

Portale 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 RILASCIA ALCUNA GARANZIA, ESPRESSA O IMPLICITA, COMPRESE A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, GARANZIE DI COMMERCIABILITÀ, 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, CONSEQUENZIALE, ACCIDENTALE O INDIRETTO, 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 INFORMATA SULLA POSSIBILITÀ DI TALI DANNI.

L'UTENTE RICONOSCE CHE LA NATURA DI INTERNET PREVEDE RISCHI DI SICUREZZA INTRINSECHI E CHE HIKVISION DECLINA QUALSIASI RESPONSABILITÀ IN RELAZIONE A FUNZIONAMENTI ANOMALI, VIOLAZIONE DELLA RISERVATEZZA O ALTRI DANNI RISULTANTI DA ATTACCHI INFORMATICI, INFEZIONE DA VIRUS O ALTRI RISCHI LEGATI ALLA SICUREZZA SU INTERNET; TUTTAVIA, HIKVISION FORNIRÀ TEMPESTIVO SUPPORTO TECNICO, SE NECESSARIO.

i

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

Indice

Capitolo 1 Introduzione	1
1.1 Destinatari	1
1.2 Soggetti di Hik-ProConnect	1
1.3 Ambiente di funzionamento	2
Capitolo 2 Gestione account	3
2.1 Registrazione di un account amministratore di installazione	4
2.2 Gestione delle informazioni sull'azienda	7
2.3 Autenticazione account	9
2.4 Gestione di ruoli e autorizzazioni	10
2.5 Invito dei dipendenti	11
2.6 Accettazione dell'invito e registrazione dell'account installatore	12
2.7 Impostazione delle informazioni sull'account	13
Capitolo 3 Accesso	15
Capitolo 4 Panoramica del Portale Hik-ProConnect	17
Capitolo 5 Co-Branding	24
Capitolo 6 Gestione delle piattaforme	25
Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site	25 25
Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma	25 25 27
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 	25 25 27 28
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 6.4 Assegnazione della piattaforma all'installatore 	25 25 27 28 29
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 6.4 Assegnazione della piattaforma all'installatore 6.5 Invio della richiesta per diventare proprietario della piattaforma 	25 25 27 28 29 29 30
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 6.4 Assegnazione della piattaforma all'installatore 6.5 Invio della richiesta per diventare proprietario della piattaforma 6.6 Invio della richiesta di autorizzazione al proprietario della piattaforma 	25 25 27 28 29 30 32
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 6.4 Assegnazione della piattaforma all'installatore 6.5 Invio della richiesta per diventare proprietario della piattaforma 6.6 Invio della richiesta di autorizzazione al proprietario della piattaforma 	25 25 27 28 29 30 32 34
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 6.4 Assegnazione della piattaforma all'installatore 6.5 Invio della richiesta per diventare proprietario della piattaforma 6.6 Invio della richiesta di autorizzazione al proprietario della piattaforma Capitolo 7 Gestione di un dispositivo 7.1 Aggiunta di un dispositivo 	25 25 27 28 29 30 32 34 34
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 6.4 Assegnazione della piattaforma all'installatore 6.5 Invio della richiesta per diventare proprietario della piattaforma 6.6 Invio della richiesta di autorizzazione al proprietario della piattaforma Capitolo 7 Gestione di un dispositivo 7.1 Aggiunta di un dispositivi rilevati online 	25 25 27 28 29 30 32 34 34 34
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 6.4 Assegnazione della piattaforma all'installatore 6.5 Invio della richiesta per diventare proprietario della piattaforma 6.6 Invio della richiesta di autorizzazione al proprietario della piattaforma Capitolo 7 Gestione di un dispositivo 7.1 Aggiunta di un dispositivi rilevati online 7.1.2 Aggiunta di dispositivi tramite il servizio Hik-Connect (P2P) 	25 25 27 28 29 30 32 34 34 34 34 34
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 6.4 Assegnazione della piattaforma all'installatore 6.5 Invio della richiesta per diventare proprietario della piattaforma 6.6 Invio della richiesta di autorizzazione al proprietario della piattaforma Capitolo 7 Gestione di un dispositivo 7.1 Aggiunta di un dispositivi rilevati online 7.1.2 Aggiunta di dispositivi tramite il servizio Hik-Connect (P2P) 7.1.3 Aggiunta di dispositivi tramite l'indirizzo IP o il nome di dominio 	25 25 27 28 29 30 32 34 34 34 34 34 34 34 34 34 34
 Capitolo 6 Gestione delle piattaforme 6.1 Panoramica della pagina Site 6.2 Aggiunta di una nuova piattaforma 6.3 Aggiunta di piattaforme esistenti 6.4 Assegnazione della piattaforma all'installatore 6.5 Invio della richiesta per diventare proprietario della piattaforma 6.6 Invio della richiesta di autorizzazione al proprietario della piattaforma Capitolo 7 Gestione di un dispositivo 7.1 Aggiunta di un dispositivi rilevati online 7.1.2 Aggiunta di dispositivi tramite il servizio Hik-Connect (P2P) 7.1.3 Aggiunta di dispositivi in un batch 	25 25 27 28 29 30 32 34

7.3 Approvazione dell'autorizzazione per i dispositivi	
7.4 Migrazione di dispositivi dall'account Hik-Connect	47
7.5 Aggiunta di una regola di collegamento	51
7.5.1 Aggiunta di una regola di collegamento personalizzata	52
7.5.2 Aggiunta di regole di collegamento basate su modelli predefiniti	58
7.5.3 Tutorial video	61
7.6 Aggiunta di regole di eccezione	62
7.7 Attivazione della funzione che consente al dispositivo di inviare notifiche	65
7.8 Sistema di conteggio	66
7.8.1 Attivazione del servizio di conteggio delle persone per i canali	66
7.8.2 Aggiunta di un gruppo per il conteggio delle persone	67
7.9 Attivazione del servizio di controllo della temperatura per i canali	70
7.10 Upgrade del firmware del dispositivo	73
7.11 Scollegamento di un dispositivo dal relativo account corrente	74
7.12 Reimpostazione della password del dispositivo	74
7.13 Configurazione del DDNS dei dispositivi	76
7.14 Visualizzazione di video in tempo reale	77
7.15 Visualizzazione di video registrati	77
7.16 Uso e configurazione del sistema AX Pro	78
7.17 Configurazione da remoto	
Capitolo 8 Servizio di archiviazione cloud	83
8.1 Diagramma di flusso	
8.2 Acquisto di servizi di archiviazione cloud	
8.3 Impostazione dell'archiviazione cloud per Hik-ProConnect Box	
8.4 Impostazione dell'archiviazione cloud per un DVR cloud	92
8.5 Test di rete	95
8.6 Attivazione o rinnovo di servizi per un canale	95
8.7 Visualizzazione dei dettagli relativi all'archiviazione cloud	97
Capitolo 9 Servizio di monitoraggio dello stato	98
Capitolo 10 monitoraggio dello stato	100
10.1 Visualizzazione dello stato dei dispositivi in tutte le piattaforme	

10.2 Visualizzazione dello stato dei dispositivi in piattaforme specifiche	
10.3 Topologia di rete	
10.4 Centro eccezioni	114
Capitolo 11 Ricerca dei registri operativi	116
Capitolo 12 Strumenti	117

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'amministratore di installazione e all'installatore le informazioni e le istruzioni essenziali sull'uso del portale Hik-ProConnect per la gestione delle attività di sicurezza. Questo manuale descrive come gestire le autorizzazioni e i dipendenti dell'azienda, aggiungere piattaforme nuove o esistenti, richiedere l'autorizzazione per accedere alla piattaforma da parte dell'utente finale, gestire e configurare i dispositivi appartenenti alla piattaforma, controllare lo stato di integrità dei dispositivi per la manutenzione, ecc.

1.2 Soggetti di Hik-ProConnect

Di seguito vengono presentati i soggetti (ovvero qualsiasi elemento fisico o concettuale) inclusi in Hik-ProConnect.

- Amministratore di installazione: dispone dell'accesso completo alle funzioni di Hik-ProConnect.
- Installatore: gli installatori sono "account secondario" dell'amministratore di installazione e sono controllati dalle autorizzazioni che ne limitano l'operatività. Ad esempio, possono solo gestire le piattaforme che vengono a loro assegnate.
- Piattaforma: rappresenta una posizione fisica dove sono installati i dispositivi e tramite cui l'installatore/amministratore di installazione può gestire e configurare i dispositivi.

- Gestione piattaforma: quando viene assegnata una piattaforma all'installatore, questi ne diventa il responsabile e può gestire e configurarne i dispositivi.
- Proprietario piattaforma: quando l'installatore trasferisce la proprietà della piattaforma all'utente finale, questi ne diventa il proprietario. L'installatore può inoltre richiedere al proprietario l'autorizzazione ad operare sulla piattaforma in modo da gestirla.

1.3 Ambiente di funzionamento

Di seguito è riportato il sistema consigliato per l'esecuzione del Portale.

Sistema operativo

Microsoft Windows[®] 7/8.1/10 (a 32 bit e 64 bit).

CPU

CPU Intel[®] Core[™] i5-4460 a 3.20 GHz e superiore.

RAM

8 GB o superiore (almeno 4 GB).

Scheda grafica

NVIDIA[®] GeForce GT 730

Browser web

Internet Explorer 11 (a 32 bit e 64 bit) e superiore e versioni di Firefox (a 32 bit e 64 bit) e Chrome (a 32 bit e 64 bit) rilasciate negli ultimi sei mesi.

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.



Figura 2-1 Diagramma di flusso della gestione account per Paesi e aree geografiche

• **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*.

iNota

Se viene richiesto di immettere il codice di autenticazione al momento della registrazione dell'account amministratore di installazione, è necessario fornire le informazioni aziendali dopo aver effettuato l'accesso all'account. Per i dettagli, fare riferimento alla sezione *Gestione delle informazioni sull'azienda*.

Per alcuni Paesi e aree geografiche, al momento della registrazione non è richiesta l'immissione del codice di autenticazione.

- 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. Per i dettagli, fare riferimento alla sezione *Gestione di ruoli e autorizzazioni*.
- Invito dei dipendenti: è possibile invitare i dipendenti a registrare gli account come installatori e assegnare ruoli diversi per fornire loro le autorizzazioni. Per i dettagli, fare riferimento alla sezione *Invito dei dipendenti*.
- 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. Per i dettagli, fare riferimento alla sezione Accettazione dell'invito e registrazione dell'account come installatore.

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

iNota

È possibile fare clic su **Try Free Demo** nella pagina di accesso per utilizzare Hik-ProConnect senza registrare alcun account. I dati visualizzati nella versione di prova sono solo dimostrativi e non consentono di effettuare operazioni.

- 1. Nella barra degli indirizzi del browser, inserire *https://www.hik-proconnect.com*. Sarà visualizzata la pagina di accesso di Hik-ProConnect.
- 2. Nella pagina di accesso, fare clic su Register for Free.

Hik-ProConnect
Welcome
Already registered? Login
* Country/Region
United Kingdom 🗸
6 After registration, the country or region you selected for you company cannot be changed. Please select prudently.
* Email
* Verification Code Get Verification Code
Didn't receive the verification
* Password
* Confirm Password
* First Name
Register

Figura 2-2 Registrazione di un account come amministratore di installazione

3. Selezionare il Paese o l'area geografica dell'azienda.

iNota

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

- 4. Dopo la registrazione, inserire un indirizzo e-mail da associare all'account amministratore di installazione.
- 5. Per ottenere il codice di verifica, fare clic su Get Verification Code.

iNota

- Se il codice di verifica non viene immesso entro il tempo disponibile, fare clic su **Resend** per ottenerne uno nuovo.
- Se non lo si riceve, fare clic su **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.

- 6. Inserire il codice di verifica ricevuto.
- 7. Impostare la password dell'account e confermarla.

iNota

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.

- 8. Inserire il nome e il numero di telefono.
- 9. Inserire il nome dell'azienda.
- 10. Opzionale: inserire Il codice di autenticazione utilizzato per confermare la genuinità dell'installatore professionale.

iNota

- Il codice di autenticazione deve contenere 10 cifre. Per ottenerlo, seguire le istruzioni sull'interfaccia.
- Se il campo relativo al codice di autenticazione è opzionale (in base al Paese o all'area geografica di residenza), è possibile lasciarlo vuoto e autenticare l'account amministratore di installazione in un secondo momento. Per i dettagli sull'autenticazione dell'account, fare riferimento alla sezione *Autenticazione account*.
- 11. 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.
 - 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.
- 12. Qualora si accettino i dettagli riportati negli accordi, selezionare I agree to the Terms of Service and Privacy Policy.
- 13. Fare clic su **Register**.

Verrà inviata un'e-mail di conferma della registrazione all'indirizzo inserito al passaggio 4.

14. Fare clic su Verify Now nell'e-mail ricevuta.

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

Risultato

È possibile eseguire l'accesso a Hik-ProConnect con questo account, invitare i dipendenti a registrare account come installatori ed eseguire altre operazioni quali la gestione della piattaforma, 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

Se è stato inserito il codice di autenticazione al momento della registrazione di un account amministratore di installazione, per poter attivare altre funzioni sulla piattaforma, è necessario immettere le informazioni aziendali (ad esempio, nome e indirizzo dell'azienda).

Passaggi

- 1. Inserire il nome dell'azienda.
- 2. Inserire altre informazioni sulla società, quali indirizzo, codice postale, numero di telefono, ecc.
- 3. Opzionale: inserire il sito web della società.
- 4. Fare clic su **Submit**.

Una volta impostate le informazioni sulla società, sarà effettuato l'accesso alla pagina iniziale del portale Hik-ProConnect.

- 5. Opzionale: per impostare il numero di partita IVA, caricare il registro dell'azienda o modificare le altre informazioni, procedere come segue.
 - 1) Nel Portale Hik-ProConnect, accedere a **Company** → **Company Information**.
 - 2) Fare clic su 🖉 nell'angolo in alto a destra del pannello **Company Information**.
 - 3) Se necessario, modificare le informazioni, come il nome dell'azienda, il numero di telefono, l'e-mail di contatto, ecc.

iNota

Dopo la registrazione, il Paese o l'area geografica non possono essere modificati una volta selezionati durante l'associazione delle informazioni aziendali.

- 4) Opzionale: immettere o modificare il numero di partiva IVA della propria azienda. Tale numero verrà utilizzato per la verifica dell'idoneità.
- 5) Opzionale: fare clic su + per caricare un'immagine del logo dell'azienda oppure fare clic su **Edit** per caricarla nuovamente in modo da aggiornare il logo.

iNota

- L'immagine deve essere in formato JPG, JPEG o PNG.
- Il formato consigliato per l'immagine è: altezza = 200 pixel, 200 pixel ≤ larghezza ≤ 600 pixel.
- Se non si imposta il logo dell'azienda, non è possibile attivare la funzione Co-branding.
- Dopo aver modificato il logo, questo verrà aggiornato nella pagina Co-Branding, ossia una sezione destinata alla promozione del marchio agli utenti finali. Per i dettagli sulle impostazioni di co-branding, fare riferimento alla sezione **Co-Branding**.
- 6) Opzionale: inserire o modificare le informazioni relative alla descrizione che verranno visualizzate sul client mobile Hik-Connect.
- 7) Fare clic su **Save** per salvare le modifiche.
- 6. Opzionale: nella pagina Company Information, è possibile visualizzare il numero massimo di dipendenti gestibili, il confronto tra le funzioni supportate e i dispositivi gestibili del pacchetto base e del pacchetto di monitoraggio dello stato fornito da Hik-ProConnect, nonché la data di scadenza del periodo di prova.

Pacchetto gratuito

Questo pacchetto consente di gestire fino a 1.024 dispositivi (illimitati durante il periodo di prova) e fornisce funzioni di base (tra cui l'aggiunta di dispositivi in un batch, l'upgrade del firmware dei dispositivi, la gestione di piattaforme e dispositivi, la richiesta di autorizzazione per la piattaforma, la visualizzazione dello stato dei dispositivi online, la configurazione da remoto e la visualizzazione in tempo reale).

Pacchetto di monitoraggio dello stato

Questo pacchetto consente di gestire un numero illimitato di dispositivi e fornisce funzioni avanzate (ad esempio, il monitoraggio dello stato, le eccezioni, il collegamento, la gestione di ruoli e autorizzazioni, la gestione dei dipendenti, la visualizzazione dei registri operativi, il co-branding e così via).

Il pacchetto di monitoraggio dello stato è gratuito durante il periodo di prova. Una volta terminato tale periodo, è necessario effettuare il pagamento per continuare a utilizzare le funzioni di questo pacchetto e gestire un numero illimitato di dispositivi.

2.3 Autenticazione account

Quando si registra un account come amministratore di installazione, è possibile inserire il codice utilizzato per confermare l'autenticità dell'installatore professionista. Se non si inserisce un codice durante la registrazione, è possibile provare prima le funzioni in Hik-ProConnect e autenticare l'account in un secondo momento. Gli account non autenticati non possono acquistare servizi a valore aggiunto. In questa sezione viene illustrata la modalità di autenticazione dell'account amministratore di installazione dopo la registrazione.

iNota

Se è già stato inserito il codice di autenticazione durante la registrazione di un account come amministratore di installazione, è possibile saltare questa sezione.

Per autenticare l'account, è possibile procedere in uno dei modi seguenti in base al Paese o all'area geografica selezionata al momento della registrazione.

Inserimento del codice di autenticazione

Per autenticare l'account utilizzando questo metodo, prima è necessario richiedere il codice di autenticazione a Hikvision o al distributore e poi inserirlo.

 Andare a Company → Company Information e fare clic su Authenticate Now per accedere alla pagina di autenticazione dell'account. (Opzionale) Se non si ha il codice di autenticazione, è possibile richiederlo facendo clic su Get Authentication Code e inviando per e-mail a Hikvision o al distributore il modello predefinito compilato con i dati, tra cui l'indirizzo e-mail (quello utilizzato per registrare l'account amministratore di installazione) e le informazioni aziendali, come l'ID azienda, il nome e il numero di telefono.

iNota

- Per modificare le informazioni nel modello, è possibile fare clic su ∠. I contenuti modificati verranno aggiornati nelle informazioni aziendali.
- Se il server dell'e-mail non è configurato o l'indirizzo del destinatario non viene compilato automaticamente, è possibile copiare i dati e inviarli a Hikvision o al distributore utilizzando la propria casella di posta.
- 2. Dopo aver ricevuto il codice, inserirlo nella pagina di autenticazione dell'account e fare clic su **OK** per autenticarlo.

