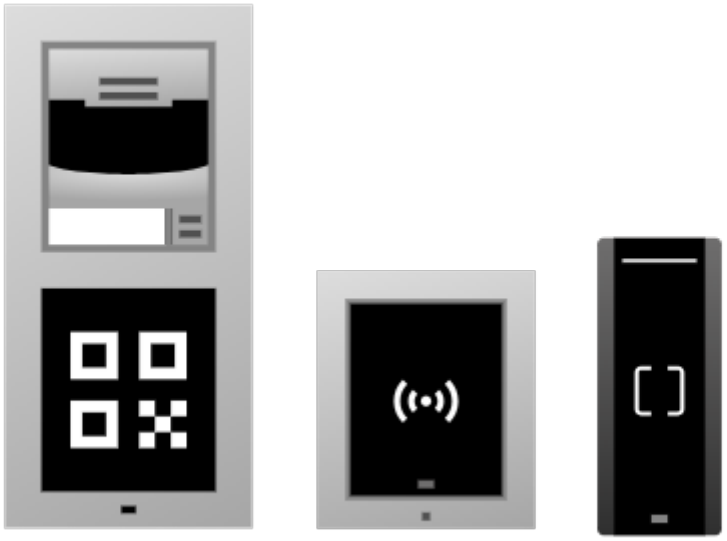
# Lettori accessi

## Manuale di configurazione



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

2N.com

# Indice

# Primo accesso

## Trovare i dispositivi sulla rete

Per accedere all'interfaccia, deve conoscere l'indirizzo IP del dispositivo o il nome di dominio del dispositivo. Il dispositivo deve essere collegato alla rete IP locale e deve essere alimentato.

### Nome del dominio

Per accedere all'interfaccia di configurazione web, può inserire un nome di dominio nel browser nel formato «hostname.local» invece dell'indirizzo IP. L'hostname di un nuovo dispositivo è costituito dal nome del prodotto e dal numero di serie del dispositivo. Quando inserisce un nome di host, utilizzi solo lettere e numeri; non utilizzi spazi, periodi, trattini o altri caratteri speciali.

**Il nome di dominio predefinito del dispositivo :** 2NAccessUnit-{numero di serie senza trattini}.local (per esempio.: «2NAccessUnit-0000000001.local»)

Il formato del nome del dispositivo specifico è specificato nel Manuale di installazione del prodotto, nel capitolo Nome di dominio.

**SUGGERIMENTO**
Può modificare l'hostname in seguito nell'interfaccia di configurazione web all'indirizzo **Sistema > Connessione di rete > scheda Configurazione avanzata > Hostname**.

L'accesso con un nome di dominio ha il vantaggio di utilizzare l'indirizzo IP dinamico del dispositivo. Mentre l'indirizzo IP dinamico cambia, il nome di dominio rimane lo stesso. È possibile generare certificati firmati da un'autorità di certificazione attendibile per un nome di dominio.

### Indirizzo IP del dispositivo

Per impostazione predefinita, il dispositivo utilizza un indirizzo IP dinamico assegnato dal server DHCP.

Per conoscere l'indirizzo IP di un dispositivo 2N sulla sua rete locale, utilizzi 2N IP Utility. L'applicazione 2N IP Utility può essere scaricata dal sito web 2N.com. Ai fini dell'installazione è necessario avere previamente installato Microsoft .NET Framework 4.7.2.

A seconda delle capacità del dispositivo, può anche scoprire l'indirizzo IP in uno dei seguenti modi:

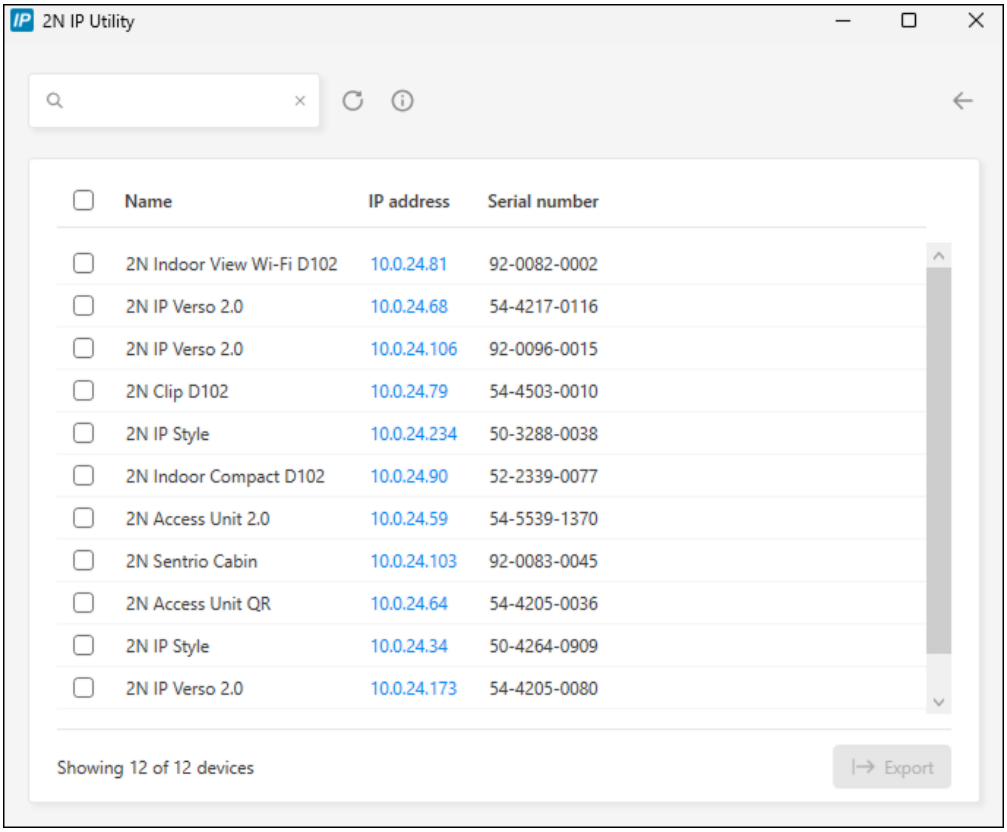
- con il pulsante RESET

### Ottenere un indirizzo IP utilizzando 2N IP Utility

Per conoscere l'indirizzo IP di un dispositivo 2N sulla sua rete locale, utilizzi 2N IP Utility. L'applicazione 2N IP Utility può essere scaricata dal sito web 2N.com. Ai fini dell'installazione è necessario avere previamente installato Microsoft .NET Framework 4.7.2.

1. Esegua il programma di installazione 2N IP Utility.
2. L'Installazione guidata guida l'utente attraverso il processo di installazione.

3. Dopo aver installato l'applicazione 2N IP Utility eseguire l'applicazione dal menu Start del sistema operativo Microsoft Windows.
   Dopo l'avvio, l'applicazione inizierà automaticamente a cercare nella rete locale tutti i dispositivi 2N e AXIS a cui è assegnato un DHCP o un indirizzo IP impostato staticamente. Questi dispositivi vengono poi mostrati nella tabella.




4. Selezioni il dispositivo che desidera configurare dall'elenco e faccia clic con il pulsante sinistro del mouse. Si aprirà la parte destra della finestra di configurazione web.

**SUGGERIMENTO**

- L'interfaccia di configurazione web è accessibile anche tramite il pulsante **Apri in un browser esterno**, che le permette di aprire l'interfaccia in una finestra separata del browser.
- Clicchi su un dispositivo nell'elenco per visualizzare le informazioni dettagliate. Clicchi sul pulsante **IP settings** per modificare l'indirizzo IP inserendo l'indirizzo IP statico desiderato o attivando il DHCP.
- L'applicazione consente anche di esportare i dispositivi selezionati in un file CSV. Innanzitutto, selezioni il dispositivo spuntando le caselle di ciascun dispositivo nell'elenco, quindi utilizzi il pulsante **Export** che appare nella parte inferiore della finestra. Il file esportato conterrà il nome, l'indirizzo IP e il numero di serie dei dispositivi selezionati.

Le credenziali predefinite sono:
Nome utente: **Admin**
Parola d'ordine: **2n**
Dopo il primo accesso è necessario modificare immediatamente la password.

**SUGGERIMENTO**
Si consiglia di utilizzare una password difficile da decifrare. Si sconsiglia di utilizzare nomi, nomi di luoghi o cose nella password, soprattutto quelli che hanno un collegamento diretto con l'utente.

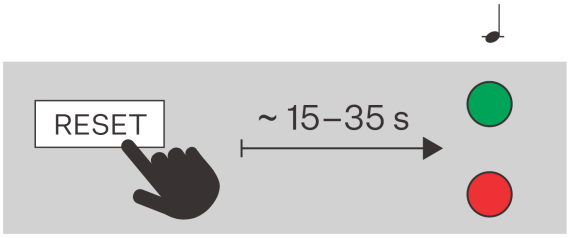
Per una maggiore sicurezza della password, consigliamo:

- utilizzare un generatore di password casuali,
- lunghezza della password di almeno 12 caratteri,
- una combinazione di caratteri diversi provenienti da set di caratteri diversi (ad esempio lettere minuscole/maiuscole, numeri, caratteri speciali, ecc.).

