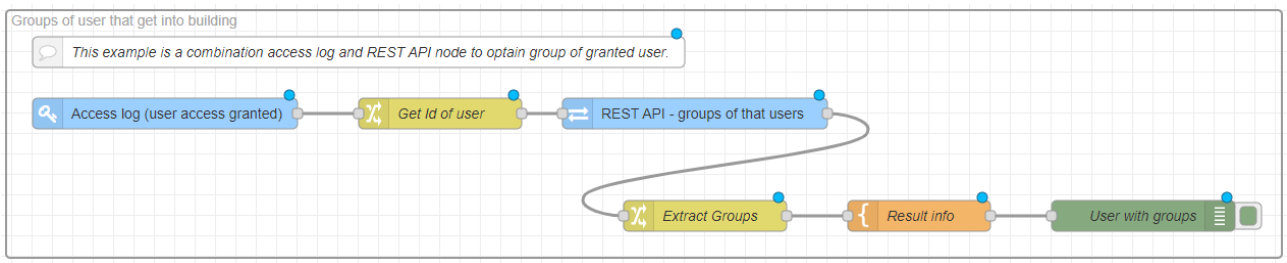
Questo flusso crea una voce nel registro di sistema. nel nodo **Write system log** è possibile impostare la Gravità, il nome e la descrizione dettagliata del record.

Create user with data



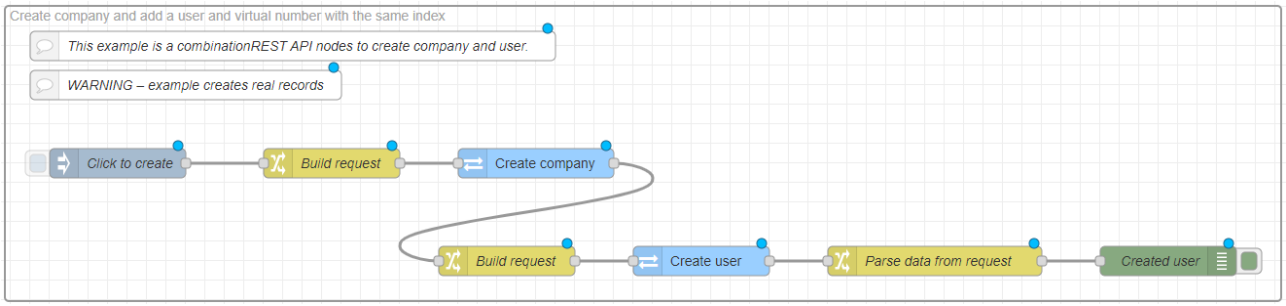
Questo flusso viene utilizzato per creare un nuovo utente. Un'attività viene avviata attivando un nodo **Inject**. Nodo **Inject** contiene un corpo del messaggio che specifica il nome dell'utente Joe Doe e la sua classificazione nell'azienda con ID 1. Questo corpo viene applicato nel nodo **Rest API - create user endpoint** e in base ad esso l'utente li crea. Nodo **Result info** imposta la dicitura del messaggio che apparirà nei messaggi di Debug.

Groups of users that get into building



Questo flusso recupera gruppi di utenti a cui è stato concesso l'accesso. Gli accessi consentiti vengono caricati dal registro accessi. Successivamente, il flusso ottiene l'ID dell'utente a cui è stato concesso l'accesso e utilizza il nodo **REST API - groups of that users** recupera i dati su questo utente. Nodo **Extrack Groups** ottiene i nomi dei gruppi di questo utente e del nodo **Result info** redigerà il testo della relazione finale.

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



Questo flusso crea una nuova azienda, il primo utente di quell'azienda e il suo numero virtuale. Un'attività viene avviata attivando un nodo**Inject**. All'avvio, verrà generato un numero intero casuale, che verrà utilizzato nel nome dell'azienda, nel nome dell'utente e fungerà da numero virtuale. Nodo**Create company** crea una società con un nome definito. Dalla risposta di questo nodo si ottiene l'ID dell'azienda, in base al quale verrà inviato il nodo successivo **Create user** crea un nuovo utente in questa azienda e gli assegna contemporaneamente un numero virtuale. Nodo **Parse data from request** quindi recupera il nome dell'azienda, il nome utente e il loro numero virtuale.

Esporta/Importa flussi

I flussi possono essere esportati in file .json e successivamente reimportati nell'interfaccia di automazione. L'esportazione e l'importazione si effettuano tramite il menu esteso in alto a destra. Gli stream spostati da un'installazione di **Access Commander** a un'altra potrebbero dover essere modificati.

Nelle opzioni di importazione sono presenti flussi di esempio precaricati per **Access Commander**. Si trova nella scheda Esempi, nella cartella Access-Commander-nodi.

ATTENZIONE
Le impostazioni delle funzionalità avanzate non supportate dalla nuova licenza non vengono salvate.

Pertanto, quando si termina la licenza Trial, non bisogna dimenticare di esportare i flussi configurati.