Invio della richiesta online

Per autenticare l'account utilizzando questo metodo, è necessario compilare il modulo con i dati e poi inviarlo effettuando una richiesta online. Una volta approvata, l'account verrà autenticato.

 Andare a Company → Company Information e fare clic su Authenticate Now per accedere alla pagina di autenticazione dell'account. (Opzionale) Se necessario, modificare le informazioni aziendali, ad esempio il nome, l'indirizzo e la città dell'azienda

- 2. (Opzionale) Fare clic su + per caricare l'immagine del biglietto da visita. Se sono stati acquistati prodotti Hikvision, indicare il distributore.
- 3. Fare clic su **Authenticate Now**. La richiesta verrà inviata. Una volta approvata, l'autenticazione dell'account verrà completata.

2.4 Gestione di ruoli e autorizzazioni

Prima di aggiungere un dipendente al sistema, è possibile creare ruoli diversi con autorizzazioni differenti per l'accesso alle risorse di sistema e quindi l'assegnazione dei ruoli ai dipendenti per conferire le relative autorizzazioni. In alternativa è possibile fornire un ruolo predefinito a un dipendente senza crearne uno. Un dipendente può disporre solo di un ruolo.

Passaggi

iNota

Sono presenti tre ruoli predefiniti nel sistema: Administrator, Site Manager e IT Manager. Le autorizzazioni dei tre ruoli sono le seguenti. Questi tre ruoli non possono essere eliminati.

- Administrator: può impostare le informazioni aziendali, gestire i dipendenti, controllare i registri operativi di tutti i dipendenti e gestire tutte le piattaforme.
- Site Manager: gestione delle piattaforme assegnate, aggiunta, configurazione ed eliminazione di dispositivi e abilitazione di servizi a valore aggiunto per gli utenti finali delle piattaforme assegnate.
- IT Manager: gestione di tutte le piattaforme, assegnazione di piattaforme ad altri dipendenti, abilitazione o modifica di servizi a valore aggiunto per tutti gli utenti finali e visualizzazione del registro delle operazioni di tutti i dipendenti.

1. Fare clic su **Company** \rightarrow **Role and Permission** per visualizzare tutti i ruoli.

- 2. Aggiungere un ruolo.
 - 1) Nella schermata principale, fare clic su **Company** → **Role and Permission** → **Add Role** per aprire il pannello Add Role.
 - 2) Inserire il nome del ruolo e selezionarne le autorizzazioni.

Gestire tutte le piattaforme

Gestione di tutte le piattaforme, inclusa l'aggiunta e la modifica, l'assegnazione della piattaforma al Site Manager, l'invito al proprietario della piattaforma, le richieste per l'autorizzazione nella piattaforma, la ricerca di piattaforme, la gestione dei dispositivi nella piattaforma (aggiunta, eliminazione, modifica, aggiornamento), le richieste di autorizzazione dei dispositivo e il monitoraggio dello stato. Questa autorizzazione può essere assegnata a non più di 18 dipendenti.

Gestire la piattaforma assegnata

Gestione della piattaforma assegnata al dipendente, inclusi la modifica della piattaforma, l'invito al proprietario della piattaforma, la richiesta dell'autorizzazione a gestire le informazioni della piattaforma, l'aggiunta di una piattaforma esistente, l'aggiunta di una nuova piattaforma, la gestione dei dispositivi della piattaforma (aggiunta, eliminazione, modifica e aggiornamento), e l'eliminazione della piattaforma.

iNota

È necessario concedere questa autorizzazione a un dipendente prima di assegnargli una piattaforma.

Gestire account e ruolo

Accedere alle pagine Employee e Role and Permission per aggiungere ed eliminare account e ruoli. Non sarà possibile visualizzare la pagina Dipendente, ruolo e autorizzazione senza questa autorizzazione.

Gestire informazioni aziendali

Accedere alla pagina Company Information e modificare le informazioni sull'azienda (come il nome, il logo, gli indirizzi, ecc). Se non si dispone di questa autorizzazione, non è possibile visualizzare la pagina Company Information.

Gestione di pacchetti di servizi e ordini

Visualizzare ordini, acquistare pacchetti di servizi, come quelli per il monitoraggio dello stato e per i dipendenti.

3) Opzionale: inserire le note sul ruolo nel campo Description.

4) Fare clic su OK.

3. Opzionale: selezionare i ruoli aggiunti, quindi fare clic su **Delete** per eliminare quelli selezionati.

iNota

Non è possibile eliminare un ruolo assegnato a un dipendente.

2.5 Invito dei dipendenti

L'amministratore di installazione e l'installatore con le autorizzazioni per gestire account e ruoli possono invitare i dipendenti a gestire le risorse nel sistema.

Passaggi

- 1. Aprire il pannello Add Employee.
 - − Nella schermata principale, fare clic su **Company** \rightarrow **Employee** \rightarrow **Add Employee**.
 - Nella schermata principale, fare clic su Company → Role and Permission → Add Employee nella colonna Operation.

2. Opzionale: fare clic su Add Role per aggiungere un nuovo ruolo.

iNota

Per i dettagli relativi ai ruoli, fare riferimento alla sezione *Gestione di ruoli e autorizzazioni*.

- 3. Inserire l'e-mail del dipendente da invitare.
- Selezionare un ruolo per il dipendente. Per i dettagli relativi alla gestione dei ruoli, fare riferimento alla sezione *Gestione di ruoli e autorizzazioni*. Il sistema mostra le autorizzazioni del ruolo.
- 5. Fare clic su Add.

Il dipendente invitato riceverà un'e-mail all'indirizzo fornito, contenente un collegamento di invito. Per registrare un account, il dipendente deve fare clic sul link, dopodiché può visualizzare le sue informazioni nell'elenco dei dipendenti.

6. Opzionale: selezionare uno o più dipendenti e fare clic su **Delete** per eliminare quelli selezionati, se necessario.

2.6 Accettazione dell'invito e registrazione dell'account installatore

L'amministratore di installazione e l'installatore, i cui ruoli dispongono dell'autorizzazione **Manage Account and Role**, possono invitare gli altri dipendenti a registrare degli account installatore. I dipendenti possono accettare l'invito e registrare account installatore per la gestione di piattaforme e dispositivi.

Prima di iniziare

L'amministratore di installazione e l'installatore, i cui ruoli dispongono dell'autorizzazione **Manage Account and Role**, devono innanzitutto invitare il dipendente. Per i dettagli, fare riferimento alla sezione *Invito dei dipendenti*.

Passaggi

- 1. Una volta invitato il dipendente, questo riceverà un'e-mail da Hik-ProConnect.
- 2. Fare clic sul tasto o sul collegamento nell'e-mail per aprire la pagina di registrazione dell'installatore.
- 3. Nella pagina di registrazione, impostare la password dell'account e confermare la password.

iNota

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.

- 4. Inserire il nome e il numero di telefono del dipendente.
- 5. Qualora si accettino i dettagli riportati negli accordi, selezionare I agree to the Terms of Service and Privacy Policy.
- 6. Fare clic su **Register**.

Risultato

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

2.7 Impostazione delle informazioni sull'account

Una volta eseguito l'accesso, è possibile modificare le informazioni di base dell'account corrente e la password se necessario.

Nella pagina iniziale, fare clic sul nome nell'angolo in alto a destra e selezionare Account Settings.

Impostazione delle informazioni di base

Impostare le informazioni di base dell'account corrente, tra cui il nome dell'installatore, indirizzo e-mail e numero di telefono associati, ecc.

Fare clic su per impostare il profilo dell'account corrente.

Modifica password

consente di modificare la password del dispositivo.

iNota

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.

Modifica dell'e-mail associata all'account

Se necessario, è possibile modificare l'indirizzo e-mail associato all'account corrente.

- 1. Nella pagina Basic Information delle impostazioni dell'account, fare clic su ∠.
- 2. Inserire un nuovo indirizzo e-mail nel campo New Email.
- 3. Fare clic su Get Verification Code.

Verrà inviato un codice di verifica alla nuova casella di posta elettronica indicata.

- 4. Inserire il codice di verifica ricevuto nel campo Verification Code.
- 5. Inserire la password dell'account corrente.
- 6. Fare clic su **Save**.

Elimina account amministratore installatore

Se l'account amministratore di installazione non è più utilizzato, è possibile eliminarlo nella pagina Informazioni di base delle impostazioni di account.

iNota

- L'eliminazione dell'account amministratore di installazione non può essere annullata. Le informazioni e gli account aziendali NON POSSONO essere ripristinati dopo l'eliminazione. Eseguire il backup dei dati importanti prima di eliminare l'account.
- Se sono presenti piattaforme autorizzate sotto l'account corrente, non è possibile eliminarlo.
- 1. Nella pagina Basic Information delle impostazioni dell'account, fare clic su **Delete Installer Admin Account**.
- 2. Inserire la password dell'account amministratore di installazione e fare clic su Next.
- 3. Fare clic su **Delete Installer Admin Account** per confermare l'eliminazione.

Capitolo 3 Accesso

Dopo l'accesso tramite un account amministratore di installazione o installatore, è possibile gestire le risorse (tra cui piattaforme, dispositivi, ruoli, ecc.) ed eseguire operazioni quali il monitoraggio dello stato e così via.

Prima di iniziare

Assicurarsi di aver registrato un account. Per i dettagli relativi alla registrazione, fare riferimento alla sezione **Registrazione di un account amministratore di installazione** o **Accettazione dell'invito e registrazione dell'account installatore**.

Passaggi

- 1. Nella barra degli indirizzi del browser, inserire *https://www.hik-proconnect.com*. Sarà visualizzata la pagina di accesso di Hik-ProConnect.
- 2. Selezionare il Paese o l'area geografica in cui si trova l'account dall'elenco a discesa sotto il logo Hik-ProConnect.
- 3. Inserire e-mail di registrazione e password.
- 4. Opzionale: ripristinare la password in caso di smarrimento.
 - 1) Fare clic su Forgot Password per accedere alla pagina di reimpostazione della password.
 - 2) Fare clic su 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.

iNota

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) Fare clic su OK.

Per opzione predefinita, sarà necessario effettuare l'accesso con la nuova password.

5. Fare clic su Login.

iNota

- Se un utente con un account nuovo o già registrato ha inserito il codice di autenticazione nella pagina di registrazione, quando accede alla piattaforma 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 alla piattaforma deve inserire il nome dell'azienda per completare le informazioni di autenticazione della stessa.

Per opzione predefinita, si accederà alla pagina di elenco delle piattaforme.

Capitolo 4 Panoramica del Portale Hik-ProConnect

Il Portale Hik-ProConnect è un portale B/S della piattaforma Hik-ProConnect. La società di installazione dei dispositivi di sorveglianza può registrare un account amministratore di installazione su Hik-ProConnect e questo può invitare i dipendenti a registrare degli account come installatori. Ciascuna società dispone di un solo amministratore di installazione, ma può avere più installatori.

Dopo la registrazione, l'amministratore di installazione e gli installatori possono accedere a Hik-ProConnect tramite browser web e visualizzare la pagina iniziale del Portale Hik-ProConnect.

Moduli principali

Il Portale Hik-ProConnect è diviso in sette moduli principali. È possibile accedere a questi moduli tramite il pannello di navigazione sulla sinistra.

iNota

È possibile fare clic su \equiv o su \equiv per bloccare o sbloccare il pannello di navigazione a sinistra del Portale.

Modulo	Descrizione
Home	Nella schermata principale, è possibile visualizzare la panoramica delle piattaforme, i dispositivi gestiti, le eccezioni ricevute e altri elementi, come le funzioni utilizzate di frequente, le piattaforme visitate di recente, la procedura guidata, le documentazioni, ecc.
Piattaforma	Una piattaforma rappresenta una posizione fisica dove sono installati i dispositivi e tramite cui l'installatore/amministratore di installazione può gestirli e configurarli.
Monitoraggio delle condizioni	 Sono disponibili due parti nel modulo Monitoraggio dello stato: Stato di integrità: l'installatore può visualizzare tutti i dispositivi o quelli che presentano uno stato normale o anomalo, individuare i dispositivi con anomalie ed eseguire rapidamente la risoluzione dei problemi. Centro eccezioni: una volta impostate le regole di eccezione, quando si verifica un'eccezione sul dispositivo, questo invia una notifica al Portale. È possibile visualizzare tutte le notifiche ricevute in Exception Center.

Tabella 4-1 Modu	li principali del	Portale Hik-ProConnect

Modulo	Descrizione
Azienda	 Il modulo Azienda si occupa di tutti gli aspetti di gestione e amministrazione di ogni società di installazione. È composto dalle cinque parti seguenti: Informazioni aziendali: consente di gestire le informazioni aziendali. Co-Branding: abilitare la visualizzazione del logo aziendale sul client mobile di Hik-Connect per promuovere il marchio agli utenti finali. Dipendente: Ciascuna società dispone di un solo amministratore di installazione, ma può avere più installatori. l'amministratore di installazione può invitare i dipendenti aziendali a registrare degli account come installatori e assegnare autorizzazioni diverse ai dipendenti in base alle esigenze. L'installatore, il cui ruolo dispone dell'autorizzazione Manage Account and Role, può inoltre invitare gli altri dipendenti a registrare account come installatori. Ruolo e autorizzazione: un ruolo definisce i diritti di un dipendente in rapporto alle funzioni del sistema. Una volta creato un ruolo e specificate le autorizzazioni, è possibile assegnarlo ai dipendenti in base alle esigenze. Registro operazioni: consente di visualizzare i registri operativi relativi agli account e alle piattaforme presenti nell'azienda corrente.
Business	 Market dei servizi: Hik-ProConnect fornisce pacchetti di servizi a valore aggiunto acquistabili o rinnovabili. I miei servizi: in questa sezione è possibile visualizzare tutti i servizi acquistati e i dettagli, come il pacchetto gratuito e quello relativo ai servizi di archiviazione cloud. Ordini: in questa sezione è possibile visualizzare l'elenco degli ordini e i relativi dettagli.
Strumenti	Hik-ProConnect fornisce alcuni strumenti online per migliorare l'efficienza del lavoro.
Centro tutorial	Contiene video tutorial da guardare per conoscere meglio Hik-ProConnect.

Presentazione della schermata principale



Figura 4-1 Schermata principale

Tabella 4-2 Descrizione della schermata prin	cipale
--	--------

N.	Name	Introduzione				
1	Banner	Sono disponibili alcuni banner che indicano le caratteristiche, le funzioni e le informazioni importanti di Hik-ProConnect.				
		Nota 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.				
2	Panoramica della piattaforma	 È possibile visualizzare il numero totale di piattaforme gestite. Inoltre, è possibile utilizzare le opzioni: Not Invited: per conoscere il numero di piattaforme i cui proprietari non sono stati invitati. Non accettato: per conoscere il numero di piattaforme i cui proprietari non hanno accettato l'invito. Non autorizzato: per conoscere il numero di piattaforme per cui non sono state concesse le autorizzazioni. 				
		i Nota È possibile fare clic su > per accedere all'elenco delle piattaforme. Per istruzioni dettagliate sulla gestione della piattaforma, fare riferimento alla sezione Gestione della <i>piattaforma</i> .				

N.	Name	Introduzione
3	Panoramica delle eccezioni	È possibile visualizzare il numero di eccezioni ricevute e le proporzioni di ciascun tipo di eccezione.
		Passare il cursore sul grafico a torta per visualizzare le proporzioni dettagliate e la quantità.
		i Nota È possibile fare clic su View All Exceptions per accedere a Exception Center al fine di controllare le eccezioni ricevute. Per istruzioni dettagliate su come usare Exception Center, fare riferimento alla sezione Exception Center.
4	Device Overview	È possibile visualizzare il numero di dispositivi che presentano anomalie, tra cui la panoramica dei dispositivi e il tipo di ciascuno di essi.
		i Nota
		È possibile fare clic su > per accedere a Health Status al fine di controllare i dettagli relativi allo stato del dispositivo. Per i dettagli relativi allo stato, fare riferimento alle sezioni <i>Visualizzazione dello stato dei dispositivi di tutte le piattaforme</i> e <i>Visualizzazione dello stato dei dispositivi di determinate</i> <i>piattaforme</i> .
5	Funzioni usate di frequente	È possibile visualizzare le funzioni utilizzate di frequente. Fare clic su queste icone per accedere rapidamente a queste funzioni, se necessario.
	Piattaforme visitate	È possibile visualizzare le ultime cinque piattaforme visitate.
6	di recente	Fare clic sul nome della piattaforma per accedere alla pagina Site Details.
		Contiene video tutorial da guardare per conoscere meglio Hik-ProConnect e i modi corretti di utilizzare la piattaforma.
7	Centro tutorial	Fare clic su un video per aprire una pagina web e avviare la riproduzione. Fare clic su View All per visualizzare tutti i video in Centro tutorial.

Download del client mobile Hik-ProConnect

Nella schermata principale, fare clic su 📃 nell'angolo in alto a destra, quindi scansionare il codice QR per scaricare il client mobile Hik-ProConnect.

Visualizzazione delle eccezioni ricevute di recente

Quando il Portale riceve una notifica di eccezione, vengono visualizzati i relativi dettagli in una finestra che compare nell'angolo in alto a destra. È possibile fare clic su 🧳 (il numero indica i messaggi non letti) nell'angolo in alto a destra per visualizzare le eccezioni ricevute di recente dal Portale.



Figura 4-2 Eccezioni ricevute di recente

iNota

Innanzitutto, è necessario impostare le regole di eccezione del dispositivo affinché il Portale possa ricevere le notifiche. Per i dettagli, fare riferimento alla sezione *Aggiunta di regole di eccezione*.

È possibile fare clic su **Clear** per cancellare i record visualizzati in questa finestra. È possibile verificare in qualsiasi momento queste eccezioni nel Centro eccezioni.

Fare clic su **View All** per accedere a Exception Center e visualizzare tutte le eccezioni ricevute dal Portale. Per i dettagli, fare riferimento alla sezione *Centro eccezioni*.

Business

Nella schermata principale, fare clic su e nell'angolo in alto a destra, quindi selezionare **Service Package** o **Order** per visualizzare i dettagli dei servizi e gli ordini dell'account.