## Trovare l'indirizzo IP utilizzando l'hardware

Per conoscere l'indirizzo IP attuale procedere come segue:

1. Tenere premuto il pulsante RESET.
   a. Attendere fino a quando i LED rosso e verde sull'apparecchio si accendono contemporaneamente e viene emesso un segnale acustico (circa 15–35 s).
2. Rilasciare il pulsante RESET.
3. Il dispositivo annuncerà automaticamente l'indirizzo IP corrente tramite voce.




**NOTA**
L'intervallo di tempo dalla pressione del pulsante RESET alla prima segnalazione luminosa e sonora è compreso tra 15 e 35 s, dipende sempre dal modello specifico del dispositivo.

## Commutazione DHCP

Per impostazione predefinita, il dispositivo utilizza un indirizzo IP dinamico assegnato dal server DHCP.

## Indirizzo IP dinamico

Il DHCP (Dynamic Host Configuration Protocol) è un protocollo di rete che mantiene un elenco di indirizzi IP disponibili e li assegna automaticamente ai dispositivi della rete locale. L'indirizzo IP assegnato è dinamico, quindi al dispositivo può essere assegnato un nuovo indirizzo IP dopo un periodo di tempo (tempo di locazione).

## Indirizzo IP statico

Se l'indirizzo IP del dispositivo deve rimanere invariato, deve disabilitare l'assegnazione dell'indirizzo IP da parte del server DHCP sul dispositivo. Può disattivare il server DHCP nell'interfaccia di configurazione web o utilizzando l'hardware del dispositivo.

**NOTA**
I valori specifici per l'indirizzo IP statico possono essere impostati solo nell'interfaccia di configurazione web del dispositivo.

## Impostazione dei parametri di rete nell'interfaccia di configurazione web

1. Vada all'interfaccia di configurazione web.
2. Acceda a **Sistema > Connessione di rete > scheda Impostazioni di base > Impostazioni indirizzo IP**.
3. Imposta i parametri di rete desiderati.
4. Salvi le sue modifiche.

## Commutazione del DHCP sull'hardware del dispositivo

A seconda delle capacità del dispositivo, l'indirizzo IP può essere commutato come segue:

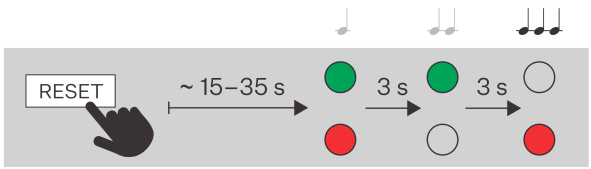
- con il pulsante RESET

**SUGGERIMENTO**
Per la posizione del pulsante RESET, faccia riferimento al Manuale di installazione del prodotto.

### Impostazione di un indirizzo IP dinamico utilizzando il pulsante RESET

Per impostare la configurazione di rete di un dispositivo con indirizzo IP dinamico (DCHP ON), seguire i punti seguenti:

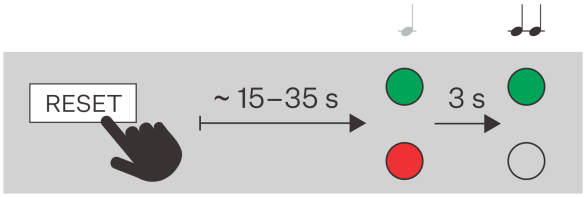
1. Tenere premuto il pulsante RESET.
   a. Attendere fino a quando i LED rosso e verde sull'apparecchio si accendono contemporaneamente e viene emesso un segnale acustico (circa 15–35 s).
   b. Attendere fino allo spegnimento del LED rosso e all'attivazione della segnalazione sonora (ulteriori 3 s circa).
   c. Attendere fino allo spegnimento del LED rosso, poi alla sua riaccensione e infine all'attivazione della segnalazione sonora (ulteriori 3 s circa).
2. Rilasciare il pulsante RESET.



### Impostazione di un indirizzo IP statico utilizzando il pulsante RESET

Per impostare la configurazione di rete del dispositivo sulla modalità con indirizzo IP statico (DHCP OFF), procedere come segue:

1. Tenere premuto il pulsante RESET.
   a. Attendere fino a quando i LED rosso e verde sull'apparecchio si accendono contemporaneamente e viene emesso un segnale acustico (circa 15–35 s).
   b. Attendere fino allo spegnimento del LED rosso e all'attivazione della segnalazione sonora (ulteriori 3 s circa).
2. Rilasciare il pulsante RESET.




**NOTA**

Dopo il riavvio il dispositivo avrà i seguenti parametri di rete impostati:

- Indirizzo IP: 192.168.1.100
- Maschera di rete: 255.255.255.0
- Gateway predefinito: 192.168.1.1

## Accesso alla configurazione del dispositivo basata sul web

La configurazione del dispositivo avviene attraverso un'interfaccia di configurazione basata sul web, accessibile da un browser web.

Per accedere all'interfaccia, deve conoscere l'indirizzo IP del dispositivo o il nome di dominio del dispositivo. Il dispositivo deve essere collegato alla rete IP locale e deve essere alimentato.

L'interfaccia di configurazione basata sul web è accessibile anche dal portale My2N collegato o dallo strumento di configurazione 2N Access Commander.

### Acceda all'interfaccia di configurazione web

1. Avvii il suo browser internet.
2. Inserisca l'indirizzo IP del dispositivo o il nome di dominio del dispositivo (veda il capitolo Trovare i dispositivi sulla rete (p. 3)).
3. Se non è stato generato un certificato per l'indirizzo IP, potrebbe ricevere un avviso relativo a un certificato di sicurezza non valido. In questo caso, deve confermare di voler accedere all'interfaccia di configurazione web.
4. Verrà visualizzata la schermata di accesso.

5. Inserisci le tue informazioni di accesso.
   Le credenziali predefinite sono:
   - Nome utente: **Admin**
   - Parola d'ordine: **2n**
6. Dopo il primo accesso bisognerà cambiare la password.

## Accesso da 2N Access Commander

1. Acceda all'interfaccia di Access Commander.
2. Vada a Dispositivi.
3. Per il dispositivo selezionato, premere .

## Modifica della password

Deve cambiare la password predefinita per accedere completamente alle funzioni dell'interfaccia di configurazione web. Non è possibile configurare il dispositivo senza modificare la password predefinita.

**SUGGERIMENTO**
Si consiglia di utilizzare una password difficile da decifrare. Si sconsiglia di utilizzare nomi, nomi di luoghi o cose nella password, soprattutto quelli che hanno un collegamento diretto con l'utente.

Per una maggiore sicurezza della password, consigliamo:

- utilizzare un generatore di password casuali,
- lunghezza della password di almeno 12 caratteri,
- una combinazione di caratteri diversi provenienti da set di caratteri diversi (ad esempio lettere minuscole/maiuscole, numeri, caratteri speciali, ecc.).

## Browser consigliati

L'interfaccia di configurazione web è ottimizzata per i browser basati su Chrome (come Google Chrome, Microsoft Edge o Opera). Quando si utilizzano altri browser, potrebbero esserci lievi differenze di funzionalità nell'aspetto dell'interfaccia.

# Impostazioni di base del dispositivo

## Aggiornamento del firmware

Le nuove versioni del firmware sono disponibili sul server di aggiornamento. Se l'interfaccia di configurazione web non ha accesso a Internet, è possibile caricare manualmente il file del firmware sul dispositivo.

**NOTA**
Gli aggiornamenti del firmware non sono automatici. Per garantire l'integrità del sistema ed eliminare i guasti involontari, tutti gli aggiornamenti devono essere confermati o avviati manualmente dall'utente. Prima di eseguire qualsiasi aggiornamento, controlli le note di rilascio della nuova versione e verifichi la compatibilità con la sua infrastruttura esistente.

### Ottenere il firmware dal server di aggiornamento

1. Vada su **Sistema > Manutenzione > scheda Firmware**.
2. Clicchi su Controlla gli aggiornamenti.
3. Quando un aggiornamento è disponibile, vengono caricate le sue note di rilascio. Per avviare l'aggiornamento, clicchi su Upgrade nell'intestazione della finestra.
4. Dopo che il firmware è stato caricato con successo, il dispositivo si riavvia automaticamente. Dopo il riavvio, il dispositivo è completamente disponibile con il nuovo firmware. Gli aggiornamenti del firmware non influiscono sulla configurazione.