Stati di errore

Quando si lavora con le automazioni, possono occasionalmente verificarsi errori che ne compromettono la stabilità e la funzionalità. Se si verifica una condizione di errore, la scheda Automazione di **Access Commander** segnala la condizione e propone di riavviare la piattaforma Node-RED in modalità di sicurezza. La modalità di sicurezza interrompe temporaneamente l'esecuzione dei flussi e consente di riparare in modo sicuro i flussi che provocano la condizione di errore. Il riavvio dei flussi si attiva con il pulsante Deploy.

Esistono due condizioni di errore fondamentali:

- **Node-RED non risponde**
  Questa condizione si verifica quando Node-RED non risponde. Nessuna automazione impostata è in esecuzione. Questo problema può essere causato da vari fattori, come sovraccarico del sistema, errori nelle impostazioni del flusso o conflitti tra moduli di terze parti importati.
- **Node-RED è instabile**
  L'instabilità di Node-RED si manifesta riavviando ripetutamente la piattaforma, il che può interrompere il funzionamento dell'automazione e causare la perdita di dati. In genere si verifica un riavvio ripetuto se uno dei flussi non è configurato correttamente e attiva un riavvio. Tutti gli streaming sono sospesi per tutta la durata del riavvio.

Nome dell'installazione

Il nome dell'installazione specifica di **Access Commander** viene visualizzato nell'intestazione dell'interfaccia web e viene mostrato a tutti gli utenti connessi. Il nome predefinito di **Access Commander** può essere modificato, ad esempio, con l'indirizzo dell'edificio gestito da una determinata installazione.

Per modificare il nome, andare in **Impostazioni > Configurazione > scheda Nome installazione**. È possibile utilizzare la modifica del nome per distinguere le singole installazioni se una persona gestisce più installazioni. Il nome dell'installazione viene scritto anche nelle e-mail inviate alle aziende.

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.

1. Le impostazioni vengono effettuate in **Impostazioni > Configurazione > E-mail**.
2. 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.
3. 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).
4. 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**.
5. Puoi verificare le impostazioni effettuate inviando una email di prova.

Autenticazione a due fattori

L'autenticazione a due fattori offre un livello superiore di sicurezza dell'account utente in Access Commander. Per accedere, l'utente inserisce le credenziali di accesso e poi deve confermare l'accesso utilizzando l'applicazione di autenticazione. Una volta che l'amministratore ha abilitato la necessità dell'autenticazione a due fattori, all'utente viene richiesto di collegare l'account alla propria applicazione di autenticazione al successivo accesso.

Access Commander non le richiede di verificare nuovamente la sua identità ogni volta che accede o esegue azioni protette. Una volta completata la verifica, il sistema si ricorda di lei per un periodo di tempo limitato:

- 7 giorni per i login normali
- 5 minuti per le azioni considerate critiche per la sicurezza, come la modifica delle chiavi API, l'aggiornamento della propria password o la modifica della password di root.

Il sistema può ricordare fino a due dispositivi autenticati. Se si autentica da un nuovo dispositivo, il dispositivo ricordato più vecchio viene rimosso. Se cerca di eseguire un'azione critica per la sicurezza al di fuori della

finestra temporale consentita, il sistema le chiederà semplicemente di autenticarsi di nuovo prima di poter procedere.

1. L'autenticazione a due fattori viene impostata dall'amministratore nella scheda **Impostazioni > Configurazione > Autenticazione a due fattori**.
2. L'amministratore può selezionare gli utenti che richiedono l'autenticazione a due fattori.
   Opzioni per richiedere la verifica in due fasi
   - **Opzionale**
     L'autenticazione a due fattori è facoltativa. Gli utenti possono attivarlo da soli sul proprio profilo.
   - **Richiesto per gli utenti con il ruolo**
     Ogni utente a cui è stato assegnato un ruolo deve confermare il proprio accesso utilizzando un'applicazione di autenticazione.
   - **Obbligatorio**
     Tutti gli utenti devono confermare il loro accesso utilizzando l'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:

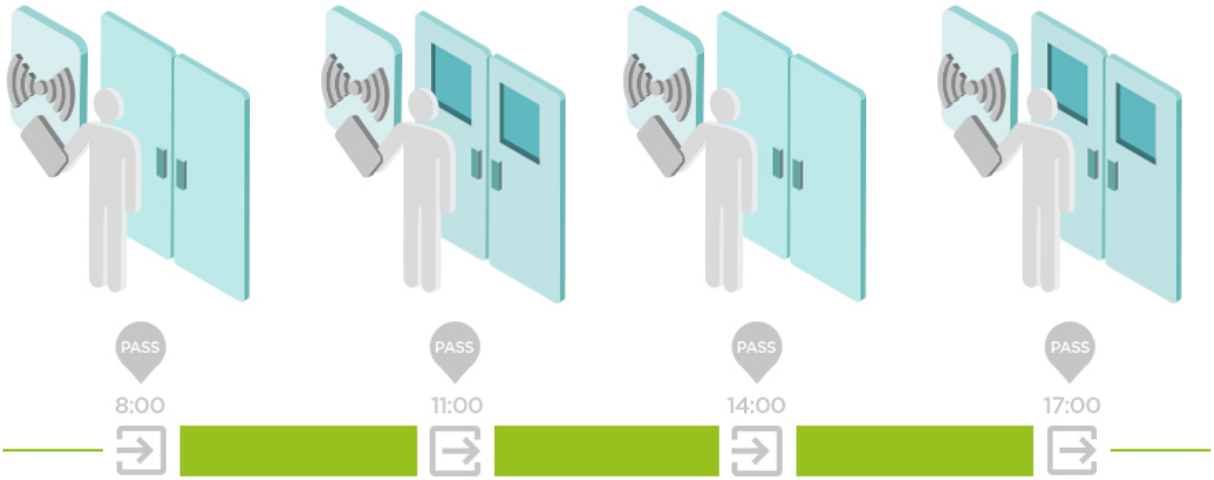
1. Fare clic sull'immagine dell'utente nell'angolo in alto a destra per aprire il menu utente.
2. Utilizzare la scheda Applicazioni di autenticazione per collegare l'account all'applicazione di autenticazione selezionata. Seguite le istruzioni riportate in **Access Commander**.
3. Selezionare Mostra profilo.

