



# Client mobile Hik-ProConnect

Manuale utente

## Informazioni legali

©2020 Hikvision Europe B.V. Tutti i diritti riservati.

### Informazioni sul presente Manuale

Il presente Manuale contiene le istruzioni per l'uso e la gestione del prodotto. Le figure, i grafici, le immagini e tutte le altre informazioni di seguito riportate servono unicamente a scopi illustrativi ed esplicativi. Le informazioni contenute nel Manuale sono soggette a modifiche, senza alcun preavviso, in seguito ad aggiornamenti del firmware o ad altri motivi. La versione più recente del presente Manuale è disponibile sul sito web di Hikvision (<https://www.hikvision.com/>).

Si consiglia di utilizzare questo Manuale sotto la guida e l'assistenza di professionisti formati nel supporto del prodotto.

### Marchi commerciali

**HIKVISION** e gli altri marchi registrati e loghi di Hikvision sono di proprietà di Hikvision nelle varie giurisdizioni.

Gli altri marchi registrati e loghi menzionati di seguito appartengono ai rispettivi proprietari.

### Esclusione di responsabilità

NELLA MISURA MASSIMA CONSENTITA DALLA LEGGE APPLICABILE, IL PRESENTE MANUALE E IL PRODOTTO DESCRITTO, INSIEME ALL'HARDWARE, AL SOFTWARE E AL FIRMWARE, SONO FORNITI "COSÌ COME SONO" E "CON TUTTI I DIFETTI E GLI ERRORI". HIKVISION NON RILASCI ALCUNA GARANZIA, ESPRESSA O IMPLICITA, COMPRESA A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, GARANZIE DI COMMERCIALIZZABILITÀ, QUALITÀ SODDISFACENTE, O IDONEITÀ PER UN USO SPECIFICO. L'USO DEL PRODOTTO DA PARTE DELL'UTENTE È A RISCHIO DELL'UTENTE STESSO. IN NESSUN CASO HIKVISION SARÀ RITENUTA RESPONSABILE VERSO L'UTENTE PER QUALSIASI DANNO STRAORDINARIO, CONSEGUENZIALE, ACCIDENTALE O INDIRECTO, COMPRESI TRA GLI ALTRI, DANNI PER LA PERDITA DI PROFITTI AZIENDALI, INTERRUZIONI DI ATTIVITÀ O PERDITA DI DATI, DANNEGGIAMENTO DI SISTEMI O PERDITA DI DOCUMENTAZIONE, SIANO ESSI BASATI SU INADEMPIENZA DI CONTRATTO, ILLECITO (COMPRESA LA NEGLIGENZA), RESPONSABILITÀ DI DANNO DA PRODOTTI, O ALTRIMENTI, IN RELAZIONE ALL'USO DEL SOFTWARE, ANCHE QUALORA HIKVISION SIA STATA INFORMATATA SULLA POSSIBILITÀ DI TALI DANNI.

L'UTENTE ACCETTA CHE LA NATURA DI INTERNET PREVEDE RISCHI DI PROTEZIONE INTRINSECHI, E CHE HIKVISION NON SI ASSUME ALCUNA RESPONSABILITÀ IN CASO DI FUNZIONAMENTO ANOMALO, VIOLAZIONE DELLA RISERVATEZZA, O ALTRI DANNI RISULTANTI DA ATTACCHI CIBERNETICI, INFEZIONE DA VIRUS O ALTRI RISCHI LEGATI ALLA SICUREZZA SU INTERNET; TUTTAVIA, HIKVISION FORNIRÀ TEMPESTIVO SUPPORTO TECNICO OVE NECESSARIO.

L'UTENTE ACCETTA DI UTILIZZARE IL PRODOTTO IN CONFORMITÀ A TUTTE LE LEGGI APPLICABILI, E DI ESSERE IL SOLO RESPONSABILE DI GARANTIRE LA CONFORMITÀ ALLA LEGGE APPLICABILE DEL PROPRIO UTILIZZO. IN PARTICOLARE, L'UTENTE È RESPONSABILE DELL'USO DEL PRODOTTO IN UN MODO CHE NON VIOLI I DIRITTI DI TERZE PARTI, COMPRESI A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, DIRITTI DI PUBBLICITÀ, DIRITTI DI PROPRIETÀ INTELLETTUALE O DIRITTI ALLA PROTEZIONE DEI DATI E ALTRI DIRITTI SULLA PRIVACY. L'UTENTE NON DEVE UTILIZZARE IL PRODOTTO PER QUALSIASI USO FINALE VIETATO, COMPRESI LO SVILUPPO O LA PRODUZIONE DI ARMI DI DISTRUZIONE DI MASSA, LO SVILUPPO O LA PRODUZIONE DI ARMI CHIMICHE O BIOLOGICHE, QUALSIASI ATTIVITÀ IN CONTESTI CORRELATI A QUALUNQUE ESPLOSIVO NUCLEARE O CICLO DI COMBUSTIBILE NUCLEARE NON SICURO OPPURE A SOSTEGNO DI VIOLAZIONI DEI DIRITTI DELL'UOMO.

IN CASO DI CONFLITTO TRA IL PRESENTE MANUALE E LA LEGGE VIGENTE, PREVARRÀ QUEST'ULTIMA.

## Significato dei simboli

I simboli contenuti nel presente documento sono definiti di seguito.

Simbolo	Descrizione
 <b>Pericolo</b>	Indica situazioni potenzialmente pericolose che, se non evitate, causano o potrebbero causare lesioni gravi o mortali.
 <b>Attenzione</b>	Indica una potenziale situazione di pericolo che, se non evitata, potrebbe provocare danni all'apparecchiatura, perdite di dati, riduzione delle prestazioni o imprevisti.
 <b>Nota</b>	Fornisce informazioni aggiuntive per evidenziare o integrare punti importanti del testo principale.

---

# Indice

<b>Capitolo 1 Introduzione</b> .....	<b>1</b>
1.1 Destinatari.....	1
1.2 Ambiente di funzionamento .....	1
<b>Capitolo 2 Gestione account</b> .....	<b>2</b>
2.1 Registrazione di un account amministratore di installazione.....	3
2.2 Gestione delle informazioni sull'azienda .....	6
<b>Capitolo 3 Accesso</b> .....	<b>8</b>
<b>Capitolo 4 Panoramica del client mobile Hik-ProConnect</b> .....	<b>9</b>
<b>Capitolo 5 Gestione di una piattaforma</b> .....	<b>14</b>
5.1 Presentazione della pagina Site .....	14
5.2 Aggiunta di una nuova piattaforma .....	15
5.3 Aggiunta di piattaforme esistenti .....	18
5.4 Invio della richiesta per diventare proprietario della piattaforma.....	19
5.5 Invio della richiesta di autorizzazione al proprietario della piattaforma.....	21
<b>Capitolo 6 Gestione di un dispositivo</b> .....	<b>22</b>
6.1 Aggiunta di un dispositivo.....	22
6.1.1 Connessione di un dispositivo offline alla rete .....	22
6.1.2 Aggiunta di un dispositivo tramite la scansione del codice QR .....	23
6.1.3 Aggiunta di dispositivi tramite il servizio Hik-Connect (P2P).....	25
6.1.4 Aggiunta di un dispositivo tramite l'indirizzo IP o il nome dominio .....	28
6.2 Richiesta dell'autorizzazione per un dispositivo .....	30
6.3 Approvazione dell'autorizzazione per i dispositivi.....	30
6.4 Aggiunta di una regola di collegamento .....	31
6.4.1 Aggiunta di una regola di collegamento personalizzata .....	32
6.4.2 Aggiunta di regole di collegamento basate su modelli predefiniti.....	37
6.4.3 Tutorial video .....	40
6.5 Aggiunta di regole di eccezione .....	40
6.6 Attivazione della funzione che consente al dispositivo di inviare notifiche.....	43
6.7 Upgrade del dispositivo .....	44

---

6.8 Scollegamento di un dispositivo dal relativo account corrente .....	45
6.9 Reimpostazione della password del dispositivo .....	45
6.10 Configurazione del DDNS dei dispositivi .....	46
6.11 Visualizzazione di video in tempo reale .....	48
6.12 Visualizzazione di video registrati .....	48
6.13 Uso e configurazione del sistema AX Pro .....	49
6.14 Gestione degli switch .....	52
6.14.1 Attività dello switch .....	52
6.14.2 Topologia di rete .....	54
6.15 Altre funzioni.....	56
<b>Capitolo 7 Gestione dell'archiviazione cloud .....</b>	<b>57</b>
7.1 Impostazione dell'archiviazione cloud per Hik-ProConnect Box .....	57
7.2 Impostazione dell'archiviazione cloud per un DVR cloud.....	60
7.3 Test di rete .....	62
<b>Figura 8 Centro eccezioni.....</b>	<b>63</b>

# Capitolo 1 Introduzione

Hik-ProConnect è una soluzione di sicurezza convergente basata su cloud che aiuta a gestire i servizi dei clienti e ad aumentare gli affari con offerte di abbonamento. Grazie a una piattaforma semplice e affidabile, è possibile monitorare da remoto lo stato di integrità del sistema relativo alle piattaforme dei clienti (e persino risolvere i problemi). Hik-ProConnect consente di personalizzare le soluzioni di sicurezza dei clienti utilizzando dispositivi Hikvision completamente convergenti, che offrono funzioni video, antintrusione, accesso, videocitofono e altre ancora. Hik-ProConnect fornisce agli installatori o utenti finali più modalità e client di accesso alla piattaforma o alla gestione delle risorse.

- **Portale Hik-ProConnect:** è il portale che consente ad amministratori di installazione e installatori di accedere a Hik-ProConnect per gestire le società di sicurezza, inclusi la gestione di autorizzazioni, dipendenti, piattaforme, dispositivi e il monitoraggio dello stato dei dispositivi.
- **Client mobile Hik-ProConnect:** è il client mobile che consente ad amministratori di installazione e installatori di accedere a Hik-ProConnect per gestire le piattaforme, richiedere l'autorizzazione all'utente finale per gestire le informazioni della piattaforma, gestire e configurare i dispositivi, ecc.
- **Client mobile Hik-Connect:** è il client mobile che consente agli utenti finali di gestire i dispositivi, accettare gli inviti dell'installatore a diventare proprietari della piattaforma, approvare le richieste di autorizzazione inviate dall'installatore per permettergli di gestire le informazioni della piattaforma, ecc.

## 1.1 Destinatari

Questo manuale fornisce all'installatore le informazioni e le istruzioni essenziali sull'uso del client mobile Hik-ProConnect per la gestione delle attività di sicurezza.

Questo manuale descrive come aggiungere una piattaforma nuova o esistente per la sua gestione, richiedere l'autorizzazione per l'accesso alla piattaforma da parte dell'utente finale, gestire e configurare i dispositivi, ecc.

## 1.2 Ambiente di funzionamento

Di seguito sono riportati i requisiti di sistema consigliati per l'esecuzione del client mobile.

### Requisiti di sistema

Per iOS: iOS 10 o versioni successive (a partire da iPhone 6 o iPad Air).

Per Android: Android 5.0 o versioni successive.

### Memoria

Per iOS: 1 GB o superiore.

Per Android: 2 GB o superiore.

## Capitolo 2 Gestione account

Sono disponibili due tipi di account: amministratore di installazione e installatore. Ciascuna società dispone di un solo amministratore di installazione, ma può avere più installatori.

### Amministratore di installazione

All'amministratore di installazione è consentito l'accesso a tutte le funzioni del sistema. In genere, l'amministratore di installazione può essere il gestore della società di installazione.

### Installatore

Gli installatori sono degli "account secondari" che fanno capo all'amministratore di installazione e sono limitati dalle autorizzazioni a loro concesse. Ad esempio, la gestione delle piattaforme a loro assegnate. In genere, gli installatori sono dei dipendenti della società di installazione. L'azienda che si occupa dell'installazione deve prima effettuare la registrazione di un account come amministratore di installazione e poi invitare i dipendenti a registrare gli account come installatori.

Il diagramma di flusso dell'intero processo viene riportato di seguito.

---

#### Nota

Attualmente, le ultime tre fasi del diagramma di flusso (Set Role and Permission, Invite Employees e Accept Invitation and Register Installer Accounts) sono disponibili solo sul Portale. Per istruzioni dettagliate su questi tre passaggi, fare riferimento al *Manuale utente del Portale Hik-ProConnect*.

---



**Figura 2-1 Diagramma di flusso della gestione account**

- **Registrazione di un account amministratore di installazione:** la società di installazione dell'impianto di sorveglianza deve per prima cosa registrare un account amministratore di installazione prima di accedere alle funzioni di Hik-ProConnect. Per i dettagli, fare riferimento alla sezione **Registrazione di un account amministratore di installazione**.
- **Inserire le informazioni sull'azienda:** una volta registrato un account amministratore di installazione, è necessario associare le informazioni aziendali (tra cui nome dell'azienda, Paese, logo, numero di licenza commerciale, ecc.) all'account per garantire un servizio ottimale. Per i dettagli, fare riferimento alla sezione **Gestione delle informazioni sull'azienda**.
- **Impostazione di ruolo e autorizzazione:** prima di aggiungere un dipendente al sistema, è possibile creare ruoli diversi con autorizzazioni differenti per l'accesso alle risorse di sistema.
- **Invito dei dipendenti:** è possibile invitare i dipendenti a registrare gli account come installatori e assegnare ruoli diversi per fornire loro le autorizzazioni.
- **Accettazione dell'invito e registrazione degli account installatore:** I dipendenti possono accettare l'invito e registrare account installatore per la gestione di piattaforme e dispositivi.

## 2.1 Registrazione di un account amministratore di installazione

la società di installazione dell'impianto di sorveglianza deve per prima cosa registrare un account amministratore di installazione prima di accedere alle funzioni di Hik-ProConnect.

### Passaggi

1. Nella pagina di accesso, toccare **Registered** per accedere alla pagina di registrazione.

< Register

\* Country/Region

Mainland China >

After registration, the country or region you selected for you company cannot be changed. Please select prudently.

\* Email

Enter email.

\* Verification Code

Verification Code [Get Verification Code](#)

[Didn't receive the verification code?](#)

\* Password

Enter password.

\* Confirm Password

Confirm Password

\* First Name

Enter first name

Register

Figura 2-2 Pagina di registrazione

2. Selezionare il Paese/l'area geografica dell'azienda.

---

 **Nota**

Dopo la registrazione, non sarà possibile modificare il Paese o l'area geografica selezionati per l'azienda.

---

3. Inserire un indirizzo e-mail da associare all'account amministratore di installazione.

4. Per ottenere il codice di verifica, toccare **Get Verification Code**.

---

 **Nota**

- Se il codice di verifica non viene immesso entro il tempo disponibile, toccare **Resend** per ottenerne uno nuovo.
  - Se non lo si riceve, toccare **Didn't receive the verification code?** per maggiori informazioni.
- 

Verrà inviata un'e-mail contenente il codice di verifica all'indirizzo inserito nel passaggio precedente.

5. Inserire il codice di verifica ricevuto.

6. Impostare la password dell'account e confermarla.

---

 **Nota**

Si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Inoltre, si consiglia di cambiare regolarmente la password, specialmente nel sistema ad alta sicurezza. La modifica mensile o settimanale consente di proteggere meglio il prodotto.

---

7. Inserire il nome e il numero di telefono.

8. Inserire il nome dell'azienda.

9. Opzionale: inserire il codice di autenticazione utilizzato per confermare la genuinità dell'installatore professionale.

---

 **Nota**

- Il codice di autenticazione deve contenere 10 cifre. Per ottenere il codice di autenticazione, seguire le istruzioni visualizzate sull'interfaccia. Se il campo relativo al codice di autenticazione è opzionale, è possibile lasciarlo vuoto e autenticare l'account amministratore di installazione in un secondo momento tramite il Portale Hik-ProConnect. Per i dettagli su come effettuare l'autenticazione dell'account, consultare il *Manuale utente del Portale Hik-ProConnect*.
-

10. Opzionale: spuntare la casella **I would like to receive newsletters about new product introduction, service introduction, and questionnaires from Hikvision. I understand that at any time I can unsubscribe.** per effettuare l'iscrizione. È possibile annullarla nella pagina **Me** → **About**.
  - Se l'iscrizione va a buon fine, si riceverà un'e-mail di conferma in pochi minuti. Se necessario, è possibile annullare l'iscrizione facendo clic sull'URL presente nell'e-mail.
  - Dopo l'iscrizione, verranno inviate e-mail sugli ultimi prodotti, servizi, questionari e su offerte speciali all'indirizzo utilizzato per la registrazione dell'account.
11. Qualora si accettino i dettagli riportati negli accordi, selezionare **I agree to the Terms of Service and Privacy Policy**.
12. Toccare **Register**.

Verrà inviata un'e-mail di conferma della registrazione all'indirizzo inserito al passaggio di cui sopra.
13. Toccare **Verify Now** nell'e-mail ricevuta.

Una volta terminata la verifica, si accederà alla pagina di accesso di Hik-ProConnect.

### **Risultato**

È possibile accedere a Hik-ProConnect con questo account ed effettuare altre operazioni, quali la gestione di piattaforme, ecc.