### Caricare un nuovo firmware dalla memoria

1. Vada su **Sistema > Manutenzione > scheda Firmware**.
2. Clicchi su Carica il firmware.
3. Nella finestra di dialogo che si apre, selezioni un file dal suo repository.
4. Confermi il caricamento del file cliccando su Upload.
   Il dispositivo controlla il file del firmware e non consente il caricamento di un file errato o corrotto.
5. Dopo che il firmware è stato caricato con successo, il dispositivo si riavvia automaticamente. Dopo il riavvio, il dispositivo è completamente disponibile con il nuovo firmware. Gli aggiornamenti del firmware non influiscono sulla configurazione.

**NOTA**
La funzionalità, l'affidabilità e la sicurezza del dispositivo dipendono dal firmware installato. L'aggiornamento regolare del firmware alla versione attuale fa parte dei termini di utilizzo del prodotto. Gli errori che possono essere causati dall'utilizzo di una versione del firmware non aggiornata non possono essere rivendicati. Il firmware attuale implementa l'esperienza del cliente e i requisiti nell'ambito della sicurezza dei dati personali.

# Rubrica

La sezione Directory è una parte fondamentale della configurazione del dispositivo. Lei crea gli utenti nella directory e gestisce i loro diritti di accesso.

## Aggiungere manualmente un utente a una directory

1. Nella pagina Directory, faccia clic su Aggiungi utente.
2. Si aprirà il dettaglio utente. Nella scheda Informazioni personali, dia un nome all'utente.
3. Imposta le opzioni di accesso in base a Accessi (p. 10).

## Gestione massiva degli utenti in Access Commander o My2N

Se il dispositivo è gestito tramite gli strumenti di configurazione di massa Access Commander o My2N, qualsiasi modifica apportata all'interfaccia di configurazione basata sul web viene sovrascritta dalle impostazioni dello strumento di configurazione di massa. Un utente creato direttamente nell'interfaccia web sarà cancellato.

La colonna titolare nella tabella della directory elenca lo strumento di configurazione bulk che ha creato l'utente. La colonna del titolare di è nascosta per impostazione predefinita.

# Accessi

Una delle funzioni di base del dispositivo è quella di gestire l'accesso e lo sblocco della serratura elettrica della porta. Il dispositivo gestisce l'accesso in base alla valutazione delle richieste di accesso secondo regole di accesso predefinite. Se il dispositivo giudica legittima la richiesta, attiva l'interruttore della porta che controlla la serratura elettrica della porta. Questo sbloccherà la porta.

Oltre all'autenticazione convenzionale dell'utente (carta RFID, biometria, Bluetooth, ecc.), l'interruttore può essere attivato anche tramite segnali e interfacce esterne, offrendo opzioni di integrazione e automazione flessibili. I diversi modi di attivare l'interruttore della porta sono descritti di seguito:

## Autenticazione dell’utente

L'utente utilizza il suo metodo di autenticazione e se le sue autorizzazioni di utente sono conformi alle regole di accesso, gli viene concesso l'accesso. L'accesso consentito attiverà l'interruttore della porta.

La configurazione è descritta nel capitolo Impostazioni di accesso dell'utente (p. 12).

## Controllo dell'interruttore nell'interfaccia di configurazione web

1. Vada su **Integrazione > Interruttori**.
2. Trovi la scheda interruttore che controlla la porta.

> **NOTA**
> La funzione dell'interruttore della porta nel dispositivo è svolta da **Interruttore 1**.

3. Sotto **Controllo manuale degli interruttori** faccia clic su Mantenere.
4. L'interruttore rimarrà acceso fino a quando non annullerà di nuovo il controllo manuale.

## Spegnimento in base al profilo orario

Nell'interfaccia di configurazione web, può impostare l'interruttore in modo che mantenga la porta sbloccata per un periodo di tempo predeterminato, ad esempio durante la pausa pranzo.

1. Vada su **Integrazione > Interruttori**.

2. Trovi la scheda interruttore che controlla la porta.

> **NOTA**
> La funzione dell'interruttore della porta nel dispositivo è svolta da **Interruttore 1**.

3. Clicchi sulla freccia → dell'interruttore selezionato per accedere ai suoi dettagli.
4. Nella scheda **Stato** abilita l'opzione **Interruttore di attesa temporizzato**.
5. Selezioni i profili temporali in cui il selettore deve essere trattenuto o inserisca un periodo di tempo personalizzato.

## Disattivare l'interruttore da una chiamata (DTMF)

## Impostazioni del codice DTMF

1. Vada su **Integrazione > Interruttori**.
2. Trovi la scheda interruttore che controlla la porta.

> **NOTA**
> La funzione dell'interruttore della porta nel dispositivo è svolta da **Interruttore 1**.

3. Clicchi sulla freccia → dell'interruttore selezionato per accedere ai suoi dettagli.
4. Nella scheda Codici di attivazione **di**, può impostare i codici che potrà inserire tramite DTMF durante una chiamata con il dispositivo.
   La validità di ogni codice può essere limitata nel tempo.

> **NOTA**
> Per il primo codice di attivazione, può impostare che venga elaborato come una forma più vecchia del codice. In questa forma, non sarà necessario confermare il codice con un asterisco quando lo inserisce sulla tastiera del telefono.

## Utilizzo del codice DTMF

1. Una volta collegato al dispositivo, inserisca il codice di attivazione sulla tastiera del telefono e confermi con un asterisco.

> **NOTA**
> La ricezione dei segnali DTMF è abilitata per impostazione predefinita sul dispositivo. Può controllare le autorizzazioni nella pagina Servizio chiamate (SIP/Chiamate locali) nella scheda Audio , nella scheda Ricezione DTMF .

## Disconnessione dell'interruttore tramite API HTTP

L'utilizzo completo, compresa una descrizione dell'autorizzazione HTTP API necessaria, è descritto nel manuale HTTP API di per i dispositivi 2N. L'interruttore della porta è controllato dall'endpoint `api switch ctrl`. Per lo switch 1, il comando si presenta così: `https://ip_adresa/api/switch/ctrl?switch=1&action=on`.

## Spegnimento tramite automazione

L'impostazione dell'automazione è descritta nel manuale Automation. L'interruttore viene attivato dall'azione **ActivateSwitch**.

## Impostazioni di accesso dell'utente

Per autenticarsi con successo all'unità di controllo accessi e sbloccare la porta, l'utente deve soddisfare due condizioni: avere i diritti di accesso assegnati al dispositivo e avere almeno un metodo di autenticazione stabilito. I metodi di autenticazione disponibili dipendono dal dispositivo specifico e possono includere carte RFID, PIN numerico, codice QR per la scansione da parte della fotocamera, ecc.

## Impostazioni di autenticazione:

1. Vada a **Directory**.
2. Apra i dettagli dell'utente cliccando sulla riga o selezioni Aggiungi utente per creare un nuovo utente.
3. Nella scheda **Autenticazione** imposta tutti i metodi con cui l'utente si autenticherà, vedere Metodi di autenticazione (p. 12).
4. Nella scheda Impostazioni di accesso di **di**, inserisca quando all'utente deve essere concesso l'accesso per entrare e uscire.
   - In qualsiasi momento
   - Profilo orario - offre l'impostazione di **Profili orari**
   - Personalizzato - utilizzi il pulsante Modifica per impostare intervalli di tempo unici per questo utente.

   Impostare una data di scadenza per limitare l'accesso dell'utente a un periodo di calendario specifico.
   La concessione di **Eccezioni** fornirà all'utente un accesso permanente che non limiterà nemmeno il blocco temporaneo del dispositivo indicato dalle regole di accesso (vedere Regole di accesso (p. 14)).

## Metodi di autenticazione

**ATTENZIONE**
I metodi di autenticazione disponibili dipendono dal dispositivo specifico e dai moduli collegati.

### Scheda RFID

A un utente possono essere assegnate fino a 2 schede RFID.

L'identificatore può essere inserito manualmente utilizzando la tastiera o letto inserendo la scheda in un lettore USB collegato al computer.

#### Requisiti della carta RFID

- L'identificatore deve essere un numero esadecimale.
- La lunghezza minima dell'identificatore è di 6 caratteri.
- È possibile utilizzare solo le schede supportate dal dispositivo - il tipo di scheda deve essere abilitato nelle impostazioni del modulo (vedere **Access > Moduli**).

**SUGGERIMENTO**
Può leggere l'identificatore di una scheda esistente dal registro all'indirizzo **Sistema > Registro eventi**. Carichi la carta nuova/non assegnata sul dispositivo e poi copi il suo identificatore (UUID) dal registro. Dopo aver inserito l'identificatore tra le carte RFID, l'utente può iniziare a usare la carta per l'autenticazione.

### MY2N

**My2N** - utilizzato per collegarsi all'applicazione My2N consentendo l'autenticazione via Bluetooth.

### Codice PIN / Codice QR

Il PIN serve come codice di accesso numerico personale, che l'utente inserisce sulla tastiera del dispositivo o può essere letto dalla fotocamera del dispositivo sotto forma di codice QR.