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

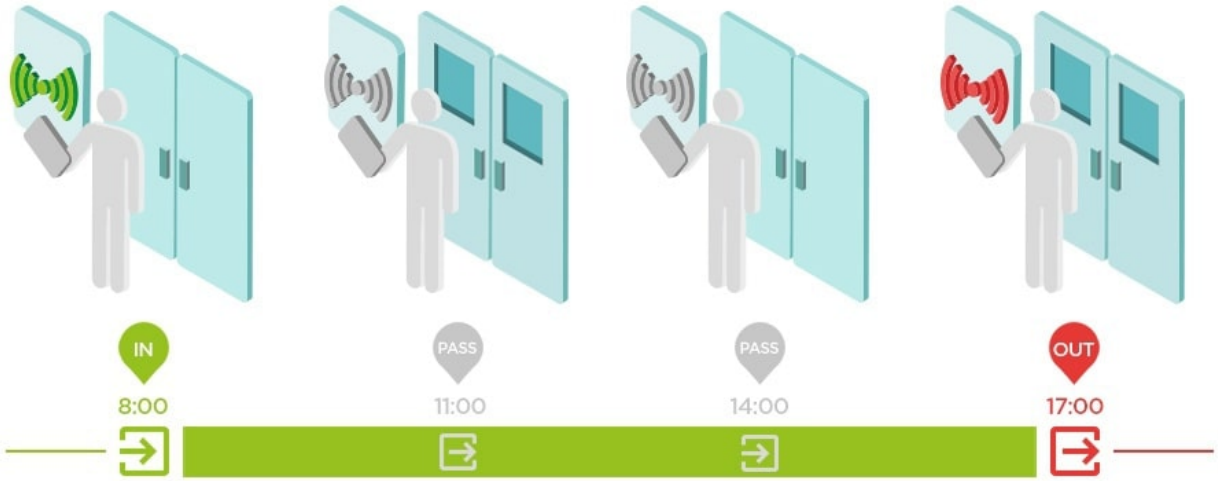
- **FREE**



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**

  Per un funzionamento corretto, il dispositivo deve essere impostato per entrare e uscire dall'area.



- **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

È possibile dividere logicamente ogni dispositivo in due punti di accesso - arrivo e partenza. Ogni punto di accesso rappresenta un passaggio in una direzione e determina se l'utente del dispositivo entra o esce dalla zona. Un punto di accesso può essere controllato da uno o più moduli del dispositivo. Tutti i moduli assegnati gestiscono quindi i passaggi in direzione del punto di accesso specifico. I punti di accesso sono utilizzati soprattutto nelle situazioni in cui un dispositivo si trova al confine di due zone e la direzione del movimento tra di esse deve essere registrata con precisione (ad esempio, per le funzioni anti-passback).

I punti di accesso sono utilizzati anche per tracciare gli utenti nel modulo Presenza (p. 82). I punti di accesso sono utilizzati anche per tracciare l'ingresso e l'uscita nel modulo Restrizioni di zona (p. 84).

NOTA
Nell'interfaccia di configurazione web di ogni dispositivo, i punti di accesso sono indicati come **Entrata** e **Uscita**. Per configurarle, accedere a **Accesso > Regole di accesso > selezionare la scheda « Accesso e uscita »**.

Abilitazione dei punti di accesso in Access Commander

1. Vai alla pagina Zone v **Access Commander**.
2. Nell'angolo in alto a destra, premi e abilitare l'uso dei punti di accesso.