Periodo di prova

Nella schermata principale, fare clic su 🙃 nell'angolo in alto a destra per visualizzare la durata del periodo di prova dell'account.

iNota

È disponibile la prova gratuita di tutte le funzioni entro una data specifica. Successivamente, sarà necessario acquistare alcune funzionalità se necessario.

Invio di feedback

in caso di domande e suggerimenti sul sistema, è possibile inviarcele.

Nella schermata principale, fare clic sul nome nell'angolo in alto a destra e selezionare **Feedback** per aprire la relativa finestra.

In alternativa, fare clic sull'icona 📋 nella schermata principale per aprire la finestra Feedback.

Selezionare un tipo di feedback e quindi inserire suggerimenti e domande nella finestra a comparsa e allegare un'immagine se necessario.

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.

Fare clic su **Submit** per inviare il feedback.

Iscrizione/annullamento dell'iscrizione alla newsletter

Se l'amministratore di installazione non ha effettuato l'iscrizione alla newsletter di Hik-ProConnect al momento della registrazione dell'account, può farlo selezionando il nome nell'angolo in alto a

destra e scegliere **Subscribe to Newsletters** oppure facendo clic sull'icona 📄 nella schermata principale.

Dopo l'iscrizione, verranno inviate e-mail sugli ultimi prodotti, servizi, questionari e su offerte speciali all'indirizzo utilizzato per la registrazione dell'account.

È possibile annullare l'iscrizione in qualsiasi momento nella pagina **About**. Dopo l'annullamento dell'iscrizione, la newsletter non verrà più inviata.

About

Nella pagina iniziale, fare clic sul nome nell'angolo in alto a destra e selezionare **About**. È possibile visualizzare la versione del sistema corrente e leggere i contratti tra cui i termini del servizio, l'informativa sulla privacy e la licenza Open Source.

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.

Visualizzazione del manuale utente, della scheda tecnica o dell'elenco dei dispositivi compatibili

Nella schermata principale, fare clic su ② vicino al nome nell'angolo in alto a destra e fare clic su User Manual per aprire il manuale utente del Portale Hik-ProConnect. È inoltre possibile fare clic su User Manual, Datasheet o Device Compatibility List nell'angolo in basso a destra della schermata principale per aprire il manuale utente, la scheda tecnica o l'elenco dei dispositivi compatibili.

È possibile inserire delle parole chiave per cercare informazioni su istruzioni, dettagli delle specifiche o modello di dispositivo nel manuale utente, nella scheda tecnica e nell'elenco dei dispositivi compatibili.

Procedura guidata

È disponibile una procedura guidata per il processo di configurazione e funzionamento. Esistono due modi per aprire la procedura guidata:

- Nella schermata principale, fare clic su ② vicino al nome nell'angolo in alto a destra e fare clic su **Wizard**.
- In alternativa, fare clic sull'icona 🔋 nella schermata principale.

Fare clic su **Next** o **Previous** per navigare nella procedura guidata. È possibile fare clic sull'immagine a destra per visualizzare l'immagine ingrandita e controllarne i dettagli se necessario.

Fare clic su **Skip** per chiudere la procedura guidata.

Esci

Nella pagina iniziale, fare clic sul nome nell'angolo in alto a destra, quindi selezionare **Log Out** per uscire dall'account corrente e tornare alla pagina di accesso.

Capitolo 5 Co-Branding

Questa funzione aiuta a far conoscere il proprio marchio e rafforza l'immagine dei propri prodotti e servizi. Abilitandola, gli utenti finali potranno visualizzare il logo, l'indirizzo e il numero di telefono della propria azienda tramite Hik-Connect Mobile Client.

Nella schermata principale, fare clic su **Company** → **Co-Branding**. Attivare **Co-Branding** e passare il cursore sull'area Logo per visualizzare il pulsante **Edit**. Fare clic su **Edit** per caricare il logo aziendale. Dopo aver modificato il logo, questo verrà aggiornato nella pagina Company Information.

iNota

- 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 tutti i dispositivi di un utente finale sono gestiti dalla stessa azienda di installazione, il logo della stessa viene visualizzato sulla pagina di accesso e nella sezione About dell'account Hik-Connect dell'utente finale.
- Se i dispositivi di un utente finale sono gestiti da diverse aziende di installazione, l'utente può visitare la pagina relativa ai dettagli del dispositivo dell'account Hik-Connect per visualizzare il logo e i dettagli dell'azienda.

Capitolo 6 Gestione delle piattaforme

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, modificare, assegnare o eliminare piattaforme, invitare l'utente finale come proprietario della piattaforma, richiedere l'autorizzazione al proprietario della piattaforma per operare su di essa, ecc.

6.1 Panoramica 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, assegnarle, invitare l'utente a diventarne il proprietario, trasferire i dispositivi dall'account Hik-Connect, ecc. Fare clic sulla scheda **Site** per accedere alla pagina Site.

Ad	d New Site	Assign Migr	ate Devices from H	Hik-Connect Account				Search	Q
	Site Name 🕴	Address ‡	Site Owner 🔅	Device \$		Site Manager 💠	Status 🕆	Opera	tion
	Demo home	221 shutB street. London	Mr. Han	Encoding Device: 1	📓 Security Control Panel: 1	MIKE	Authorized and Monitoring	+	1
	Demo shop	02 shut street. London	Manager James	Encoding Device: 1 Access Control Device: 2	Security Control Panel: 1	MIKE	Authorized and Monitoring	+	100
	Demo office	225 shutA street. London	Manager A	Encoding Device: 1 Access Control Device: 2	Security Control Panel: 1	MIKE	Authorized and Monitoring	+	100

Figura 6-1 Pagina Site

Sono presenti diversi stati per le piattaforme nell'elenco relativo.

Non invitato

La piattaforma è stata aggiunta di recente e l'utente finale non è stato invitato a diventarne il proprietario.

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

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

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

iNota

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

Operazioni supportate	Non invitato	Non accettato Non registrato	Invitato, non autorizzato	Autorizzato e in monitoraggio
Cerca piattaforma	V	V	V	V
Assegna piattaforma	V	V	V	V
Invita proprietario piattaforma	V	V	×	×
Gestisci dispositivo	V	V	×	V
Modifica piattaforma	V	V	×	V
Elimina piattaforma	V	V	×	×
Richiedi autorizzazione	×	×	v	×

Tabella 6-1 Operazioni supportate nei vari stati

iNota

Per i dettagli su come trasferire i dispositivi dall'account Hik-Connect a Hik-ProConnect, fare riferimento alla sezione *Migrazione di dispositivi dall'account Hik-Connect*.

6.2 Aggiunta di una nuova piattaforma

Quando l'utente finale desidera che la società di installazione fornisca il servizio di installazione o la società di installazione assegni il dipendente che si occupi dell'installazione del dispositivo dell'utente finale specificato, l'amministratore di installazione o l'installatore con la relativa autorizzazione 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. Fare clic sulla scheda Site nella schermata principale per accedere alla pagina Site.
- 2. Fare clic su Add New Site, quindi selezionare New Site.

iNota

Se una piattaforma esistente dell'utente finale non è assegnata ad alcuna azienda di installazione, è possibile selezionare **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.

iNota

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.

iNota

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

Cerca piattaforma	Inserire le parole chiave nel campo di ricerca e fare clic su $ {f Q} $ per visualizzare i risultati nell'elenco.
Visualizza dettagli	Fare clic sul nome della piattaforma per visualizzarne i dettagli tra cui
della piattaforma	i dispositivi gestiti, le informazioni sulla piattaforma e così via.

Modifica piattaforma	Nell'area a destra della pagina Site Details, fare clic su 🖉 per modificare il nome, l'indirizzo, la città, lo stato/la provincia/l'area geografica della piattaforma e scegliere se spuntare la casella Sync Time & Time Zone to Device .		
Elimina piattaforma	Passare il cursore su \cdots nella colonna Operation e fare clic su $\bar{\mathbb{II}}$ per eliminare la piattaforma.		
Invita proprietario piattaforma	Per le piattaforme con lo stato Not Invited , fare clic su 2, nella colonna Operation sulla pagina Site o fare clic su Invite nella pagina Site Details per invitare un utente finale a diventare proprietario della piattaforma.		
	Per i dettagli, fare riferimento alla sezione <i>Invio della richiesta per diventare proprietario della piattaforma</i> .		
Gestisci dispositivo	Per le piattaforme con lo stato Not Invited , Not Registered , Not Accepted o Authorized and Monitoring , è possibile fare clic sull'icona corrispondente nella colonna Operation o 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.		
	I Nota		
	Per i dettagli, fare riferimento alla sezione <i>Gestione di un dispositivo</i> .		

6.3 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. Fare clic sulla scheda Site nella schermata principale per accedere alla pagina Site.
- 2. Fare clic su Add New Site, quindi selezionare Existing Site.

Add New Site	\times
Add New Site	
New Site • Existing Site	
* Site ID:	
. When a site is not authorized to a company, you can get the site ID from sit	e
owner for managing the site.Site owner can view site ID via Hik-Connect mobile client.	
OK	

Figura 6-2 Aggiunta di una piattaforma esistente

3. Inserire l'ID della piattaforma fornito.

iNota

- È possibile ottenere l'ID della piattaforma dal proprietario, che può 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.
- 4. Fare clic su **OK**.

La piattaforma verrà aggiunta nell'elenco delle piattaforme e il proprietario riceverà una richiesta. Una volta che l'approverà, la piattaforma sarà autorizzata dall'installatore.

6.4 Assegnazione della piattaforma all'installatore

L'amministratore di installazione o gli installatori con autorizzazione all'assegnazione della piattaforma possono assegnare una piattaforma all'installatore specificato come responsabile per la gestione della piattaforma e le configurazioni dei dispositivi contenuti.

Prima di iniziare

Assicurarsi di disporre delle autorizzazioni per l'assegnazione della piattaforma.

Passaggi

- 1. Fare clic sulla scheda Site nella schermata principale per accedere alla pagina Site.
- 2. Selezionare una piattaforma da assegnare.
- 3. Fare clic su Assign.
- 4. Selezionare un installatore come gestore della piattaforma.
- 5. Fare clic su OK.

Il gestore della piattaforma assegnato può accedere ai dettagli della piattaforma ed eseguire le operazioni relative, come ad esempio aggiungere dispositivi.

6.5 Invio della richiesta per diventare proprietario della piattaforma

Dopo che l'azienda incaricata ha completato l'installazione, l'installatore deve invitare l'utente finale a diventare 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. Fare clic sulla scheda Site nella schermata principale per accedere alla pagina Site.
- 2. Selezionare una piattaforma per l'invito.
- 3. Accedere alla pagina Invita proprietario piattaforma.
 - Selezionare una piattaforma e fare clic su 2, nella colonna Operation.
 - Fare clic sul nome della piattaforma per accedere alla pagina Site Details e fare clic su Invite.
- 4. 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.

iNota

Quando questa funzione è attiva e la piattaforma è stata consegnata, se necessario, è possibile accedere alla pagina Site Details e fare clic sulla scheda **Device** per disattivare il servizio Hik-Connect su uno o tutti i dispositivi presenti su tale piattaforma selezionando \mathcal{R} 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.

	Hik-Connect Service 🕚
DS-2CD2043GO-I	父
	\$\$ E\$ \$
DS-2CD4B26FWD-IZ(E35039529)	

Figura 6-3 Disattivazione del servizio Hik-Connect

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

iNota

- È possibile 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.

- 8. Inserire i commenti, ad esempio il motivo dell'invito, che l'utente può visualizzare quando riceve tale invito tramite il client mobile Hik-Connect.
- 9. Fare clic su **OK** 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.

iNota

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.

10. Opzionale: prima che l'utente finale accetti l'invito, fare clic su **Invite Again** per inviarlo di nuovo.

iNota

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

6.6 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. Fare clic sulla scheda Site nella schermata principale per accedere alla pagina Site.
- 2. Selezionare una piattaforma.
- 3. Accedere alla pagina Richiedi autorizzazione.
 - Selezionare una piattaforma e fare clic su 🍰 nella colonna Operation.
 - Fare clic sul nome della piattaforma per accedere alla pagina Site Details e fare clic su Apply for Authorization.
- 4. Inserire i commenti e fare clic su **OK** per inviare la richiesta.

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.

- 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.
- 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.
- 5. Opzionale: fare clic sul nome della piattaforma e accedere alla pagina Dettagli piattaforma e richiedere l'autorizzazione.

Capitolo 7 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 e campanelli. Una volta aggiunti al sistema, è possibile gestire e configurare le impostazioni necessarie dei dispositivi, tra cui la configurazione da remoto dei parametri, la configurazione della regola di eccezione, la configurazione della regola di collegamento, il conteggio delle persone, il monitoraggio della temperatura, ecc.

iNota

Alcune funzioni potrebbero non essere disponibili in determinati Paesi e regioni.

7.1 Aggiunta di un dispositivo

Sono disponibili tre modi per aggiungere i dispositivi alla piattaforma. 1. Aggiunta dei dispositivi rilevati online. 2. Aggiunta dei dispositivi tramite Hik-Connect (P2P). 3. Aggiunta di un singolo dispositivo o importazione di più dispositivi in un batch tramite l'indirizzo IP del dispositivo o il nome di dominio.

7.1.1 Aggiunta dei dispositivi rilevati online

Il Portale può rilevare i dispositivi disponibili connessi alla sua stessa rete, il che gli consente di riconoscere le informazioni relative ai dispositivi (ad esempio, l'indirizzo IP). In base alle informazioni, è possibile aggiungere rapidamente i dispositivi.

iNota

- Accertarsi che i dispositivi che si utilizzeranno siano correttamente installati e connessi alla rete secondo le specifiche dei produttori.
- È' possibile aggiungere e rilevare contemporaneamente fino a 15 dispositivi online.

Fare clic su **Site** a sinistra per visualizzare l'elenco delle piattaforme. A questo punto, prima di aggiungere i dispositivi online, accedere alla pagina Online Device utilizzando una delle due modalità indicate di seguito.

- Fare clic su + nella colonna Operation dell'elenco delle piattaforme e selezionare **Online Device**.
- Fare clic sul nome della piattaforma per accedere alla pagina Site List, quindi andare a Device → Add Device → Online Device.

I dispositivi connessi alla stessa LAN del Portale vengono visualizzati nell'elenco dei dispositivi sulla pagina Device. Qui è possibile trovare il numero di serie e l'indirizzo IP del dispositivo, lo stato di attivazione (attivato o non), lo stato di Hik-Connect (connesso al servizio Hik-Connect o non), ecc.

Controllare i dispositivi online da aggiungere e fare clic su **Add**. Prima di poter aggiungere i dispositivi, effettuare alcune o tutte e 4 le operazioni riportate di seguito in base allo stato dei dispositivi.**Tabella 7-1 Descrizione dei passaggi**

Passaggio	Descrizione		
	Se sono presenti dispositivi non attivati, attivarli. Per i dettagli, fare riferimento alla sezione Attivazione del dispositivo .		
Attiva dispositivo	Durante l'attivazione, sarà attivato automaticamente il protocollo di configurazione dell'host dinamico (DHCP) in modo da allocare gli indirizzi IP del dispositivo. Dopo l'attivazione, se necessario, è possibile fare clic su ∠ nella colonna Operation dell'elenco dei dispositivi online per disabilitare manualmente il DHCP.		
Inserimento della password del dispositivo	Inserire la password dell'amministratore del dispositivo. Per i dettagli, fare riferimento alla sezione <i>Inserimento della password</i> .		
Connessione automatica al servizio Hik-Connect	Connettere i dispositivi al servizio Hik-Connect. Per i dettagli, fare riferimento alla sezione <i>Connessione al servizio Hik-Connect</i> .		
Acquisizione automatica del codice di verifica del	Se un dispositivo è connesso correttamente al servizio Hik-Connect, il sistema acquisisce automaticamente il suo codice di verifica.		
dispositivo	Per i dettagli, fare riferimento alla sezione Acquisizione del codice di verifica del dispositivo.		

- 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.

Una volta aggiunti i dispositivi al Portale, se necessario, è possibile effettuare le seguenti operazioni.

Operazione	Descrizione
Modifica del dispositivo	Fare clic sul nome del dispositivo e modificarlo. In alternativa, è possibile spostare il cursore sul dispositivo e poi fare clic su per modificarne il nome.
	Fare clic su 🗟 per configurare la regola di collegamento del dispositivo.
Configurazione della regola di collegamento	I Nota Per i dettagli, fare riferimento alla sezione Aggiunta di regole di collegamento personalizzate .
	Attivare la funzione Health Monitoring Service per abilitare il servizio di monitoraggio dello stato sul dispositivo.
Attivazione del servizio di monitoraggio dello stato	 Nota Assicurarsi che la capacità relativa al dispositivo del pacchetto di monitoraggio acquistato sia sufficiente, altrimenti questa funzione non sarà disponibile. Il servizio di monitoraggio dello stato è disponibile solo in determinati Paesi e aree geografiche. Per i dettagli sul servizio di monitoraggio dello stato, fare riferimento alla sezione <i>Servizio di monitoraggio dello stato</i>.
	Fare clic su … → 両 per eliminare il dispositivo.
Eliminazione dei dispositivi	Se la piattaforma dispone dell'autorizzazione, non è possibile eliminare il dispositivo.

Tabella 7-2 Operazioni disponibili dopo l'aggiunta di dispositivi

Operazione	Descrizione	
	Dopo aver aggiunto il dispositivo, la piattaforma 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.	
Aggiornamento del firmware del dispositivo	È necessario aggiornare i dispositivi incompatibili con Hik-ProConnect.	
	 Selezionare Upgrade to Compatible Version nella colonna Upgrade or Not, quindi fare clic su Add and Upgrade. Inserire il nome utente e la password per aggiungere e aggiornare il 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. Fare clic su Set Device Type e selezionare un tipo di dispositivo dall'elenco a discesa. Dopo la selezione, sarà possibile modificarlo nuovamente.	
Scollegamento di un dispositivo dal relativo account corrente	Se la procedura di aggiunta di un dispositivo non è andata a buon fine e questo è stato aggiunto a un altro account, è possibile fare clic su reference per scollegarlo. Una volta scollegato, possibile aggiungere il dispositivo all'account. Per i dettagli su come scollegare un dispositivo, fare riferimento alla sezione Scollegamento di un dispositivo dal relativo account corrente	

Attiva dispositivo

Se sono presenti dei dispositivi non attivi tra i dispositivi selezionati, per attivarli è necessario creare una password di amministratore per tutti i dispositivi non attivi.

iNota

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.