**ATTENZIONE**
I codici QR possono essere letti solo con la fotocamera interna del dispositivo.

#### Requisiti del PIN

- La lunghezza minima è di 2 cifre.
- Il codice può contenere solo cifre (0-9).
- I codici QR possono essere utilizzati solo per PIN di lunghezza compresa tra 4 e 15 cifre.
- Se utilizza la funzione Allarme silenzioso di , si consiglia di creare PIN di numero pari.

**NOTA**
Quando utilizza un codice QR esadecimale, il valore deve essere convertito in formato decimale prima di inserirlo.

Intervallo esadecimale accettato: 1000 fino a FFFFFFFF.

### 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.

### Targa

Alcuni dispositivi supportano il riconoscimento delle targhe dei veicoli utilizzando telecamere AXIS esterne dotate dell'applicazione aggiuntiva **VaxALPR**. Le targhe riconosciute vengono inviate in una richiesta HTTP all'endpoint `api/lpr/licenseplate` (più manuale HTTP API per citofoni IP).

**SUGGERIMENTO**
La procedura per aggiungere una telecamera esterna è descritta in ???.

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

**Requisiti della targa:**

- La lunghezza massima di una targa è di 10 caratteri.
- A un utente possono essere assegnate fino a 20 targhe.
- Ogni targa deve essere assegnata a un solo utente - se vengono effettuate più assegnazioni, viene utilizzato il primo record trovato.
- Le targhe vengono utilizzate nella funzione di riconoscimento dall'immagine della telecamera esterna (vedere il manuale Interoperabilità).

### Scheda virtuale

La scheda virtuale viene utilizzata per identificare l'utente nei dispositivi collegati tramite l'interfaccia Wiegand. Dopo l'autenticazione dell'utente tramite l'applicazione My2N o il lettore biometrico, l'ID della carta virtuale viene inviato all'interfaccia Wiegand (se l'invio di identificatori è abilitato nella configurazione, consulti **Access > Regole di accesso > scheda Access/Egress > Advanced**).

**Requisiti della carta virtuale:**

- L'ID deve essere un numero esadecimale (caratteri 0-9, A-F).
- La lunghezza dell'ID va da 6 a 32 caratteri.
- A un utente può essere assegnata una sola carta virtuale.

### Codice Interruttore

**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.

## Regole di accesso

La pagina **Accesso > Regole di accesso** imposta i parametri e la logica per lo sblocco della porta, che viene gestito dall'interruttore della porta del dispositivo. Questa configurazione determina come vengono valutate le richieste di accesso (autenticazione), le condizioni necessarie per l'autorizzazione dell'utente e le regole per la gestione dei singoli accessi.

Mentre lei definisce le autorizzazioni individuali nelle impostazioni dell'utente, le regole di accesso determinano quando, in quali condizioni e come queste autorizzazioni possono essere utilizzate. Ad esempio, può impostare se il passaggio della porta è consentito in una sola direzione, se l'autenticazione può attivare un allarme silenzioso o se l'utente può autenticarsi solo una volta per ogni intervallo di tempo definito.

## Condizioni della porta e della serratura

**La scheda Stato** mostra se l'interruttore della porta è attivo e se la porta è aperta.

**Porta**

- «Aprire» - l'accesso è stato concesso, l'interruttore della porta è chiuso e la porta può essere aperta.
- «Chiuso» - la porta è bloccata e non può essere aperta.

**Blocco**

- «Sbloccato» - l'interruttore è attivo, può essere azionato.
- «Bloccato» - il selettore è disattivato e non può essere controllato dalle regole di accesso.

**SUGGERIMENTO**
Il pulsante con il simbolo del lucchetto in questa scheda serve per bloccare o sbloccare il commutatore dall'interfaccia web.

## Rilevamento della porta

Nella scheda **Porte è possibile attivare**, in modo che l'apertura non autorizzata di una porta o l'apertura prolungata provochi un evento. Questo evento può poi essere seguito da automazioni. Gli eventi vengono scritti anche nel logo del dispositivo.

## Arrivo e partenza

Un dispositivo può essere utilizzato per gestire i passaggi in due direzioni. Può fissare alcuni moduli al dispositivo sul lato opposto della porta e poi impostare questi due lati separatamente. In questo modo, può limitare l'orario in cui sarà consentito il passaggio nella direzione **Arrivo** e l'orario in cui sarà consentito il passaggio nella direzione **Partenza**, oppure quali metodi di autenticazione saranno accettati in una determinata direzione, ecc.

## Assegnazione del modulo per l'arrivo o la partenza

1. Vada su **Accesso > Regole di accesso**.
2. Nella scheda **Arrivo** o **Partenza** sotto **Moduli** faccia clic su Gestione.
3. Si apre una finestra di dialogo con un elenco dei moduli di gestione degli accessi disponibili.
4. 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.

## Regole di accesso

Le regole di accesso determinano quali metodi di autenticazione saranno accettati per garantire l'accesso. Si possono impostare più regole di accesso per diversi profili temporali. Le regole di accesso possono essere utilizzate anche per determinare quando un accesso deve essere negato.

Può utilizzare le regole di accesso per limitare i metodi di autenticazione accettati, ad esempio può obbligare gli utenti a utilizzare una carta RFID dalle 8:00 alle 9:00.

**SUGGERIMENTO**

La restrizione di autenticazione è utile da utilizzare su un dispositivo che gestisce le chiavi di **2N IP Fortis**. Gli utenti saranno quindi costretti ad aggiornare regolarmente le chiavi di **2N IP Fortis** sulla loro carta RFID.

Quando imposta le regole, può scegliere se utilizzare un codice di zona per aprire la porta. **Il codice di zona** viene applicato quando il dispositivo viene suddiviso in zone in una gestione di dispositivi di massa (come Access Commander). **Il codice di zona** può anche essere impostato manualmente nella sezione **Avanzate**. Funziona in modo simile a **Codice di attivazione dell'interruttore**; inserendolo sulla tastiera del modulo attiverà l'interruttore della porta.

## Allarme silenzioso

L'allarme silenzioso è una modalità speciale di apertura della serratura che le permette di attivare un'azione di sicurezza in modo discreto. L'allarme silenzioso è utilizzato soprattutto nei locali e negli edifici che sono ricercati dai rapinatori - casinò, centri finanziari, banche, ecc. Dopo aver inserito il codice PIN, la porta si apre, ma allo stesso tempo si attiva l'allarme senza che l'aggressore se ne accorga.

L'attivazione dell'allarme silenzioso innescherà l'evento **SilentAlarm**. Questo evento può essere seguito dall'automazione, ad esempio:

- Invio di una richiesta HTTP al sistema di sicurezza.
- Acquisizione di immagini dalla fotocamera del dispositivo.
- Impostazione di una chiamata verso una destinazione preimpostata.

### Attivazione dell'allarme silenzioso

1. L'utente inserisce un codice superiore al suo normale PIN.
   Esempio: L'utente ha impostato un codice PIN «1926». Inserisca il codice «1927» per aprire la porta. La porta si apre e contemporaneamente si attiva l'evento SilentAlarm.

**ATTENZIONE**
Per poter aprire la porta con un codice PIN (anche se l'allarme silenzioso è scattato contemporaneamente), è necessario attivare la scheda **In/Out sotto**.

## Blocco dell'accesso dopo tentativi falliti

Dopo cinque tentativi di accesso consecutivi non riusciti, l'accesso sarà bloccato per 30 secondi. L'accesso non sarà consentito durante questo periodo, anche se l'autenticazione dell'utente è valida.

Questa funzione blocca l'accesso solo in base all'autorizzazione dell'utente. L'interruttore della porta può essere commutato anche con altri metodi, come il DTMF, il comando HTTP, ecc.

## Lettura codici QR

Il codice PIN di accesso assegnato all'utente o il codice di attivazione dell'interruttore possono essere letti dalla telecamera sotto forma di codice QR.

Per un caricamento corretto, deve impostare la modalità di lettura del codice QR . I codici sono sempre memorizzati nel dispositivo in formato decimale. Quando vengono letti in modalità decimale, i codici QR letti devono corrispondere esattamente ai codici PIN (da 4 a 15 cifre) memorizzati nel dispositivo. In modalità esadecimale, i codici QR vengono convertiti in formato numero decimale dopo la lettura e poi confrontati con i codici decimali memorizzati. Gli zeri preallineati vengono ignorati durante la lettura esadecimale.

**NOTA**
Intervallo esadecimale accettato: 1000 fino a FFFFFFFF.

Per la lettura del codice QR, può anche impostarlo in modo da attivare solo l'evento **CodeEntered** invece di controllare l'interruttore della porta. Questo evento può poi essere seguito da ulteriori azioni tramite le Automazioni.

Il codice QR scansionato può essere inoltrato a un sistema di controllo accessi esterno che comunica tramite un'interfaccia Wiegand (vedere ???).