Assegnazione del modulo per l'arrivo o la partenza

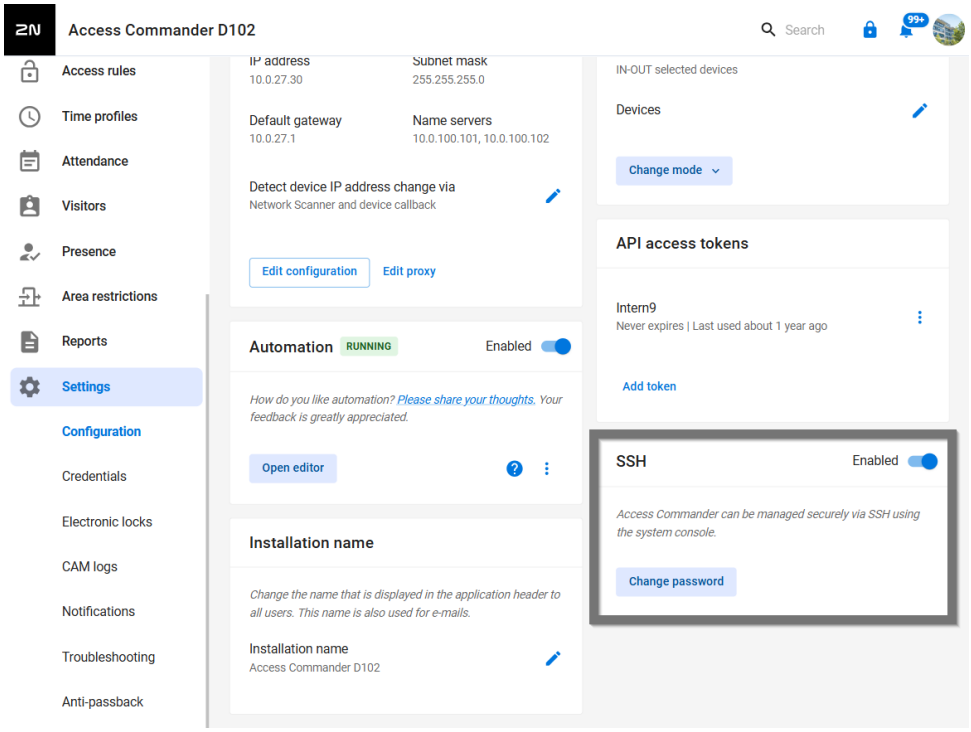
1. Accedere all'interfaccia di configurazione web del dispositivo.

> **SUGGERIMENTO**
>
> Può accedere all'interfaccia di configurazione web cliccando su nell'elenco della pagina Dispositivi.

2. Vada su **Accesso > Regole di accesso**.
3. Nella scheda **Arrivo** o **Partenza** sotto **Moduli** faccia clic su Gestione.
4. Si apre una finestra di dialogo con un elenco dei moduli di gestione degli accessi disponibili.
5. Trascini i moduli in gruppi in base alla direzione che devono fornire.

> **SUGGERIMENTO**
>
> Clicchi su per individuare un modulo specifico. Il modulo emette un segnale visivo o acustico, a seconda delle sue capacità.

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.

Usare la scheda **Impostazioni > Configurazione > SSH** per attivare Secure Shell, che fornisce una comunicazione remota sicura con la console del sistema. L'abilitazione di SSH consente di eseguire il backup e il ripristino del sistema o di riavviare completamente **Access Commander**.

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

NOTA
La password root viene modificata nella console di configurazione, non in Access Commander.

L'accesso SSH può anche essere attivato e gestito direttamente nella console di configurazione di Linux, vedere Impostazioni di Linux (p. 88).

Chiavi di crittografia per l'applicazione My2N

Gli utenti possono utilizzare l'applicazione My2N per collegarsi ai dispositivi 2N. La comunicazione tra l'applicazione My2N e il dispositivo è sempre crittografata. **Access Commander** gestisce automaticamente le chiavi di accoppiamento del sistema che vengono distribuite ai dispositivi abilitati WaveKey per garantire un accoppiamento sicuro e affidabile. Senza conoscere la chiave di crittografia, l'applicazione My2N non può autenticare l'utente. La chiave di crittografia primaria viene generata automaticamente al primo avvio del citofono o, nel caso della gestione di **Access Commander**, come parte della sua configurazione. La chiave può essere rigenerata manualmente in qualsiasi momento. La chiave di crittografia primaria viene trasferita insieme all'ID di autorizzazione al dispositivo mobile durante l'accoppiamento.

NOTA
Nel sistema vengono utilizzati due tipi di chiavi: **chiavi di corrispondenza** e **chiavi di accesso**. Le chiavi di accoppiamento vengono utilizzate per autenticare l'applicazione mobile My2N con il dispositivo. Le chiavi di accesso determinano le autorizzazioni alle funzioni all'interno dell'applicazione mobile.

Creazione di nuove chiavi

1. Accedere a **Impostazioni > Autenticazione > scheda Chiavi di crittografia per l'applicazione My2N**. È possibile generare fino a 4 chiavi di accesso. Quando tenta di generare una quinta chiave **Access Commander** avvertirà che la sua generazione eliminerà la chiave più vecchia. La scheda elenca i tempi di generazione di ciascuna chiave.
2. Cliccare su Generare una nuova chiave.

   SUGGERIMENTO
   Per motivi di sicurezza, si raccomanda di rigenerare le chiavi di accoppiamento una volta ogni periodo di tempo più lungo (ad esempio, una volta all'anno).

3. La nuova chiave generata viene caricata automaticamente nell'app My2N la prima volta che il telefono cellulare viene utilizzato con un dispositivo precedentemente accoppiato.