### **Come continuare**

Una volta registrato un account come amministratore di installazione, è possibile accedere a Hik-ProConnect con il proprio account. È necessario inserire le informazioni aziendali da associare al proprio account. Per i dettagli, fare riferimento alla sezione **Gestione delle informazioni sull'azienda**.

## **2.2 Gestione delle informazioni sull'azienda**

Per sfruttare al meglio il servizio, una volta registrato un account come amministratore di installazione, è necessario associare le informazioni aziendali (tra cui nome dell'azienda, numero di telefono, indirizzo e-mail, ecc.) all'account.

Dopo aver registrato l'account amministratore di installazione e aver effettuato l'accesso, è necessario inserire le informazioni aziendali in base alla situazione effettiva. Per i dettagli su come effettuare la registrazione di un account e l'accesso, fare riferimento alle sezioni **Registrazione di un account amministratore di installazione** e **Accesso**.

**Passaggi**

1. Inserire il nome dell'azienda.
2. Inserire numero di telefono.
3. Dopo la registrazione, inserire un indirizzo e-mail da associare all'account amministratore di installazione.
4. Inserire altre informazioni dell'azienda, come l'indirizzo, la città, lo stato/la provincia/l'area geografica e il codice postale.
5. Opzionale: inserire il sito web della società.
6. Toccare **OK**.

Una volta impostate le informazioni sull'azienda, si accede alla schermata principale del client mobile Hik-ProConnect.

---

 **Nota**

Per inserire il numero di partita IVA, caricare il registro dell'azienda o modificare le relative informazioni, è necessario accedere al Portale. Per i dettagli, fare riferimento al *Manuale utente del Portale Hik-ProConnect*.

---

## Capitolo 3 Accesso

Dopo l'accesso tramite un account amministratore di installazione, installatore o e-Partner, è possibile gestire piattaforme e dispositivi, monitorare lo stato di integrità, ecc.

### Prima di iniziare

- Assicurarsi di aver registrato un account. Per i dettagli sulla registrazione, fare riferimento al *Manuale utente del Portale Hik-ProConnect*.
- Assicurarsi di aver accettato i Termini del servizio e l'Informativa sulla privacy.

### Passaggi

1. Toccare  per avviare il client mobile.  
Viene visualizzata la pagina di accesso.
2. Selezionare il Paese/l'area geografica in cui si trova l'account e fare clic su **OK**.
3. Inserire e-mail di registrazione e password.
4. Opzionale: ripristinare la password in caso di smarrimento.
  - 1) Toccare **Forgot Password** per accedere alla pagina di reimpostazione della password.
  - 2) Toccare **Get Verification Code**.  
Verrà inviato un codice di verifica dal portale nella propria casella di posta elettronica.
  - 3) Inserire il codice di verifica ricevuto nel campo **Verification Code**.
  - 4) Inserire la nuova password e confermarla.

---

#### Nota

Si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Inoltre, si consiglia di cambiare regolarmente la password, specialmente nel sistema ad alta sicurezza. La modifica mensile o settimanale consente di proteggere meglio il prodotto.

---

- 5) Toccare **OK**.  
Per opzione predefinita, sarà necessario effettuare l'accesso con la nuova password.
5. Toccare **Login**.

---

#### Nota

- Se un utente con un account nuovo o già registrato ha inserito il codice di autenticazione nella pagina di registrazione, quando accede al client mobile deve fornire le informazioni di autenticazione dell'azienda, tra cui l'occupazione, l'indirizzo completo (via, stato/provincia/area geografica e città) e il numero di telefono.
  - Se l'utente ha già registrato un account e non ha inserito il codice di verifica nella pagina di registrazione, quando accede al client mobile deve inserire il nome dell'azienda per completare le informazioni di autenticazione della stessa.
-

## Capitolo 4 Panoramica del client mobile Hik-ProConnect

Il client mobile Hik-ProConnect fornisce accesso a Hik-ProConnect dal proprio smartphone. Una volta effettuato l'accesso a Hik-ProConnect tramite il client mobile, viene visualizzata la schermata principale.

### Moduli principali

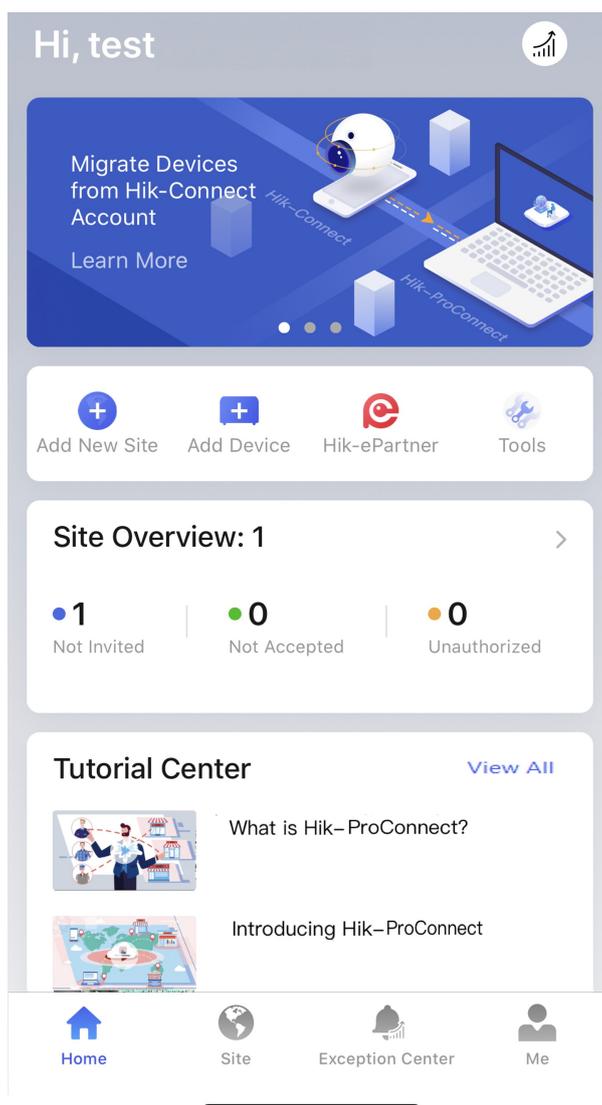
Il client mobile Hik-ProConnect è diviso in quattro moduli principali. È possibile accedere a questi moduli tramite il pannello di navigazione sulla parte inferiore.

**Tabella 4-1 Moduli principali del client mobile Hik-ProConnect**

Modulo	Descrizione
Schermata principale	Nella schermata principale è possibile visualizzare la panoramica delle piattaforme, i dispositivi gestiti, le eccezioni ricevute e altri elementi, come le funzioni principali e il Centro tutorial.
Piattaforma	Nel modulo Piattaforma, viene visualizzato l'elenco delle piattaforme. Una piattaforma rappresenta una posizione fisica in cui sono installati i dispositivi e tramite cui l'installatore/amministratore di installazione può gestirli e configurarli.
Centro eccezioni	Dopo aver impostato le regole di eccezione, quando si verifica un'eccezione sul dispositivo, questo invia una notifica al client mobile (se il campo <b>Received by</b> nella regola contiene il valore <b>Mobile Client</b> ) ed è possibile visualizzare tutte le notifiche relative alle eccezioni ricevute dal client mobile in Exception Center.
Io	<p><b>Visualizzazione delle informazioni sull'account:</b> è possibile visualizzare le informazioni sull'account corrente, tra cui nome, profilo e numero di telefono.</p> <hr/> <p> <b>Nota</b></p> <p>È possibile modificare le informazioni sull'account tramite il Portale di Hik-ProConnect. Per ulteriori dettagli, consultare il <i>Manuale dell'utente del Portale Hik-ProConnect</i>.</p> <hr/> <p><b>Iscrizione alla newsletter:</b> se l'amministratore di installazione non si è iscritto alla newsletter al momento della registrazione dell'account, può farlo in questa sezione.</p>

Modulo	Descrizione
	<p>Dopo l'iscrizione, verranno inviate e-mail sugli ultimi prodotti, servizi, questionari e su offerte speciali all'indirizzo utilizzato per la registrazione dell'account.</p> <p>È possibile annullare l'iscrizione in qualsiasi momento nella pagina <b>Me</b> → <b>About</b>. Dopo l'annullamento dell'iscrizione, la newsletter non verrà più inviata.</p> <hr/> <p><b>Modifica password:</b> consente di modificare la password del dispositivo.</p> <hr/> <p> <b>Nota</b></p> <p>Si consiglia vivamente di creare una password complessa (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Inoltre, si consiglia di cambiare regolarmente la password, specialmente nel sistema ad alta sicurezza. La modifica mensile o settimanale consente di proteggere meglio il prodotto.</p> <hr/> <p><b>Informazioni:</b> è possibile visualizzare la versione della piattaforma corrente e leggere i contratti tra cui i termini del servizio, l'informativa sulla privacy e la licenza Open Source.</p> <p>Dopo aver effettuato l'iscrizione alla newsletter, è possibile annullarla da questa sezione in qualsiasi momento. Dopo l'annullamento dell'iscrizione, la newsletter non verrà più inviata.</p> <hr/> <p><b>Guida:</b> consente di aprire il manuale dell'utente del client mobile Hik-ProConnect. È possibile inserire delle parole chiave per cercare le informazioni desiderate nel manuale dell'utente.</p> <hr/> <p><b>Commenti:</b> in caso di domande e suggerimenti sul sistema, è possibile inviarcele.</p> <ol style="list-style-type: none"> <li>1. Selezionare un tipo di feedback e quindi inserire suggerimenti e domande nella finestra a comparsa e allegare un'immagine se necessario.</li> <li>2. Inserire un indirizzo e-mail. Una volta ricevuto il feedback, invieremo un'e-mail all'indirizzo indicato se ci è possibile arrivare a una conclusione.</li> <li>3. Fare clic su <b>Submit</b>.</li> </ol> <hr/> <p><b>Esci:</b> consente di uscire dall'account corrente e tornare alla pagina di accesso.</p>

## Presentazione della schermata principale



**Figura 4-1 Schermata principale**

**Tabella 4-2 Descrizione della schermata principale**

Name	Introduzione
Banner	<p>Sono disponibili alcuni banner che indicano le caratteristiche, le funzioni e le informazioni importanti di Hik-ProConnect.</p> <hr/> <p><b>Nota</b></p> <p>È possibile invitare gli utenti finali a scaricare o aggiornare il client mobile Hik-Connect (versione 4.7.1 e successive) inviando loro il codice QR o il link per il download.</p> <hr/>

Name	Introduzione
Scelta rapida	<p>I tasti di scelta rapida per le funzioni principali vengono forniti sul client mobile Hik-ProConnect.</p> <ul style="list-style-type: none"> <li>● <b>Add New Site:</b> aggiungere una nuova piattaforma per gestire i dispositivi dell'utente finale. Per istruzioni dettagliate, fare riferimento alla sezione <b>Aggiunta di una nuova piattaforma</b>.</li> <li>● <b>Add Device:</b> aggiungere i dispositivi a una piattaforma manualmente o tramite la scansione del codice QR sul dispositivo. Per i dettagli, fare riferimento alla sezione <b>Aggiunta di un dispositivo</b>.</li> <li>● <b>Linkage Rule:</b> impostare una regola di collegamento per definire le risorse collegate e le azioni collegate quando la sorgente rileva l'evento di attivazione. Per istruzioni dettagliate, fare riferimento alla sezione <b>Aggiunta di regole di collegamento</b>.</li> <li>● <b>Hik-ePartner:</b> un'applicazione mobile progettata appositamente per i partner Hikvision. Toccare <b>Hik-ePartner</b> per aprire o scaricare l'applicazione (a seconda che sia stata scaricata o non). Serve a fornire una gamma completa di servizi e supporto per i partner Hikvision, tra cui: <ul style="list-style-type: none"> <li>○ Consultare e cercare le informazioni sui prodotti, le promozioni e gli eventi programmati di Hikvision.</li> <li>○ Guadagnare punti e riscattare regali.</li> <li>○ Strumenti di installazione.</li> <li>○ Chattare in tempo reale con i rappresentanti del supporto Hikvision.</li> </ul> </li> <li>● <b>Tools:</b> fornisce alcuni strumenti online per migliorare l'efficienza del lavoro.</li> </ul>
Panoramica della piattaforma	<p>È possibile visualizzare il numero totale di piattaforme gestite. Inoltre, è possibile utilizzare le opzioni:</p> <ul style="list-style-type: none"> <li>● <b>Not Invited:</b> per conoscere il numero di piattaforme i cui proprietari non sono stati invitati.</li> <li>● <b>Not Accepted:</b> per conoscere il numero di piattaforme i cui proprietari non hanno accettato l'invito.</li> <li>● <b>Unauthorized:</b> per conoscere il numero di piattaforme di cui non si dispongono le autorizzazioni.</li> </ul> <hr/> <p> <b>Nota</b></p> <p>È possibile fare clic su  per accedere all'elenco delle piattaforme. Per istruzioni dettagliate su come gestire le piattaforme, fare riferimento alla sezione <b>Gestione della piattaforma</b>.</p> <hr/>

Name	Introduzione
Panoramica delle eccezioni	<p>È possibile visualizzare il numero di eccezioni ricevute e le proporzioni di ciascun tipo di eccezione.</p> <hr/> <p> <b>Nota</b></p> <p>È possibile fare clic su &gt; per accedere a <b>Exception Center</b> al fine di controllare le eccezioni ricevute. Per istruzioni dettagliate su come usare Exception Center, fare riferimento alla sezione <b>Centro eccezioni</b>.</p> <hr/>
Centro tutorial	<p>Contiene video tutorial da guardare per conoscere meglio Hik-ProConnect e i modi corretti di utilizzare il prodotto.</p> <p>Toccare un video per aprire una pagina web e avviare la riproduzione.</p> <p>Toccare <b>View All</b> per visualizzare tutti i video in Centro tutorial.</p>

---

## Capitolo 5 Gestione di una piattaforma

Una piattaforma può essere considerata come un'area o una posizione con fuso orario e indirizzo reali, corrispondenti ad esempio all'indirizzo di casa o dell'azienda dell'utente finale. L'installatore può aggiungere i dispositivi autorizzati dell'utente finale alla piattaforma e utilizzarla per gestirli e configurarli da remoto.

La funzione di gestione della piattaforma consente di aggiungere ed eliminare piattaforme, invitare l'utente finale come proprietario della piattaforma, richiedere l'autorizzazione dal proprietario della piattaforma per operare, ecc.

### 5.1 Presentazione della pagina Site

Sulla pagina Site, è possibile visualizzare le piattaforme assegnate (l'amministratore di installazione e gli installatori con l'autorizzazione Manage All Sites possono visualizzare tutte le piattaforme aziendali) ed effettuare alcune operazioni su di esse, ad esempio cercarle, aggiungerle, invitare l'utente a diventarne il proprietario, ecc.

Sono presenti diversi stati per le piattaforme nell'elenco.

#### **Non invitato**

Indica che la piattaforma è appena stata aggiunta e che l'utente finale proprietario della piattaforma non è stato invitato o che non ha accettato l'invito.

#### **Non registrato**

Indica che l'invito è stato inviato all'utente finale che però non ha registrato un account Hik-Connect.

#### **Non accettato**

Indica che l'invito è stato inviato, ma non è stato accettato dall'utente finale che ha registrato un account Hik-Connect.

#### **Invitato, non autorizzato (visualizzato come Autorizzazione senza commissione)**

Indica che l'utente finale ha accettato l'invito come proprietario della piattaforma, ma questa non è stata autorizzata dall'installatore.

#### **Autorizzato e in monitoraggio (visualizzato come Indirizzo e-mail o Numero di telefono)**

Indica che l'installatore ha ricevuto l'autorizzazione per operare sulla piattaforma da parte dell'utente finale.

---

#### **Nota**

In base allo stato della piattaforma, l'amministratore di installazione e gli installatori con autorizzazione alla gestione della piattaforma possono eseguire le operazioni indicate nella tabella di seguito.

---

Tabella 5-1 Operazioni supportate nei vari stati

Operazioni supportate	Non invitato	Non accettato Non registrato	Invitato, non autorizzato (visualizzato come Autorizzazione senza commissione)	Autorizzato e in monitoraggio (visualizzato come Indirizzo e-mail o Numero di telefono)
Cerca piattaforma	√	√	√	√
Invita proprietario piattaforma	√	√	×	×
Gestisci dispositivo	√	√	×	√
Modifica piattaforma	√	√	×	√
Elimina piattaforma	√	√	×	×
Richiedi autorizzazione	×	×	√	×

## 5.2 Aggiunta di una nuova piattaforma

Quando l'utente finale desidera che la società di installazione fornisca il servizio di installazione, l'amministratore di installazione o l'installatore con le relative autorizzazioni devono creare una nuova piattaforma che gestisca i dispositivi dell'utente finale.

### Prima di iniziare

Assicurarsi di disporre delle autorizzazioni per l'aggiunta di una nuova piattaforma.

### Passaggi

1. Toccare la scheda **Site** nella parte inferiore per accedere alla pagina Site.
2. Toccare  per accedere alla pagina Add New Site.

< Add New Site

\*Site Name  
Enter site name.

\*Time Zone  
(UTC-07:00) Arizona >

\*Address  
Enter street and number, P.O. box, c/o.  
Enter apartment, suite, unit, building, floor, etc.

\*City  
Enter city.

State/Province/Region  
Enter state, province, or region.