Inserimento della password del dispositivo

Per i dispositivi attivati ma non connessi al servizio Hik-Connect, è necessario inserire la password dell'amministratore nella finestra a comparsa. La password dell'amministratore viene creata all'attivazione del dispositivo.

Se la stessa password è condivisa con più dispositivi, abilitare l'opzione **Batch Enter admin Password** per inserire la password per tutti i dispositivi in un batch. Se le password dei dispositivi sono errate, viene richiesto di inserire quelle corrette.

iNota

Prima di inserire la password amministratore, assicurarsi che i dispositivi abbiano indirizzi IP diversi poiché non è possibile aggiungere quelli con indirizzi IP uguali. Fare clic su 🖉 nella colonna Operation, quindi modificare l'indirizzo IP del dispositivo.

Connetti al servizio Hik-Connect

Dopo aver inserito le password amministratore del dispositivo, il sistema avvierà automaticamente la connessione al servizio Hik-Connect. Non è possibile aggiungere i dispositivi che non si connettono al servizio Hik-Connect.

iNota

Per evitare che si verifichi un'eccezione di connessione, assicurarsi che i dispositivi abbiano indirizzi IP diversi e che quelli dei dispositivi da collegare si trovino nello stesso segmento di rete del computer su cui è in esecuzione Hik-ProConnect. Fare clic su ∠ nella colonna Operation, quindi modificare l'indirizzo IP del dispositivo.

Acquisizione del codice di verifica del dispositivo

Se un dispositivo è connesso correttamente al servizio Hik-Connect, il sistema acquisisce automaticamente il suo codice di verifica. Se il sistema non riesce ad acquisire i codici di verifica dei dispositivi, è necessario inserirli manualmente.

Se lo stesso codice di verifica è condiviso da più dispositivi, abilitare **Batch Enter Verification Code** e inserire il codice di verifica per tutti.

iNota

Per i dispositivi EZVIZ non è richiesta la password amministratore, ma è necessario disporre del codice di verifica.

7.1.2 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.
- Il dispositivo deve essere stato attivato e connesso al servizio Hik-Connect.

Passaggi

- 1. Fare clic su **Site** a sinistra per visualizzare l'elenco delle piattaforme.
- 2. Aprire la pagina Aggiunta manuale.
 - Fare clic su + nella colonna Operation dell'elenco delle piattaforme e selezionare Manual Adding.
 - − Fare clic sul nome della piattaforma per accedere alla pagina Site List, quindi andare a Device
 → Add Device → Manual Adding.
- 3. Selezionare Hik-Connect (P2P) come modalità di aggiunta.
- 4. Inserire il numero di serie e il codice di verifica del dispositivo.

iNota

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.

5. Fare clic su Next.

iNota

Hik-ProConnect inizia a controllare la compatibilità della versione del firmware del dispositivo. Se il dispositivo non è compatibile con Hik-ProConnect, non è possibile utilizzare alcune funzioni (tra cui il monitoraggio dello stato, la regola di collegamento e la configurazione da remoto). Se la piattaforma dispone dell'autorizzazione, il controllo della versione del firmware non viene effettuato. È necessario aggiornare i dispositivi incompatibili con Hik-ProConnect.

- 1) Selezionare Upgrade to Compatible Version nella colonna Upgrade or Not, quindi fare clic su Add and Upgrade.
- 2) Inserire il nome utente e la password per aggiungere e aggiornare il dispositivo.

6. Selezionare il dispositivo da aggiungere.

iNota

La casella **Enable Health Monitoring Service** è selezionata per impostazione predefinita e non può essere modificata. 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.

7. Fare clic su Add.

- 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.

Modifica nome dispositivo	Fare clic sul nome del dispositivo e modificarlo. In alternativa, è possibile spostare il cursore sul dispositivo e poi fare clic su ∠ per modificarlo.
Eliminazione dei dispositivi	Fare clic su $\rightarrow \overline{\square}$.
Aggiornamento del dispositivo	Fare riferimento alla sezione Aggiornamento del firmware 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. Fare clic su Set Device Type e selezionare un tipo di dispositivo dall'elenco a discesa. Dopo la selezione, sarà possibile modificarlo nuovamente.
Visualizzazione dello stato del DDNS	Fare clic su ••• e passare il cursore su ﷺ. Per i dettagli su come configurare il DDNS, fare riferimento alla sezione Configurazione del DDNS dei dispositivi .

Attivazione del servizio di	Attivare la funzione Health Monitoring Service per abilitare il servizio di monitoraggio dello stato sul dispositivo.	
monitoraggio dello stato	i Nota	
	 Assicurarsi che la capacità relativa al dispositivo del pacchetto di monitoraggio acquistato sia sufficiente, altrimenti questa funzione non sarà disponibile. 	
	 Il servizio di monitoraggio dello stato è disponibile solo in determinati Paesi e aree geografiche. 	
	 Per i dettagli sul servizio di monitoraggio dello stato, fare riferimento alla sezione Servizio di monitoraggio dello stato. 	
Configurazione del servizio di archiviazione cloud	Per Hik-ProConnect Box e i DVR cloud, è possibile fare clic su Cloud Storage Service per configurare il servizio di archiviazione cloud. Per i dettagli, fare riferimento alle sezioni <i>Impostazione dell'archiviazione</i>	
	cloud per Hik-ProConnect Box e Impostazione dell'archiviazione cloud per i DVR cloud.	

iNota

Se la piattaforma dispone dell'autorizzazione, non è possibile eliminare il dispositivo (eccetto i dispositivi aggiunti tramite IP/dominio).

7.1.3 Aggiunta di dispositivi tramite l'indirizzo IP o il nome di 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

iNota

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

- 1. Fare clic su **Site** a sinistra per visualizzare l'elenco delle piattaforme.
- 2. Aprire la pagina Aggiunta manuale.
 - Fare clic su + nella colonna Operation dell'elenco delle piattaforme e selezionare Manual Adding.

- − Fare clic sul nome della piattaforma per accedere alla pagina Site List, quindi andare a Device
 → Add Device → Manual Adding.
- 3. Selezionare IP/Domain come modalità di aggiunta.
- 4. Inserire il nome, l'indirizzo IP/il nome di dominio, il numero di porta, il nome utente e la password del dispositivo.

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.

5. Fare clic su Add.

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

Camera Online	0
IP/Domain: Device Type: Unknown 🕕	
The device's QR code.	E ···

Figura 7-1 Codice QR del dispositivo aggiunto

OperationsDescriptio nCrittografia del codice QR del dispositivo	 Un codice QR viene generato e visualizzato nell'area relativa alle informazioni 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. 1. Fare clic su per visualizzare il codice QR. 2. Inserire una password per crittografare il codice QR, quindi fare clic su Save.
Visualizzazione e modifica delle informazioni del dispositivo	 Fare clic sull'indirizzo IP o sul nome di dominio del dispositivo per visualizzare le sue informazioni di base. Se le informazioni del dispositivo sono state modificate o si verifica un'eccezione di rete, è possibile cambiarle di conseguenza. Selezionare un dispositivo e fare clic su ••• → ∠ per modificarne il nome, l'indirizzo IP/nome di dominio, il numero di porta, il nome utente e la password.

Impostazione del tipo per un dispositivo sconosciuto	Se dopo aver aggiunto il dispositivo Hik-ProConnect non ne riconosce il tipo, è possibile impostarlo manualmente. Fare clic su Set Device Type e selezionare un tipo di dispositivo dall'elenco a discesa. Dopo la selezione, sarà possibile modificarlo nuovamente.	
Attivazione del servizio di monitoraggio dello stato	Attivare la funzione Health Monitoring Service per abilitare il servizio di monitoraggio dello stato sul dispositivo.	
	i Nota	
	 Assicurarsi che la capacità relativa al dispositivo del pacchetto di monitoraggio acquistato sia sufficiente, altrimenti questa funzione non sarà disponibile. 	
	 Il servizio di monitoraggio dello stato è disponibile solo in determinati Paesi e aree geografiche. 	
	 Per i dettagli sul servizio di monitoraggio dello stato, fare riferimento alla sezione Servizio di monitoraggio dello stato. 	

Elimina dispositivo Fare clic su $\bullet \bullet \bullet \rightarrow \overline{\square}$.

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

7.1.4 Aggiunta di dispositivi in un batch

È possibile aggiungere più dispositivi al client in un batch inserendo i loro parametri in un modello predefinito.

Prima di iniziare

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

Passaggi

iNota

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

- 1. Fare clic su Site a sinistra per visualizzare l'elenco delle piattaforme.
- 2. Aprire la pagina Aggiunta manuale.
 - Fare clic su + nella colonna Operation dell'elenco delle piattaforme e selezionare Manual Adding.
 - Fare clic sul nome della piattaforma per accedere alla pagina Site List, quindi andare a Device → Add Device → Manual Adding.
- 3. Selezionare **Batch Import** come modalità di aggiunta.
- 4. Fare clic su **Download Template** e salvare il modello predefinito (file CSV) sul computer.
- 5. Aprire il modello scaricato e inserire le informazioni richieste relative ai dispositivi da aggiungere nella colonna corrispondente.
- 6. Fare clic su Upload Template per caricare il modello modificato su Hik-ProConnect.
- 7. Se necessario, dopo aver aggiunto il dispositivo, effettuare le seguenti operazioni.



Figura 7-2 Codice QR del dispositivo aggiunto

OperationsDescriptio nCrittografia del codice QR del dispositivo Un codice QR viene generato e visualizzato nell'area relativa alle informazioni 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 Hik-Connect.

- 1. Fare clic su 🔡 per visualizzare il codice QR.
- 2. Inserire una password per crittografare il codice QR, quindi fare clic su **Save**.

Visualizzazione e modifica delle informazioni del dispositivo	Fare clic sull'indirizzo IP o sul nome di dominio del dispositivo per visualizzare le sue informazioni di base. Se le informazioni del dispositivo sono state modificate o si verifica un'eccezione di rete, è possibile cambiarle di conseguenza. Selezionare un dispositivo e fare clic su $\bullet \bullet \bullet \neq \mathbb{Z}$ per modificarne il nome, l'indirizzo IP/nome di dominio, il numero di porta, il nome utente e la password.
Impostazione del	Se dopo aver aggiunto il dispositivo Hik-ProConnect non ne riconosce
tipo per un	il tipo, è possibile impostarlo manualmente. Fare clic su Set Device
dispositivo	Type e selezionare un tipo di dispositivo dall'elenco a discesa. Dopo la
sconosciuto	selezione, sarà possibile modificarlo nuovamente.
Elimina dispositivo	Fare clic su $\bullet \bullet \bullet \Rightarrow \square$.

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

7.2 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. Fare clic sul nome di una piattaforma per accedere alla pagina dei relativi dettagli.
- 2. Nella scheda **Device**, fare clic su **Apply for Permission** → **Apply for Configuration Permission/Apply for Live View Permission/Apply for Playback Permission**.
- 3. Selezionare i dispositivi per cui si desidera richiedere l'autorizzazione e fare clic su Apply.
- 4. Nell'elenco a discesa Validity Period, selezionare un periodo di validità per l'autorizzazione.

iNota

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 **Apply** per richiedere l'autorizzazione all'utente finale.

Se l'utente finale approva la richiesta, si ottengono le autorizzazioni corrispondenti.

7.3 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 consegnata.

Passaggi

- 1. Fare clic su una piattaforma nel relativo elenco per accedere alla pagina Site Details.
- 2. Fare clic su un dispositivo per visualizzare la pagina Device Details.
- 3. Nell'area Permission, selezionare un'autorizzazione e fare clic su $\Im \rightarrow OK$ per approvarla.

- 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.

7.4 Migrazione di dispositivi dall'account Hik-Connect

È possibile effettuare la migrazione dei dispositivi presenti nell'account Hik-Connect all'account Hik-ProConnect. Dopo il trasferimento si potranno ancora gestire i dispositivi nel proprio account Hik-Connect e sarà possibile continuare a utilizzare il servizio Hik-Connect.

Nei due casi seguenti, è necessario effettuare la migrazione dei dispositivi dall'account Hik-Connect a Hik-ProConnect.

- **Caso 1**: Prima di utilizzare Hik-ProConnect, l'installatore ha gestito i dispositivi dell'utente finale tramite il client mobile Hik-Connect dopo che l'utente finale li ha condivisi con l'account Hik-Connect dell'installatore.
- **Caso 2**: prima di utilizzare Hik-ProConnect, l'installatore ha già un account Hik-Connect a cui ha aggiunto i dispositivi.

Nelle due circostanze appena descritte, è possibile effettuare la migrazione di questi dispositivi (inclusi quelli condivisi dagli utenti finali con l'installatore o quelli aggiunti nell'account Hik-Connect di quest'ultimo) all'account Hik-ProConnect al fine di aggiungerli rapidamente e comodamente nonché migliorarne la gestione e la manutenzione.



Figura 7-3 Migrazione dei dispositivi dall'account Hik-Connect a Hik-ProConnect

Esistono tre modi per aprire la finestra Hik-Connect Device Migration.

- Nella schermata principale, fare clic sul nome nell'angolo in alto a destra e selezionare **Hik-Connect Device Migration**.
- Nella schermata principale, fare clic su Migrate Devices from Hik-Connect Account in Frequently Used Functions.
- Nella pagina Site, fare clic su **Migrate Devices from Hik-Connect account** nella parte superiore dell'elenco delle piattaforme.

Accedere all'account Hik-Connect

Innanzitutto, è necessario accedere all'account Hik-Connect.

1 Log into Hik-Connect Account	Select Device	Configure Site	Finish
	Log into your Hik	-Connect account.	
	🔋 Phone Number	💙 User Name/Email	
	* Account Singapore +65 🗸	Enter Phone Number	
	* Password		
	Authori	ze and Login	
	Allow Following Opera	tions:	
	Get Your Account Info Information	rmation and Device	

Figura 7-4 Accesso all'account Hik-Connect

È possibile effettuare l'accesso utilizzando il numero di telefono o il nome utente (oppure l'indirizzo e-mail).

Selezionare **Get Your account Information and Device Information** per consentire a Hik-ProConnect di ottenere queste informazioni, quindi fare clic su **Authorize and Login** per accedere all'account Hik-Connect.

Selezione dei dispositivi da migrare

In secondo luogo, è necessario selezionare i dispositivi da migrare.

Dopo l'accesso, i dispositivi aggiunti all'account Hik-Connect e quelli condivisi con l'installatore vengono visualizzati nell'elenco dei dispositivi. Tale elenco non comprende quelli già aggiunti a Hik-ProConnect.

È possibile filtrare i dispositivi selezionando **Show All Devices**, **Show My Devices Only** (i dispositivi aggiunti all'account Hik-Connect) o **Show Others' Devices Only** (i dispositivi condivisi dall'utente finale con l'account Hik-Connect dell'installatore) nell'elenco a discesa.

Selezionare i dispositivi da migrare su Hik-ProConnect e fare clic su Next.

Configurazione della piattaforma per i dispositivi in My Devices

In terzo luogo, per consentire la migrazione dei dispositivi, è necessario impostare le informazioni relative alla piattaforma su Hik-ProConnect.

È possibile aggiungere i dispositivi inseriti nell'account Hik-Connect (visualizzato nell'elenco My Devices) alla stessa o a diverse piattaforme in base alle proprie esigenze.

		1 — Log into Hik-Com Account	nect Select Device	3 Configure Site	(4) Finish			
Site Time Zone	ur devices will be migrat (UTC+08:00) Beijing, Cl	ed to installer account) and the following sites will be created	The devices will be assig	gned to these sites. For o	thers' devices, authorization	is required before migration.	
My Devic	e Add to Difference	ent Sites () A	dd to the Same Site	Number	of Devices	Apply for Permission		*
Migrate	d Site 1		(UTC+08:00) Beijing, Chongqing, H	H 🗸 1 in Tota	al 🗸	You have site authorizatio permission by default.	n, configuration, and live view	
Migrate	d Site 2		(UTC+08:00) Beijing, Chongqing, H	H 💙 1 in Tot	al 🗸	You have site authorizatio permission by default.	n, configuration, and live view	
Others' D	evice 🚯 The	user will receive a notification	on Hik-Connect Mobile Client. After authorizatio	n, you can manage the de	vices on Hik-ProConnect.			*
Site Na	ime	Site Owner 1	ime Zone	Number of Dev	Apply for Permissi	on		
🖌 Site,			(UTC+08:00) Beijing, Chongqing, H 🗸	2 in Total 🗸	Site Authorization	Configuration ~	✓ Live View ✓	
						Previous	Migrate	

Figura 7-5 Configurazione della piattaforma per i dispositivi in My Devices

Aggiungi a diverse piattaforme

Se i dispositivi sono condivisi con diversi utenti finali, selezionare questa opzione per aggiungerli a piattaforme differenti.

Per i dispositivi condivisi con gli utenti finali, il sistema crea automaticamente delle piattaforme utilizzando i nomi di tali utenti, quindi assegna i dispositivi alle piattaforme create. Se esiste già una piattaforma il cui proprietario è l'utente finale, vengono visualizzate le informazioni relative a tale piattaforma (nome e fuso orario) e vengono aggiunti automaticamente i dispositivi corrispondenti.

Per i dispositivi non condivisi, il sistema crea automaticamente una piattaforma denominata in base al nome utente dell'account Hik-Connect, quindi li assegna a tale piattaforma. È possibile passare il mouse sul nome della piattaforma e fare clic su *e* per modificarlo.

Aggiungi alla stessa piattaforma

È inoltre possibile aggiungere questi dispositivi alla stessa piattaforma. Il sistema crea automaticamente una piattaforma denominata in base al nome utente dell'account Hik-Connect, quindi aggiunge tutti i dispositivi selezionati a tale piattaforma.

È possibile passare il mouse sul nome della piattaforma e fare clic su *e* per modificarlo. Per impostazione predefinita, dopo la migrazione, si dispone dell'autorizzazione per accedere alle piattaforme create automaticamente, nonché quella per configurare e visualizzare i dispositivi in tempo reale nell'elenco My Devices.

Configurazione della piattaforma e delle autorizzazioni per i dispositivi in Others' Devices

In quarto luogo, è necessario impostare sia le informazioni relative alla piattaforma su Hik-ProConnect sia l'autorizzazione per i dispositivi condivisi.