## Anti-passback

L'anti-passback è un'estensione del sistema di controllo degli accessi che impedisce il rientro durante un intervallo di tempo stabilito. Il dispositivo in questa modalità consentirà all'utente di entrare solo una volta in un determinato periodo di tempo. Dopo che un utente è entrato con successo, il sistema registra questo evento e l'utente può accedere nuovamente al sistema solo dopo che è trascorso il tempo specificato. Questo tempo viene impostato quando è abilitato l'Anti-passback.

**Modalità anti-passback:**

- «Hard» - L'utente non può attraversare il dispositivo in nessuna direzione per il periodo di tempo impostato. All'utente viene negato l'accesso fino alla scadenza dell'intervallo o al ripristino dell'accesso da parte dell'amministratore del dispositivo.
- «Soft» - Le violazioni delle regole vengono solo registrate e possono avvisare l'amministratore, ma l'utente può accedere.

## Trasferimento dati per Wiegand

**ATTENZIONE**
Per inoltrare i dati Wiegand, un modulo di espansione Wiegand deve essere collegato correttamente al dispositivo. Il modulo di espansione Wiegand di solito non è incluso nella confezione del prodotto.

La funzione di inoltro Wiegand consente al dispositivo di inoltrare i dati di identificazione dell'utente autenticato a un sistema di controllo accessi esterno che comunica tramite l'interfaccia Wiegand. Questo garantisce l'integrazione dei dispositivi 2N con i sistemi di controllo accessi tradizionali. L'impostazione le consente di selezionare il gruppo appropriato per l'instradamento dei dati.

L'inoltro dei dati per Wiegand si imposta in **Accesso > Regole di accesso > I/O > Avanzate**. L'invio delle autorizzazioni agli utenti che hanno letto il loro codice QR è impostato nella scheda **Accesso/Esci** per abilitare la lettura del codice QR.

## Impostazione dell'interruttore della porta

L'interruttore della porta è una funzione logica del dispositivo che controlla la serratura elettrica della porta. L'interruttore può essere attivato in vari modi (ad esempio tramite comando HTTP, scheda RFID o segnale DTMF).

La funzione dell'interruttore della porta nel dispositivo è svolta da **Interruttore 1**.

La pagina **Access > Moduli** può quindi essere utilizzata per assegnare un modulo di accesso specifico per controllare un altro switch.

## Impostazione dell'interruttore della porta

1. Colleghi i contatti elettrici della serratura (ad esempio, il contatto magnetico) all'ingresso designato sul citofono.
2. Nell'interfaccia di configurazione web, vada su **Integrazione > Interruttori**.
3. Apra le impostazioni dello Switch 1 cliccando sulla freccia nell'intestazione della scheda.

4. Nella scheda Configurazione **dell'interruttore**, imposti i parametri dell'uscita hardware che l'interruttore della porta deve controllare.
   - **Uscita controllata** - specifica l'uscita che commuta la serratura elettrica della porta.
   - **Modalità** - Monostabile / Bistabile.
   - **Tempo di accensione** - impostare il tempo di attivazione per un interruttore monostabile. Questo valore non è applicato in modalità bistabile.
   - **Tipo di uscita** - nella modalità «Security», l'uscita funziona in modalità invertita, il che significa che è permanentemente accesa e controlla il relè di sicurezza utilizzando una sequenza di impulsi specifica. Se si utilizza una serratura inversa (cioè la serratura viene bloccata quando si applica l'alimentazione), impostare il tipo di uscita su «Inverse».

   **SUGGERIMENTO**
   Se utilizza un relè di sicurezza, imposti il tipo di uscita su «Sicurezza».

   Se a un'uscita sono collegati più interruttori con un tipo di uscita impostato in modo diverso, essi vengono controllati in base alla seguente priorità:

   1. Security
   2. Invertito
   3. Normale
5. Nelle schede **Codici di attivazione** e **Codici di attivazione**, può impostare ulteriori modalità di attivazione dell'interruttore. Se non imposta nessun altro metodo, l'interruttore verrà attivato solo consentendo l'accesso all'utente.
6. Salvi le modifiche.

## Moduli

La pagina **Access > Moduli** offre una gestione centrale di tutte le tecnologie hardware di accesso sul dispositivo. Ogni modulo ha una propria scheda nella pagina che ne consente la gestione. Qui vengono gestiti sia i moduli direttamente integrati nell'unità principale del dispositivo, sia quelli collegati tramite VBUS.

Ogni modulo può essere nominato e gli si può assegnare un interruttore specifico da controllare. Altri parametri dipendono dal tipo di modulo.

Nelle impostazioni di fabbrica, tutti i moduli controllano l'interruttore della porta.

**NOTA**
Se le versioni del firmware del modulo da collegare e dell'unità principale non sono compatibili, il modulo non verrà rilevato. In questo caso, aggiorni il firmware del dispositivo (Aggiornamento del firmware (p. 9)) dopo aver collegato il modulo.

## Impostazione dell'accesso Bluetooth

L'autenticazione dell'utente tramite Bluetooth avviene tramite l'app My2N, che l'utente deve aver scaricato sul proprio cellulare.

GET IT ON Google Play

Download on the App Store

**ATTENZIONE**
L'impostazione del codice di accoppiamento deve attualmente essere effettuata nella vecchia interfaccia di configurazione.

## Crea un codice di accoppiamento sul dispositivo

1. Vada su **Directory** e apra il dettaglio dell'utente per il quale desidera creare il codice di corrispondenza.
2. Nell'intestazione dell'interfaccia di configurazione web, clicchi su Vada alla vecchia interfaccia.
   Apre i dettagli dell'utente nella vecchia interfaccia di configurazione.
3. Nel blocco **WaveKey**, faccia clic su  .
   Nella finestra di dialogo che si aprirà, verrà generato un codice di accoppiamento che dovrà inserire nell'applicazione My2N sul suo dispositivo.
4. Apra l'app My2N e inserisca il PIN di accoppiamento.

   **NOTA**
   Se ha già un'app collegata a un altro dispositivo, può inserire il PIN di abbinamento tramite l'icona Aggiungi nella parte superiore dello schermo.
5. Segua le istruzioni del suo telefono cellulare - si avvicini al dispositivo in modalità di accoppiamento e clicchi su Avvia l'accoppiamento.

**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.

## Metodi di autenticazione Bluetooth

Nell'interfaccia di configurazione web si possono impostare diversi metodi di autenticazione Bluetooth.

- **Direttamente nell'applicazione mobile** - l'utente seleziona la porta che desidera aprire direttamente nell'applicazione mobile My2N. Se il suo dispositivo mobile si trova nel raggio d'azione del dispositivo 2N, si connetterà con il dispositivo e se le regole di accesso sono soddisfatte, la porta si sbloccherà.
- **Avvicinando il cellulare al dispositivo e toccando il dispositivo** - un utente con un dispositivo mobile e Bluetooth abilitato si avvicina al dispositivo 2N e tocca la posizione di autenticazione Bluetooth sul dispositivo 2N, che di solito è contrassegnata dall'icona Bluetooth . Una volta stabilita la connessione e verificati i diritti di accesso, la porta viene sbloccata.

- **Rilevamento del movimento** - I dispositivi 2N con telecamera rilevano il movimento nell'ambiente circostante, attivando automaticamente il Bluetooth. Se un dispositivo 2N rileva un dispositivo mobile dell'utente con accesso valido nel raggio d'azione, la porta si sblocca.

### Impostazione dei metodi di autenticazione Bluetooth accettati

1. Vada su **Access > Moduli**.
2. Nella scheda **per il modulo Bluetooth** selezioni i metodi possibili nel campo **Avvia autenticazione**.
3. Se ha selezionato «rilevamento del movimento», selezioni il profilo con cui deve essere rilevato il movimento.

**NOTA**
I profili di rilevamento del movimento sono impostati in **Personalizzazione > Telecamera > Telecamera interna**.

## Ascensore

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).

### Collegamento all'ascensore

1. Colleghi gli ingressi dei controllori di ascensori al relè AXIS A9188 e colleghi il relè alla rete IP. Prenda nota dell'indirizzo IP del relè.
   Segua la documentazione del modulo relè I/O AXIS A9188, disponibile all'indirizzo http://www.axis.com.
2. Apra l'interfaccia di configurazione web del dispositivo 2N che deve gestire gli accessi all'ascensore.
3. Vada su **Integration > Access Control > scheda Elevator**.
4. Nella scheda **Moduli relè (AXIS A9188)**, abiliti uno dei moduli.
5. Clicchi sull'icona della matita e inserisca l'indirizzo IP del modulo relè nella casella che si apre.
6. Se l'accesso al relè è soggetto ad autenticazione, inserisca il nome utente e la password nella scheda **Generale**.
7. Quando il modulo relè è abilitato, i piani gestiti da questo modulo appariranno nella scheda **Pavimenti di ascensori**. Può dare un nome a ciascun piano.