Sync Time & Time Zone to Device

⚠ Time zone cannot be edited after adding the site.

OK

If the end user already has a site and it is not authorized to any company, you can get the site ID from the end user for managing the site.

[Add Existing Site](#)

Figura 5-1 Aggiunta di una nuova piattaforma

 **Nota**

- Se una piattaforma esistente dell'utente finale non è assegnata ad alcuna azienda di installazione, è possibile selezionare **Add existing Site** per aggiungerla.
  - Se non si dispone dell'autorizzazione per aggiungere una nuova piattaforma, dopo aver fatto clic su **Add New Site**, si accede alla pagina Add Existing Site per aggiungerla.
- Per i dettagli, fare riferimento alla sezione **Aggiunta di piattaforme esistenti**.

3. Impostare il nome, il fuso orario, l'indirizzo, la città e lo stato/la provincia/l'area geografica della piattaforma.

 **Nota**

È necessario selezionare il fuso orario corretto dei dispositivi che non sarà possibile modificare una volta aggiunta la piattaforma.

4. Opzionale: Selezionare **Sync Time & Time Zone to Device** per sincronizzare l'ora e il fuso orario della piattaforma con quelli dei dispositivi aggiunti ad essa.
5. Fare clic su **OK** per aggiungere una nuova piattaforma all'elenco.
6. Opzionale: in base allo stato e all'autorizzazione della piattaforma, eseguire una delle seguenti operazioni.

---

 **Nota**

Per i dettagli sulle operazioni supportate in uno stato diverso della piattaforma, fare riferimento alla sezione **Presentazione della pagina Site**.

---

- |  |   |
|--|---|
| <b>Cerca piattaforma</b>                     | Inserire le parole chiave nel campo di ricerca e toccare <b>Search</b> per visualizzare i risultati nell'elenco.  |
| <b>Visualizza dettagli della piattaforma</b> | Toccare la piattaforma per visualizzarne i dettagli tra cui i dispositivi gestiti, le informazioni e così via.  |
| <b>Modifica piattaforma</b>                  | Toccare  nell'angolo in alto a destra sulla pagina Site Details, quindi toccare <b>Manage Site Information</b> per modificare le informazioni della piattaforma.<br>È possibile modificare il nome, l'indirizzo, la città e lo stato/la provincia/l'area geografica della piattaforma. Se si dispone dell'autorizzazione per gestire la piattaforma, è anche possibile scegliere se spuntare la casella <b>Sync Time &amp; Time Zone to Device</b> . |
| <b>Elimina piattaforma</b>                   | Toccare  nell'angolo in alto a destra dalla pagina Site Details, quindi toccare <b>Delete Site</b> per eliminare la piattaforma.   |
| <b>Invita proprietario piattaforma</b>       | Per la piattaforma con stato <b>Not Invited</b> , toccare <b>Invite Now</b> nella pagina Site Details per invitare un utente finale a diventare proprietario della piattaforma.   |

---

 **Nota**

Per i dettagli, fare riferimento alla sezione **Invio della richiesta per diventare proprietario della piattaforma**.

---

- |                             |   |
|-----------------------------|---|
| <b>Gestisci dispositivo</b> | Per le piattaforme autorizzate o con lo stato <b>Not Invited</b> , <b>Not Registered</b> o <b>Not Accepted</b> , è possibile accedere alla pagina Site Details per gestire i dispositivi ed effettuare operazioni quali l'aggiunta di dispositivi alla piattaforma, l'upgrade di dispositivi, la richiesta di autorizzazione alla visualizzazione in tempo reale o alla configurazione, l'aggiunta di regole di collegamento e di eccezione, ecc. |
|-----------------------------|---|

---

 **Nota**

Per i dettagli, fare riferimento alla sezione **Gestione di un dispositivo**.

---

## 5.3 Aggiunta di piattaforme esistenti

Quando una piattaforma non è assegnata a un'azienda o lo era in precedenza, ma è stata successivamente rimossa e risulta quindi non associata, è possibile aggiungerla richiedendone l'autorizzazione al proprietario.

### Passaggi

1. Toccare la scheda **Site** nella parte inferiore per accedere alla pagina Site.
2. Toccare **Add New Site** → **Add Existing Site**.

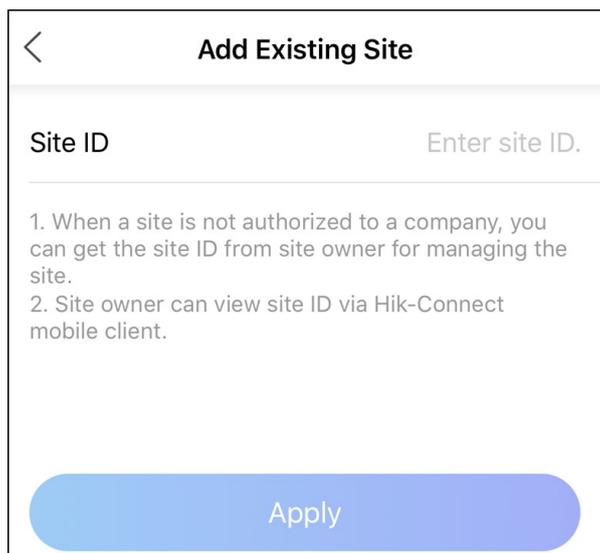


Figura 5-2 Aggiunta di una piattaforma esistente

3. Inserire l'ID della piattaforma.

---

### Nota

- È possibile ottenere l'ID della piattaforma dal proprietario, che è in grado di visualizzarlo tramite il client mobile Hik-Connect.
- Chiedere agli utenti finali di scaricare o aggiornare Hik-Connect Mobile Client (versione 4.7.1 o successiva). È possibile inviare il codice QR o il link per il download visualizzato nel banner sulla schermata principale del Portale.

4. Fare clic su **Apply**.

La piattaforma sarà aggiunta nell'elenco delle piattaforme e il proprietario riceverà una richiesta. Una volta approvata la richiesta da parte del proprietario della piattaforma, questa sarà autorizzata dall'installatore.

## 5.4 Invio della richiesta per diventare proprietario della piattaforma

Dopo che l'azienda incaricata ha completato l'installazione, l'installatore deve invitare il proprietario della piattaforma per consegnargliela. Se necessario, quando invita il proprietario della piattaforma, l'installatore può anche richiedere le autorizzazioni specifiche per la manutenzione dei dispositivi.

### Prima di iniziare

Assicurarsi che lo stato della piattaforma sia **Not Invited** e di disporre dell'autorizzazione per gestirla, ad esempio Manage All Sites e Manage Assigned Site.

### Passaggi

1. Nell'elenco piattaforme, toccare una piattaforma per accedere alla pagina Dettagli piattaforma.
2. Toccare **Invite Now** per accedere alla pagina Invite Site Owner.
3. Opzionale: selezionare **Allow Me to Disable Hik-Connect Service**. Dopo aver consegnato la piattaforma all'utente finale, è possibile disattivare il servizio Hik-Connect sui dispositivi al fine di impedirgli di eseguire le operazioni su di essi tramite il client mobile Hik-Connect.

---

### Nota

Quando questa funzione è attiva e la piattaforma è stata consegnata, se necessario, è possibile accedere alla pagina Site Details e toccare la scheda **Device** per disattivare il servizio Hik-Connect su uno o tutti i dispositivi presenti su tale piattaforma selezionando  o disabilitando il pulsante **Hik-Connect Service**. È possibile anche eliminare i dispositivi dall'account Hik-Connect dell'utente finale senza l'autorizzazione di quest'ultimo.

---

4. Selezionare **Email** o **Phone Number** come modalità di invito.
5. Inserire l'indirizzo e-mail o il numero di telefono del proprietario della piattaforma.
6. Opzionale: dopo aver consegnato la piattaforma al proprietario, selezionare le autorizzazioni da concedere all'installatore.

---

### Nota

- Toccare  per impostare il periodo di validità delle autorizzazioni alla configurazione e alla visualizzazione in tempo reale, quindi selezionare i dispositivi.
  - Se non si dispone dell'autorizzazione per gestire i dispositivi o questi non vengono aggiunti alla piattaforma, non è possibile selezionare le autorizzazioni per la configurazione e la visualizzazione in tempo reale quando si invita il proprietario della piattaforma.
  - Se si selezionano le seguenti autorizzazioni, quando l'utente finale accetta l'invito, verranno concesse le autorizzazioni all'installatore. Non è necessario che l'installatore richieda di nuovo l'autorizzazione al proprietario della piattaforma.
-

**Gestione informazioni piattaforma**

Autorizzazione a gestire le informazioni sulla piattaforma.

**Configuration**

Autorizzazione alla configurazione dei dispositivi selezionati nella piattaforma.

**Visualizzazione in tempo reale**

Autorizzazione alla visualizzazione live dei dispositivi selezionati nella piattaforma.

**Playback**

Autorizzazione per richiedere la riproduzione dei video relativi ai dispositivi selezionati nella piattaforma.

7. Inserire i commenti, ad esempio il motivo dell'invito, che l'utente può visualizzare quando riceve tale invito tramite il client mobile Hik-Connect.
  8. Toccare **Invite** per inviare l'invito.
    - L'utente riceverà l'invito tramite e-mail o messaggio contenente un link per il download del client mobile Hik-Connect. L'utente può scaricare o aprire il client mobile Hik-Connect tramite il link.
    - Se non lo ha ancora fatto, l'utente deve prima registrare un account Hik-Connect. Dopo aver registrato l'account e accettato l'invito tramite il client mobile Hik-Connect, l'utente diventerà il proprietario della piattaforma.
- 

 **Nota**

Chiedere agli utenti finali di scaricare o aggiornare Hik-Connect Mobile Client (versione 4.7.1 o successiva). È possibile inviare il codice QR o il link per il download visualizzato nel banner sulla schermata principale.

---

- Se è necessario effettuare la manutenzione dei dispositivi aggiunti al client mobile Hik-Connect, ma non ancora inseriti nella piattaforma e gestiti tramite essa, dopo che l'utente finale ha accettato l'invito ed è diventato il proprietario della piattaforma, può approvare le autorizzazioni relative a questi dispositivi richieste dall'installatore.
9. Opzionale: prima che l'utente finale accetti l'invito, toccare **Not Registered** o **Not Accepted** per inviarlo di nuovo.
- 

 **Nota**

È possibile inviare al massimo cinque inviti al giorno e gli inviti precedenti saranno invalidati inviandone un altro.

---

## 5.5 Invio della richiesta di autorizzazione al proprietario della piattaforma

Una volta che la piattaforma (senza autorizzazioni selezionate al momento dell'invio dell'invito al proprietario) è stata consegnata al proprietario e, a questo punto, è necessario effettuare la manutenzione dei dispositivi aggiunti ad essa, l'installatore gli deve inviare una richiesta per ottenere l'autorizzazione. Una volta approvata l'autorizzazione, l'installatore può gestire e configurare i dispositivi della piattaforma. Inoltre, il proprietario può aggiungere un dispositivo sul client mobile Hik-Connect e autorizzare l'installatore a effettuare ulteriori operazioni di gestione e configurazione.

### Passaggi

1. Selezionare una delle seguenti modalità per richiedere l'autorizzazione.
  - Toccare il messaggio in blu riguardante l'autorizzazione mancante nell'elenco delle piattaforme.
  - Toccare la piattaforma per accedere alla pagina Site Details. Toccare  nell'angolo in alto a destra e poi **Apply for Authorization**.
2. Toccare **OK** per confermare l'operazione.

Il proprietario della piattaforma riceverà e gestirà la richiesta tramite il client mobile Hik-Connect. Una volta che il proprietario approva la richiesta, l'installatore ottiene l'autorizzazione e può effettuare le operazioni sulla piattaforma.

Se è necessario effettuare la manutenzione dei dispositivi aggiunti al client mobile Hik-Connect, ma non ancora inseriti nella piattaforma e gestiti tramite essa, dopo aver espresso il consenso, il proprietario può selezionarli e approvare le autorizzazioni relative a questi dispositivi richieste dall'installatore.

---

### Nota

- Chiedere agli utenti finali di scaricare o aggiornare Hik-Connect Mobile Client (versione 4.5.0 o successiva). È possibile inviare il codice QR o il link per il download visualizzato nel banner sulla schermata principale del Portale.
  - Per quanto riguarda il sistema AX Pro, dopo averlo aggiunto a Hik-ProConnect, è possibile utilizzare gli account installatore e amministratore di installazione per accedere a tale sistema. Se l'installatore elimina Ax Pro da Hik-ProConnect, di conseguenza verranno eliminati anche gli account. Se si modifica la password di accesso all'account installatore, viene modificata anche quella per accedere al sistema AX Pro con tale account.
  - Dopo aver autorizzato l'installatore ad accedere alla piattaforma contenente il sistema AX Pro, è possibile utilizzare l'account installatore e amministratore di installazione per accedere a tale sistema. Ciò si applica anche all'account autorizzato a gestire tutte le piattaforme.
  - Se un installatore consegna la piattaforma contenente il sistema AX Pro a un utente finale, quest'ultimo può utilizzare il suo account Hik-Connect per accedere anche a tale sistema, mentre l'account installatore viene eliminato da Ax Pro. Ciò si applica anche all'account amministratore di installazione.
  - Per i dettagli relativi alle operazioni sul client mobile Hik-Connect, fare riferimento al manuale utente del client mobile Hik-Connect.
-

---

## Capitolo 6 Gestione di un dispositivo

Hik-ProConnect supporta più tipi di dispositivi, tra cui dispositivi di codifica, pannelli del controllo di sicurezza, videocitofoni, dispositivi di controllo degli accessi, NVR/DVR e campanelli. Dopo averli aggiunti al sistema, è possibile gestirli e configurare le impostazioni necessarie, tra cui la configurazione da remoto dei parametri relativi al dispositivo, la configurazione delle regole di eccezione e di collegamento, ecc. Una volta aggiunte le telecamere di conteggio persone e i dispositivi di controllo della temperatura, è anche possibile attivare questi servizi e impostare i relativi parametri sul Portale (alcune funzioni potrebbero non essere disponibili in determinati Paesi e regioni).

### 6.1 Aggiunta di un dispositivo

Sono disponibili tre modi per aggiungere i dispositivi alla piattaforma. 1. Aggiunta di dispositivi eseguendo la scansione del codice QR. La scansione del codice QR su un dispositivo consente di aggiungerne uno solo alla piattaforma, mentre la scansione del codice QR generato da iVMS-4500 o iVMS-4200 consente di aggiungere più dispositivi a una piattaforma in un batch. 2. Aggiunta dei dispositivi tramite Hik-Connect (P2P). 3. Aggiunta di un dispositivo tramite l'indirizzo IP o il nome di dominio.

#### 6.1.1 Connessione di un dispositivo offline alla rete

Quando si aggiunge un dispositivo al client mobile, se il dispositivo è offline, è necessario prima connettere il dispositivo a una rete.

##### Passaggi

1. Aggiungere un dispositivo al client mobile.
2. Toccare **Connect to Network** nella finestra a comparsa.
3. Selezionare un tipo di dispositivo e quindi seguire le istruzioni sull'interfaccia per eseguire le operazioni relative.

---

##### Nota

- Verificare che il dispositivo sia acceso.
  - Per connettere il pannello di controllo di sicurezza wireless alla rete, se il sistema operativo dello smartphone è Android, consentire al client mobile l'accesso alla posizione, altrimenti NON sarà possibile collegarsi al Wi-Fi.
-

## 6.1.2 Aggiunta di un dispositivo tramite la scansione del codice QR

È possibile aggiungere un solo dispositivo a una piattaforma eseguendo la scansione del codice QR del dispositivo oppure aggiungerne più di uno tramite la scansione del codice QR generato da iVMS-4200 o iVMS-4500.

### Prima di iniziare

Accertarsi che i dispositivi che si utilizzeranno siano correttamente installati e connessi alla rete secondo le specifiche dei produttori.

### Passaggi

1. Toccare una piattaforma sull'elenco delle piattaforme per accedere alla pagina contenente i relativi dettagli.
2. Toccare **Add Device** per accedere alla pagina Add Device.
3. Eseguire la scansione del codice QR per aggiungere i dispositivi alla piattaforma.
  - Scansionare il codice QR del dispositivo. È possibile eseguire la scansione del codice QR allineandolo con il fotogramma di scansione. Se è presente un codice QR nell'album del telefono, toccare **Album** per estrarlo dall'album locale. Questa modalità consente di aggiungere un solo dispositivo alla volta alla piattaforma.

---

#### Nota

- Di solito il codice QR è stampato sull'etichetta nella parte posteriore del dispositivo.
  - Se l'ambiente in cui si esegue la scansione è poco illuminato, toccare  per attivare il flash.
  - Consentire al client mobile l'accesso alla raccolta foto del telefono.
- 
- Eseguire la scansione di un codice QR generato da iVMS-4200 o iVMS-4500. Dopo la scansione del codice QR, si accede alla pagina per selezionare i dispositivi da aggiungere. Selezionare i dispositivi e toccare **OK** per aggiungerli alla piattaforma. Questa modalità consente di aggiungere più dispositivi alla volta alla piattaforma.
4. Opzionale: eseguire le seguenti operazioni se si verificano le seguenti situazioni.
    - Se il codice QR contiene solo le informazioni sul numero di serie del dispositivo, è necessario accedere manualmente alla pagina di aggiunta. In tal caso aggiungere manualmente il dispositivo. Per i dettagli, fare riferimento alla sezione **Aggiunta di un dispositivo tramite Hik-Connect (P2P)**.
    - Se il dispositivo è offline occorre connetterlo a una rete. Per i dettagli, fare riferimento alla sezione **Connessione di un dispositivo offline alla rete**.
    - Se il dispositivo non è attivo, toccare **Activate** sulla finestra a comparsa, quindi creare una password amministratore del dispositivo e toccare **Activate** per attivarlo.