La chiave generata può essere cancellata cliccando su .

SUGGERIMENTO
Per un livello di sicurezza superiore, è preferibile effettuare l'accoppiamento utilizzando il **codice QR** , che contiene la chiave pubblica. Se il codice QR non è disponibile, può utilizzare l'accoppiamento del **PIN** .

ATTENZIONE
L'accoppiamento del codice QR è supportato solo sui dispositivi con firmware HIP 2.50.0 e successivi (inclusa la serie 3.0). In un ambiente con Access Commander è possibile visualizzare il **codice QR** , ma l'accoppiamento su versioni precedenti di HIP avrà successo solo utilizzando il **PIN** .

NOTA

- Se l'applicazione My2N non ha accesso a nessuna chiave di crittografia valida, non può essere utilizzata per l'autenticazione dell'utente. Per ripristinare la funzionalità dell'applicazione, questa deve essere riaccoppiata con il dispositivo collegato a Access Commander, che caricherà le chiavi di crittografia valide nell'applicazione My2N.
- Consentire l'accesso al dispositivo dipende dai diritti di accesso impostati dell'utente.

Modalità di compatibilità della scheda RFID

Se **Access Commander** segnala che la nuova tessera appena aggiunta è già in uso nel sistema, il motivo potrebbe essere che la modalità di compatibilità della tessera RFID è abilitata. Questa modalità viene attivata dall'amministratore in **Impostazioni > Autenticazione > scheda Impostazioni modalità compatibilità**.

ATTENZIONE

- La modalità di compatibilità deve essere attivata solo in caso di problemi con il caricamento delle carte precedentemente registrate. L'uso della modalità di compatibilità può influire sui meccanismi di autenticazione
- La modalità di compatibilità non è consigliabile combinare con l'uso di carte protette dalle tecnologie PiCard.

Chiavi PICard

Nella scheda **Impostazioni > Accesso > Chiavi PICard** sono memorizzate le chiavi di crittografia dell'applicazione 2N PICard Commander. Se le chiavi di crittografia sono caricate in **Access Commander**, la scheda visualizza il nome del progetto PICard Commander e l'identificativo numerico di esportazione della chiave. La scheda consente di eliminare le chiavi caricate da **Access Commander**.

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

Importa chiavi di crittografia PICard

1. Accedere a **Impostazioni > Accesso > scheda Tasti PICard**.
2. Dopo aver cliccato su Importare carica il file della chiave di crittografia dal tuo repository.
3. Inserisci una password per proteggere il file se ne imposti una durante l'esportazione dall'applicazione PICard Commander.

PICard Commander è un'applicazione software per la crittografia delle credenziali di accesso sulle carte di accesso. L'applicazione crea progetti che generano una serie di chiavi di crittografia e di lettura. Le chiavi di lettura del progetto possono essere importate in un dispositivo 2N o in **Access Commander**, che poi distribuisce le chiavi di lettura ai dispositivi 2N collegati.

Lettori USB abilitati

Per facilitare la registrazione di alcuni metodi di autenticazione degli utenti, è possibile utilizzare lettori USB collegati al computer su cui si accede ad **Access Commander**. I lettori devono essere abilitati in **Access Commander** in **Impostazioni > Accesso > scheda Lettori USB consentiti**.

1. Accedere a **Impostazioni > Accesso > scheda Lettore USB abilitato.**
2. Fare clic su Abilita lettori per aprire la finestra di dialogo.
3. L'attivazione/disattivazione dell'uso di un dispositivo USB esterno avviene in una finestra di dialogo.
4. Successivamente, l'abilitazione del lettore viene modificata facendo clic su Change.

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

Registri CAM

I registri CAM vengono utilizzati per registrare automaticamente diversi fotogrammi che precedono e seguono un evento selezionato. In **Impostazioni > Registri CAM**, è possibile gestire i diversi tipi di eventi per i quali generare 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
- **Chiamata**
  - Chiamata avviata

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.

Serrature elettroniche

Il sistema **Access Commander** fornisce la gestione degli accessi tramite serrature elettroniche 2N Fortis, che vengono sbloccate da carte RFID con tecnologia MIFARE® DESFire®. Quando si configurano le serrature elettroniche, a ogni serratura viene assegnata una chiave di crittografia. Le chiavi della serratura vengono quindi memorizzate sulle carte RFID degli utenti autorizzati. Se le chiavi sulla scheda e nella serratura coincidono, il meccanismo di chiusura viene sbloccato.

Una carta di accesso RFID può essere utilizzata per accedere a un massimo di 90 porte con serrature 2N Fortis, a seconda del numero di profili orari applicati. Se la capacità di memoria della carta viene superata, la scrittura dei dati sulla carta fallirà. L'evento di mancata scrittura viene registrato nel registro degli accessi al sistema. Se si utilizzano i Gruppi di chiusura, è possibile scrivere più porte su una singola scheda rispetto all'assegnazione individuale. Se si utilizzano i Gruppi di chiusura, si possono registrare più porte per scheda rispetto all'assegnazione individuale.