🚯 Your devices will b	Log into Hik-Com Account	ect Select Device	3 Configure Site	G Finish here sites. For others' devices, authorizati	
Site Time Zone (UTC+08:00) Br	eijing, Chongqing, Hong Kong,	sho the following sites will be bread	o, the devices will be assigned to t		on a required before migration.
My Device Add t	to Different Sites 🚺 🛛 🔿 A	dd to the Same Site			*
Site Name	Site Owner	Time Zone	Number of Devi	ces Apply for Permission	
Migrated Site 1		(UTC+08:00) Beijing, Chongqing,	H 🗸 1 in Total 🗸	You have site authorizat permission by default.	ion, configuration, and live view
Migrated Site 2		(UTC+08:00) Beijing, Chongqing,	H 🗸 1 in Total 🗸	You have site authorizat permission by default.	ion, configuration, and live view
Others' Device	The user will receive a notification	on Hik-Connect Mobile Client. After authorizat	on, you can manage the devices on H	ilk-ProConnect.	*
Site,	[(UTC+08:00) Beijing, Chongqing, H 🗸	2 in Total 🗸 🖉 Si	te Authorization	✓ Live View ✓
				Previous	Migrate

Figura 7-6 Configurazione della piattaforma e delle autorizzazioni per i dispositivi in Others' Devices

I dispositivi condivisi con l'installatore dagli utenti finali (visualizzati nell'elenco Others' Devices) vengono aggiunti a diverse piattaforme. Il sistema crea automaticamente delle piattaforme denominate in base ai nomi degli utenti finali, quindi aggiunge tutti i dispositivi selezionati a tali piattaforme. Se esiste già una piattaforma il cui proprietario è l'utente finale, vengono visualizzate le informazioni relative a tale piattaforma (nome e fuso orario) e vengono aggiunti automaticamente i dispositivi corrispondenti.

È possibile passare il mouse sul nome della piattaforma e fare clic su Z per modificarlo. Nell'elenco **Apply for Permission**, è necessario selezionare le autorizzazioni da richiedere agli utenti finali per l'accesso ai dispositivi. Per impostazione predefinita, si dispone dell'autorizzazione di accesso alle piattaforme create automaticamente. Dopo la migrazione, gli utenti finali riceveranno una notifica sul client mobile Hik-Connect. Dopo che gli utenti finali approveranno l'autorizzazione, sarà possibile gestire i dispositivi su Hik-ProConnect.

Impostazione del fuso orario

In quinto luogo, è possibile impostare il fuso orario dei dispositivi, se necessario. È possibile impostare il fuso orario per ciascun dispositivo oppure selezionarne uno nell'elenco a discesa **Set Time Zone** nell'angolo in alto a sinistra per impostare quello dei dispositivi in un batch.

Avvio della migrazione

Infine, avviare la migrazione dei dispositivi.

Dopo aver impostato le autorizzazioni per l'accesso alle piattaforme e ai dispositivi, selezionare i dispositivi nell'elenco My Devices e Others' Devices e fare clic su **Migrate** per avviare la migrazione.

Il sistema invia una richiesta agli utenti finali per i dispositivi condivisi da loro nell'elenco Others' Devices. Dopo che gli utenti finali avranno approvato la richiesta di autorizzazione, i dispositivi saranno trasferiti.

Fare clic su **Continue** per selezionare altri dispositivi da migrare oppure fare clic su **Finish and View** per visualizzare quelli migrati dopo la creazione delle piattaforme nel relativo elenco.

7.5 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 7-7 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.

7.5.1 Aggiunta di una regola di collegamento personalizzata

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

Passaggi

iNota

- Se il periodo di prova dell'account 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.
- Se la sorgente o la risorsa collegata è un pannello di controllo di sicurezza Axiom, quando la modalità conforme a EN50131 è abilitata sul dispositivo, assicurarsi di aver effettuato l'autenticazione inserendo la password del dispositivo, altrimenti non è possibile eseguire la configurazione della regola di collegamento.
- 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. Fare clic su Site per accedere alla pagina Site List.
- 2. Aprire il pannello Add Linkage Rule.
 - Selezionare una piattaforma e fare clic su $\rightarrow \mathbb{R}$ nella colonna Operation.
 - Fare clic sul nome di una piattaforma per accedere alla pagina Site Details, quindi fare clic su Linkage Rule → Add Linkage Rule.
 - Fare clic sul nome di una piattaforma per accedere alla pagina Site Details, quindi selezionare un dispositivo e fare clic su <a>[].
- 3. Impostare le informazioni necessarie.

Nome regola di collegamento

Creare un nome per la regola di collegamento.

Pulsante di attivazione

Definire cosa attiva l'azione di collegamento.

Seleziona sorgente

Select a resource as the Source.

Imposta evento di attivazione

Selezionare un evento come evento di attivazione.

iNota

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

Risorsa	Abilitazione evento
Telecamera	 Rilevamento di movimenti Rilevamento volti Intrusione Rilevamento attraversamento linea
Dispositivo di controllo degli accessi	Allarme anti-manomissione
Porta collegata a dispositivo di controllo degli accessi	 Anomalia nell'apertura della porta Allarme anti-manomissione
Postazione porta	• Chiamata
Area del pannello di controllo di sicurezza	 Inserimento modalità assenza Disinserito Inserimento parziale Alarm, ad esempio Instant Zone Alarm, 24-Hour Annunciating Zone Alarm e Delayed Zone Alarm.
zona (rilevatore) collegata al pannello di controllo di sicurezza	 Alarm, ad esempio Triggering Alarm, come Instant Zone Alarm, 24-Hour Annunciating Zone Alarm e Delayed Zone Alarm.
Campanello	ChiamataRilevamento PIR

Tabella 7-3 Eventi di attivazione	disponibili p	er tini diversi	di risorse
	alspointsin p		ur 113013C

impostazioni

Fare clic su Add per selezionare le azioni di collegamento e le risorse collegate.

iNota

- Una volta selezionata un'azione di collegamento, vengono visualizzate le risorse disponibili da impostare come risorse collegate.
- È possibile selezionare fino a 128 azioni di collegamento o 10 risorse collegate.

Azione di collegamento

Selezionare le azioni di collegamento.

Risorsa collegata	Azione di collegamento	Descrizione	
	Capture	La telecamera acquisisce un'immagine quando rileva l'evento di attivazione.	
		La telecamera registra un video quando rileva l'evento di attivazione.	
		i Nota	
	Recording	Il video registrato inizia 5 secondi prima del rilevamento dell'evento di attivazione e dura 30 secondi.	
Telecamera (canale)	Richiamo di valori preconfigurati	Selezionare un preset dall'elenco a discesa relativo in modo che venga richiamato quando si rileva un evento di attivazione.	
		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.	
		i Nota	
		Assicurarsi di aver configurato i preset della telecamera PTZ. Per i dettagli, consultare il manuale d'uso della telecamera PTZ.	

Risorsa collegata	Azione di collegamento	Descrizione
		Selezionare un pattugliamento dall'elenco a discesa relativo in modo che venga richiamato quando si rileva un evento di attivazione.
Chiamata di pattugliamenti		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.
		i Nota Assicurarsi di aver configurato i pattugliamenti della telecamera PTZ. Per i dettagli, consultare il manuale d'uso della telecamera PTZ.
		Selezionare una sequenza dall'elenco a discesa relativo in modo che venga richiamata quando si rileva un evento di attivazione.
	Richiama sequenza	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.
		i Nota
		Assicurarsi di aver configurato la sequenza della telecamera PTZ. Per i dettagli, consultare il manuale d'uso della telecamera PTZ.
	Inserimento	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.
	Disinserisci	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.
	Abilita mascheramen	Il mascheramento della privacy sarà visualizzato sulle immagini in tempo reale della telecamera quando viene

Risorsa collegata	Azione di collegamento	Descrizione
	to privacy	rilevato un evento di attivazione.
		iNota Assicurarsi di aver configurato il mascheramento di privacy della telecamera. Per i dettagli, consultare il manuale d'uso della telecamera.
	Disabilita mascheramen to 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	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.
pannello di controllo di sicurezza	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	Open Door	La porta relativa al dispositivo di controllo accessi sarà attivata quando viene rilevato l'evento di attivazione.
collegata a dispositivo di controllo	Remain Open	La porta relativa al dispositivo di controllo accessi resterà aperta quando viene rilevato l'evento di attivazione.
degli accessi	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	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.
allarme	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.

Risorsa collegata

Selezionare le risorse come sorgente di attivazione dell'azione di collegamento.

iNota

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.

iNota

Dopo aver selezionato le azioni di collegamento e le risorse collegate, è possibile spuntare le caselle di controllo, quindi fare clic su **Delete** per eliminare le azioni di collegamento e le risorse di collegamento selezionati.

Programma di collegamento

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

Tutti i giorni

L'azione di collegamento esterno 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.

iNota

Le date contrassegnate in blu sono quelle selezionate.

4. Fare clic su OK.

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

5. Opzionale: se necessario, dopo aver aggiunto la regola di collegamento, effettuare le seguenti operazioni.

Modifica della regola di collegamento	Fare clic su $\rightarrow \mathbb{Z}$ per modificare la regola di collegamento.
Eliminazione della regola di collegamento	Fare clic su $\cdots \rightarrow \ensuremath{\bar{\mathbb{I}}}$ per eliminare la regola di collegamento.
Disattivazione della regola di collegamento	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*.

iNota

- 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 del Portale.

7.5.2 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**.

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).

Tabella 7-5 Descrizione dei modelli

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

iNota

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. Fare clic su ③ Site per accedere alla pagina Site List.
- 2. Aprire il pannello Add Linkage Rule.
 - Fare clic sul nome di una piattaforma per accedere alla pagina Site Details e selezionare la scheda Linkage Rule, quindi passare il cursore sul modello Forced Entry Alarm nella sezione Linkage Template e fare clic su Create by Template.
 - Fare clic su ··· → □ nella colonna Operation, quindi selezionare il modello Forced Entry
 Alarm a sinistra del pannello Add Linkage Rule.

Fare clic sul nome di una piattaforma per accedere alla pagina Site Details, quindi fare clic su
 External Linkage Rule → Add External Linkage Rule e poi selezionare il modello Forced Entry
 Alarm a sinistra del pannello Add Linkage Rule.

Customize Linkage Rule	Add Linkage Rule			
 ₽ Intrusion ● Carnera ● Alarm Output ● Hik-Connect Mobile Client 	 1. You cannot set linkage rules for: Devices with no configuration permission: Devices with health monitoring service disabled. 2. Make sure the notification of the device is enabled, or the linkage rule will not be activated. Linkage Rule Name 			
Forced Entry Alarm C Camera PTZ Access Control Device Alarm Output His Genera Multic Chart	 When Select ✓ Detects Intrusion 			
Hik-Connect Mobile Client	2 Trigger Following Actions			
	Sector → No device can be selected.			
 ▲ Back to Home/Office ● Disarm Camera ● Enable Privacy Mask 	Action Capture			
 Away Arm Camera Disable Privacy Mask 	Action Alarm Output			
	3 Linkage Schedule			
	Set Linkage Schedule			
 Visitor Calling Camera Hik-Connect Mobile Client 	All Days Custom			
	OK Cancel			

Figura 7-8 Aggiunta di una regola di collegamento in base a un modello

3. 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

Fare clic su **Select** per selezionare le risorse collegate utilizzate per attivare le azioni di collegamento, quindi fare clic su **Add**.

- 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.

iNota

Le date contrassegnate in blu sono quelle selezionate.

4. Fare clic su OK.

- La regola di collegamento viene visualizzata nell'elenco Linkage Rule.
- 5. 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 o dettagli, consultare la sezione **Attivazione della funzione che** consente al dispositivo di inviare notifiche.

iNota

- 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.

7.5.3 Tutorial video

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

7.6 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. 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 notifica. 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. Accedere al modulo Site.
- 2. Fare clic sul nome di una piattaforma per accedere alla pagina Site Details, quindi fare clic su **Exception**.

Le regole di eccezione di tutti i dispositivi aggiunti a questa piattaforma vengono visualizzate per impostazione predefinita.

3. Opzionale: Fare clic su **Unfold Channels** per visualizzare tutti i canali del dispositivo.

Esempio

Saranno visualizzate tutte le telecamere dei dispositivi di codifica. Saranno visualizzate tutte le zone e le uscite di allarme dei pannelli di controllo di sicurezza.

- 4. Impostare i tipi di eccezione in grado di attivare l'invio della notifica.
 - 1) Spostare il cursore sul campo **Exception** del dispositivo o del canale e fare clic su 🖉.

.u.⊚ ()							
Name	Exception	Received by	Recipient	Schedule			
[(All Exceptions	<u>/</u>	Site Manager				
Camera 01	All Exceptions		Site Manager	All Days			

Figura 7-9 Modifica dell'eccezione

2) Selezionare i tipi di eccezione per cui si desidera impostare le relative regole.

iNota

- 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.

3) Fare clic su **OK**.

- 5. Impostare la modalità di ricezione delle notifiche.
 - 1) Spostare il cursore sul campo **Received by** e fare clic su **2**.
 - 2) 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.

iNota

Per controllare le notifiche di eccezione ricevute dal Portale, fare riferimento alla sezione *Centro eccezioni*.

Client Mobile

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

E-mail

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

- 3) Fare clic su **OK**.
- 6. Impostare il destinatario delle notifiche.
 - 1) Spostare il cursore sul campo **Recipient** e fare clic su 🖉.
 - 2) Selezionare **Site Manager** o **Installer Admin**. Il destinatario riceve in tempo reale la notifica quando l'eccezione è rilevata.

iNota

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

- 3) Fare clic su **OK**.
- 7. Impostare l'ora in cui inviare le notifiche al destinatario.
 - 1) Spostare il cursore sul campo Schedule e fare clic su 🖉.
 - 2) Selezionare il programma.

Tutti i giorni

Il destinatario riceve le notifiche da lunedì a domenica, 7 giorni su 7, 24 ore su 24.

Custom

È possibile personalizzare i giorni e il periodi di tempo dei giorni selezionati in base alle esigenze.

- 3) Fare clic su **OK**.
- 8. Opzionale: impostare o modificare le regole di eccezione relative ai dispositivi presenti sulla piattaforma in un batch.
 - 1) Fare clic su Batch Edit.
 - 2) Selezionare i dispositivi o i canali per cui impostare le regole di eccezione.
 - 3) Fare clic su 🖉 nella parte inferiore per impostare/modificare i tipi di eccezione, la modalità di ricezione, il destinatario e l'ora di notifica.

Batch Edit	y to				Enable All			
	()				Enable			
Name	Exception	Received by	Recipient	Schedule				
Camera 01	(All Exceptions	e .	Site Manager	All Days				
Fold Channels : 1 🛠								
	()				Enable			
Name	Exception	Received by	Recipient	Schedule				
v	All Exceptions	e .	Site Manager	All Days				
Unfold Channels : 1 🛛								
All Exception	∠ Received by	🖉 Recipient	<u> </u>	<u>/</u>	OK Cancel			

Figura 7-10 Impostazione/modifica delle regole di eccezione in un batch

4) Fare clic su **OK** per salvare le impostazioni.

- 9. Opzionale: una volta impostata una regola, è possibile copiare le impostazioni delle regole su altri dispositivi o canali per effettuare delle impostazioni rapide.
 - 1) Fare clic su Copy to.
 - 2) Nel campo Copy Exception Settings from, selezionare i dispositivi o i canali come risorse.
 - 3) Nel campo To, selezionare le risorse target dello stesso tipo di quelle selezionate.
 - 4) Fare clic su **Copy** per copiare le impostazioni della regola sulle risorse target, quindi tornare all'elenco delle regole di eccezione. In alternativa, è possibile fare clic su **Copy and Continue** per copiare le impostazioni della regola e continuare a copiare le altre impostazioni.
- 10. Una volta impostata la regola di eccezione, è necessario attivare il pulsante **Enable** nell'angolo in alto a destra per abilitarla oppure **Enable All** per abilitare tutte le regole di eccezione dei dispositivi presenti nella piattaforma.

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.

7.7 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

iNota

Il dispositivo deve supportare questa funzione.

- 1. Fare clic su Site per accedere alla pagina Site List.
- 2. Fare clic su una piattaforma nel relativo elenco per accedere alla pagina Site Details.
- 3. Selezionare la scheda Device.
- 4. Fare clic su $\cdots \rightarrow \bigcirc$ per aprire la finestra Notification Settings.
- 5. Impostare i parametri.

Notifica

Verificare che la funzione sia abilitata.

Pianificazione notifiche

Dopo aver abilitato la funzione, impostare un orario in cui caricare gli eventi rilevati dalla sorgente sul sistema Hik-ProConnect e nel client mobile Hik-Connect.

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

6. Fare clic su **OK**.

- Dopo aver consegnato la piattaforma all'utente finale, ricordargli che la funzione che consente alla sorgente di inviare notifiche deve restare attiva sul client mobile Hik-Connect, altrimenti l'azione di collegamento NON viene abilitata, indipendentemente dal fatto che l'evento di attivazione venga rilevato o meno dalla 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.
7.8 Sistema di conteggio

La funzione di conteggio delle persone fornita dalla telecamera adibita a tale funzione viene utilizzata per calcolare il numero di persone che entrano, escono o passano attraverso un'area. Dopo aver aggiunto le telecamere di conteggio persone alle piattaforme di Hik-ProConnect, è possibile integrare le funzioni di conteggio delle persone di queste telecamere per implementare il monitoraggio in tempo reale della densità delle persone all'interno di un'area specifica. Ciò è utile nell'ambito di determinati scenari commerciali e di tutela della salute, ad esempio per limitare il flusso di clienti in un centro commerciale durante il periodo di saldi.

iNota

- La funzione di conteggio delle persone non è disponibile in determinati Paesi e regioni.
- La densità delle persone qui riportata si riferisce al numero di persone presenti nello stesso momento in un'area limitata.

7.8.1 Attivazione del servizio di conteggio delle persone per i canali

Se si desidera utilizzare le funzioni per il conteggio delle persone su Hik-Connect, occorre prima attivare il servizio di conteggio delle persone per i canali relativo alle telecamere di conteggio persone.