### Impostazione dell'accesso pubblico al piano

1. Nella scheda **Elevator Floors**, selezioni i piani che devono essere accessibili al pubblico (l'accesso non è soggetto ad autorizzazione).
2. Clicchi sull'icona della matita accanto al piano selezionato.
3. Nelle impostazioni aperte, attivi **Accesso pubblico.**
4. Opzionalmente, può limitare l'orario di accesso al pubblico selezionando un profilo orario o impostando un orario di accesso personalizzato.

# Impostazioni avanzate

## Impostazioni della fotocamera e del video

La telecamera dell'unità di accesso **2N QR** rileva i movimenti intorno al dispositivo e legge i codici QR.

### Impostazioni interne della fotocamera

1. Vada su **Personalizzazione > Fotocamera**.
2. Nella scheda **Fotocamera interna** faccia clic su → .
3. La scheda Impostazioni le permette di modificare i parametri di base dell'immagine della fotocamera.
4. Dopo il salvataggio, le modifiche si rifletteranno nell'anteprima della fotocamera.

### Modalità

La modalità fotocamera consente di impostare la combinazione ottimale di modalità di esposizione e frequenza di alimentazione per ottenere immagini stabili e di alta qualità. Questa modalità viene utilizzata per ridurre lo sfarfallio indesiderato che può verificarsi quando si utilizza l'illuminazione artificiale o quando la frequenza di rete varia. Quando installa le telecamere in ambienti interni, è possibile selezionare un metodo adeguato per sopprimere lo sfarfallio causato dalle sorgenti luminose, mentre quando le posiziona all'esterno, può attivare una modalità di soppressione della luce solare diretta per garantire un adattamento ottimale dell'immagine alle condizioni di illuminazione attuali.

### LED IR

La funzione di retroilluminazione LED IR viene utilizzata per garantire un'immagine di alta qualità anche in presenza di bassi livelli di luce ambientale. Questa modalità si attiva quando le condizioni di luce scendono al di sotto del livello impostato. Il livello limite delle condizioni di luce viene impostato solo dopo l'abilitazione dell'illuminazione del LED IR.

**NOTA**
Se il consumo di energia consentito potrebbe essere superato - ad esempio, quando sono in funzione contemporaneamente più moduli di espansione alimentati con PoE - il livello di alimentazione IR viene ottimizzato automaticamente per mantenere la stabilità del dispositivo.

### Impostazioni avanzate

**Modalità Giorno/Notte** - consente di passare dalle immagini a colori a quelle in bianco e nero a seconda delle condizioni di illuminazione. Imposti **Sempre giorno**, se desidera che la telecamera utilizzi un filtro di soppressione IR e che la retroilluminazione IR sia spenta. L'impostazione "Sempre notte", invece, spegne il filtro e accende l'illuminazione IR, che passa l'immagine alla modalità in bianco e nero, adatta alla visione notturna. La modalità Auto fa passare la fotocamera tra questi due stati in base al livello di luce ambientale.

**Contrasto locale** - migliora i dettagli e le texture aumentando le differenze di luminosità tra aree adiacenti dell'immagine (bordi).

**Mappatura dei toni** - aumenta la luminosità e la visibilità dell'immagine, ma può causare una leggera distorsione del colore.

**Tempo di esposizione massimo** - Specifica il tempo massimo di esposizione dell'immagine. Se è a disposizione più luce, non è necessario che l'otturatore resti aperto per tutto il tempo e la telecamera imposta automaticamente il periodo di esposizione reale più corto.

## Rilevamento dei movimenti

Il rilevamento del movimento sui dispositivi 2N è una funzione che rileva automaticamente il movimento nel campo visivo della telecamera interna e consente di attivare varie azioni, come l'attivazione del Bluetooth o l'invio di una notifica.

Per ottenere prestazioni ottimali, il rilevamento può essere calibrato in base all'ambiente e alle condizioni, ad esempio modificando i parametri di sensibilità e l'area che deve essere monitorata dalla telecamera.

## Impostazioni del rilevamento dei movimenti

1. Vada su **Personalizzazione > Fotocamera**.
2. Nella scheda **Fotocamera interna** faccia clic su .
3. Nella scheda **Anteprima della telecamera** faccia clic sull'icona della matita accanto al parametro **Rilevamento del movimento**.
4. Si apre una finestra con le impostazioni del profilo di rilevamento del movimento.
5. Espanda la scheda del profilo che desidera impostare.
6. Regolando il quadrato nell'anteprima della fotocamera di un'area specifica in cui la fotocamera deve registrare il movimento.

> **ATTENZIONE**
> L'area dell'immagine è relativa al ritaglio dell'immagine corrente. Se cambia il taglio dell'immagine della telecamera, le aree esistenti rimarranno le stesse, ma copriranno effettivamente una parte diversa dello spazio. Pertanto, si raccomanda sempre di controllare e regolare queste aree dopo aver modificato un ritaglio.

7. Selezionare la modalità di acquisizione del movimento per il profilo, vedere Modalità di profilo (p. 22)
8. Regoli altri parametri, se necessario, in base alla modalità.
9. Si ricordi sempre di abilitare il profilo!
10. Per salvare le sue modifiche, clicchi sul pulsante **Salva** o **Salva e chiudi** nella parte superiore della pagina.

### Modalità di profilo

### Avvio degli eventi

In questa modalità, la fotocamera cattura movimenti istantanei, una tantum. Un esempio di caso d'uso è scattare una foto quando qualcuno entra in una stanza o quando un veicolo passa vicino al dispositivo.

L'attivazione dell'evento innescato può essere ritardata utilizzando il ritardo impostato.

Utilizzi il filtro per definire i tipi di movimenti che desidera che la fotocamera ignori - ad esempio, oggetti piccoli (piccoli uccelli) o movimenti ripetitivi (alberi nel vento).

### Registrazione

Questo profilo innesca un evento di 30 secondi quando viene rilevato un movimento. Se durante questo periodo si verifica un altro movimento, il profilo combinerà tutto in un unico evento. Questa modalità è adatta al monitoraggio continuo ed evita la creazione di un gran numero di record brevi.

Utilizzi il filtro per definire i tipi di movimenti che desidera che la fotocamera ignori - ad esempio, oggetti piccoli (piccoli uccelli) o movimenti ripetitivi (alberi nel vento).

### Rilevamento del volto

Il profilo rileva il movimento quando un volto appare nell'area monitorata. Un evento può verificarsi anche quando un'immagine statica di un volto (ad esempio una fotografia) appare nell'inquadratura.

### Rilevamento di persone in arrivo

Il profilo riconosce solo le persone in movimento e ignora le immagini statiche dei volti.

## Informativa sulla privacy

La funzione privacy maschera una parte dell'immagine in modo che non sia visibile o registrata nel video. Questa opzione è ideale per le situazioni in cui desidera proteggere le aree sensibili dell'immagine, ad esempio. Ad esempio, se il dispositivo è posizionato alla reception e la telecamera riprende anche il corridoio dove si muovono gli estranei, può nascondere l'area del corridoio.

**ATTENZIONE**
La protezione della privacy può limitare l'attività di lettura dei codici QR o il rilevamento del movimento. Non consigliamo di utilizzare contemporaneamente la protezione della privacy e queste funzioni.

## Impostazioni del rilevamento dei movimenti

1. Vada su **Personalizzazione > Fotocamera**.
2. Nella scheda **Fotocamera interna** faccia clic su .
3. Nella scheda **Anteprima della telecamera** faccia clic sull'icona della matita accanto al parametro **Privacy**.
4. Nell'anteprima della fotocamera, regoli il quadrato per coprire l'area che desidera mascherare.

   **ATTENZIONE**
   L'area dell'immagine è relativa al ritaglio dell'immagine corrente. Se cambia il taglio dell'immagine della telecamera, le aree esistenti rimarranno le stesse, ma copriranno effettivamente una parte diversa dello spazio. Pertanto, si raccomanda sempre di controllare e regolare queste aree dopo aver modificato un ritaglio.

5. Selezionare la modalità di occultamento:
   - **Colore** - l'area selezionata verrà sovrapposta con il colore di sua scelta.
   - **Mosaico** - l'area selezionata sarà pixelata. Imposta la dimensione del mosaico in base al livello di anonimizzazione dei dati necessario.
6. Non dimentichi di attivare la protezione della privacy nell'intestazione delle impostazioni dei parametri!
7. Per salvare le sue modifiche, clicchi sul pulsante **Salva** o **Salva e chiudi** nella parte superiore della pagina.

## Fotocamera esterna

La telecamera esterna viene aggiunta al dispositivo 2N come flusso video (RTSP). Il collegamento di una telecamera esterna le permette di passare da una vista all'altra durante una chiamata. La funzione della telecamera esterna è quindi puramente di imaging.