---

#### Nota

Durante l'attivazione, sarà attivato automaticamente il protocollo di configurazione dell'host dinamico (DHCP) in modo da allocare gli indirizzi IP del dispositivo.

---

- Se il servizio Hik-Connect è disabilitato sul dispositivo, toccare **Enable** sulla finestra a comparsa, quindi creare un codice di verifica del dispositivo e toccare **Enable** per abilitare il servizio.

---

 **Nota**

Chiedere agli utenti finali di scaricare o aggiornare Hik-Connect Mobile Client (versione 4.7.1 o successiva). È possibile inviare il codice QR o il link per il download visualizzato nel banner sulla schermata principale del Portale.

---

Il dispositivo sarà visualizzato nell'elenco dei dispositivi.

---

 **Nota**

- Il servizio di monitoraggio dello stato è attivo sui dispositivi aggiunti per impostazione predefinita. Non è possibile aggiornare il firmware, impostare le regole di collegamento (quelle esistenti non saranno valide), impostare e ricevere le eccezioni e controllare il monitoraggio dello stato di quei dispositivi che hanno la funzione di monitoraggio dello stato disabilitata.
  - Dopo aver aggiunto il dispositivo, Hik-ProConnect inizia a controllare la compatibilità della versione del firmware del dispositivo. Se il dispositivo non è compatibile con Hik-ProConnect, alcune funzioni (tra cui il monitoraggio dello stato, la regola di collegamento e la configurazione da remoto) non risultano disponibili.
  - Per quanto riguarda il sistema AX Pro, dopo averlo aggiunto a Hik-ProConnect, è possibile utilizzare gli account installatore e amministratore di installazione per accedere a tale sistema. Se l'installatore elimina Ax Pro da Hik-ProConnect, di conseguenza verranno eliminati anche gli account. Se si modifica la password di accesso all'account installatore, viene modificata anche quella per accedere al sistema AX Pro con tale account.
  - Dopo aver autorizzato l'installatore ad accedere alla piattaforma contenente il sistema AX Pro, è possibile utilizzare l'account installatore e amministratore di installazione per accedere a tale sistema. Ciò si applica anche all'account autorizzato a gestire tutte le piattaforme.
  - Se un installatore consegna la piattaforma contenente il sistema AX Pro a un utente finale, quest'ultimo può utilizzare il suo account Hik-Connect per accedere anche a tale sistema, mentre l'account installatore viene eliminato da Ax Pro. Ciò si applica anche all'account amministratore di installazione.
- 

5. Opzionale: se necessario, eseguire le seguenti operazioni dopo aver aggiunto il dispositivo.

**Configurazione da remoto**

Toccare il dispositivo e poi  per configurare da remoto i relativi parametri.

---

 **Nota**

- Per i dettagli, consultare il manuale d'uso del dispositivo.
  - La configurazione da remoto è supportata solo da dispositivi di codifica, campanelli e pannelli di controllo di sicurezza.
-

**Eliminazione dei dispositivi**

Nella pagina Device, toccare ●●● → **Delete Device** per eliminare il dispositivo.

**Generazione del codice QR del dispositivo**

- Se un dispositivo viene aggiunto tramite la scansione del codice QR generato da iVMS-4200/iVMS-4500, è possibile generare un codice QR del dispositivo. Se un utente finale non ha aggiunto il dispositivo all'account Hik-Connect, può farlo eseguendo la scansione di tale codice QR tramite il client mobile Hik-Connect.
  - Nella parte superiore destra della pagina Device, toccare ●●● → **Generate QR Code** per aprire la finestra Generate QR Code.
  - **Opzionale:** (opzionale) inserire una password per crittografare il codice QR, quindi toccare **Next**.
  - Toccare **Save** per salvare sul telefono il codice QR generato.

**Impostazione del tipo per un dispositivo sconosciuto**

Se dopo aver aggiunto il dispositivo Hik-ProConnect non ne riconosce il tipo, è possibile impostarlo manualmente.

1. Accedere alla pagina dei dettagli di un dispositivo, quindi toccare  sul tipo di dispositivo per accedere alla pagina Device Type.
2. Selezionare un tipo per il dispositivo.

Dopo la selezione, sarà possibile modificarlo nuovamente.

**Modifica informazioni sul dispositivo**

Se le informazioni dei dispositivi aggiunti tramite la scansione del codice QR generato da iVMS-4200/ iVMS-4500 sono state modificate o si verifica un'eccezione di rete, è possibile cambiarle di conseguenza.

Accedere alla pagina Device e toccare **IP/Domain** per modificare il nome, l'indirizzo IP, il numero di porta, il nome utente o la password del dispositivo, quindi toccare **Save**.

 **Nota**

- Si consiglia vivamente di crittografare il codice QR del dispositivo per motivi di sicurezza.
- Se la piattaforma dispone dell'autorizzazione, non è possibile eliminare il dispositivo (eccetto i dispositivi aggiunti tramite IP/dominio).

### 6.1.3 Aggiunta di dispositivi tramite il servizio Hik-Connect (P2P)

Se un dispositivo è connesso al servizio Hik-Connect, è possibile aggiungerlo manualmente a una piattaforma inserendo il suo numero di serie e codice di verifica.

## Prima di iniziare

Accertarsi che i dispositivi che si utilizzeranno siano correttamente installati e connessi alla rete secondo le specifiche dei produttori.

## Passaggi

1. Toccare una piattaforma sull'elenco delle piattaforme per accedere alla pagina contenente i relativi dettagli.
2. Toccare **Add Device** per accedere alla pagina di scansione, quindi toccare **Manually Add** per accedere alla pagina per l'aggiunta manuale.
3. Inserire il numero di serie e il codice di verifica del dispositivo.



### Nota

Il numero di serie e il codice di verifica predefiniti del dispositivo sono di solito situati sulla sua etichetta. Se non è possibile individuare il codice di verifica, inserire quello creato al momento dell'abilitazione del servizio Hik-Connect.

- 
4. Toccare **Add**.



### Nota

- Il servizio di monitoraggio dello stato è attivo sui dispositivi aggiunti per impostazione predefinita. Non è possibile aggiornare il firmware, impostare le regole di collegamento (quelle esistenti non saranno valide), impostare e ricevere le eccezioni e controllare il monitoraggio dello stato di quei dispositivi che hanno la funzione di monitoraggio dello stato disabilitata.
  - Dopo aver aggiunto il dispositivo, Hik-ProConnect inizia a controllare la compatibilità della versione del firmware del dispositivo. Se il dispositivo non è compatibile con Hik-ProConnect, alcune funzioni (tra cui il monitoraggio dello stato, la regola di collegamento e la configurazione da remoto) non risultano disponibili. È necessario aggiornare i dispositivi incompatibili con Hik-ProConnect. Per aggiornare e aggiungere il dispositivo, toccare **Add and Upgrade**. Per alcuni dispositivi, è necessario inserire il nome utente e la password. È inoltre possibile aggiornare il dispositivo nella pagina dedicata ad esso.
  - Per quanto riguarda il sistema AX Pro, dopo averlo aggiunto a Hik-ProConnect, è possibile utilizzare gli account installatore e amministratore di installazione per accedere a tale sistema. Se l'installatore o l'amministratore di installazione elimina AX Pro da Hik-ProConnect, di conseguenza verranno eliminati anche gli account. Se si modifica la password di accesso all'account installatore, viene modificata anche quella per accedere al sistema AX Pro con tale account.
  - Se un installatore o amministratore di installazione consegna la piattaforma contenente il sistema AX Pro a un utente finale, quest'ultimo può utilizzare il suo account Hik-Connect per accedere anche a tale sistema, mentre l'account installatore o amministratore di installazione viene eliminato da AX Pro.
-

5. Opzionale: eseguire le seguenti operazioni se si verificano le seguenti situazioni.
- Se il dispositivo è offline occorre connetterlo a una rete. Per i dettagli, fare riferimento alla sezione **Connessione di un dispositivo offline alla rete**.
  - Se il dispositivo non è attivo, toccare **Activate** sulla finestra a comparsa, quindi creare una password amministratore del dispositivo e toccare **Activate** per attivarlo.

---

 **Nota**

Durante l'attivazione, sarà attivato automaticamente il protocollo di configurazione dell'host dinamico (DHCP) in modo da allocare gli indirizzi IP del dispositivo.

---

- Se il servizio Hik-Connect è disabilitato sul dispositivo, toccare **Enable** sulla finestra a comparsa, quindi creare un codice di verifica del dispositivo e toccare **Enable** per abilitare il servizio.

Il dispositivo sarà visualizzato nell'elenco dei dispositivi.

6. Opzionale: se necessario, effettuare le seguenti operazioni.

**OperazioniDescrizione**    Nella pagina Device, toccare ● ● ● → **Delete** per eliminare il dispositivo.

**Eliminazione del dispositivo**

**Impostazione del tipo per un dispositivo sconosciuto**    Se dopo aver aggiunto il dispositivo Hik-ProConnect non ne riconosce il tipo, è possibile impostarlo manualmente.

1. Accedere alla pagina dei dettagli di un dispositivo, quindi toccare  sul tipo di dispositivo per accedere alla pagina Device Type.
2. Selezionare un tipo per il dispositivo.

Dopo la selezione, sarà possibile modificarlo nuovamente.

**Configurazione DDNS**    Dopo aver aggiunto il dispositivo, lo stato del DDNS viene visualizzato nell'area del dispositivo. Se è necessario configurare il DDNS, toccare **Configure**. Per i dettagli su come configurare il DDNS, fare riferimento alla sezione **Configurazione del DDNS dei dispositivi**.

---

 **Nota**

- Se la piattaforma dispone dell'autorizzazione, non è possibile eliminare il dispositivo (eccetto i dispositivi aggiunti tramite IP/dominio).
  - Se i dispositivi dispongono di una versione del firmware non valida o precedente, è possibile configurare il DDNS in modo che Hik-ProConnect possa gestirli correttamente.
  - La funzione che consente di configurare il DDNS è supportata solo dai dispositivi di codifica aggiunti tramite il servizio Hik-Connect.
-

## 6.1.4 Aggiunta di un dispositivo tramite l'indirizzo IP o il nome dominio

Se si conosce l'indirizzo IP o il nome di dominio di un dispositivo, è possibile aggiungerlo a Hik-ProConnect specificando il suo indirizzo IP/nome di dominio, nome utente, password, ecc.

### Prima di iniziare

Accertarsi che i dispositivi che si utilizzeranno siano correttamente installati e connessi alla rete secondo le specifiche dei produttori.

### Passaggi

---

#### Nota

Questa funzione è supportata solo dai dispositivi di codifica mappati in WAN.

---

1. Toccare una piattaforma sull'elenco delle piattaforme per accedere alla pagina contenente i relativi dettagli.
  2. Toccare **Add Device** → **Manually Add** per accedere alla pagina Add Device.
  3. Selezionare **IP/Domain** come modalità di registrazione.
  4. Inserire il nome, l'indirizzo IP, il numero di porta, il nome utente e la password del dispositivo.
  5. Toccare **Add**.
- 

#### Attenzione

La complessità della password del dispositivo può essere controllata automaticamente. Si consiglia vivamente di modificare la password scelta (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Inoltre, si consiglia di cambiare regolarmente la password, specialmente nel sistema ad alta sicurezza. La modifica mensile o settimanale consente di proteggere meglio il prodotto.

Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.

---

---

#### Nota

Il servizio di monitoraggio dello stato è attivo sui dispositivi aggiunti per impostazione predefinita. Non è possibile aggiornare il firmware, impostare le regole di collegamento (quelle esistenti non saranno valide), impostare e ricevere le eccezioni e controllare il monitoraggio dello stato di quei dispositivi che hanno la funzione di monitoraggio dello stato disabilitata.

---

6. Opzionale: se necessario, effettuare le seguenti operazioni.

<b>Modifica delle informazioni del dispositivo</b>	<p>OperationsDescription</p> <p>Se le informazioni dei dispositivi aggiunti tramite l'IP/il dominio sono state modificate o si verifica un'eccezione di rete, è possibile cambiarle di conseguenza.</p> <p>Accedere alla pagina Device e toccare <b>IP/Domain</b> per modificare il nome, l'indirizzo IP, il numero di porta, il nome utente o la password del dispositivo, quindi toccare <b>Save</b>.</p>
<b>Generazione del codice QR del dispositivo</b>	<ul style="list-style-type: none"> <li>● È possibile generare un codice QR del dispositivo aggiunto. Se un utente finale non ha aggiunto il dispositivo all'account Hik-Connect, può farlo eseguendo la scansione di tale codice QR tramite il client mobile Hik-Connect.             <ul style="list-style-type: none"> <li>● Nella parte superiore destra della pagina Device, toccare ● ● ● → <b>Generate QR Code</b> per aprire la finestra Generate QR Code.</li> <li>● <b>Opzionale:</b> (opzionale) inserire una password per crittografare il codice QR, quindi toccare <b>Next</b>.</li> <li>● Toccare <b>Save</b> per salvare sul telefono il codice QR generato.</li> </ul> </li> </ul>
<b>Impostazione del tipo per un dispositivo sconosciuto</b>	<p>Se dopo aver aggiunto il dispositivo Hik-ProConnect non ne riconosce il tipo, è possibile impostarlo manualmente.</p> <ol style="list-style-type: none"> <li>1. Accedere alla pagina dei dettagli di un dispositivo, quindi toccare  sul tipo di dispositivo per accedere alla pagina Device Type.</li> <li>2. Selezionare un tipo per il dispositivo.</li> </ol> <p>Dopo la selezione, sarà possibile modificarlo nuovamente.</p>
<b>Elimina dispositivo</b>	<p>Nella pagina Device, toccare ● ● ● → <b>Delete Device</b>.</p>

### Nota

- Si consiglia vivamente di crittografare il codice QR del dispositivo per motivi di sicurezza.
- Per quanto riguarda il sistema AX Pro, dopo averlo aggiunto a Hik-ProConnect, è possibile utilizzare gli account installatore e amministratore di installazione per accedere a tale sistema. Se l'installatore elimina Ax Pro da Hik-ProConnect, di conseguenza verranno eliminati anche gli account. Se si modifica la password di accesso all'account installatore, viene modificata anche quella per accedere al sistema AX Pro con tale account.
- Dopo aver autorizzato l'installatore ad accedere alla piattaforma contenente il sistema AX Pro, è possibile utilizzare l'account installatore e amministratore di installazione per accedere a tale sistema. Ciò si applica anche all'account autorizzato a gestire tutte le piattaforme.
- Se un installatore consegna la piattaforma contenente il sistema AX Pro a un utente finale, quest'ultimo può utilizzare il suo account Hik-Connect per accedere anche a tale sistema, mentre l'account installatore viene eliminato da Ax Pro. Ciò si applica anche all'account amministratore di installazione.

- Chiedere agli utenti finali di scaricare o aggiornare Hik-Connect Mobile Client (versione 4.7.1 o successiva). È possibile inviare il codice QR o il link per il download visualizzato nel banner sulla schermata principale del Portale.
  - Se la piattaforma dispone dell'autorizzazione, non è possibile eliminare il dispositivo (eccetto i dispositivi aggiunti tramite IP/dominio).
- 

## 6.2 Richiesta dell'autorizzazione per un dispositivo

Una volta consegnata una piattaforma all'utente finale, se è necessario visualizzare il video in tempo reale o i video registrati dei dispositivi aggiunti alla piattaforma oppure configurarli, è possibile richiedere l'autorizzazione appropriata all'utente finale.

### Passaggi

1. Toccare una piattaforma per accedere alla pagina con i suoi dettagli.
  2. Toccare un dispositivo per accedere alla pagina Device Details.
  3. Nell'area Device Permission, selezionare **Configuration**, **Live View** o **Playback** e toccare  per accedere alla pagina Apply for Permission.
  4. Selezionare un periodo di validità per l'autorizzazione.
- 

### Nota

È possibile scegliere tra **Permanent**, **1 Hour**, **2 Hours**, **4 Hours** o **8 Hours** come periodo di validità.

---

5. Opzionale: inserire i commenti relativi all'autorizzazione.
6. Fare clic su **Send** per inviare la richiesta all'utente finale.  
Se l'utente finale approva la richiesta, sarà possibile visualizzare il video in tempo reale e/o configurare i dispositivi.

## 6.3 Approvazione dell'autorizzazione per i dispositivi

Se non sono necessarie le autorizzazioni per la configurazione e la visualizzazione in tempo reale dei dispositivi o se si termina la configurazione prima del previsto, è possibile approvare manualmente le autorizzazioni.

### Prima di iniziare

Assicurarsi che la piattaforma dei dispositivi sia stata assegnata all'installatore.