Prima di iniziare

- Assicurarsi di aver aggiunto le telecamere di conteggio persone alla piattaforma di destinazione. Per i dettagli, fare riferimento alla sezione **Aggiunta di un dispositivo**
- Assicurarsi di disporre delle autorizzazioni per la configurazione del dispositivo. In alternativa, è necessario richiedere le autorizzazioni. Per i dettagli, fare riferimento alla sezione *Richiesta dell'autorizzazione per un dispositivo*.

Passaggi

- 1. Fare clic su Site per accedere alla pagina Site List.
- 2. Fare clic su una piattaforma per accedere alla pagina Site Details, quindi selezionare la scheda **People Counting**.
 - Le telecamere di conteggio persone vengono visualizzate nell'area Device.
- 3. Fare clic su > per aprire il pannello Device.
- I canali del dispositivo vengono visualizzati nel pannello.
- 4. Fare clic su Activate per aprire la finestra Activate People Counting Service.
- 5. Inserire il nome utente e la password dell'account amministratore del dispositivo.
- 6. Fare clic su **OK** per attivare il servizio di conteggio persone per il canale.

7.8.2 Aggiunta di un gruppo per il conteggio delle persone

Un gruppo per il conteggio delle persone contiene le telecamere di conteggio persone installate in una determinata area. Un gruppo per il conteggio delle persone definisce due elementi, cioè i confini dell'area (rappresentati dalle telecamere aggiunte al gruppo) e il numero massimo di persone che possono restare in tale area. Le telecamere aggiunte al gruppo rilevano le persone in entrata e in uscita e, allo stesso tempo, calcolano i relativi dati. In questo modo, la piattaforma può stabilire se la quantità di persone che si trovano nell'area ha raggiunto il valore massimo consentito e, nel frattempo, invia i relativi dati al client mobile Hik-Connect, che visualizza in tempo reale il numero di persone che si trovano nell'area e di quelle che possono ancora entrarvi. Ciò consente agli utenti finali di utilizzare Hik- Connect per monitorare da remoto la densità delle persone nell'area e adottare provvedimenti appropriati per tempo. La funzione risulta utile nell'ambito di vari scenari in cui è necessario limitare il flusso di persone in una determinata area. Esempio: supponiamo che il cliente sia il responsabile di un supermercato. Durante una pandemia dovuta a una malattia da contatto, è possibile impostare le telecamere di conteggio persone all'entrata e all'uscita del supermercato come gruppo per il conteggio delle persone e abilitarlo. In questo modo, il cliente può intervenire tempestivamente in base ai dati trasmessi a Hik-Connect per ridurre il rischio di infezione dei clienti nel supermercato.

Prima di iniziare

- Assicurarsi di disporre dell'autorizzazione per configurare le telecamere di conteggio persone. 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*
- Accertarsi di aver abilitato il servizio di conteggio persone per i canali. Per i dettagli, fare riferimento alla sezione *Attivazione del servizio di conteggio persone per i canali*.
- Assicurarsi che le impostazioni di conteggio delle persone (ad esempio, la direzione relativa all'entrata) siano state configurate sulla telecamera. Per i dettagli, consultare il manuale d'uso della telecamera.

Passaggi

iNota

Per i dettagli su come visualizzare i dati relativi al conteggio delle persone sul client mobile Hik-Connect, fare riferimento al *Manuale utente del client mobile Hik-Connect*.

- 1. Fare clic su Site per accedere alla pagina Site List.
- 2. Fare clic su una piattaforma per accedere alla pagina Site Details, quindi selezionare la scheda **People Counting**.
- 3. Fare clic su Add Group per accedere al pannello Add Group.
- 4. Impostare le informazioni necessarie.

Nome gruppo

Creare un nome per il gruppo di conteggio delle persone. Ad esempio, se è necessario contare i clienti presenti al primo piano di un centro commerciale, è possibile assegnare il nome "1st Floor" al gruppo.

Seleziona canale

Fare clic su Add, quindi selezionare i canali da aggiungere al gruppo.

iNota

- È possibile selezionare solo i canali per cui è stato abilitato il servizio di conteggio delle persone.
- È possibile aggiungere fino a 16 canali a un gruppo di conteggio delle persone.
- È possibile aggiungere un canale a un massimo di 16 gruppi di conteggio delle persone.

Modalità calcolo

Impostare la modalità di calcolo per ciascun canale selezionato.

Standard

Conta il numero di persone in entrata, ossia quelle che entrano nell'area, rilevate dalla telecamera e il numero di persone in uscita, cioè quelle che escono dall'area. Selezionare questa modalità quando la direzione di entrata configurata sulla telecamera è uguale a quella effettiva.

iNota

Fare riferimento all'immagine riportata di seguito: le frecce blu rappresentano la direzione effettiva di entrata e uscita delle persone, mentre le frecce rosse rappresentano la direzione di entrata configurata sulla telecamera.

Inversa

conta il numero di persone in ingresso rilevate dalla telecamera come quelle che escono dall'area e il numero di persone in uscita come quelle che entrano nell'area. Selezionare questa modalità quando la direzione di ingresso configurata sulla telecamera è opposta rispetto alla direzione effettiva di calcolo.

iNota

Fare riferimento all'immagine riportata di seguito: le frecce blu rappresentano la direzione effettiva di entrata e uscita delle persone, mentre le frecce rosse rappresentano la direzione di entrata configurata sulla telecamera.



Figura 7-11 Modalità di calcolo

N. massimo di persone consentito

Definire il numero massimo di persone (intervallo: da 1 a 100.000) che possono restare nello stesso tempo in un'area specifica.

Push Alarm to Hik-Connect If Max. People Reached

Dopo l'attivazione, viene inviata una notifica di allarme al client mobile Hik-Connect se viene raggiunto il valore impostato in **Max. People Allowed**.

iNota

Ricordare all'utente finale che, per poter visualizzare le notifiche sul client mobile Hik-Connect, la funzione che consente a tale client di riceverle deve restare attiva. Per i dettagli su come attivare le notifiche su Hik-Connect, fare riferimento al *Manuale utente del client mobile Hik-Connect*.

5. Fare clic su **OK**.

Il gruppo di conteggio delle persone viene visualizzato nella scheda **People Counting** ed è attivo per impostazione predefinita. L'utente finale può visualizzare i dati relativi al conteggio delle persone sul client mobile Hik-Connect.

iNota

È possibile aggiungere fino a 16 gruppi di conteggio delle persone a una piattaforma.

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

Modifica gruppo Passare il cursore su , quindi fare clic su Z per modificare il gruppo.

Cancellazione di un gruppo	Passare il cursore su 🔍 🔍 , quindi fare clic su 🔟 per eliminare il gruppo.		
	i Nota		
	Se si elimina un gruppo di conteggio delle persone, viene eliminata anche la funzione correlata.		
Disattivazione di un gruppo specifico	Impostare 🚺 su 🔘 per disattivare il gruppo.		
Sighto sheeiiico	i Nota		
	Se si disattiva il gruppo, le funzioni per il conteggio delle persone sul client mobile Hik-Connect non saranno disponibili.		
Abilitazione/ disabilitazione di gruppi in batch	Fare clic su Enable All o su Disable All per attivare o disattivare tutti i gruppi.		
	i Nota		
	Se si disattiva il gruppo, le funzioni per il conteggio delle persone sul client mobile Hik-Connect non saranno disponibili.		

7.9 Attivazione del servizio di controllo della temperatura per i canali

Se sono stati aggiunti alla piattaforma dei dispositivi che supportano la funzione di controllo della temperatura, è necessario attivare il servizio correlato sui canali di tali dispositivi e poi impostare i relativi parametri su ciascuno di essi. Dopodiché, la funzione di controllo della temperatura di questi dispositivi sarà disponibile e l'utente finale potrà visualizzare le temperature superficiali delle persone presenti nella visualizzazione in tempo reale dei canali sul client mobile Hik-Connect. È anche possibile abilitare varie funzioni per consentire ai canali di effettuare diverse operazioni, tra cui inviare un allarme di temperatura anomala a Hik-Connect, caricare immagini acquisite della persona la cui temperatura è anomala su Hik-Connect, rilevare se le persone indossano la mascherina e caricare l'allarme di rilevamento di un volto senza mascherina su Hik-Connect.

Prima di iniziare

Assicurarsi di aver aggiunto i dispositivi che supportano la funzione di controllo della temperatura alla piattaforma di destinazione.

Passaggi

iNota

La funzione di controllo della temperatura non è disponibile in determinati Paesi e regioni.

- 1. Fare clic su Site per accedere alla pagina Site List.
- 2. Fare clic su una piattaforma per accedere alla pagina Site Details, quindi selezionare la scheda **Temperature Screening**.
 - Vengono visualizzati solo i dispositivi che supportano la funzione di controllo della temperatura.
- 3. Fare clic su > per aprire il pannello Channel. Vengono visualizzati i canali del dispositivo.
- 4. Fare clic su **Activate** per aprire la finestra Activate Temperature Screening Service.
- 5. Inserire il nome utente e la password dell'account amministratore del dispositivo.
- 6. Fare clic su **OK** per attivare il servizio di controllo della temperatura sul canale.
- 7. Impostare i parametri relativi al controllo della temperatura.
 - 1) Fare clic su Settings per impostare i parametri relativi al controllo della temperatura.

Soglia di temperatura

Per il canale di una telecamera di controllo della temperatura, impostare una soglia che, se superata, attiva l'allarme di temperatura anomala.

Per il canale di un terminale di riconoscimento facciale, definire un intervallo di temperatura superficiale normale. Se la temperatura superficiale rilevata non rientra nell'intervallo, viene attivato un allarme di temperatura anomala.

Rilevamento mascherina

Dopo l'attivazione, il dispositivo di controllo della temperatura rileva la presenza della mascherina.

Archivia le informazioni sul controllo della temperatura

Dopo l'attivazione, le informazioni di controllo della temperatura vengono caricate sulla piattaforma Hik-ProConnect.

Se questa opzione viene disattivata, la piattaforma e il client mobile Hik-Connect non possono ricevere le informazioni relative al controllo della temperatura dai dispositivi utilizzati per tale funzione, inclusi gli allarmi di temperatura anomala, le registrazioni della temperatura normale, gli allarmi di rilevamento di volti senza mascherina, nonché le immagini acquisite relative ai volti delle persone con temperatura superficiale anomala.

Push Alarm to Hik-Connect If Abnormal Temp. Rilevamento eseguito

Dopo l'attivazione, se vengono rilevate temperature superficiali anomale, vengono inviati i relativi allarmi al client mobile Hik-Connect.

iNota

Ricordare all'utente finale che, per poter visualizzare le notifiche sul client mobile Hik-Connect, la funzione che consente a tale client di riceverle deve restare attiva. Per i dettagli su come attivare le notifiche su Hik-Connect, fare riferimento al *Manuale utente del client mobile Hik-Connect.*

Salva le registrazioni con temperatura normale

Salvare i record relativi alla temperatura normale sulla piattaforma Hik-ProConnect.

Carica immagini acquisite

Dopo l'attivazione, il dispositivo di controllo della temperatura acquisisce l'immagine del volto della persona con temperatura anomala e carica tale immagine sulla piattaforma.

iNota

Se questa opzione viene disattivata, l'utente finale non può visualizzare l'immagine acquisita sul client mobile Hik-Connect.

Invia un allarme a Hik-Connect se vengono rilevate persone senza mascherina

Dopo l'attivazione, se una persona non indossa la mascherina, viene inviato un allarme al client mobile Hik-Connect.

iNota

Ricordare all'utente finale che, per poter visualizzare le notifiche sul client mobile Hik-Connect, la funzione che consente a tale client di riceverle deve restare attiva. Per i dettagli su come attivare le notifiche su Hik-Connect, fare riferimento al *Manuale utente del client mobile Hik-Connect.*

2) Fare clic su **OK**.

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

Disattivazione della funzione di controllo della temperatura di un dispositivo specifico

Impostare C su C per disattivare la funzione di controllo della temperatura del dispositivo.

iNota

Se questa opzione viene disattivata, l'utente finale non può utilizzare la funzione di controllo della temperatura del dispositivo sul client mobile Hik-Connect. Disattivazione della funzione di controllo della temperatura di tutti i dispositivi Fare clic su **Disable All** per disattivare la funzione di controllo della temperatura di tutti i dispositivi.

iNota

Se questa opzione viene disattivata, l'utente finale non può utilizzare la funzione di controllo della temperatura dei dispositivi sul client mobile Hik-Connect.

7.10 Upgrade del firmware del dispositivo

Nella pagina Device List, viene visualizzato il simbolo 🕥 vicino al nome del dispositivo se è disponibile un upgrade. È possibile effettuare l'upgrade del dispositivo per garantire la compatibilità con Hik-ProConnect.

Passaggi

iNota

- La funzione è supportata dai pannelli di controllo di sicurezza (incluso il sistema AX Pro), i campanelli, da alcuni modelli di telecamere IP, Hik-ProConnect e dai DVR cloud.
- Il sistema supporta l'upgrade del dispositivo di codifica, di alcuni dispositivi di controllo degli accessi e di videocitofoni collegati alla stessa LAN del computer su cui è in esecuzione la piattaforma.
- Inoltre è possibile aggiornare i dispositivi nel modulo Monitoraggio dello stato. Per i dettagli, fare riferimento alla sezione *Monitoraggio dello stato*.
- È inoltre possibile eseguire l'upgrade dei dispositivi quando vengono aggiunti. Per i dettagli, fare riferimento alla sezione **Aggiunta dei dispositivi rilevati online** e **Aggiunta dei dispositivi tramite Hik-Connect (P2P)**.
- 1. Fare clic sul nome della piattaforma per accedere alla pagina dei dettagli.
- 2. Fare clic su **Upgrade Device**, quindi selezionare i dispositivi aggiornabili.
- 3. Fare clic su **Upgrade**.
- 4. Opzionale: se sono presenti dispositivi su cui è attiva la modalità conforme a EN50131, inserire le password del dispositivo e fare clic su **OK**.

iNota

- Una volta avviato, l'upgrade non può essere interrotto. Evitare interruzioni dell'alimentazione o della connessione durante l'aggiornamento.
- È possibile abilitare la modalità conforme a EN50131 nella pagina di configurazione del dispositivo tramite il client web. Per i dettagli, consultare il manuale utente del dispositivo.

Viene visualizzata una finestra che mostra l'avanzamento dell'upgrade. Se non è possibile effettuare l'upgrade di alcuni dispositivi, le cause vengono visualizzate nella finestra.

7.11 Scollegamento di un dispositivo dal relativo account corrente

Quando si aggiungono dispositivi rilevati online e uno di questi 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).

iNota

Per i dettagli su come aggiungere i dispositivi rilevati online, fare riferimento alla sezione **Aggiunta** *dei dispositivi rilevati online*.

Nella pagina su cui è indicato il risultato della procedura di aggiunta, fare clic su 🥙 nella colonna Operation, quindi inserire la password del dispositivo e fare clic su **OK** per scollegarlo dall'account corrente. Una volta scollegato, è possibile fare clic su 🙂 nella colonna Operation per aggiungere il dispositivo al proprio account.

iNota

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

7.12 Reimpostazione della password del dispositivo

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

iNota

- 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 computer su cui è in esecuzione il Portale Hik-ProConnect.

Fare clic su Site e inserire la piattaforma su cui si trova il dispositivo.

Selezionare il dispositivo, quindi fare clic su $\bullet \bullet \bullet \to \mathscr{P}$ 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 7-12 Diagramma di flusso della procedura di reimpostazione della password di un dispositivo

7.13 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

iNota

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

- 1. Fare clic sulla scheda **Site** nella schermata principale per accedere alla pagina Site.
- 2. Selezionare un dispositivo e fare clic su $\bullet \bullet \bullet \to \mathbb{R}$ per aprire la finestra DDNS Settings.
- 3. Attivare il pulsante Enable DDNS per visualizzare i parametri del DDNS.

iNota

È possibile fare clic su **How to set port?** per ottenere informazioni su come eseguire la configurazione.

4. 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. 5. Inserire il nome di dominio del dispositivo.

6. 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.

7. Fare clic su **OK**.

7.14 Visualizzazione di video in tempo reale

Tramite la visualizzazione live delle telecamere gestite, è possibile controllare se la telecamera è installata e posizionata correttamente acquisendo immagini, effettuando registrazioni, tramite il brandeggio, ecc.

Fare clic su **Encoding Device** nella parte superiore della pagina per visualizzare tutti i dispositivi di codifica della piattaforma. Selezionare un dispositivo di codifica e fare clic su per avviare la visualizzazione in tempo reale. La visualizzazione in tempo reale resta attiva per un massimo di cinque minuti. Una volta terminata, è comunque possibile avviarla nuovamente. Passare il cursore sulla finestra della visualizzazione in tempo reale e fare clic sulle icone nella barra degli strumenti per iniziare la registrazione, eseguire lo zoom digitale e le operazioni di brandeggio, acquisire un'immagine, modificarne la qualità e attivare/disattivare l'audio. Fare doppio clic sull'immagine della visualizzazione live per accedere alla modalità a schermo intero e fare di nuovo doppio clic per uscirne.

iNota

- Sono supportate fino a 16 finestre per la visualizzazione in tempo reale.
- 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.
- Assicurarsi che il dispositivo sia online, altrimenti non è possibile utilizzare la funzione.

7.15 Visualizzazione di video registrati

La riproduzione video mostra cosa accade quando si verifica un'emergenza. Se un utente finale approva la richiesta di riprodurre il video, è possibile visualizzare la relativa registrazione sul dispositivo.

iNota

- Assicurarsi che l'account disponga dell'autorizzazione per la riproduzione. Senza quest'ultima, infatti, non è possibile accedere alla pagina di riproduzione. Per i dettagli su come richiedere l'autorizzazione per un dispositivo, fare riferimento alla sezione *Richiesta dell'autorizzazione per un dispositivo*.
- Questa funzione deve essere supportata dal dispositivo.
- Assicurarsi di aver programmato l'orario di registrazione sul dispositivo e che su questo siano stati memorizzati i video.

Nella scheda Device, selezionare un dispositivo e fare clic su 🕟 per accedere alla pagina Playback. È possibile selezionare la data e l'ora sul calendario per visualizzare le riproduzioni relative a un determinato intervallo di tempo.