Fortis Commander

Fortis Commander è un'applicazione indipendente che collega le serrature elettroniche **Fortis** al sistema **Access Commander**. L'applicazione imposta i blocchi in base al file di progetto creato in **Access Commander**u che contiene la configurazione dei blocchi. Il file è criptato e può essere utilizzato solo su un'installazione specifica.

Connettori e installazione

Fortis Commander è progettato per essere installato su un computer Windows con supporto Bluetooth Low Energy (BLE).

L'applicazione è disponibile sul sito web 2N Download Centre.

Procedura d'installazione

1. Scarichi il pacchetto di installazione dal link fornito.
2. Esegua il programma di installazione e completi l'installazione seguendo le istruzioni sullo schermo.

File di progetto

Il file di progetto viene creato in **Access Commander** e contiene la configurazione completa del progetto. Il file è crittografato e protetto da password.

Impostazione dei blocchi in Access Commander

Prima di caricare le chiavi su singole serrature, deve associare **Access Commander** con **Fortis Commander**.

Generazione della Master Encryption Key (MEK) e preparazione del progetto

1. Accedere ad Access Commander.
2. Accedere a **Impostazioni > Serrature elettroniche**.
3. Nella scheda **Initial Settings** fare clic su Generate Keys.
4. Creare la chiave di crittografia principale.

ATTENZIONE
La chiave di crittografia principale non può essere visualizzata o modificata in seguito .

NOTA
In base alla chiave di crittografia principale (MEK), **2N Access Commander** genera una serie di chiavi di crittografia. Pertanto, la chiave deve essere unica e sufficientemente sicura. Il set di chiavi si basa sulla chiave di crittografia master, quindi i progetti con la stessa chiave di crittografia master generano gli stessi set di chiavi. Se un progetto viene perso, è possibile creare un nuovo progetto con la stessa chiave di crittografia master e continuare la crittografia.

5. Dopo aver generato le chiavi e impostato la password per il file di progetto, può scaricare **il file di progetto**, che è un'immagine della configurazione della serratura elettronica nel sistema **Access Commander**.
6. Nella scheda **di Fortis Commander** clicchi su Download Application, da dove inizierà a scaricare **Fortis Commander** (applicazione per la configurazione di serrature elettroniche).

ATTENZIONE
Le informazioni sul progetto sono dati sensibili. Proteggeteli dagli abusi.

Configurazione della serratura elettronica con Fortis Commander

1. Installi **Fortis Commander** e lo apra.
2. Clicchi su Apri progetto e apra il file di progetto scaricato in Esplora file.
3. Nella finestra di dialogo che appare, inserisca la password per il file di progetto.
4. Dopo aver aperto il file di progetto, selezioni Collegare al dispositivo e colleghi la carta servizi alla serratura.

5. Clicchi su **Assign**, che assegna il blocco al progetto.
6. Scolleghi il dispositivo e clicchi su **File > Chiudi progetto**.
7. Una volta completata la configurazione, apra il sistema **Access Commander**. Vada alla scheda **Impostazioni > Serrature elettroniche** e clicchi nuovamente su Fortis Commander. Carichi il file di progetto.

NOTA
Quando sposta la serratura da un'installazione all'altra o quando effettua un reclamo, deve eseguire un reset di fabbrica . Questa operazione ripristina le impostazioni di fabbrica del lucchetto e rimuove tutte le configurazioni precedenti.

Procedura di aggiornamento della configurazione

1. Apportare modifiche in **Access Commander**.
2. Scarichi il nuovo file di progetto.
3. Carichi il file su **Fortis Commander** e apporti le modifiche necessarie ai lucchetti.
4. Se apporta altre modifiche a **Access Commander**u, scarichi sempre un nuovo file di progetto.

ATTENZIONE
Per ogni modifica della configurazione in **Access Commander**u deve scaricare un nuovo file di progetto - non può utilizzare un file più vecchio che è già stato caricato su **Fortis Commander**.

Blocco e sblocco permanente

L'app le consente di bloccare e sbloccare in modo permanente il lucchetto. La funzione viene utilizzata per gli interventi di assistenza o per il controllo di emergenza senza l'uso di una scheda.

Raccolta di eventi da serrature elettroniche che utilizzano carte / chip RFID

Impostazioni della raccolta eventi

1. Apra **Impostazioni > Serrature elettroniche > Eventi scheda**.
2. Selezioni il tipo di evento:
   - **Raccogliere gli eventi di accesso e di sistema** - Tutti gli eventi di accesso e di sistema vengono registrati sulla scheda/chip e scritti nel **Registro di sistema** e nel **Registro di accesso**.
   - **Raccogliere solo gli eventi di sistema** - vengono registrati solo gli eventi di sistema, gli eventi di accesso non vengono memorizzati sulle schede.
   - **Non raccolga eventi sulle schede** - nessun evento viene scritto nella scheda; è possibile accedervi solo attraverso **Fortis Commander**u.

SUGGERIMENTO
La selezione del set di eventi appropriato può ridurre il carico del sistema e l'utilizzo della memoria. Tuttavia, un protocollo dettagliato è importante per la diagnostica e gli audit di sicurezza.