### Passaggi

1. Toccare una piattaforma nell'elenco Site List per accedere alla pagina Site Details.
  2. Toccare una piattaforma in Site Details per accedere alla pagina Device Details.
  3. Nell'area Permission, selezionare un'autorizzazione e toccare ● ● ● → **Release Permission** → **Release Permission** per approvarla.
-

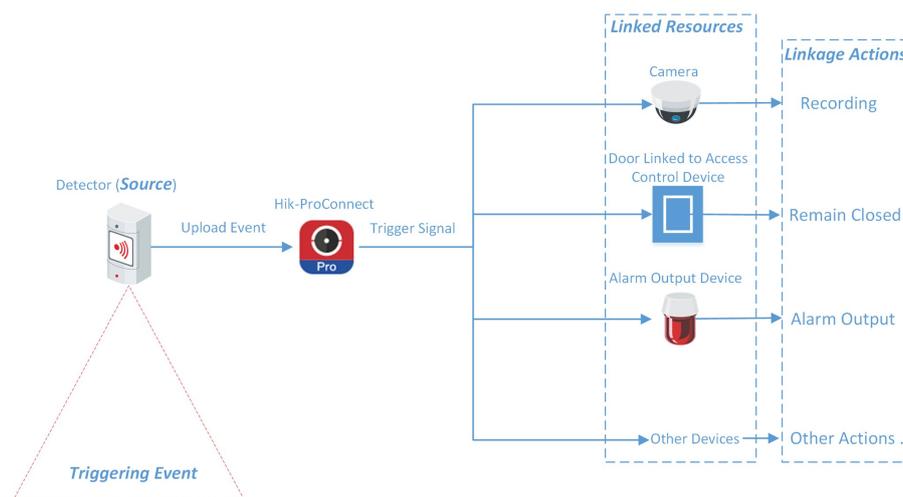
### Nota

- Dopo la rinuncia, l'autorizzazione non sarà più disponibile. Dovrà essere richiesta di nuovo, se necessaria.
- Se la validità dell'autorizzazione è impostata su **Permanent**, non è necessario approvarla.

## 6.4 Aggiunta di una regola di collegamento

Un collegamento (fare riferimento all'immagine riportata di seguito) è un processo in cui un evento rilevato dalla risorsa A attiva le azioni della risorsa B, C, D, ecc. È possibile aggiungere una regola utilizzando il modello predefinito o personalizzarla per definire tale collegamento. La regola contiene cinque elementi, tra cui Source (risorsa A), Triggering Event (l'evento rilevato dal dispositivo A), Linked Resources (risorsa B, C, D, ecc.), Linkage Actions (azioni della risorsa B, C, D, ecc.) e Linkage Schedule (l'ora programmata in cui si attiva il collegamento). I collegamenti possono essere utilizzati per avvisare il personale della sicurezza, effettuare l'upgrade del livello di sicurezza, salvare le prove, ecc, quando si verifica un evento specifico.

L'immagine riportata di seguito illustra il processo di collegamento.



**Figura 6-1 Collegamento**

### Esempio

Supponiamo che l'utente finale sia il responsabile di una gioielleria e che il negozio debba effettuare l'upgrade del livello di sicurezza durante le ore non lavorative. Nel negozio sono stati installati: un rilevatore PIR collegato a un pannello di controllo di sicurezza, una sirena collegata al pannello di controllo di sicurezza e diverse telecamere IP.

In questo caso, è possibile impostare una regola di collegamento per attivare l'uscita di allarme e registrare gli eventi di oggetti in movimento nel negozio durante le ore non lavorative. Nella regola di collegamento è necessario impostare quanto segue:

- Source: il rilevatore PIR nel negozio.

- Evento di attivazione: movimento rilevato.
- Linked Resources: l'uscita di allarme (in questo caso, la sirena) e le telecamere IP nel negozio.
- Linkage Actions:
  - Per la sirena: l'attivazione dell'uscita di allarme (ad esempio, la sirena) invia un avviso acustico.
  - Per le telecamere IP: le telecamere IP iniziano a registrare.
- Linkage Schedule: ore non lavorative di ogni giorno.

### 6.4.1 Aggiunta di una regola di collegamento personalizzata

Se i modelli predefiniti non soddisfano le proprie esigenze, è possibile personalizzare le regole di collegamento.

#### Passaggi



- Se il periodo di prova offerto all'azienda scade, le regole di collegamento aggiunte restano attive per 3 mesi, ma il collegamento non viene abilitato. Dopo 3 mesi, le regole di collegamento vengono cancellate.
- Assicurarsi di disporre dell'autorizzazione per configurare i dispositivi. In caso contrario è necessario richiedere prima l'autorizzazione. Per i dettagli su come richiedere l'autorizzazione, fare riferimento alla sezione **Richiesta dell'autorizzazione per un dispositivo**.
- La sorgente e la risorsa collegata non possono coincidere.
- Non è possibile configurare due regole di collegamento completamente identiche. In altre parole, non è possibile configurare due regole con sorgente, evento di attivazione, risorsa collegata e azione di collegamento identici.
- Quando la sorgente è un dispositivo aggiunto tramite l'IP/il dominio, il dispositivo inserito tramite Hik-Connect non può essere impostato come risorsa collegata per l'attivazione della registrazione.

- 
1. Toccare una piattaforma nell'elenco Site List per accedere alla pagina Site Details.
  2. Toccare **Linkage Rule** per accedere alla pagina Linkage Rule.
  3. Toccare **Add Linkage Rule** per accedere alla pagina Add Linkage Rule.
  4. Selezionare la sorgente e l'evento di attivazione, quindi toccare **Next**.



Assicurarsi che l'evento di attivazione selezionato sia già stato configurato sul dispositivo. Per informazioni sulla configurazione dell'evento sul dispositivo, consultare il manuale dell'utente del dispositivo.

---

Tabella 6-1 Eventi di attivazione disponibili per tipi diversi di risorse

Sorgente	Abilitazione evento
Telecamera	<ul style="list-style-type: none"> <li>● Rilevamento di movimenti</li> <li>● Rilevamento volti</li> <li>● Intrusione</li> <li>● Rilevamento attraversamento linea</li> </ul>
Dispositivo di controllo degli accessi	<ul style="list-style-type: none"> <li>● Rete disconnessa</li> <li>● Allarme anti-manomissione</li> </ul>
Porta collegata a dispositivo di controllo degli accessi	<ul style="list-style-type: none"> <li>● Anomalia nell'apertura della porta</li> <li>● Allarme anti-manomissione</li> </ul>
Postazione porta	<ul style="list-style-type: none"> <li>● Chiamata</li> </ul>
Area del pannello di controllo di sicurezza	<ul style="list-style-type: none"> <li>● Inserimento modalità assenza</li> <li>● Disinserito</li> <li>● Inserimento parziale</li> <li>● Alarm, ad esempio Instant Zone Alarm, 24-Hour Annunciating Zone Alarm e Delayed Zone Alarm.</li> </ul>
zona (rilevatore) collegata al pannello di controllo di sicurezza	<ul style="list-style-type: none"> <li>● Alarm, ad esempio Instant Zone Alarm, 24-Hour Annunciating Zone Alarm e Delayed Zone Alarm.</li> </ul>
Campanello	<ul style="list-style-type: none"> <li>● Chiamata</li> <li>● Rilevamento PIR</li> </ul>

5. Toccare **Add Linkage** per selezionare le azioni di collegamento e le risorse collegate, quindi toccare **Next**.

#### Nota

- Per la configurazione delle azioni di collegamento della stessa sorgente, se le risorse collegate di quest'ultima sono delle telecamere (ossia, i canali), è possibile impostare al massimo quattro azioni di collegamento. Ad esempio, se si impostano l'acquisizione di immagini e la registrazione (entrambe considerate due azioni di collegamento) come azioni di collegamento della telecamera 1, è possibile impostare solo altre due azioni di collegamento, come l'acquisizione di immagini e la registrazione per la telecamera 2 o l'acquisizione di immagini per il canale 2 e la registrazione per il canale 3 oppure la registrazione per il canale 2 e l'acquisizione di immagini per il canale 3.
- È possibile selezionare fino a 128 azioni di collegamento o 10 risorse collegate.

Tabella 6-2 Descrizione dell'azione di collegamento

Risorsa collegata	Azione di collegamento	Descrizione
Telecamera (canale)	Acquisizione immagini	La telecamera acquisisce un'immagine quando rileva l'evento di attivazione.
	Recording	<p>La telecamera registra un video quando rileva l'evento di attivazione.</p> <hr/> <p> <b>Nota</b></p> <p>Il video registrato inizia 5 secondi prima del rilevamento dell'evento di attivazione e dura 30 secondi.</p> <hr/>
	Richiamo di valori preconfigurati	<p>Selezionare un preset dall'elenco a discesa relativo in modo che venga richiamato quando si rileva un evento di attivazione.</p> <p>Un preset è una posizione predefinita in un'immagine, corrispondente a una data configurazione dei valori di posizione verticale e orizzontale, messa a fuoco, zoom e altri parametri. Richiamando un preset, la telecamera PTZ si sposterà sulla posizione predefinita dell'immagine.</p> <hr/> <p> <b>Nota</b></p> <p>Assicurarsi di aver configurato i preset della telecamera PTZ. Per i dettagli, consultare il manuale d'uso della telecamera PTZ.</p> <hr/>
Chiamata di pattugliamenti	<p>Selezionare un pattugliamento dall'elenco a discesa relativo in modo che venga richiamato quando si rileva un evento di attivazione.</p> <p>Un pattugliamento è un movimento di brandeggio predefinito composto da una serie di punti chiave (ad esempio i preset) che presentano una sequenza designata. Richiamando un pattugliamento, la telecamera PTZ si sposterà su tutti i punti chiave alla velocità impostata per fornire una visuale dinamica.</p>	

Risorsa collegata	Azione di collegamento	Descrizione
		<hr/> <p> <b>Nota</b></p> <p>Assicurarsi di aver configurato i pattugliamenti della telecamera PTZ. Per i dettagli, consultare il manuale d'uso della telecamera PTZ.</p> <hr/>
	Richiama sequenza	<p>Selezionare una sequenza dall'elenco a discesa relativo in modo che venga richiamata quando si rileva un evento di attivazione.</p> <p>Una sequenza è un movimento di brandeggio predefinito con un determinato tempo di sosta, configurato su una certa posizione. Richiamando una sequenza, la telecamera PTZ si sposta in base al percorso predefinito.</p> <hr/> <p> <b>Nota</b></p> <p>Assicurarsi di aver configurato la sequenza della telecamera PTZ. Per i dettagli, consultare il manuale d'uso della telecamera PTZ.</p> <hr/>
	Inserimento	<p>La telecamera può essere inserita e pertanto gli eventi relativi a essa saranno caricati sul client mobile Hik-Connect quando verrà rilevato un evento di attivazione.</p>
	Disinserisci	<p>La telecamera può essere disinserita e pertanto gli eventi relativi a essa non saranno caricati sul client mobile Hik-Connect quando verrà rilevato un evento di attivazione.</p>
	Abilita mascheramento privacy	<p>Il mascheramento della privacy sarà visualizzato sulle immagini in tempo reale della telecamera quando viene rilevato un evento di attivazione.</p> <hr/> <p> <b>Nota</b></p> <p>Assicurarsi di aver configurato il mascheramento di privacy della telecamera. Per i dettagli, consultare il manuale d'uso della telecamera.</p> <hr/>

Risorsa collegata	Azione di collegamento	Descrizione
	Disabilita mascheramento privacy	Il mascheramento della privacy NON sarà visualizzato sulle immagini in tempo reale della telecamera quando viene rilevato un evento di attivazione.
Uscita allarme	Uscita allarme	L'uscita di allarme della risorsa collegata si attiva quando viene rilevato l'evento di attivazione.
Area del pannello di controllo di sicurezza	Inserimento parziale	Lo stato di attivazione relativo all'area del pannello di controllo di sicurezza passa a Stay quando viene rilevato l'evento di attivazione.
	Inserimento totale	Lo stato di attivazione relativo all'area del pannello di controllo di sicurezza passa ad Away quando viene rilevato l'evento di attivazione.
	Disinserisci	L'area del pannello di controllo di sicurezza si disattiva quando viene rilevato l'evento di attivazione.
Porta collegata a dispositivo di controllo degli accessi	Open Door	La porta relativa al dispositivo di controllo accessi sarà attivata quando viene rilevato l'evento di attivazione.
	Remain Open	La porta relativa al dispositivo di controllo accessi resterà aperta quando viene rilevato l'evento di attivazione.
	Remain Closed	La porta relativa al dispositivo di controllo accessi resterà chiusa quando viene rilevato l'evento di attivazione.
Postazione porta	Open Door	La porta collegata alla postazione porta sarà automaticamente aperta quando viene rilevato l'evento di attivazione.
Ingresso allarme	Inserisci ingresso di allarme	L'ingresso di allarme sarà inserito e pertanto gli eventi relativi a esso saranno caricati sul client mobile Hik-Connect quando verrà rilevato un evento di attivazione.
	Disinserisci ingresso di allarme	L'ingresso di allarme sarà disinserito e pertanto gli eventi relativi a esso NON saranno caricati sul client mobile Hik-Connect quando verrà rilevato un evento di attivazione.

6. Configurare l'ora programmata durante la quale si attiva il collegamento.

1) Selezionare le date nella settimana.

2) Impostare l'ora di inizio e l'ora di fine del periodo programmato di ciascuna data.

3) Toccare **Next**.

7. Creare un nome per la regola di collegamento.

8. Toccare **Enable**.

La regola di collegamento viene visualizzata nell'elenco Linkage Rule.

9. Opzionale: Impostare  su  per disattivare la regola di collegamento.

### Come continuare

Se è stata abilitata la regola di collegamento, assicurarsi che la funzione che consente alla sorgente di inviare notifiche sia attiva. Per i dettagli su come attivare la funzione che consente al dispositivo di inviare notifiche, fare riferimento alla sezione **Attivazione della funzione che consente al dispositivo di inviare notifiche**.

#### Nota

- Se la funzione che consente alla sorgente di inviare notifiche è disattivata, l'azione di collegamento NON viene abilitata, indipendentemente dal fatto che l'evento di attivazione venga rilevato o meno dalla sorgente.
- Avvisare l'utente finale dopo la consegna della piattaforma che la notifica della sorgente deve essere mantenuta attiva sul client mobile Hik-Connect, altrimenti l'azione di collegamento NON sarà attivata, indipendentemente dalla rilevazione dell'evento di attivazione da parte della sorgente. Per i dettagli su come attivare la funzione che consente a un dispositivo o canale specifico di inviare notifiche di allarme, consultare il *Manuale utente del client mobile Hik-Connect*.
- Invitare gli utenti finali a scaricare o aggiornare il client mobile Hik-Connect (versione 4.7.1 e successive). È possibile inviare il codice QR o il link per il download visualizzato nel banner sulla schermata principale.

## 6.4.2 Aggiunta di regole di collegamento basate su modelli predefiniti

Per aggiungere regole di collegamento, è possibile utilizzare sei modelli predefiniti, tra cui Intrusion, Forced Entry Alarm, Back to Home/Office, Away, Visitor Calling e Perimeter Zone Alarm. Ciascuno dei sei modelli è progettato per applicazioni tipiche (vedere l'elenco riportato di seguito) di regole di collegamento.

### Prima di iniziare

È necessario disporre dell'autorizzazione per la configurazione dei dispositivi. In alternativa, è necessario richiedere le autorizzazioni. Per i dettagli su come richiedere l'autorizzazione, fare riferimento alla sezione **Richiesta dell'autorizzazione per un dispositivo**.

Tabella 6-3 Descrizione dei modelli

Modello	Descrizione
Intrusione	Il modello Intrusion: viene utilizzato per migliorare il livello di sicurezza tramite l'attivazione di azioni di collegamento, tra cui l'acquisizione, la registrazione e l'uscita di allarme, quando si verifica un evento di intrusione (ingresso di persone, veicoli o altri oggetti in un'area predefinita).

Modello	Descrizione
Allarme ingresso forzato	Il modello Forced Entry Alarm: viene utilizzato per migliorare il livello di sicurezza tramite l'attivazione di azioni di collegamento, tra cui l'acquisizione, la registrazione, la permanenza della chiusura della porta, l'uscita di allarme e la chiamata a un preset, quando si verifica un evento di attraversamento di una linea (persone, veicoli o altri oggetti che attraversano una linea virtuale predefinita).
Tornare a Casa/Ufficio	Il modello Back to Home/Office: viene utilizzato per ridurre il livello di sicurezza e abilitare la protezione della privacy tramite l'attivazione di azioni di collegamento, tra cui la disattivazione e l'attivazione del mascheramento della privacy, quando si rientra a casa o in ufficio.
Away	Il modello Away: viene utilizzato per migliorare il livello di sicurezza e annullare la protezione della privacy tramite l'attivazione di azioni di collegamento, tra cui l'attivazione e la disattivazione del mascheramento della privacy quando si esce da casa o dall'ufficio.
Chiamata visitatore	Il modello Visitor Calling: viene utilizzato per migliorare il livello di sicurezza tramite l'attivazione di azioni di collegamento, tra cui l'acquisizione e la registrazione, quando i visitatori effettuano chiamate dalla postazione esterna.
Allarme zona perimetrale	Modello Perimeter Zone Alarm: viene utilizzato per migliorare il livello di sicurezza tramite l'attivazione di azioni di collegamento, tra cui l'acquisizione, la registrazione, la chiamata a un preset, l'uscita di allarme e la permanenza della chiusura della porta, quando vengono rilevate persone o altri oggetti in prossimità degli accessi (tra cui porte, finestre, porte della cantina, ecc) di una proprietà.