È possibile selezionare i canali dall'elenco a discesa in alto a destra. Trascinare la barra temporale in basso per passare a un altro video. Passare il cursore sulla barra temporale e ingrandirla per specificare l'ora. Passare il cursore su una finestra di riproduzione e fare clic sulle icone nella barra degli strumenti per acquisire un'immagine, effettuare riprese video, eseguire lo zoom digitale, scaricare i video e attivare l'audio.

Per i dispositivi (inclusi quelli inseriti online) aggiunti tramite il servizio Hik-Connect e che non dispongono di un DDNS configurato, la riproduzione durerà massimo cinque minuti. Per i dispositivi aggiunti tramite l'IP/il nome di dominio e quelli (inclusi i dispositivi inseriti online) aggiunti tramite il servizio Hik-Connect e che dispongono di un DDNS configurato, la durata della riproduzione è illimitata.

iNota

Sono supportate fino a quattro finestre di riproduzione.

7.16 Uso e configurazione del sistema AX Pro

È possibile utilizzare il pannello di controllo di sicurezza AX Pro per effettuare operazioni quali l'attivazione/disattivazione dell'area, la cancellazione degli allarmi, l'esclusione delle aree, ecc, nonché per configurare da remoto il pannello di controllo sul Portale. È inoltre possibile richiedere il PIN (necessario per effettuare l'upgrade del firmware di AX Pro) e cambiare la lingua di AX Pro. Fare clic su Site per accedere alla pagina Site List, quindi fare clic sul nome di una piattaforma per entrare in Site Details.

Uso di AX Pro da remoto

Fare clic su AX Pro per aprire il pannello delle funzioni. È possibile effettuare le seguenti operazioni.

Operazione	Descrizione		
Attivazione di parte dei dispositivi in un'area specifica	Selezionare la scheda Area , quindi fare clic su Stay Arming per attivare parte dei dispositivi nell'area.		
Attivazione di tutti i dispositivi in un'area specifica	Selezionare la scheda Area, quindi fare clic su Away Arming.		
Disattivazione di un'area specifica	Selezionare la scheda Area , quindi fare clic su Disarm .		

Tabella 7-6 Descrizione dell'operazione

Operazione	Descrizione
Attivazione di parte dei dispositivi in più aree	Selezionare la scheda Area , quindi scegliere le aree e fare clic su 1 .
Attivazione di tutti i dispositivi in più aree	Selezionare la scheda Area , quindi scegliere le aree e fare clic su
Disattivazione di più aree	Selezionare la scheda Area , quindi scegliere le aree e fare clic su <a>href="https://doi.org/10.1111/10.111111111111111111111111111
Cancellazione degli allarmi di più aree	Selezionare la scheda Area , quindi scegliere le aree e fare clic su
Visualizzazione dei dispositivi di ciascuna area	Selezionare la scheda Device , quindi fare clic su v e selezionare un'area per visualizzare solo i dispositivi collegati ad essa oppure selezionare All per visualizzare quelli collegati a tutte le aree.
Esclusione di aree	Selezionare la scheda Device , quindi selezionare un'area (ovvero un rilevatore) e attivare il pulsante Bypass per escluderla.

AX PRO1	×
Basic Information Device Name : AX PRO1 Device Type : Security Co Device Serial No. : Q98	ontrol Panel
Area	Device
Area 1	Arming Disarm

Figura 7-13 Pannello delle funzioni di AX Pro

Configurazione da remoto di AX Pro

È possibile fare clic su 🕸 per accedere alla pagina web del pannello di controllo di sicurezza e configurare il dispositivo.

iNota

Per i dettagli su come configurare il pannello di controllo di sicurezza, fare riferimento al manuale utente del dispositivo.

Richiedere un PIN

È possibile fare clic su $\bullet \bullet \bullet \rightarrow \square$ per aprire la finestra Apply for a PIN in modo da visualizzare il codice PIN.



Figura 7-14 Finestra Apply for a PIN

Cambia lingua

iNota

È necessario richiedere un PIN. Per i dettagli, fare riferimento alla sezione *Richiesta di un PIN*.

È possibile fare clic su $\bullet \bullet \bullet \rightarrow \Rightarrow$ per aprire la finestra Language e poi impostare la lingua del dispositivo e inserire il PIN.

Language		\times
i Make sure a po when switching	wer failure or network outage does not happen language. Otherwise, the device may be crashed.	
Device Name	AX PRO	
Device Serial No.	-	
Device Language	English 🗸	
* PIN	Enter PIN	
	OK Cancel	

Figura 7-15 Finestra Language

7.17 Configurazione da remoto

È possibile eseguire la configurazione da remoto del dispositivo, se necessario.

iNota

Solo il gestore della piattaforma può eseguire le seguenti operazioni e configurazioni di una piattaforma. Per i dettagli su come assegnare una piattaforma, fare riferimento alla sezione *Assegnazione della piattaforma all'installatore*.

Fare clic su **Site** per accedere alla pagina Site List. Fare clic sul nome di una piattaforma per accedere alla pagina relativa. A questo punto, fare clic sulla scheda **Device** per visualizzare i dispositivi della piattaforma.

Fare clic su 🔯 per aprire la pagina di configurazione da remoto del dispositivo e impostare i relativi parametri.

iNota

- La configurazione da remoto è supportata solo da campanelli, dispositivi di codifica, postazioni interne e pannelli di controllo di sicurezza.
- Assicurarsi che il dispositivo sia online, altrimenti non è possibile utilizzare la funzione.
- Non è necessario inserire nome utente e password del dispositivo prima di accedere alla pagina di configurazione da remoto dei campanelli.
- Se sono già stati inseriti il nome utente e la password del dispositivo di codifica durante l'aggiunta, non è necessario inserire queste informazioni prima della configurazione da remoto. I dispositivi NVR e DVR supportano il riavvio, la formattazione HDD e le impostazioni di rete.
- Per i dispositivi di controllo della sicurezza:
 - se il dispositivo di controllo della sicurezza si trova nella stessa LAN del Portale, è necessario inserire il nome utente e la password prima di accedere alla pagina di configurazione da remoto.
 - Se i dispositivi Axiom Hub e Axiom Hybrid non si trovano nella stessa LAN ed è abilitata la modalità conforme a EN50131, prima è necessario inserire le password amministratore dei dispositivi per la verifica. Dopodiché, una volta inserita la password dell'account di impostazione, è possibile accedere alla pagina di configurazione da remoto.
- Per i dispositivi di codifica e di controllo della sicurezza che non si trovano nella stessa rete locale del Portale, alcune operazioni di configurazione da remoto (come la gestione dell'account del dispositivo, l'abilitazione di Hik-Connect, il ripristino del dispositivo, ecc.) non sono disponibili.
- Per i dettagli sulla configurazione da remoto, fare riferimento al manuale utente del dispositivo.
- Se i parametri del dispositivo sono stati modificati da un altro software o client (come la pagina del dispositivo, il client mobile Hik-ProConnect, iVMS-4200, HikCentral Professional, ecc.) e quelli sulla pagina di configurazione da remoto del Portale non sono aggiornati, è possibile aggiornarli facendo clic su **Clear Cache** nell'elenco a discesa in alto a destra della pagina di configurazione da remoto.

Capitolo 8 Servizio di archiviazione cloud

Hik-ProConnect offre una soluzione di archiviazione cloud per i video relativi agli eventi, ovvero le riprese registrate quando un evento predefinito viene rilevato dal canale di un dispositivo di codifica.

Dopo aver aggiunto un dispositivo di archiviazione cloud alla piattaforma e aver configurato le relative impostazioni, il dispositivo funzionerà come supporto di trasmissione e trasferirà i video degli eventi dei canali collegati ad esso al cloud. A seconda dei tipi di pacchetti di servizi di archiviazione cloud acquistati dal market, le riprese verranno conservate per 7 o 30 giorni sul cloud.

iNota

I dispositivi di archiviazione cloud supportati includono Hik-ProConnect Box e i DVR compatibili con il sistema cloud (in seguito semplificato come DVR cloud).

8.1 Diagramma di flusso

Il diagramma di flusso riportato di seguito mostra le procedure consigliate per usare il servizio di archiviazione cloud con Hik-ProConnect Box e il DVR cloud.

Diagramma di flusso per Hik-ProConnect Box



La tabella seguente illustra la descrizione di ciascun passaggio del diagramma di flusso.

Tabella 8-1 Descrizione del diagramma di flusso

Passaggio	Descrizione
Aggiungere	Aggiungere telecamere, NVR o DVR a una piattaforma. Per i
telecamere/NVR/DVR a una	dettagli, fare riferimento alla sezione Aggiunta di un
piattaforma	dispositivo .

Passaggio	Descrizione			
	Aggiungere Hik-ProConnect Box alla stessa piattaforma tramite Hik-Connect P2P. Per i dettagli, fare riferimento alle sezioni Aggiunta dei dispositivi tramite Hik-Connect (P2P), Aggiunta di dispositivi in un batch e Aggiunta di dispositivi rilevati online.			
Aggiungere Hik-ProConnect Box alla stessa piattaforma	i Nota			
	Se Hik-ProConnect Box viene aggiunto tramite il nome IP o di dominio, non è possibile utilizzare il servizio di archiviazione cloud.			
	Impostare l'archiviazione cloud per Hik-ProConnect. Per i dettagli, fare riferimento alla sezione <i>Impostazione dell'archiviazione cloud per Hik-ProConnect Box</i> .			
	L'elenco seguente illustra le descrizioni di ciascun passaggio secondario.			
Impostare l'archiviazione cloud	 Test di rete: verificare le condizioni della rete per conoscere le impostazioni consigliate relative all'archiviazione cloud. Per i dettagli, fare riferimento alla sezione <i>Test di rete</i>. Aggiungere canali a Hik-ProConnect Box: per consentire a quest'ultimo di acquisire i dati relativi ai video dei canali. Impostare la risoluzione e l'evento: configurare la risoluzione dei canali e gli eventi che attiveranno la registrazione dei video da parte del canale. Acquistare pacchetti di servizi di archiviazione cloud: comprare i pacchetti di archiviazione cloud dal market dei servizi. Per i dettagli, fare riferimento alla sezione <i>Acquisto di servizi di archiviazione cloud</i>. 			
	iNota È inoltre possibile acquistare la licenza del servizio dal distributore.			
	• Attivare il servizio di archiviazione cloud per i canali: abilitare il servizio di archiviazione cloud per uno o più canali specifici utilizzando i pacchetti di servizi di archiviazione cloud o la licenza acquistati. Per i dettagli, fare riferimento alla sezione <i>Attivazione o rinnovo di servizi per un canale</i> .			

Diagramma di flusso per il DVR cloud



La tabella seguente illustra la descrizione di ciascun passaggio del diagramma di flusso.

Tabella 8-2 Descrizione del diagramma di flusso

Passaggio	Descrizione
Aggiungere un DVR cloud a	Aggiungere un DVR cloud a una piattaforma tramite Hik-Connect P2P. Per i dettagli, fare riferimento alle sezioni Aggiunta dei dispositivi tramite Hik-Connect (P2P), Aggiunta di dispositivi in un batch e Aggiunta di dispositivi rilevati online.
una piattaforma	i Nota
	Se il DVR cloud viene aggiunto tramite il nome IP o di dominio, non è possibile utilizzare il servizio di archiviazione cloud.

Passaggio	Descrizione		
Impostare l'archiviazione cloud	Impostare l'archiviazione cloud per il DVR cloud. Per i dettag fare riferimento alla sezione <i>Impostazione dell'archiviazione</i> <i>cloud per un DVR cloud</i> .		
	L'elenco seguente illustra le descrizioni di ciascun passaggio secondario.		
	 Test di rete: verificare le condizioni della rete per conoscere le impostazioni consigliate relative all'archiviazione cloud. Per i dettagli, fare riferimento alla sezione <i>Test di rete</i>. Attivare l'archiviazione cloud per i canali: abilitare l'archiviazione cloud per i canali del DVR cloud. Impostare il tipo di streaming e l'evento: configurare il tipo di streaming (principale secondario) per i canali e gli eventi che li attiveranno per registrare i video. Acquistare pacchetti di servizi di archiviazione cloud: comprare i pacchetti di archiviazione cloud dal market dei servizi. Per i dettagli, fare riferimento alla sezione <i>Acquisto di servizi di archiviazione cloud</i>. 		
	i Nota È inoltre possibile acquistare la licenza del servizio dal distributore.		
	• Attivare il servizio di archiviazione cloud per i canali: abilitare il servizio di archiviazione cloud per uno o più canali specifici utilizzando i pacchetti di servizi di archiviazione cloud o la licenza acquistati. Per i dettagli, fare riferimento alla sezione <i>Attivazione o rinnovo di servizi per un canale</i> .		

8.2 Acquisto di servizi di archiviazione cloud

È necessario acquistare il servizio di archiviazione cloud dal market prima di poterlo utilizzare.

Prima di iniziare

Assicurarsi di disporre dell'autorizzazione per gestire i pacchetti di servizi e gli ordini.

Passaggi

- Nella schermata principale, fare clic su Business → Service Market per accedere alla pagina Service Market.
- 2. Nell'area Cloud Service, fare clic su **Online Purchase** per accedere alla pagina di acquisto. È possibile visualizzare quattro tipi di pacchetti di servizi di archiviazione cloud e i relativi prezzi.
- 3. Fare clic su 🔥 o inserire manualmente un numero per definire la quantità di pacchetti da acquistare.

iNota

- È possibile acquistare uno o più pacchetti alla volta. Il periodo di validità del servizio è di un anno a partire dalla data di acquisto, pertanto è necessario effettuare l'attivazione entro tale periodo.
- Le voci **7-Day** e **30-Day** si riferiscono al periodo di archiviazione sul cloud dei video relativi all'evento. Le voci **Monthly** e **Annual** si riferiscono alla durata del servizio a partire dalla data di attivazione.

Esempio

Ad esempio, se si seleziona **7-Day Monthly Package**, i video vengono salvati sul cloud per 7 giorni e sovrascritti da quelli nuovi a partire dall'ottavo giorno. Il servizio dura un mese dall'attivazione.

I pacchetti di servizi selezionati vengono visualizzati sul lato destro della pagina.

4. Fare clic su 🖉 per inserire il numero di partita IVA, quindi selezionare 🗹 per confermare.

iNota

Il numero di partita IVA inserito verrà visualizzato nella ricevuta di pagamento.

- 5. Selezionare **Credit/Debit Cards** come metodo di pagamento.
- 6. Fare clic su **Checkout** per accedere alla pagina di pagamento e terminare l'operazione.
- 7. Opzionale: Fare clic su **Business** → **My Service** → **Cloud Storage Details** per visualizzare i pacchetti di servizi acquistati nell'elenco.

8.3 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

iNota

Se al momento dell'aggiunta di Hik-ProConnect Box si ignora il passaggio per impostare l'archiviazione cloud, è possibile fare clic sulla periferica nell'elenco dei dispositivi per aprire il pannello delle relative impostazioni al fine di impostare l'archiviazione cloud in un secondo momento.

1. Aggiungere Hik-ProConnect Box a una piattaforma tramite Hik-Connect P2P.

iNota

- Per i dettagli su come aggiungere Hik-ProConnect Box, fare riferimento alle sezioni Aggiunta dei dispositivi tramite Hik-Connect (P2P), Aggiunta di dispositivi in un batch o Aggiunta di dispositivi rilevati online.
- Se si aggiunge Hik-ProConnect Box tramite il nome IP o di dominio, non è possibile utilizzare la funzione di archiviazione cloud.

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

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

iNota

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

Viene visualizzata la finestra Add Channel.

Add Channel	×
 According to the network test, it is rec for cloud storage of high definition vio channels for cloud storage of standard 	ommended that you set no more than 19 channels leo (resolution for reference: 1920*1080), or 31 l definition video (resolution for reference: 704*576)
Select Device	
DS-2CD	~
Select Channel	
	Camera 01
Device Ir	nformation 🔨
* Device IP Address	* Port
192.168	8001
* User Name	* Password
	OK Cancel

Figura 8-1 Finestra Add Channel

- 4. Aggiungere canali a Hik-ProConnect Box per abilitare la funzione di archiviazione cloud.
 - 1) Selezionare un dispositivo (ad esempio, NVR e telecamera di rete) dall'elenco a discesa nella finestra Add Channel.

A questo punto, vengono visualizzati i relativi canali ed è possibile fare clic su **Device Information** per vedere o modificare le informazioni del dispositivo, tra cui l'indirizzo IP, il numero di porta, il nome utente e la password.

- 2) Attivare i pulsanti per aggiungere canali specifici a Hik-ProConnect Box e quindi abilitare la funzione di archiviazione cloud su di essi.
- 3) Inserire le informazioni del dispositivo su cui si trova il canale, inclusi l'indirizzo IP, il numero di porta, il nome utente e la password.

4) Fare clic su OK.

Dopodiché si accede alla pagina Cloud Storage Settings su cui è possibile visualizzare i canali già aggiunti a Hik-ProConnect Box.

Cloud Storage Settings		×
	I. According to the network test, it is recommended that you get no more think 13 channels for cloud stronge of high definition video (resolutions) for effective. 35/37 2880; et al. Course to cloud stronge of stratedied effectives video (resolution for reference. TMP 576); 2. Cours there thereasy as set the events the clouder, schooling more detection, stronge, and enable Notry Surveillance Center.	
	Max. Channels: 8 Unleed Channels: 5 Add Channel (7) Available Bandwith (Latest Tested; 15990 Mays Bandwith Required (Estimated)200 Maps	
Router Cloud Storage Device	Contrast 02 Contrast 02 D3 Standard Definition V Coccupied Bandwidth: 500 ktps	2g.
Drijinira Camera	Chunde DPCamera D2 Could Storage Service 1 Standard Definition V Occupied Sandwidth: 500 kbps	ıac
Network Camera His ProConnect Box Connection	Cannea 01 Control Cont	ug.
	OK Cancel	

Figura 8-2 Pagina Cloud Storage Settings

5. Selezionare **Standard Definition** o **High Definition** dall'elenco a discesa in base alla risoluzione consigliata che viene visualizzata nella pagina Cloud Storage Settings (se è stato eseguito il test di rete).

iNota

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).

6. Fare clic su **Event Settings** per impostare gli eventi che attiveranno l'azione di registrazione di video da parte del canale.

iNota

Gli eventi che supportano tale azione includono il rilevamento di movimenti, l'intrusione e l'attraversamento di una linea. L'impostazione è uguale per tutti questi eventi, pertanto verrà illustrata brevemente solo la procedura per configurare il rilevamento di movimenti. Per i dettagli su come impostare gli altri eventi, fare riferimento al manuale utente del canale (telecamera).