**ATTENZIONE**
I codici QR possono essere letti solo con la fotocamera interna del dispositivo.

### Aggiungere una telecamera esterna:

1. Vada su **Personalizzazione > Fotocamera**.
2. Nella scheda **Telecamera esterna** seleziona Aggiungi telecamera.
3. Nella finestra di dialogo che si apre, abiliti la fotocamera.
4. Inserisca l'indirizzo sorgente del flusso della telecamera IP esterna nel formato `rtsp://ip_address_camera/parametri`.
5. Se il flusso della telecamera esterna è soggetto ad autenticazione, inserisca in **i dati di accesso al flusso**.
6. Salvi le sue modifiche cliccando su Aggiungi fotocamera.
7. Se la telecamera esterna deve essere la telecamera principale del dispositivo, dopo averla salvata nella scheda **Telecamera esterna** clicchi su Imposta come sorgente predefinita.
   Quando parla con il dispositivo, viene visualizzata prima l'immagine della fotocamera impostata come sorgente predefinita.

## Crea un flusso video dalla fotocamera del dispositivo

La funzione di streaming video viene utilizzata per trasmettere il video in diretta dalla telecamera del dispositivo attraverso la rete a un dispositivo di ricezione, come un'applicazione su un telefono cellulare, un software di localizzazione o un computer in un lettore video. Questo processo assicura che gli utenti possano guardare i video in tempo reale da una varietà di dispositivi.

### Creare un flusso video

1. Vai a **Integration > Video**.
2. Abilita il servizio del server RTSP di .
3. Impostare i parametri del flusso, vedere Parametri del flusso video (p. 24).
4. Nella scheda **Restrizioni di connessione** può inserire gli indirizzi IP da cui sarà disponibile il flusso. Se non sono stati inseriti indirizzi IP, è possibile collegarsi da qualsiasi indirizzo IP.
5. Nella scheda **Flussi preconfigurati**, specifichi se il flusso deve essere accessibile:
   - anonimamente
   - con autenticazione - imposti i dettagli dell'autenticazione nella scheda Autenticazione di .
6. Nella scheda **Flussi preconfigurati** può trovare gli indirizzi IP dei flussi configurati in base al codec video selezionato.

## Parametri del flusso video

### Impostazioni generali del flusso

**Compensazione del jitter** - impostare la capacità di buffer per la compensazione jitter nelle trasmissioni di pacchetti audio. Una memoria più lunga significa una maggiore immunità alle interruzioni, ma un maggiore ritardo audio.

**Valore QoS DSCP** - imposta la priorità dei pacchetti RTP audio e video nella rete. Il valore impostato è inviato al campo TOS (Type of Service) nel IP packet header.

**Abilita la modalità UDP unicast** - abilita la modalità di invio dei dati del flusso audio e video utilizzando il protocollo RTP/UDP. Se la modalità è off i dati audio/video stream sono inviati solo attraverso RTP/RTSP.

**Porta RTP iniziale** - impostare la porta locale RTP di partenza nel range di lunghezza 60 porte da utilizzare per le trasmissioni audio e video. Il valore predefinito è 4800 (ovvero il range usato è 4800–4859).

**Zipstream** - seleziona il livello di compressione iniziale Zipstream (per H.264). AXIS Zipstream conserva tutti i dettagli forensi importanti di cui avete bisogno; e allo stesso tempo riduce i requisiti per la trasmissione dati e l'archivio in media del 50%.

### Impostazione di flussi di formato personalizzati

1. Nella scheda **Streams del formato personalizzato** faccia clic su Generate stream URL. Si aprirà una finestra di dialogo.
2. Nella finestra di dialogo, imposti:
   - **Codec** - seleziona tra i codec disponibili
   - **Abilita audio** - specifica se trasmettere solo il video o il video con l'audio.
   - **Risoluzione** - imposta la risoluzione dell'immagine.
   - **Framerate** - imposta la frequenza dei fotogrammi del video registrato.
   - **Bitrate** - imposta il bitrate
   - **Zipstream** - seleziona il livello di compressione iniziale Zipstream (per H.264). AXIS Zipstream conserva tutti i dettagli forensi importanti di cui avete bisogno; e allo stesso tempo riduce i requisiti per la trasmissione dati e l'archivio in media del 50%.
3. L'indirizzo del flusso con i parametri viene caricato automaticamente nella parte inferiore della finestra di dialogo.
4. Copi l'indirizzo del flusso e salvi le modifiche.

# Impostazioni audio

## Impostazione del volume del dispositivo

Per regolare il volume del suo dispositivo, vada su **Personalizzazione > Audio**.

## Suoni dell'utente

Il dispositivo esegue diverse azioni che sono accompagnate da un suono (squillo, commutazione, ecc.). Può modificare i suoni riprodotti in **Personalizzazione > Suoni utente**.

È inoltre possibile caricare sul dispositivo fino a 10 suoni utente personalizzati.

## Altre caratteristiche audio del dispositivo

## Rilevamento del rumore

Il dispositivo può monitorare il suono ricevuto dal microfono e quando il livello del segnale del microfono supera una soglia impostata, il dispositivo può generare un evento `Event.NoiseDetected`. Questo evento può essere seguito da altri eventi di automazione (veda Automazione (p. 32)).

### Attivazione del rilevamento del rumore

1. Vada a **Integration > Audio**.
2. Nell'intestazione della scheda **Rilevamento del rumore**, attivi la funzione.
3. Nel parametro **Livello soglia rumore**, specifichi il valore [dB] che attiva l'evento **Event.NoiseDetected** quando viene superato.
4. Nel parametro **Ritardo inizio allarme** può impostare la quantità di tempo in cui il rumore deve essere superiore a un livello di soglia perché l'evento venga attivato.
5. Nel parametro **Ritardo fine allarme**, invece, può specificare la quantità di tempo in cui il segnale deve essere al di sotto della soglia perché l'evento termini.

## Prova audio

Il risultato dell'ultimo test si trova in **Integrazione > Audio > scheda Generale > scheda Test audio**.

I dispositivi 2N possono eseguire un controllo regolare dell'altoparlante e del microfono integrati. Durante il test, l'altoparlante del dispositivo genera uno o più toni brevi. Utilizzando il microfono incorporato, il tono generato viene percepito e se viene rilevato correttamente, il test viene dichiarato riuscito. La durata del test

è di circa 4 s. Se il test non ha successo (,che può essere causato, ad esempio, da un rumore ambientale estremo), il test viene ripetuto un'altra volta tra dieci minuti. Il risultato dell'ultimo test può essere visualizzato nell'interfaccia di configurazione web del dispositivo o elaborato con Automation.

**NOTA**
Se all'avvio del test audio è in corso una chiamata, il test audio viene posticipato fino al termine della chiamata. Il test audio avrà luogo subito dopo la fine della chiamata.

# Profili temporali

Alcune delle funzioni svolte dal dispositivo dipendono dal tempo. La sezione Profili orari di **di** le permette di preimpostare degli intervalli di tempo da cui può poi selezionare queste funzioni. Ciò significa che non deve inserire manualmente l'ora ogni volta che la imposta. Può dare un nome al profilo temporale per una maggiore chiarezza.

## Creazione del profilo temporale:

1. Vada su **Personalizzazione > Profili orari**.
2. Clicchi su vuoto per creare un nuovo profilo.
3. Inserisca il nome del profilo.
4. Clicchi su Salva. Si aprirà il dettaglio del profilo.
5. Imposta gli intervalli in cui il profilo orario deve essere attivo.
   1. Clicchi sull'intervallo desiderato.
   2. Può specificare l'inizio e la fine nel menu aperto.

   **NOTA**
   La riga **Festività** è utilizzata per impostare diversi intervalli di tempo durante i giorni selezionati, vedere Vacanze (p. 26).
6. Salvi le modifiche.

## Vacanze

Nella configurazione del dispositivo, può definire diversi giorni che saranno contrassegnati come festivi. Per questi giorni vengono quindi impostati degli intervalli speciali nei profili orari. In genere si tratta di giorni come i giorni festivi, le ferie aziendali e altri giorni speciali.

Per ogni festività, può specificare se si applica solo ad un determinato anno o se si ripete nello stesso giorno ogni anno. Le vacanze possono essere pianificate con diversi anni di anticipo.

## Ambienti di vacanza:

1. Vada su **Personalizzazione > Profili orari > scheda Ferie**.
2. Selezioni l'anno per il quale desidera impostare la festività.
3. Clicchi sul giorno nel calendario:
   - Il primo clic indica la festività che si ripeterà ogni anno nel giorno e nel mese indicati.
   - Un secondo clic cambia la festività in una festività unica per l'anno selezionato.
4. Salvi le modifiche.

# Impostazione dell'interruttore di protezione

L'interruttore di protezione rileva l'apertura del coperchio del dispositivo, che viene valutata dal software come una chiusura logica dell'interruttore. In questo modo, l'interruttore indica una potenziale manomissione fisica del dispositivo.