Esportazione di eventi da una scheda

La scheda memorizza un massimo di **16 primi eventi**. Gli eventi possono essere letti in due modi:

- In **Access Commander**, faccia clic sull'icona nella casella di ricerca nell'intestazione e carichi la scheda.
- Utilizzando un dispositivo con **2N OS**, gli eventi vengono letti dalla carta e inviati a **Access Commander**u.

Caricare gli eventi sul lucchetto

1. Apra **Impostazioni > Serrature elettroniche > Fortis Commander** e clicchi su Download File.
2. Apra il file in **Fortis Commander**.
3. Nell'applicazione **Fortis Commander**, si colleghi alla serratura elettronica.
4. Carichi nuovamente il file aggiornato su **Access Commander**.
5. Una volta caricati, gli eventi vengono visualizzati in **Log di accesso** e **Log di sistema**.

Operazioni di servizio

Queste operazioni sono disponibili per **Fortis Cylinder**:

- **Smontaggio** - smontaggio di serrature a scopo di assistenza.
- **Sostituzione della batteria** - sostituzione della batteria nella serratura.

ATTENZIONE
Le operazioni di servizio non sono rilevanti per altri tipi di serrature.

NOTA
Dalla modalità di assistenza, la serratura torna alla modalità normale premendo il pulsante Lock per bloccare in modo permanente.

Aggiornare la scheda

Le carte di accesso degli utenti devono essere aggiornate regolarmente. L'utente aggiorna la scheda collegandola al dispositivo IP 2N sul quale dispone di diritti di accesso validi. La carta deve essere tenuta in mano dal lettore del dispositivo fino all'accensione dell'interruttore di apertura della porta. L'interruttore di apertura della porta si attiva solo dopo l'aggiornamento dell'accesso alle serrature

È possibile modificare la validità predefinita di dieci giorni delle tessere all'indirizzo **Impostazioni > Serrature elettroniche > scheda Parametri tessera**.

ATTENZIONE
Se si modificano i diritti di accesso ai lucchetti in **Access Commander**, le modifiche si rifletteranno sulla tessera di accesso dell'utente solo dopo che questa è stata aggiornata sul lettore di tessere del dispositivo 2N! Per motivi di sicurezza, si consiglia di impostare un periodo di validità più breve per le carte, in modo da garantire che vengano aggiornate regolarmente.

I lettori IP, i dispositivi che consentono l'aggiornamento delle schede e le relative impostazioni sono descritti nel capitolo Impostazioni del lettore del dispositivo IP (p. 29).

Schede compatibili

NOTA
Ai fini della presente documentazione, il termine **carta** qualsiasi identificatore compatibile che utilizzi la tecnologia MIFARE DESFire.

Per aprire le serrature elettroniche 2N Fortis Non è possibile utilizzare carte con ID casuale.

Le carte con tecnologia PICard non possono essere utilizzate per aprire le serrature elettroniche 2N Fortis.

Profili temporali sulle serrature elettroniche

Le serrature elettroniche supportano profili temporali con le seguenti limitazioni:

- I giorni festivi non sono validi.
- È possibile impostare fino a 4 intervalli di tempo diversi nell'arco di una giornata.
- All'interno di un profilo temporale è possibile definire 4 programmi di intervalli giornalieri.

SUGGERIMENTO
Ciò significa che, ad esempio, è possibile avere impostazioni diverse per lunedì, martedì, mercoledì e giovedì, ma per venerdì, sabato e domenica è necessario utilizzare una delle impostazioni esistenti.

ATTENZIONE
Se il profilo temporale viola le restrizioni specificate, la regola di accesso verrà ignorata e all'utente non verrà concesso l'accesso.

Schede per la manutenzione

Le schede di manutenzione consentono l'accesso autorizzato alla serratura. Consentono di mettere in funzione la serratura, di cambiare la batteria, di smontare la serratura.

ATTENZIONE
La scheda di manutenzione non può essere utilizzata contemporaneamente come scheda di accesso utente.

Impostazioni della scheda Manutenzione

1. In **Access Commander** andate su **Impostazioni > Serrature elettroniche**.
2. Nella scheda **Manutenzione** fare clic su Creare.

3. Nella finestra di dialogo che si apre, selezionare il tipo di scheda che si desidera creare.
   - Impostazione di nuovi lucchetti - attiva in modalità di servizio i nuovi lucchetti precedentemente configurati nelle impostazioni di fabbrica.
   - Servizio - attiva la modalità di servizio per la serratura già impostata.
   - Smontaggio - per lo smontaggio della serratura a cilindro 2N Fortis già impostata, consultare il Manuale di installazione 2N Fortis.
   - Sostituzione della batteria - per la sostituzione della batteria della serratura a cilindro 2N Fortis già impostata, vedere il Manuale di installazione 2N Fortis.

   SUGGERIMENTO
   Una carta fisica può essere caricata contemporaneamente con **Setting New Locks** e qualsiasi altra carta servizi. Si consiglia una combinazione di **Setting New Locks** e **Service**.
4. Fare clic su Continuare a.
5. Collegare la scheda al lettore RFID USB collegato. Attendere che i dati vengano caricati sulla scheda.