## Passaggi

### Nota

La procedura di aggiunta di regole di collegamento è simile per tutti i modelli, pertanto verranno illustrati solo i passaggi per aggiungere una regola di collegamento basata sul modello Forced Entry Alarm.

1. Toccare una piattaforma sull'elenco delle piattaforme per accedere alla pagina contenente i relativi dettagli.
2. Toccare **Linkage Rule** per accedere alla pagina Linkage Rule.
3. Toccare un modello di collegamento per accedere alla pagina Template Configuration.
4. Impostare le informazioni necessarie.

**Nome regola di collegamento**

Creare un nome per la regola di collegamento.

**Quando**

Selezionare una risorsa come sorgente da utilizzare per rilevare un evento di attraversamento della linea dall'elenco a discesa.

**Trigger the Following Actions**

Toccare **Select** per selezionare le risorse collegate utilizzate per attivare le azioni di collegamento, quindi selezionare **Add**.

---

 **Nota**

- È possibile impostare una sola azione di collegamento.
  - Per i dettagli sulle azioni di collegamento, fare riferimento alla **Tabella 2**.
- 

**Programma di collegamento**

Stabilire l'ora programmata durante la quale si attiva il collegamento.

**Tutti i giorni**

L'azione di collegamento è sempre attiva da lunedì a domenica, 7 giorni su 7, 24 ore su 24.

**Custom**

Selezionare le date all'interno della settimana e quindi specificare l'ora di inizio e l'ora di fine di ciascuna data selezionata.

---

 **Nota**

Le date contrassegnate in blu sono quelle selezionate.

---

**5. Toccare **Enable**.**

La regola di collegamento viene visualizzata nell'elenco Linkage Rule.

**6. Opzionale: Impostare  su  per disattivare la regola di collegamento.****Come continuare**

Se è stata abilitata la regola di collegamento, assicurarsi che la funzione che consente alla sorgente di inviare notifiche sia attiva. Per i dettagli su come attivare la funzione, fare riferimento alla sezione **Attivazione della funzione che consente al dispositivo di inviare notifiche**.

 **Nota**

- Se la funzione che consente alla sorgente di inviare notifiche è disattivata, l'azione di collegamento NON viene abilitata, indipendentemente dal fatto che l'evento di attivazione venga rilevato o meno dalla sorgente.
  - Avvisare l'utente finale dopo la consegna della piattaforma che la notifica della sorgente deve essere mantenuta attiva sul client mobile Hik-Connect, altrimenti l'azione di collegamento NON sarà attivata, indipendentemente dalla rilevazione dell'evento di attivazione da parte della sorgente. Per i dettagli su come attivare la funzione che consente a un dispositivo o canale specifico di inviare notifiche di allarme, consultare il *Manuale utente del client mobile Hik-Connect*.
  - Invitare gli utenti finali a scaricare o aggiornare il client mobile Hik-Connect (versione 4.7.1 e successive). È possibile inviare il codice QR o il link per il download visualizzato nel banner sulla schermata principale.
- 

### 6.4.3 Tutorial video

Il seguente video spiega che cos'è una regola di collegamento e come impostarla.

## 6.5 Aggiunta di regole di eccezione

Una regola di eccezione viene utilizzata per monitorare in tempo reale lo stato delle risorse gestite. Quando la risorsa ha un'eccezione, essa invierà una notifica a Hik-ProConnect per informare di questa eccezione l'installatore specificato. Al momento, sono disponibili due tipi di eccezione: eccezioni del dispositivo e eccezioni del canale.

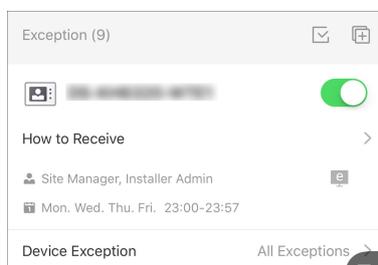
### Prima di iniziare

- Assicurarsi di disporre dell'autorizzazione per configurare il dispositivo (se quest'ultimo la supporta). Per informazioni su come richiedere l'autorizzazione per la configurazione, fare riferimento alla sezione ***Richiesta dell'autorizzazione per un dispositivo***.
- Assicurarsi di aver abilitato sul dispositivo la funzione per inviare notifiche al sistema (se il dispositivo la supporta). Per i dettagli, fare riferimento alla sezione ***Attivazione della funzione che consente al dispositivo di inviare notifiche***.

È possibile aggiungere una regola per definire tale eccezione. La regola contiene cinque elementi, tra cui **Source** (dispositivo A o canale A), **Exception** (l'eccezione si è verificata sul dispositivo A o sul canale A), **Received by** (la sorgente invia una notifica al destinatario in determinate modalità), **Recipient** (chi riceve la notifica) e **Schedule** (quando il destinatario riceve la notifica).

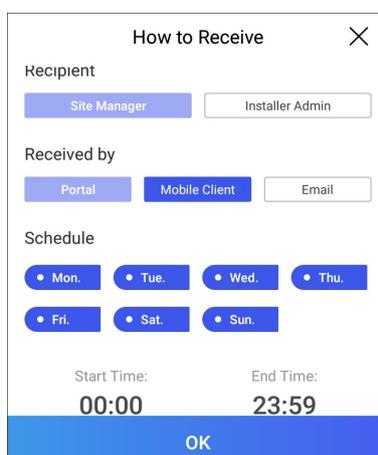
## Passaggi

1. Toccare il nome di una piattaforma per accedere alla pagina Site Details, quindi toccare **Exception** in basso.  
Vengono visualizzate rispettivamente le regole di eccezione di tutti i dispositivi aggiunti a questa piattaforma.



**Figura 6-2 Aggiunta di una regola di eccezione**

2. Toccare **How to Receive** nel pannello di un dispositivo per impostare i campi **Recipient**, **Received by** e **Schedule** della regola.



**Figura 6-3 How to Receive**

- 1) Nel campo **Recipient**, selezionare **Site Manager** o **Installer Admin**. Il destinatario riceve in tempo reale la notifica quando l'eccezione è rilevata.

---

### Nota

Per opzione predefinita viene selezionato il Responsabile della piattaforma e non è possibile modificarlo.

---

- 2) Nel campo **Received by**, selezionare le modalità di ricezione in base alle esigenze.

### **Portale**

Quando viene rilevata un'eccezione, il dispositivo invia una notifica al Portale in tempo reale.

Il Portale viene selezionato per opzione predefinita e non è possibile modificarlo.

## Client Mobile

Quando viene rilevata un'eccezione, il dispositivo invia una notifica al client mobile Hik-ProConnect in tempo reale.

---

### Nota

Per i dettagli su come controllare le eccezioni ricevute dal client mobile, fare riferimento alla sezione **Centro eccezioni**.

---

## E-mail

Quando viene rilevata un'eccezione, il dispositivo invia una notifica a Hik-ProConnect e il sistema manda in tempo reale un'e-mail con i dettagli dell'eccezione agli indirizzi e-mail dei destinatari.

- 3) Nel campo **Schedule**, impostare l'ora in cui inviare le notifiche al destinatario in base alle esigenze, includendo i giorni e l'ora per i giorni selezionati.
  - 4) Fare clic su **OK**.
3. Toccare **Device Exception** o **Channel Exception** per selezionare i tipi di eccezioni in grado di attivare l'invio di notifiche.
- 

### Nota

- Per le eccezioni **Offline**, è possibile impostare la soglia di durata della permanenza offline. Quando il dispositivo o il canale è offline per un periodo superiore alla soglia impostata, viene attivata l'eccezione offline.
  - La soglia della permanenza offline deve essere compresa tra 5 e 120 minuti.
- 

4. Opzionale: impostare le regole di eccezione relative ai dispositivi presenti sulla piattaforma in un batch.
    - 1) Toccare .
    - 2) Selezionare i dispositivi o i canali su cui impostare le regole di eccezione e toccare **Next**.
    - 3) Impostare i tipi di eccezione, inclusa l'eccezione del dispositivo e l'eccezione del canale, quindi toccare **Next**.
    - 4) Impostare la modalità di ricezione, il destinatario e l'ora.
    - 5) Toccare **Finish** per salvare le impostazioni.
  5. Opzionale: una volta impostata una regola, è possibile copiare le impostazioni delle regole su altri dispositivi o canali per effettuare delle impostazioni rapide.
    - 1) Toccare .
    - 2) Selezionare i dispositivi o i canali come risorse da cui copiare.
    - 3) Selezionare le risorse target dello stesso tipo di quelle selezionate.
    - 4) Toccare **OK** per copiare le impostazioni della regola delle risorse su quelle di destinazione.
  6. Una volta impostata la regola di eccezione, per abilitarla sul dispositivo è necessario attivare l'interruttore della regola in alto a destra.

Una volta abilitata la regola, questa sarà attiva e quando si verificherà un'eccezione, il dispositivo invierà una notifica in base alle impostazioni della regola.
-

## 6.6 Attivazione della funzione che consente al dispositivo di inviare notifiche

Dopo aver aggiunto e attivato una regola di collegamento o di eccezione, è necessario abilitare la funzione che consente al dispositivo sorgente di inviare notifiche affinché gli eventi rilevati vengano caricati sul sistema Hik-ProConnect e nel client mobile Hik-Connect. Tale caricamento è la condizione preliminare per attivare le azioni di collegamento e le regole di eccezione definite nel dispositivo sorgente.

### Passaggi

1. Toccare una piattaforma per accedere alla pagina con i suoi dettagli.
2. Selezionare la scheda **Device**.
3. Toccare un dispositivo per accedere alla pagina Site Details.
4. Toccare  → **Notification** per accedere alla pagina Notification Settings.
5. Impostare i parametri.

### Notifica

Verificare che la funzione sia abilitata.

### Pianificazione notifiche

Dopo aver attivato la funzione, impostare l'ora di caricamento degli eventi rilevati dalla sorgente.

È possibile selezionare le date e poi specificare l'ora di inizio e quella di fine di ciascuna data selezionata.

6. Toccare **OK**.

---

### Nota

- Avvisare l'utente finale dopo la consegna della piattaforma che la notifica della sorgente deve essere mantenuta attiva sul client mobile Hik-Connect, altrimenti l'azione di collegamento NON sarà attivata, indipendentemente dalla rilevazione dell'evento di attivazione da parte della sorgente. Per i dettagli su come attivare la funzione che consente a un dispositivo o canale specifico di inviare notifiche di allarme, consultare il *Manuale utente del client mobile Hik-Connect*.
  - Invitare gli utenti finali a scaricare o aggiornare il client mobile Hik-Connect (versione 4.7.1 e successive). È possibile inviare il codice QR o il link per il download visualizzato nel banner sulla schermata principale del Portale.
-

## 6.7 Upgrade del dispositivo

Se il client mobile Hik-ProConnect rileva nuove versioni del firmware dei dispositivi, quali pannelli di controllo di sicurezza, campanelli, Hik-ProConnect Box, DVR cloud e alcuni modelli di telecamere IP, è possibile effettuare l'upgrade tramite il client mobile.

### Passaggi

---

#### Nota

- L'aggiornamento del dispositivo deve essere supportato dal firmware del dispositivo. Rivolgersi al nostro supporto tecnico per i dettagli.
- È inoltre possibile aggiornare il dispositivo quando lo si aggiunge. Per i dettagli, fare riferimento alla sezione **Aggiunta di un dispositivo tramite Hik-Connect (P2P)**.

- 
1. Nella pagina di elenco delle piattaforme, toccare il nome di una piattaforma per accedere alla pagina relativa.
  2. Se non è stata eseguita l'autenticazione di sicurezza, toccare **Authenticate** per effettuare questa operazione. Per i dettagli, fare riferimento alla sezione **Altre funzioni**.

---

#### Nota

- Non saranno rilevate nuove versioni senza l'autenticazione di sicurezza.
- L'icona  appare vicino al nome del dispositivo per cui è disponibile un upgrade.

- 
3. Toccare il nome del dispositivo per accedere alla pagina relativa.
  4. Toccare **Upgrade**.
  5. Opzionale: per i pannelli di controllo di sicurezza con modalità conforme a EN50131, inserire la password del dispositivo.
  6. Toccare **OK** per avviare l'upgrade.

---

#### Nota

- Può essere necessario qualche minuto per l'aggiornamento del dispositivo. È possibile tornare alla pagina precedente per eseguire altre operazioni.
  - Una volta avviato, l'upgrade non può essere interrotto. Evitare interruzioni dell'alimentazione o della connessione durante l'aggiornamento.
-

## 6.8 Scollegamento di un dispositivo dal relativo account corrente

Quando si aggiunge un dispositivo tramite la scansione del codice QR o utilizzando la modalità manuale e questo viene inserito in un altro account, prima di poterlo aggiungere a quello proprio, è necessario scollegare tale dispositivo. La funzione di scollegamento può essere utilizzata quando è necessario aggiungere un dispositivo a un nuovo account, ma non si dispone dell'autorizzazione per eliminarlo dal vecchio account (ad esempio, se si dimentica la password di quest'ultimo).

### Nota

Assicurarsi che il telefono su cui è in esecuzione il client mobile sia connesso alla stessa LAN del dispositivo. In assenza di questa condizione, questa funzione non sarà disponibile.

Toccare **Unbind** nella pagina del risultato dell'operazione di aggiunta, quindi inserire la password del dispositivo e toccare **Finish** per scollegarlo dall'account a cui è stato aggiunto. Una volta scollegato, è possibile aggiungere il dispositivo all'account.

### Nota

Se il firmware del dispositivo non supporta la funzione di scollegamento, è necessario inserire un codice CAPTCHA dopo aver immesso la password del dispositivo.

## 6.9 Reimpostazione della password del dispositivo

Se il proprietario della piattaforma e l'installatore hanno smarrito la password di un dispositivo, è possibile reimpostarla.

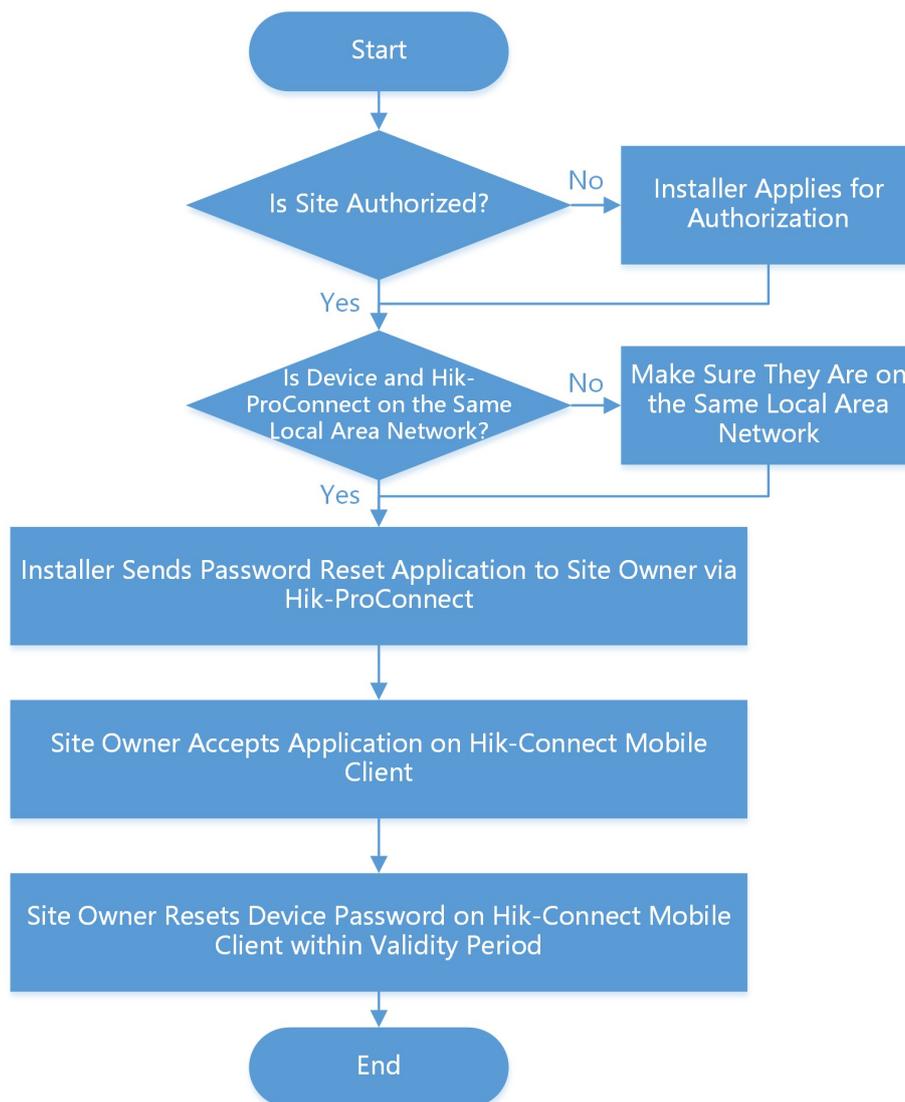
### Nota

- Non tutti i tipi/modelli di dispositivo supportano la reimpostazione della password tramite la piattaforma Hik-ProConnect. Ad esempio, il pannello di controllo di sicurezza AX Pro non supporta questa funzione.
- Prima di reimpostare la password, ricordarsi di richiedere al proprietario della piattaforma l'autorizzazione per accedere al dispositivo. Per i dettagli, fare riferimento alla sezione ***Richiesta di autorizzazione al proprietario della piattaforma***.
- Assicurarsi che il dispositivo si trovi nella stessa rete locale del telefono o tablet su cui è in esecuzione il client mobile Hik-ProConnect.