Quando attiva un interruttore di protezione, può disattivare tutti gli altri interruttori o impostare l'Automazione per attivare un'azione successiva, come l'invio di un'e-mail, la creazione di una richiesta HTTP o l'attivazione di un allarme silenzioso.

**NOTA**
A seconda del tipo di dispositivo, l'interruttore di protezione può essere integrato nell'unità principale oppure deve essere installato come modulo aggiuntivo. Per le procedure di installazione, faccia riferimento al manuale di installazione del dispositivo specifico.

## Blocco di altri interruttori quando il coperchio viene aperto

Il dispositivo consente di garantire che gli altri interruttori siano bloccati durante l'apertura del coperchio (cioè quando l'interruttore di protezione è attivato). Questo impedisce anche l'attivazione dell'interruttore della porta e impedisce l'ingresso attraverso la porta che controlla il dispositivo.

### Procedura di impostazione del blocco dell'interruttore

1. Vada su **Integrazione > I/O**.
2. Nella scheda **Interruttore di protezione**, assegni un interruttore di protezione all'ingresso.
3. Abilita l'opzione Blocco automatico degli interruttori .

## Eventi dell'interruttore di protezione

L'attivazione dell'interruttore di protezione innesca gli eventi. Questi eventi possono essere collegati a Automazione (p. 32).

- L'apertura del coperchio attiva l'evento `TamperSwitchActivated (stato: in)`.
  Se l'interruttore è assegnato come ingresso nella **sezione I/O**, viene generato un evento aggiuntivo `InputChange (porta: tamper, stato: false)`.
- La chiusura del coperchio attiva l'evento `TamperSwitchActivated (stato: out)`.
  Se l'interruttore è assegnato come ingresso **alla sezione I/O**, viene generato un evento aggiuntivo `InputChange (porta: tamper, stato: true)`.

# Sistema

## Impostazioni di data e ora

**ATTENZIONE**
Se il dispositivo è gestito da uno strumento di gestione di massa (2N Access Commander / 2N My2N), l'orario del dispositivo può essere gestito da questo strumento. Le modifiche manuali nell'interfaccia web del dispositivo non influiscono sull'impostazione dell'ora.

### Sincronizzazione con NTP

Se il dispositivo è collegato a Internet, l'ora e la data possono essere sincronizzate tramite NTP.

1. Vada su **Sistema > Data e ora**.
2. Nella scheda **delle Impostazioni di sincronizzazione dell'ora** attivi l'opzione **Ora automatica da NTP o Internet**.
3. Inserisca l'indirizzo del server NTP di sua scelta.

### Aggiornamento dell'ora in caso di interruzione del servizio

1. Vada su **Sistema > Data e ora**.
2. Nella scheda **delle Impostazioni di sincronizzazione dell'ora** faccia clic su Sincronizzazione con il browser.
   Questo sincronizza l'ora del dispositivo con quella del computer.

**NOTA**
I dispositivi 2N sono dotati di un orologio di backup in tempo reale che consente di superare un'interruzione di corrente fino a diversi giorni.

## Impostazioni di rete

Per impostazione predefinita, il dispositivo utilizza un indirizzo IP dinamico assegnato dal server DHCP.

Una corretta configurazione dell'indirizzo IP è fondamentale per garantire che i suoi dispositivi siano collegati alla rete in modo stabile e affidabile.

1. Per impostare i parametri di rete del dispositivo, vada su **Sistema > Connessione di rete**.

2. In Impostazioni di base > Impostazioni indirizzo IP, può attivare o disattivare il server DHCP.

### Impostazione indirizzo IP statico:

a. Disattiva l'opzione **server DHCP**.
b. Inserisca l'indirizzo IP desiderato, la maschera di sottorete, il gateway predefinito e i server DNS.
c. Salvi le sue modifiche. Riavvio del dispositivo.

### Impostazioni DHCP

a. Abilita l'opzione **server DHCP**.
b. Inserisca l'indirizzo IP desiderato, la netmask, il gateway predefinito e i server DNS.
c. Salvi le sue modifiche. Riavvio del dispositivo.

**NOTA**
Se utilizza un server RADIUS e un meccanismo di autenticazione basato su 802.1x per i dispositivi collegati alla sua rete, può configurare il dispositivo per utilizzare l'autenticazione EAP-MD5 o EAP-TLS. La scheda 802.1x serve per impostare questa funzione.

## Licenza

Alcune funzioni sono disponibili solo con la licenza appropriata. Per una panoramica delle licenze e se sono attive, veda **Sistema > Licenze > scheda Informazioni generali.** Nella scheda **Caratteristiche con licenza** troverà una panoramica delle funzionalità disponibili che sono soggette a licenza.

**NOTA**
Dopo aver selezionato la licenza appropriata, contatti il suo rivenditore 2N. Se è un partner 2N, può contattare il nostro servizio clienti all'indirizzo customercare@2n.com. La preghiamo di includere il numero di serie del dispositivo nella sua richiesta.

### Aggiornamento della chiave di licenza

La chiave di licenza attuale è disponibile sul server di aggiornamento. Se l'interfaccia di configurazione web non ha accesso all'Internet pubblico, può caricare manualmente il file della chiave sul dispositivo.

Ad ogni riavvio del dispositivo, viene ricaricata l'ultima chiave di licenza disponibile.

### Licenza Trial

La licenza di prova le consente di utilizzare temporaneamente tutte le funzioni della licenza Gold e della licenza Microsoft Teams per un massimo di 800 ore dopo l'attivazione. Una licenza di prova attivata non può essere sospesa.

Per attivare una licenza di prova, vada su **Sistema > Licenze > scheda Licenza di prova**.

**ATTENZIONE**
Un'ora della licenza di prova viene rimossa ogni volta che il dispositivo viene riavviato.

# Porti utilizzati

| Servizio | Porta | Protocollo | Direzione | Abilitato per impostazione predefinita | Regolabile | Impostazioni |
|---|---|---|---|---|---|---|
| 802.1x | – | – | In/Out | × | × | – |
| DHCP | 68 | UDP | In/Out | ✓ | × | – |
| DNS | 53 | TCP/UDP | In/Out | ✓ | × | – |
| Eco (rilevamento dispositivo)* | 8002 | UDP | In/Out | ✓ | × | – |
| FTP | 21 | TCP | Out | × | × | – |
| 2N IP Eye | 8003 | UDP | Out | × | × | – |
| HTTP | 80 | TCP | In/Out | ✓ | ✓ | **Sistema > Connessioni di rete > scheda SERVER WEB** |
| HTTPS | 443 | TCP | In/Out | ✓ | ✓ | **Sistema > Connessioni di rete > scheda SERVER WEB** |
| Cliente NTP | 123 | UDP | In/Out | ✓ | × | – |
| SLP | 427 | UDP | In/Out | ✓ | × | – |
| SMTP | 25 | TCP | Out | × | ✓ | **Integrazioni > Notifica via e-mail** |
| Syslog | 514 | UDP | Out | × | × | – |

| Servizio | Porta | Protocollo | Direzione | Abilitato per impostazione predefinita | Regolabile | Impostazioni |
|---|---|---|---|---|---|---|
| TFTP | 69 | UDP | Out | × | × | – |
| My2N Knocker | 443 | TCP | Out | ✓ | × | – |
| My2N Tribble Tunnel | 443 | TCP | Out | ✓ | × | – |
| SNMP Agent | 161 | UDP | In/Out | ✓ | × | – |
| SNMP Trap | 162 | UDP | Out | ✓ | × | – |
| Multicast receiver (Automation) | 4433 | UDP | In | × | × | – |
| Multicast DNS | 5353 | UDP | In/Out | ✓ | × | – |

# Automazione

La configurazione standard del dispositivo 2N copre gli scenari più comuni. Per i casi avanzati, come la necessità di personalizzare il dispositivo in base a requisiti specifici o di integrarlo con sistemi di terze parti, è possibile utilizzare la funzione Automazione. L'automazione le consente di definire una logica personalizzata per il comportamento del dispositivo che risponde a diversi eventi, segnali o combinazioni di condizioni. Per esempio, le azioni specifiche possono essere attivate premendo un determinato pulsante di chiamata rapida, attivando un allarme silenzioso, rilevando una porta aperta, attivando un ingresso o rilevando un movimento vicino al dispositivo.

## Impostazioni di automazione:

1. Nell'interfaccia web del dispositivo, vada su **Integrazione > Automazione**.
2. Nella panoramica delle funzioni, abiliti il numero di funzioni desiderato.
3. Clicchi su  per aprire l'interfaccia di configurazione dell'automazione.
4. Nell'intestazione dell'interfaccia Automazioni, digiti il nome della funzione sotto la quale verrà salvata la funzione.
5. Creare un flusso di automazione.
   Una descrizione dettagliata della funzione e della configurazione dell'Automazione è disponibile in Automazione manuale.
6. Una volta completata la funzione, clicchi su SAVE ed esca dall'interfaccia di automazione.


Lettori accessi – Manuale di configurazione



**2N.com**