La validità dei dati sulla scheda di manutenzione è di un anno. Dopo questo periodo di tempo, i dati dovranno essere cancellati e la scheda dovrà essere nuovamente impostata.

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.

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.

L'elenco delle notifiche è visualizzato anche nella pagina **Registri di sistema > Notifiche**.

I record possono essere scaricati in un file CSV cliccando sul pulsante Export 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 > Notifiche**.
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 sono impostati nei dettagli del tipo di notifica. Per aprire i dettagli del tipo di notifica, fare clic sulla notifica selezionata nell'elenco della 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.

Le notifiche appaiono in **Access Commander** sotto l'icona nella barra superiore, 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. 101).

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 .

Impostazioni di rete

Per impostare una connessione di rete, andare su **Impostazioni > Configurazione > scheda Rete**. La scheda visualizza i parametri di rete correnti di **Access Commander** e consente di impostarli. L'impostazione dei singoli parametri può essere effettuata dopo aver attivato 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.

Rilevamento della modifica dell'indirizzo IP del dispositivo

Access Commander stabilisce una connessione con i dispositivi tramite i loro indirizzi IP. Per evitare la perdita della connessione a un dispositivo con un indirizzo IP dinamico, sono disponibili due metodi per rilevare gli indirizzi IP

- **Network Scanner**
  Access Commander esegue periodicamente una scansione del segmento di rete locale utilizzando il 2N Network Scanner integrato per identificare i dispositivi collegati e i loro indirizzi IP correnti.
- **Device callback**
  Questo metodo rileva gli indirizzi IP di dispositivi esterni al segmento di rete locale. I dispositivi vengono segnalati all'avvio, quando l'indirizzo IP cambia e a intervalli regolari (una volta all'ora). Per un corretto funzionamento, è necessario specificare la destinazione a cui i dispositivi verranno segnalati (di solito l'indirizzo IP di **Access Commander**).

Network Discovery

Rilevamento rete consente ad altri servizi, come **2N IP Utility** o **2N Network Scanner**, di trovare l'installazione di **Access Commander** sulla rete locale.

Può utilizzare contemporaneamente **Network Scanner** e **Axis Utility**. Tuttavia, per motivi di sicurezza, entrambi i rilevamenti di **Access Commander** possono essere completamente disattivati nelle impostazioni del sistema.

SUGGERIMENTO

Access Commander può essere mostrato o nascosto nelle applicazioni **2N Network Scanner** e **2N Axis Utility**. Lo stesso vale per l'accesso all'interfaccia web tramite **accesscommander.local**. Se sulla rete sono in esecuzione più istanze di Access Commander, il sistema assegna automaticamente nomi univoci: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local**, e altre istanze in base al numero di server presenti sulla rete.

Impostazioni proxy

Il proxy viene utilizzato per servizi quali: Richieste HTTP, sincronizzazione FTP, aggiornamenti, ecc.

NOTA
Il proxy per FTP con autenticazione TLS non è supportato.

1. Accedere a **Impostazioni > Configurazione > scheda Rete**.
2. Selezionare Modifica proxy.
3. Nella finestra di dialogo che si apre, digitare gli indirizzi dei server proxy per i protocolli desiderati.
4. Nell'ultimo campo è possibile inserire gli indirizzi per i quali il server proxy non deve essere applicato. Le connessioni a localhost e agli indirizzi IP nell'intervallo 127.0.0.1/8 non saranno mai instradate attraverso un server proxy.
5. Dopo aver modificato le impostazioni, **2N Access Commander** si riavvia automaticamente.

Utilizzo di NodeRED

L'applicazione NodeRED ignora le impostazioni proxy del sistema. Per un corretto funzionamento, il server proxy deve essere configurato esplicitamente su ogni nodo NodeRED che ne richiede l'uso.

Informazioni aggiuntive

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

HTTP API

L'URL dell'API **Access Commander** 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.

È possibile filtrare le risposte alle richieste utilizzando Query. Il documento Data Query Customization descrive come costruire **query**.

Autenticazione

I comandi API HTTP vengono inviati con le credenziali di accesso dell'utente o utilizzando un token di autenticazione. 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 un token portatore. Quando si crea una nuova chiave di accesso API, l'amministratore può limitare la chiave alla sola lettura, in modo che la chiave autentichi solo i comandi GET. La validità della chiave può essere limitata a: 1 mese, 6 mesi, 1 anno.

ATTENZIONE
Dopo aver creato la chiave di accesso, copiarla negli appunti e utilizzarla. Non sarà possibile visualizzare la chiave in seguito.

SignalR

SignalR è uno strumento che consente la comunicazione in tempo reale tra il server e il client. Ciò significa che il server può inviare contenuto ai client connessi non appena il contenuto diventa disponibile e non deve attendere una richiesta da parte del client. I principi di base di SignalR sono descritti nel documento SignalR integration manual (solo in inglese). Elenco degli argomenti SignalR disponibili da utilizzare **Access Commander** sono descritti nel documento SignalR topics reference manual (solo in inglese).

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.

2N Access Commander – Manuale di installazione

2N.com