Accedere alla scheda  **Site** e inserire la piattaforma su cui si trova il dispositivo.

Toccare il dispositivo, quindi selezionare    → **Reset Password** per inviare una richiesta di reimpostazione della password al proprietario della piattaforma.

Per conoscere la procedura completa di reimpostazione della password di un dispositivo, fare riferimento al diagramma di flusso riportato di seguito.



**Figura 6-4 Diagramma di flusso della procedura di reimpostazione della password di un dispositivo**

## 6.10 Configurazione del DDNS dei dispositivi

Se i dispositivi dispongono di una versione del firmware non valida o precedente, è possibile configurare il DDNS in modo che Hik-ProConnect possa gestirli correttamente.

### Passaggi

---

#### Nota

Questa funzione è supportata solo dai dispositivi di codifica aggiunti tramite Hik-Connect (P2P).

---

1. Toccare una piattaforma sull'elenco delle piattaforme per accedere alla pagina contenente i relativi dettagli.

---

 **Nota**

Viene visualizzato un punto rosso vicino al nome dei dispositivi con una versione del firmware non valida o precedente e che non dispongono di un DDNS configurato.

---

2. Toccare un dispositivo per accedere alla pagina Device.
3. Toccare **DDNS Settings** per accedere alla pagina DDNS Settings.

---

 **Nota**

È possibile toccare **How to set port?** per ottenere informazioni sulla modalità di configurazione.

---

4. Attivare il pulsante **Enable DDNS**.
5. Inserire il nome di dominio del dispositivo.
6. Selezionare **Port Mapping Mode**.

**Auto**

Questa modalità consente di ottenere automaticamente la porta del servizio e la porta HTTP. Una volta ottenute, non è possibile modificarle.

**Manuale**

Questa modalità consente di inserire manualmente la porta del servizio e la porta HTTP.

7. Inserire nome utente e password.
- 

 **Attenzione**

La complessità della password del dispositivo può essere controllata automaticamente. Si consiglia vivamente di modificare la password scelta (utilizzando almeno 8 caratteri, con almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per una maggiore protezione del prodotto. Inoltre, si consiglia di cambiare regolarmente la password, specialmente nel sistema ad alta sicurezza. La modifica mensile o settimanale consente di proteggere meglio il prodotto.

Rientra nella responsabilità dell'installatore e/o dell'utente finale configurare correttamente tutte le password e altri parametri di sicurezza.

---

8. Toccare **Save**.

## 6.11 Visualizzazione di video in tempo reale

Tramite il client Hik-ProConnect, è possibile visualizzare le riprese in tempo reale delle telecamere gestite ed effettuare le operazioni correlate.

Toccare  per avviare la visualizzazione in tempo reale degli ultimi 5 minuti di un dispositivo di codifica. Durante la visualizzazione in tempo reale, è possibile eseguire il controllo PTZ (tranne Pattern), abilitare il cursore per pulire l'obiettivo della telecamera e fare clic su **High Definition** per cambiare la qualità dell'immagine. Per i dispositivi aggiunti tramite il servizio Hik-Connect e che non dispongono di un DDNS configurato, la visualizzazione in tempo reale durerà massimo cinque minuti. Per i dispositivi aggiunti tramite l'IP/il nome di dominio e quelli aggiunti tramite il servizio Hik-Connect che dispongono di un DDNS configurato, la durata della visualizzazione in tempo reale è illimitata.

---

### Nota

- Se è stata abilitata la codifica di immagini e video del dispositivo sul client mobile Hik-Connect, è necessario inserire il codice di verifica del dispositivo prima di avviare la visualizzazione live. Se non si conosce il codice di verifica del dispositivo, richiederlo all'utente finale. Per i dettagli sulla codifica di immagini e video, consultare il *Manuale dell'utente del client mobile Hik-Connect*.
  - Chiedere agli utenti finali di scaricare o aggiornare Hik-Connect Mobile Client (versione 4.7.1 o successiva). È possibile inviare il codice QR o il link per il download visualizzato nel banner sulla schermata principale del Portale.
  - Se non si dispone dell'autorizzazione per la visualizzazione live, è possibile eseguire questa operazione tramite una LAN: Connettere lo smartphone allo stesso Wi-Fi del dispositivo di codifica e fare clic su **Live View in LAN** per accedere al dispositivo e avviare la visualizzazione in tempo reale.
  - Assicurarsi che il dispositivo sia online, altrimenti non è possibile utilizzare la funzione.
- 

## 6.12 Visualizzazione di video registrati

È possibile avviare la riproduzione per visualizzare i video registrati di un dispositivo.

---

### Nota

- Assicurarsi di disporre dell'autorizzazione per avviare la riproduzione. Senza quest'ultima, infatti, non è possibile accedere alla pagina di riproduzione. Per i dettagli su come richiedere l'autorizzazione alla riproduzione, fare riferimento alla sezione ***Richiesta dell'autorizzazione per un dispositivo***.
  - Questa funzione deve essere supportata dal dispositivo.
- 

Accedere alla pagina Site, selezionare un dispositivo e fare clic su  per accedere alla pagina Playback. È inoltre possibile accedere alla pagina di riproduzione da quella relativa alla visualizzazione in tempo reale.

Per selezionare una data, fare clic su quella sotto la finestra di riproduzione.

Sulla barra degli strumenti di riproduzione, fare clic sulle icone seguenti per eseguire le funzioni desiderate.

Per i dispositivi aggiunti tramite Hik-Connect P2P, i video vengono visualizzati con colori diversi: le riprese basate sul tempo sono contrassegnate in blu, mentre quelle basate sugli eventi sono contrassegnate in giallo sulla barra temporale.

	Fare clic per selezionare un canale per la riproduzione.
	Fare clic per scaricare il video sul computer.
	Fare clic per attivare/disattivare l'audio della riproduzione.
	Fare clic per sospendere la riproduzione.
	Fare clic per selezionare la velocità di riproduzione del video.
	Fare clic per eseguire lo zoom digitale.
	Fare clic per scattare una foto.
	Fare clic per ritagliare il video e scaricarlo sul computer.

## 6.13 Uso e configurazione del sistema AX Pro

Sul client mobile, è possibile utilizzare AX Pro da remoto. Le operazioni supportate includono l'aggiunta di aree, l'attivazione/disattivazione di un'area, la cancellazione di un allarme, l'esclusione di aree, ecc. Inoltre, è possibile eseguire walk test, configurare le impostazioni relative all'ora legale ed effettuare l'upgrade del dispositivo da remoto.

Toccare una piattaforma per accedere alla pagina Site Details, quindi selezionare la scheda **Device**. Nella scheda Device, toccare un pannello di controllo di sicurezza AX Pro per accedere alla pagina Device Details.

### Uso di AX Pro da remoto

Nella pagina Device Details, è possibile effettuare le seguenti operazioni.

**Tabella 6-4 Descrizione dell'operazione**

Operazione	Descrizione
Aggiunta di aree	Selezionare la scheda <b>Area</b> , quindi toccare  per aggiungere un'area.
Attivazione di parte dei dispositivi in un'area specifica	Selezionare la scheda <b>Area</b> , quindi toccare  per attivare parte dei dispositivi nell'area.
Attivazione di tutti i dispositivi in un'area specifica	Selezionare la scheda <b>Area</b> , quindi toccare  per attivare tutti i dispositivi nell'area.

Operazione	Descrizione
Disattivazione di un'area specifica	Selezionare la scheda <b>Area</b> , quindi toccare  per disattivare l'area.
Attivazione di parte dei dispositivi in tutte le aree	Selezionare la scheda <b>Area</b> , quindi toccare  nella parte inferiore della pagina.
Attivazione di tutti i dispositivi in tutte le aree	Selezionare la scheda <b>Area</b> , quindi toccare  nella parte inferiore della pagina.
Disattivazione di tutte le aree	Selezionare la scheda <b>Area</b> , quindi toccare  nella parte inferiore della pagina.
Cancellazione degli allarmi di tutte le aree	Selezionare la scheda <b>Area</b> , quindi toccare  nella parte inferiore della pagina.
Visualizzazione dei dispositivi di ciascuna area	Selezionare la scheda <b>Device</b> , quindi toccare  e selezionare un'area per visualizzare solo i dispositivi collegati ad essa oppure selezionare <b>All</b> per visualizzare quelli collegati a tutte le aree.
Aggiungere il dispositivo periferico	<p>Selezionare la scheda <b>Device</b>, quindi toccare  per aggiungere un dispositivo.</p> <hr/> <p> <b>Nota</b></p> <p>Per i dettagli su come aggiungere un dispositivo, fare riferimento alla sezione <b>Aggiunta di un dispositivo</b>.</p> <hr/>
Esclusione di aree	Selezionare la scheda <b>Device</b> , quindi selezionare un'area (ovvero un rilevatore) e attivare il pulsante <b>Bypass</b> per escluderla.
Visualizzazione dello stato	Selezionare la scheda <b>Status</b> per visualizzare le informazioni relative allo stato del pannello di controllo, tra cui lo stato dell'alimentatore esterno, lo stato della rete Ethernet, lo stato del Wi-Fi, ecc.

## Configurazione da remoto di AX Pro

Toccare  sulla pagina Device Details per accedere alla pagina delle impostazioni e configurare da remoto AX Pro.

Tabella 6-5 Descrizione della configurazione

Configuration	Descrizione
Walk Test	<p>Il walk test viene utilizzato per verificare che i rilevatori siano in grado di individuare gli oggetti nelle aree di rilevamento.</p> <p>Toccare <b>Project Maintenance</b> → <b>Device Maintenance</b> → <b>Test</b> → <b>Start Walk Test</b>, quindi muoversi nelle aree di rilevamento. Infine, toccare <b>End Walk Test</b> per visualizzare i risultati del test e dunque lo stato (normale o anomalo).</p>
Ora legale	<p>Toccare <b>System</b> → <b>Configuration</b> → <b>DST</b> per accedere alla pagina DST Settings, quindi attivare il pulsante per abilitare l'ora legale su AX Pro.</p>
Upgrade e cambio della lingua	<hr/> <p> <b>Nota</b></p> <p>Per accedere alla funzione che consente di effettuare l'upgrade del dispositivo, è necessario disporre dell'autorizzazione. Per i dettagli su come configurare le impostazioni di autorizzazione per Ax Pro, fare riferimento al manuale utente del dispositivo.</p> <hr/> <p>Toccare <b>Project Maintenance</b> → <b>Device Upgrade</b> per accedere alla pagina Device Upgrade, quindi selezionare la lingua e inserire il PIN. Infine, toccare <b>Upgrade</b> per cambiare la lingua di AX Pro ed effettuare l'upgrade.</p> <hr/> <p> <b>Nota</b></p> <p>Se non si dispone del PIN, è possibile toccare <b>Apply for PIN</b> per richiederlo.</p> <hr/>
Altre configurazioni	<p>È possibile eseguire altre configurazioni, tra cui la gestione degli utenti, la configurazione delle opzioni di sistema, il collegamento delle telecamere IP, le impostazioni di comunicazione, ecc.</p> <hr/> <p> <b>Nota</b></p> <p>Per i dettagli sulle altre configurazioni di AX Pro, fare riferimento al manuale utente del pannello di controllo di sicurezza.</p> <hr/>

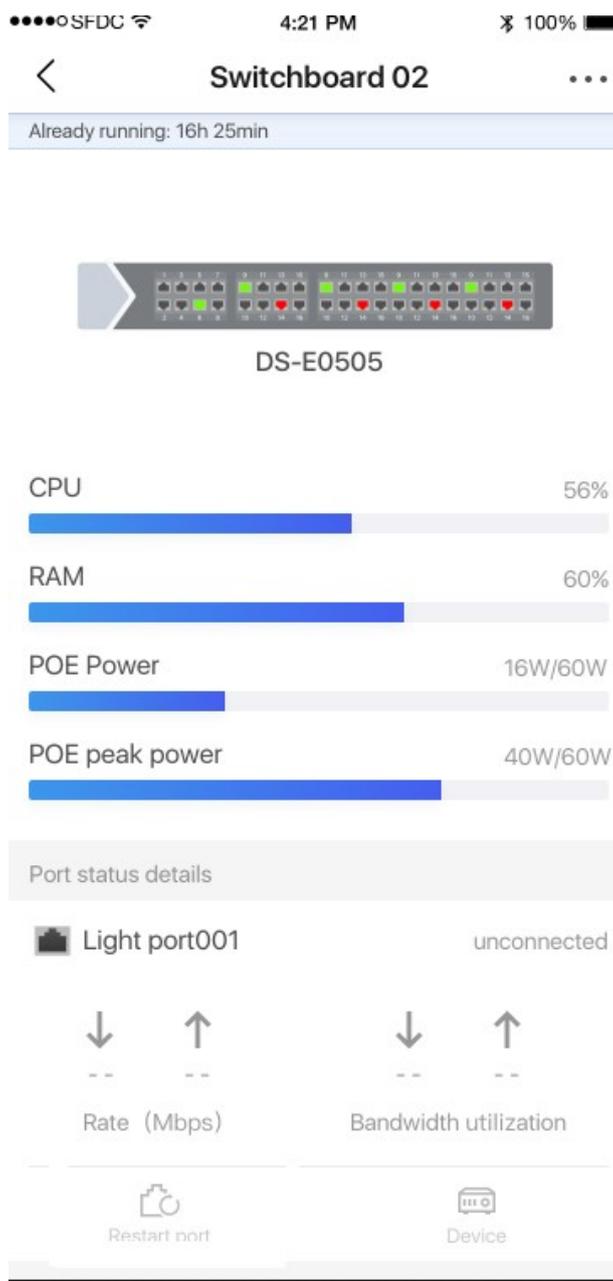
## 6.14 Gestione degli switch

È possibile gestire lo switch, visualizzarne la topologia e i dettagli dal client mobile. Inoltre, è possibile riavviare lo switch da remoto.

### 6.14.1 Attività dello switch

Nella pagina dei dettagli relativi allo switch, è possibile visualizzare l'utilizzo della CPU e della memoria, controllare lo stato della porta e riavviare il dispositivo.

Nell'elenco dei dispositivi, fare clic sul nome dello switch per accedere alla pagina dei relativi dettagli.



**Figura 6-5** Dettagli relativi allo switch

Nell'area superiore della pagina, è possibile visualizzare l'utilizzo della CPU e della memoria, l'alimentazione e il picco di potenza POE.

Nell'area centrale della pagina, è possibile visualizzare lo stato, il tipo (porta Ethernet o in fibra ottica), la frequenza e la larghezza di banda di ciascuna porta.

Effettuare le operazioni seguenti in base alle proprie esigenze.

Operazione	Descrizione
Riavviare lo switch	Fare clic su <b>Reboot</b> per riavviare lo switch.
Visualizzare dispositivo peer	Fare clic su <b>Peer Device</b> per visualizzare i dettagli del dispositivo collegato a questa porta.
Cancellare allarme	Se una porta dispone dell'allarme e si desidera eliminarlo, fare clic su <b>Clear Alarm</b> .
Riavviare porta	Per riavviare una porta che presenta anomalie, fare clic su <b>Restart Port</b> nei dettagli relativi allo stato della porta.

## 6.14.2 Topologia di rete

Se sono stati aggiunti switch a una piattaforma e sono stati connessi dispositivi ad esso, è possibile visualizzare la topologia di rete di tali dispositivi. La topologia di rete mostra i collegamenti di rete tra i dispositivi. Inoltre, indica le eccezioni di collegamento e i dispositivi che presentano anomalie, consentendo di individuare l'origine delle eccezioni e risolvere i problemi in modo visuale.

### Nota

Se non si dispone dell'autorizzazione per configurare lo switch, la topologia di rete non è disponibile. Per i dettagli su come richiedere l'autorizzazione, fare riferimento alla sezione ***Richiesta dell'autorizzazione per un dispositivo***.

Toccare una piattaforma nell'elenco per accedere alla pagina Device List, quindi fare clic su  vicino a uno switch per accedere alla pagina Network Topology. Qui sono disponibili le operazioni seguenti.

**Tabella 6-6 Operazioni disponibili**

Operazione	Descrizione
Visualizza legenda	È possibile toccare <b>More</b> per visualizzare tutte le legende.
Modifica nodo principale	Quando vengono aggiunti più switch a una piattaforma, questa seleziona casualmente uno di essi come nodo principale per impostazione predefinita per la topologia di rete. Se lo switch selezionato casualmente non è il nodo principale effettivo, è possibile toccare  per selezionare uno switch come tale.

Operazione	Descrizione
Visualizzazione dei dettagli relativi allo switch	<p>È possibile toccare uno switch sulla topologia per visualizzare le relative informazioni, tra cui quelle di base, lo stato del dispositivo e lo stato della porta.</p> <p>È inoltre possibile eseguire alcune operazioni, quali il riavvio dello switch e della porta. Per i dettagli, fare riferimento alla sezione <b>Attività dello switch</b>.</p> <hr/> <p> <b>Nota</b></p> <p>Non è possibile visualizzare i dettagli di uno switch virtuale.</p> <hr/>
Visualizza i dettagli di un altro dispositivo	<p>Toccare un dispositivo per visualizzarne i dettagli, ad esempio il modello e lo stato della rete.</p> <hr/> <p> <b>Nota</b></p> <ul style="list-style-type: none"> <li>● Se non si dispone dell'autorizzazione per configurare il dispositivo, prima è necessario richiederla.</li> <li>● Non è possibile visualizzare i dettagli di uno switch virtuale.</li> <li>● Se il dispositivo non viene aggiunto alla stessa piattaforma su cui si trova lo switch, non è possibile visualizzare i relativi dettagli.</li> </ul> <hr/>
Espandi i dispositivi in un nodo	<p>I dispositivi dello stesso tipo vengono inclusi in un nodo della topologia di rete. È possibile toccare  sul nodo per espandere tutti i dispositivi e controllare se il relativo stato di esecuzione è normale.</p> <p>Il colore dell'icona del dispositivo indica il relativo stato di esecuzione:</p> <ul style="list-style-type: none"> <li>● Grigio: normale</li> <li>● Rosso: anomalo</li> <li>● Giallo: dispositivo occupato</li> </ul>

Operazione	Descrizione
Spostare/aumentare/ridurre	È possibile trascinare la topologia di rete per spostarla. Avvicinare le dita per ridurre lo zoom e distanziarle per aumentarlo.

## 6.15 Altre funzioni

È possibile eseguire operazioni tra cui l'autenticazione della sicurezza e la configurazione da remoto, se necessario.

### Nota

Solo il gestore della piattaforma può eseguire le seguenti operazioni e configurazioni di una piattaforma. Per i dettagli sull'assegnazione di una piattaforma, fare riferimento al *Manuale utente del Portale Hik-ProConnect*.

Nella pagina dell'elenco delle piattaforme, toccare il nome di una piattaforma per accedere alla relativa pagina e visualizzarne le informazioni e i dispositivi.

### Autenticazione di sicurezza

Per il pannello di controllo di sicurezza Axiom, sarà visualizzata una notifica nell'elenco dei dispositivi della piattaforma o una pagina dei dispositivi che ricorda di eseguire l'autenticazione di sicurezza qualora sia stata abilitata la modalità conforme a EN50131 nella pagina di configurazione del dispositivo. Per motivi di sicurezza, è necessario fare clic su **Authenticate** e inserire la password del dispositivo. Se questa operazione non viene effettuata, non è possibile utilizzare le funzioni del dispositivo, tra cui il monitoraggio dello stato, la configurazione, le regole di collegamento e l'upgrade. Consultare il manuale utente del dispositivo per dettagli sull'abilitazione della modalità conforme a EN50131 nella pagina di configurazione del dispositivo.

### Configurazione da remoto

Toccare  per impostare i parametri del dispositivo (tra cui il campanello, il dispositivo di codifica e il pannello di controllo di sicurezza). Per i dettagli sulla configurazione da remoto, fare riferimento al manuale utente del dispositivo.

### Nota

- È possibile impostare solo il tipo di segnale acustico per la configurazione da remoto del campanello.
- Assicurarsi di aver eseguito l'autenticazione di sicurezza prima di avviare la configurazione da remoto.
- Se non si dispone dei permessi per la configurazione da remoto, è possibile eseguire questa operazione tramite una LAN: Collegare lo smartphone alla stessa rete Wi-Fi dei dispositivi da configurare, quindi fare clic su **Configuration in LAN** per accedere al dispositivo e avviare la configurazione da remoto.
- Assicurarsi che il dispositivo sia online, altrimenti non è possibile utilizzare la funzione.

## Capitolo 7 Gestione dell'archiviazione cloud

Se sono stati acquistati pacchetti di servizi di archiviazione cloud sul Portale, è possibile utilizzare il client mobile per aggiungere da remoto i dispositivi di archiviazione cloud alla piattaforma Hik-ProConnect. Inoltre, è possibile configurare ulteriori impostazioni per consentire al dispositivo di archiviazione cloud di passare i video relativi agli eventi dai canali dei dispositivi di codifica al cloud.

### 7.1 Impostazione dell'archiviazione cloud per Hik-ProConnect Box

Dopo aver aggiunto Hik-ProConnect Box a una piattaforma, nella pagina dei risultati della procedura viene visualizzata l'opzione per impostare l'archiviazione cloud. È possibile saltare l'impostazione, ma si consiglia di eseguirla per configurare il test di rete (opzionale), l'aggiunta di canali, le impostazioni di risoluzione dei canali, le impostazioni degli eventi e l'attivazione del servizio di archiviazione cloud. Una volta completata la configurazione, è possibile utilizzare Hik-ProConnect Box per caricare sul cloud i video relativi agli eventi dei canali collegati ad esso.

#### Passaggi

---

#### Nota

Se al momento dell'aggiunta di Hik-ProConnect Box si ignora il passaggio per impostare l'archiviazione cloud, è possibile toccare la periferica nell'elenco dei dispositivi per accedere alla pagina delle relative impostazioni, quindi selezionare **Linked Channel** al fine di impostare l'archiviazione cloud in un secondo momento.

---

1. Aggiungere Hik-ProConnect Box alla piattaforma tramite Hik-Connect P2P.
- 

#### Nota

Per i dettagli, fare riferimento alle sezioni **Aggiunta di un dispositivo tramite la scansione del codice QR** e **Aggiunta di un dispositivo tramite Hik-Connect (P2P)**.

---

Dopo aver aggiunto il dispositivo, nella finestra a comparsa dei risultati della procedura viene visualizzata l'opzione per impostare l'archiviazione cloud.

2. Per avviare la configurazione dei relativi parametri, toccare **Cloud Storage Settings**.  
A questo punto, si accede alla pagina Network Test.
3. Opzionale: Se la larghezza di banda della rete è limitata, toccare **Start** per verificarne le prestazioni, quindi selezionare **Add Channel** al termine del test.

---

 **Nota**

- Per i dettagli sul test di rete, fare riferimento alla sezione **Test di rete**.
  - È possibile toccare **Skip** per saltare il passaggio.
- 

In questo modo, si accede alla pagina Select Device to Link che visualizza i dispositivi disponibili.

4. Toccare un dispositivo per accedere alla pagina Select Channel to Enable Cloud.
  5. Attivare i pulsanti per aggiungere i canali a Hik-ProConnect Box.
  6. Toccare **Next** per accedere alla pagina Device Information.
  7. Impostare le informazioni relative al dispositivo, ad esempio l'indirizzo IP, il nome utente e la password.
  8. Toccare **Finish** per accedere alla pagina Linked Channel.
  9. Attivare il servizio di archiviazione cloud per un canale.
    - Toccare **Activate** → **Activate by Service Key**, inserire il codice della licenza, quindi selezionare **Activate**.
    - Toccare **Activate** → **Activate Purchased Package**, selezionare il tipo di pacchetto acquistato, impostare il numero di pacchetti da attivare, quindi toccare **Activate**.
- 

 **Nota**

- È possibile acquistare la licenza dal distributore. Per i dettagli, contattare il distributore del proprio Paese o della propria area geografica.
  - È possibile acquistare pacchetti di servizi di archiviazione cloud dal market dei servizi disponibile sul Portale. Per i dettagli, fare riferimento al *Manuale utente del Portale Hik-ProConnect*.
- 

10. Toccare il canale attivato per accedere alla pagina Channel Details al fine di impostare i parametri relativi all'archiviazione cloud.

**Video Definition**

Impostare **High Definition** o **Standard Definition** come definizione dei video caricati sul cloud.

---

 **Nota**

Assicurarsi che il numero di canali a definizione standard o alta non superi il limite massimo consigliato che viene visualizzato nella finestra Add Channel (se è stato eseguito il test di rete).

---

**Cloud Storage**

Modificare il servizio di archiviazione cloud attivato per il canale.

**Rilevamento di movimenti**

Impostare Motion Detection come evento per attivare l'azione di registrazione video del canale.

---

 **Nota**

Gli eventi che supportano tale azione includono il rilevamento di movimenti, l'intrusione e l'attraversamento di una linea. Sul client mobile è possibile impostare solo Motion Detection come evento che attiva tale azione.

---

**Enable Motion Detection**

Dopo aver attivato questa opzione, vengono rilevati oggetti in movimento sull'immagine del canale.

**Area Settings**

Toccare **Draw Area** per disegnare un'area sull'immagine, quindi trascinare il cursore per impostare la sensibilità del rilevamento.

Gli oggetti in movimento vengono rilevati all'interno dell'area disegnata.

**Arming Schedule**

Definire il periodo di tempo durante cui viene attivato il rilevamento di movimenti.

**Linkage Method**

Assicurarsi che l'opzione **Notify Surveillance Center** sia abilitata. Se non è attiva, il canale non registra i video relativi agli eventi anche se questi vengono rilevati.

11. Opzionale: se necessario, effettuare le seguenti operazioni.

- |   |  |
|---|--|
| <b>Cambiare il canale su cui utilizzare il servizio</b> | Nell'elenco dei canali, toccarne uno su cui è attivo il servizio per accedere alla pagina Cloud Storage Settings, quindi selezionare ⇌ per cambiare il canale su cui utilizzare il servizio di archiviazione cloud attivato. |
| <b>Eliminare un canale</b>                              | Se il servizio di archiviazione cloud non è attivo su un canale, toccare quest'ultimo nell'elenco dei canali, quindi toccare <b>Delete</b> per eliminarlo.   |

---

 **Nota**

Se su un canale è attivo il servizio, non è possibile eliminarlo.

---

## 7.2 Impostazione dell'archiviazione cloud per un DVR cloud

Dopo aver aggiunto un DVR cloud a una piattaforma, nella pagina dei risultati della procedura viene visualizzata l'opzione per impostare l'archiviazione cloud. È possibile saltare l'impostazione, ma si consiglia di eseguirla per configurare il test di rete (opzionale), le impostazioni relative alla definizione, le impostazioni dell'evento, l'attivazione dell'archiviazione cloud sui canali del DVR e per gli altri canali. Una volta completata la configurazione, è possibile utilizzare il DVR cloud per caricare sul cloud i video relativi agli eventi dei canali collegati ad esso.

### Passaggi



#### Nota

Se al momento dell'aggiunta del DVR cloud si ignora il passaggio per impostare l'archiviazione cloud, è possibile toccare la periferica nell'elenco dei dispositivi per accedere alla pagina delle relative impostazioni, quindi selezionare **Linked Channel** al fine di impostare l'archiviazione cloud in un secondo momento.

---

1. Aggiungere un DVR cloud alla piattaforma tramite Hik-Connect P2P.



#### Nota

Per i dettagli, fare riferimento alle sezioni **Aggiunta di un dispositivo tramite la scansione del codice QR** e **Aggiunta di un dispositivo tramite Hik-Connect (P2P)**.

---

Dopo aver aggiunto il dispositivo, nella finestra a comparsa dei risultati della procedura viene visualizzata l'opzione per impostare l'archiviazione cloud.

2. Per avviare la configurazione dei relativi parametri, toccare **Cloud Storage Settings**.  
A questo punto, si accede alla pagina Network Test.
3. Opzionale: Se la larghezza di banda della rete è limitata, toccare **Start** per verificarne le prestazioni, quindi selezionare **Next** al termine del test.



#### Nota

- Per i dettagli sul test di rete, fare riferimento alla sezione **Test di rete**.
  - È possibile toccare **Skip** per saltare il passaggio.
- 

Dopodiché si accede alla pagina Select Channel to Enable Cloud Storage su cui è possibile visualizzare tutti i canali del DVR cloud.

4. Attivare i pulsanti per abilitare l'archiviazione cloud sui canali del dispositivo.
5. Toccare **Next** per accedere alla pagina dell'elenco dei canali.
6. Opzionale: toccare la miniatura di un canale per visualizzarne il video in tempo reale.
7. Toccare un canale per accedere alla pagina Cloud Storage Settings.

8. Attivare il servizio di archiviazione cloud per il canale.
  - Toccare **Activate** → **Activate by Service Key**, inserire il codice della licenza, quindi selezionare **Activate**.
  - Toccare **Activate** → **Activate Purchased Package**, selezionare il tipo di pacchetto acquistato, impostare il numero di pacchetti da attivare, quindi toccare **Activate**.

---

 **Nota**

- È possibile acquistare la licenza dal distributore. Per i dettagli, contattare il distributore del proprio Paese o della propria area geografica.
- È possibile acquistare pacchetti di servizi di archiviazione cloud dal market dei servizi disponibile sul Portale. Per i dettagli, fare riferimento al *Manuale utente del Portale Hik-ProConnect*.

---

A questo punto, si accede alla pagina Cloud Storage Settings.

9. Impostare i parametri relativi all'archiviazione cloud nella pagina Cloud Storage Settings.

#### Video Definition

Impostare **High Definition** o **Standard Definition** come definizione dei video caricati sul cloud.

---

 **Nota**

Assicurarsi che il numero di canali a definizione standard o alta non superi il limite massimo consigliato che viene visualizzato nella finestra Add Channel (se è stato eseguito il test di rete).

---

#### Cloud Storage

Modificare il servizio di archiviazione cloud attivato per il canale.

#### Rilevamento di movimenti

Impostare Motion Detection come evento per attivare l'azione di registrazione video del canale.

---

 **Nota**

Gli eventi che supportano tale azione includono il rilevamento di movimenti, l'intrusione e l'attraversamento di una linea. Sul client mobile è possibile impostare solo Motion Detection come evento che attiva tale azione.

---

#### Enable Motion Detection

Dopo aver attivato questa opzione, vengono rilevati oggetti in movimento sull'immagine del canale.

#### Area Settings

Toccare **Draw Area** per disegnare un'area sull'immagine, quindi trascinare il cursore per impostare la sensibilità del rilevamento.

Gli oggetti in movimento vengono rilevati all'interno dell'area disegnata.

**Arming Schedule**

Definire il periodo di tempo durante cui viene attivato il rilevamento di movimenti.

**Linkage Method**

Assicurarsi che l'opzione **Notify Surveillance Center** sia abilitata. Se non è attiva, il canale non registra i video relativi agli eventi anche se questi vengono rilevati.

## 7.3 Test di rete

Quando la larghezza di banda della rete è limitata, l'archiviazione cloud è disponibile solo per un numero limitato di canali al fine di impedire la perdita del segnale video. Per evitare ciò, è possibile eseguire un test di rete. In base alle condizioni della rete, il risultato del test mostra il numero massimo di canali su cui è possibile attivare l'archiviazione cloud e l'impostazione di risoluzione consigliata per ciascuno di essi. Questo consente di configurare l'archiviazione cloud in modo tale che possa sfruttare al massimo la rete anche se la larghezza di banda è limitata. Nell'elenco dei dispositivi, è possibile toccare la periferica di archiviazione cloud per accedere alla pagina delle relative impostazioni e poi selezionare **Network Test** → **Start** per avviare il test di rete.

## Figura 8 Centro eccezioni

Il modulo Centro eccezioni visualizza tutta la cronologia delle notifiche delle eccezioni dei dispositivi e dei canali.

### Nota

- L'amministratore di installazione può visualizzare tutte le eccezioni dei dispositivi in tutte le piattaforme aggiunte. Gli installatori possono visualizzare solo le eccezioni dei dispositivi presenti nella piattaforma loro assegnata.
- Innanzitutto, è necessario impostare la regola di eccezione. Per i dettagli, fare riferimento alla sezione **Aggiunta di regole di eccezione**.

Toccare **Exception Center** per accedere alla pagina Exception Center come illustrato di seguito.

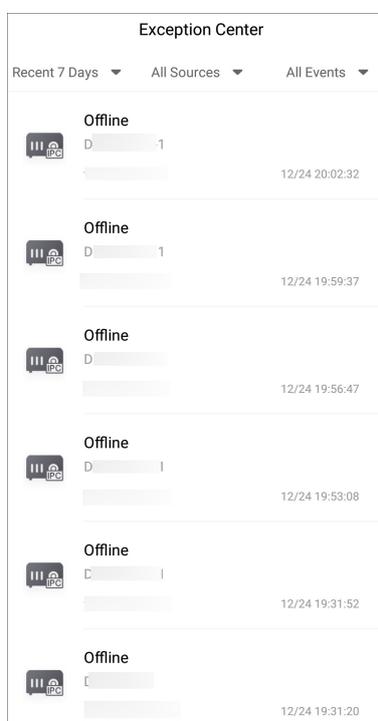


Figura 8-1 Exception Center

### Verifica dei dettagli dell'eccezione

Per filtrare le eccezioni in base alle esigenze, procedere come segue.

4. Impostare il periodo di tempo. Vengono visualizzate le eccezioni ricevute durante questo periodo.
5. Selezionare una sorgente (tra cui la piattaforma, il dispositivo e il canale) dall'elenco a discesa per visualizzare le eccezioni corrispondenti.
6. Selezionare i tipi di eccezione da verificare. I tipi di eccezione includono l'eccezione del dispositivo e l'eccezione del canale.