Enable Motion Detection

Attivare questo pulsante per abilitare il rilevamento di movimenti.

Area Settings

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

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 selezionata. Se non è attiva, il canale non registra i video relativi agli eventi anche se questi vengono rilevati.

7. Opzionale: Modificare o eliminare un canale specifico.

Edit a Channel	Fare clic su •••	\rightarrow	\Rightarrow per modificare le impostazioni del canale.
Delete a Channel	Fare clic su 🔹 🔹	\rightarrow	per eliminare il canale.

8. Fare clic su **Activate** per attivare il servizio di archiviazione cloud sul canale.

iNota

Per i dettagli su come attivare il servizio, fare riferimento alla sezione Attivazione o rinnovo di servizi per un canale.

I video relativi all'evento del canale verranno caricati sul cloud. 9. Opzionale: Fare clic su $\bullet \bullet \bullet \rightarrow \Rightarrow$ per utilizzare il servizio attivato su un altro canale. 10. Fare clic su **Finish**.

8.4 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), l'aggiunta di canali, le impostazioni per il tipo di streaming, 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

iNota

Se al momento dell'aggiunta del DVR cloud si ignora il passaggio per impostare l'archiviazione cloud, è possibile fare clic sulla periferica nell'elenco dei dispositivi per aprire il pannello delle relative impostazioni al fine di impostare l'archiviazione cloud in un secondo momento.

1. Aggiungere un DVR cloud a una piattaforma tramite Hik-Connect (P2P).

iNota

- Per i dettagli su come aggiungere un DVR di archiviazione cloud, fare riferimento alle sezioni Aggiunta dei dispositivi tramite Hik-Connect (P2P), Aggiunta di dispositivi in un batch o Aggiunta di dispositivi rilevati online.
- Se si aggiunge il DVR cloud tramite il nome IP o di dominio, non è possibile utilizzare la funzione di archiviazione cloud.

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

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

iNota

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

Dopodiché si accede alla pagina Cloud Storage Settings su cui è possibile visualizzare tutti i canali del DVR cloud.

4. Selezionare **Main Stream** o **Sub Stream** dall'elenco a discesa per scegliere il tipo di streaming del canale.

iNota

Le definizioni video di Main Stream e Sub Stream vengono visualizzate sotto l'elenco a discesa. 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).

5. Fare clic su **Event Settings** per impostare gli eventi che attiveranno l'azione di registrazione di video da parte del canale.

iNota

Gli eventi che supportano tale azione includono il rilevamento di movimenti, l'intrusione e l'attraversamento di una linea. L'impostazione è uguale per tutti questi eventi, pertanto verrà illustrata brevemente solo la procedura per configurare il rilevamento di movimenti. Per i dettagli su come impostare gli altri eventi, fare riferimento al manuale utente del canale (telecamera).

Enable Motion Detection

Attivare questo pulsante per abilitare il rilevamento di movimenti.

Area Settings

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

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 selezionata. Se non è attiva, il canale non registra i video anche se viene rilevato l'evento.

6. Attivare **Cloud Storage** per abilitare la funzione di archiviazione cloud sul canale.

iNota

Se è la prima volta che si attiva l'archiviazione cloud per un canale del DVR cloud, quest'ultimo viene riavviato automaticamente. Attendere fino al completamento del riavvio, quindi aprire il pannello delle impostazioni per terminare la procedura riportata di seguito.

7. Fare clic su **Activate** per attivare il servizio di archiviazione cloud sul canale.

iNota

Per i dettagli su come attivare il servizio, fare riferimento alla sezione **Attivazione o rinnovo di** servizi per un canale.

Il DVR cloud verrà riavviato automaticamente. Successivamente, il video relativo all'evento del canale verrà caricato sul cloud.

iNota

Quando sul canale è attivo il servizio di archiviazione cloud, non è possibile disabilitare l'opzione **Cloud storage**.

8. Fare clic su **Finish**.

9. Opzionale: Fare clic sul DVR cloud nell'elenco dei dispositivi per aprire il pannello delle impostazioni, quindi selezionare **Edit** per modificare quelle dei relativi canali.

iNota

Se si disattiva **Cloud Storage** per tutti i canali, il DVR cloud si riavvia automaticamente.

8.5 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.

iNota

Il tempo di esecuzione del test di rete è di circa un minuto.

Nell'elenco delle periferiche, fare clic sul dispositivo di archiviazione cloud per aprire il pannello delle relative impostazioni, quindi selezionare $\textcircled{} \Rightarrow$ **Start** per avviare il test di rete.

8.6 Attivazione o rinnovo di servizi per un canale

Nella pagina Cloud Storage Service, è possibile visualizzare i dettagli relativi all'archiviazione cloud dei vari canali di un dispositivo di archiviazione cloud. Se il servizio di archiviazione cloud non è attivo su un determinato canale, è necessario abilitare tale servizio prima di poterlo utilizzare. Se, invece, su questo canale è attivo un servizio in scadenza o che è già scaduto, è possibile effettuare il rinnovo.

Prima di iniziare

Assicurarsi di aver aggiunto i dispositivi di archiviazione cloud alla piattaforma. Per i dettagli, fare riferimento alla sezione **Aggiunta di un dispositivo**.

Passaggi

- 1. Nella schermata principale, fare clic su **Site** per accedere alla pagina Site List.
- 2. Fare clic su una piattaforma per accedere alla pagina dei relativi dettagli.
- 3. Selezionare la scheda Cloud Storage Service.
- 4. Accedere alla finestra Activate/Renew Cloud Storage Service.
 - Nel caso in cui il servizio non sia stato attivato per alcun canale presente sulla piattaforma, fare clic su Activate Cloud Storage Service, selezionare un dispositivo online nell'elenco, attivare Cloud Storage, quindi fare clic su Activate Service.
 - Se, invece, il servizio è stato attivato per uno o più canali presenti sulla piattaforma, fare clic su Activate Service per abilitare tale servizio su un determinato canale oppure selezionare Renew Service per effettuare il rinnovo.

Activate,	/Renew Cloud Storage Service			×
	Purchased Service Package	Activate by Se	ervice Key	
Availa	able Package		Online Purchas	e
	7-Day Monthly Package 7	7-Day Annual Package 0		
	30-Day Monthly Package 0	30-Day Annua	l Package 0	
Selec	t Package Type			
0	7-Day Monthly Package		0	
	7-Day Annual Package		0 ~	
	30-Day Monthly Package		0 ~	
	30-Day Annual Package		0	
6 ^P ir	lease note that the cloud storage se a 362 day(s).	rvice activated for this	channel will expire	
	A	ctivate/Renew	Cancel	
	If you click Activate	, you agree to Cloud St	torage Service Terr	n

Figura 8-3 Finestra Activate/Renew Cloud Storage Service

iNota

È possibile visualizzare i pacchetti disponibili acquistati e fare clic su **Online Purchase** per comprarne altri, se necessario. Per i dettagli, fare riferimento alla sezione *Acquisto di servizi di archiviazione cloud*.

- 5. Attivare o rinnovare il servizio di archiviazione cloud per un canale.
 - Fare clic su **Purchased Service Package**, selezionare un tipo di pacchetto e fare clic su (o inserire manualmente un numero) per scegliere la quantità.

- Fare clic su **Activate by Service Key** e inserire il codice della licenza a 16 cifre.

iNota

È possibile richiedere la licenza al distributore.

6. Fare clic su **Activate/Renew** per terminare l'attivazione o il rinnovo del servizio di archiviazione cloud.

iNota

Dopo aver attivato o rinnovato il servizio, è possibile visualizzare il tipo di pacchetto e la data di scadenza su ciascun canale. Quando sono presenti più pacchetti di servizi inutilizzati su un determinato canale, questi vengono elencati in base alla data di acquisto.

8.7 Visualizzazione dei dettagli relativi all'archiviazione cloud

È possibile visualizzare i dettagli relativi all'archiviazione cloud (tra cui i tipi e il numero dei pacchetti di servizi acquistati e utilizzati) e le informazioni (ad esempio, la data di scadenza e lo stato) dei servizi attivati sui vari canali dei dispositivi di archiviazione cloud. Inoltre, è possibile eseguire altre operazioni, come il rinnovo del servizio in modo da continuare a utilizzarlo. Per accedere alla pagina dei dettagli relativi all'archiviazione cloud, procedere in uno dei due modi seguenti:

- Nella schermata principale, fare clic su **Business** → **My Service** → **Cloud Storage Details**.
- Nella schermata principale, fare clic su **Business** → **My Service** → **All Services**, selezionare il pacchetto del servizio di archiviazione cloud e fare clic su **Details**.

Nella pagina relativa ai dettagli dell'archiviazione cloud, è possibile visualizzare la panoramica generale dei pacchetti di servizi di archiviazione cloud acquistati e utilizzati, visualizzare lo stato dei servizi attivati sui vari canali ed eseguire altre operazioni.

- Filter: fare clic su v per filtrare i canali dei dispositivi di archiviazione cloud in base allo stato (in scadenza o scaduto) del servizio.
- Search: inserire una parola chiave (nome del dispositivo, nome della piattaforma o nome del proprietario della piattaforma) nella casella di ricerca per visualizzare lo stato del servizio sui canali di una determinata piattaforma.
- Purchase Cloud Storage Service Package: fare clic su Online Purchase nell'angolo in alto a destra della pagina per acquistare altri pacchetti di servizi di archiviazione cloud in base alle necessità. Per i dettagli, fare riferimento alla sezione Acquisto di servizi di archiviazione cloud.

Renew Cloud Storage Service: se un servizio è in scadenza, fare clic su **Renew** per rinnovarlo. Per i dettagli, fare riferimento alla sezione *Attivazione o rinnovo di servizi per un canale*.

Capitolo 9 Servizio di monitoraggio dello stato

Hik-ProConnect offre un pacchetto gratuito permanente che fornisce una serie di funzioni di base, come la visualizzazione dello stato online dei dispositivi e la configurazione del dispositivo da remoto una volta completata la registrazione dell'account. Le capacità e funzioni del pacchetto gratuito sono limitate, pertanto a volte questo NON risulta sufficiente per soddisfare le esigenze avanzate dei clienti (cioè gli utenti finali), come la manutenzione di numerosi dispositivi. Rispetto al pacchetto gratuito, il servizio di monitoraggio dello stato consente di aggiungere un numero maggiore di dispositivi su Hik-ProConnect, monitorare lo stato di integrità delle periferiche dei clienti e configurare altre funzioni a valore aggiunto. È possibile accedere al servizio di monitoraggio dello stato acquistando i relativi pacchetti dal market dei servizi.

iNota

Il servizio di monitoraggio dello stato è temporaneamente gratuito in alcuni Paesi e aree geografiche.

Differenze tra pacchetto gratuito e pacchetto di monitoraggio dello stato

La tabella seguente illustra le differenze tra il pacchetto gratuito e il pacchetto di monitoraggio dello stato.

iNota

Per i Paesi e le aree geografiche in cui il pacchetto di monitoraggio dello stato è attualmente gratuito, i dettagli di quest'ultimo potrebbero risultare diversi rispetto a quelli visualizzati nella tabella seguente. Per i dettagli, contattare i distributori o l'assistenza in questi Paesi e aree geografiche.

Funzione	Pacchetto gratuito	Pacchetto di monitoraggio dello stato
Aggiunta di dispositivi		
Piattaforme e dispositivi		
Richiesta dell'autorizzazione		
Visualizzazione dello stato online dei dispositivi	 Supportato Dispositivi gestibili: 1024 	 Supportato Dispositivi gestibili: oltre 1024 in base al pacchetto acquistato.
Configurazione da remoto		
Visualizzazione in tempo reale/riproduzione/download di video		
Aggiornamento da remoto del firmware del dispositivo		

Funzione	Pacchetto gratuito	Pacchetto di monitoraggio dello stato
Monitoraggio delle condizioni	Supportato	Supportato
Regole di eccezione	Non supportato	Supportato
Regole di collegamento	Non supportato	Supportato
Gestione dipendenti	Non supportato	Dipendenti gestibili: 4
Gestione ruoli/autorizzazioni	Non supportato	Supportato
Ricerca registri delle operazioni dei dipendenti	Non supportato	Supportato
Co-Branding	Non supportato	Supportato

Impostazione dei dispositivi coperti dal pacchetto di monitoraggio dello stato

Il numero di dispositivi in grado di accedere al servizio di monitoraggio dello stato varia in base al pacchetto acquistato. In alcuni casi, potrebbe essere necessario modificare i dispositivi che possono accedere al servizio.

Per modificare le periferiche che possono accedere alle funzioni a valore aggiunto offerte dal pacchetto di monitoraggio dello stato, procedere come segue.

iNota

Attualmente questa funzione è disponibile solo in determinati Paesi e aree geografiche.

1. Accedere a Business \rightarrow My Service \rightarrow Health Monitoring Settings.

2. Selezionare i dispositivi dall'elenco Devices with Health Monitoring, quindi fare clic su 🗈 per attivare il servizio di monitoraggio dello stato su quelli selezionati.

In alternativa, selezionare i dispositivi dall'elenco Devices with Health Monitoring, quindi fare clic su i per disattivare il servizio di monitoraggio dello stato su quelli selezionati.

Fare clic su OK.

Health Monitoring Package Capacity: Network Camera		Used: 12/ Unimite	ed Buy Mere	
Health Monitoring Package Capacity: DVR/NVR/Network Camera/Sp	peed Dome/Security Contr	o Used: 92/ Unlimits	ed Buy More	
For devices with health monitoring disabled, you cannot upgrade device firm and check device health status.	nvare, set linkage rules (the exi	cting linkage rules will be invalid; set and receive	exceptions,	
Devices with Health Monitoring Disabled: 48	Devices with H	earth Monitoring Brabled: 90		
Search Q	Search			
V 🗋 Al Stel		*1		
~ 🗆 🛛 🖈	~			
		M DS-38 -0.88430)		
■ 05-PM (0000)		05-2CD (5438)		
× 🗆 🛛	~ @	302		
C 5-3613189-62(886586219)		D5-K11 (09315)		
V 🗌 \varTheta 🛛 Pitel	× 🗆 0	G32		
Q005.		DS-2C031 (82069)		
C G MANNA Annual		At Manager (Bastling and b		

Figura 9-1 Impostazioni di monitoraggio dello stato

Capitolo 10 monitoraggio dello stato

Il portale fornisce il modulo Monitoraggio dello stato per la gestione delle risorse del sistema. Sono disponibili due moduli nel Monitoraggio dello stato.

• Il modulo **Health Status** fornisce informazioni quasi in tempo reale sullo stato dei dispositivi aggiunti alla piattaforma. Inoltre, se sono stati aggiunti switch a una piattaforma, è possibile controllare lo stato del dispositivo e quello del collegamento in modo visuale tramite la topologia di rete. Le informazioni di stato, importanti per la manutenzione dei dispositivi gestiti sulla piattaforma Hik-ProConnect, consentono di individuare la sorgente delle eccezioni e determinare il metodo per risolvere i problemi in tempo, contribuendo a far funzionare il sistema senza intoppi.

iNota

Gli installatori sono solo in grado di visualizzare le informazioni di stato dei dispositivi della piattaforma loro assegnata. L'amministratore di installazione è in grado di visualizzare le informazioni di stato dei dispositivi in tutte le piattaforme.

• Il modulo **Exception Center** visualizza tutta la cronologia delle notifiche relative alle eccezioni dei dispositivi e dei canali.

iNota

Gli installatori sono solo in grado di visualizzare le eccezioni dei dispositivi della piattaforma loro assegnata. L'amministratore di installazione è in grado di visualizzare le eccezioni dei dispositivi in tutte le piattaforme.

10.1 Visualizzazione dello stato dei dispositivi in tutte le piattaforme

Gli installatori sono in grado di visualizzare lo stato di ciascun dispositivo in tutte le piattaforme assegnate. L'amministratore di installazione è in grado di visualizzare lo stato di ciascun dispositivo in tutte le piattaforme.

Fare clic su **Health Monitoring** \rightarrow **Health Status** sul pannello Navigation per accedere alla pagina Health Monitoring, quindi selezionare **All Sites** dall'elenco delle piattaforme.

Per ciascun tipo di dispositivo, è possibile visualizzare i dispositivi totali e quelli che presentano anomalie.

È possibile visualizzare il numero totale di dispositivi e il numero di quelli anomali di ciascun tipo di dispositivo.

Per conoscere la descrizione e le operazioni del dispositivo, fare riferimento alla tabella seguente.

Dispositivo di codifica	Fare riferimento alla sezione Dispositivo di codifica.
Dispositivo di controllo degli accessi	Fare riferimento alla sezione Dispositivo di controllo degli accessi.
Dispositivo di controllo della sicurezza	Fare riferimento alla sezione Dispositivo di controllo della sicurezza.
Dispositivo videocitofono	Fare riferimento alla sezione Dispositivo videocitofono.
Campanello	Fare riferimento alla sezione <i>Campanello</i> .
Hik-ProConnect Box	Fare riferimento alla sezione <i>Hik-ProConnect Box</i> .
Switch	Fare riferimento alla sezione Switch .

Tabella 10-1 Collegamenti per diversi tipi di dispositivi

Dispositivo di codifica

È possibile visualizzare lo stato, tra cui lo stato di rete, il numero di telecamere collegate, lo stato dell'archivio, l'uso del disco rigido, l'orario dell'ultimo controllo, lo stato di registrazione sovrascritta, ecc.

iNota

È possibile controllare la perdita del segnale video delle telecamere analogiche.

Telecamera offline

Il numero a sinistra della barra rappresenta il numero di telecamere offline/totali collegate al dispositivo.

Sono disponibili le seguenti operazioni.

- Passare il cursore sul nome del dispositivo per visualizzarne tipo e versione.
- Fare clic su 🕸 nella colonna Operation per configurare da remoto i parametri del dispositivo. Per i dettagli, consultare il manuale dell'utente del dispositivo.
- Fare clic su **Refresh** per controllare tutti i dispositivi di codifica di tutte le piattaforme.
- Selezionare Abnormal Only per visualizzare solo i dispositivi che presentano anomalie.
- Selezionare **Display Authorized Device Only** per visualizzare i dispositivi la cui autorizzazione alla configurazione è stata concessa solo all'installatore.
- Fare clic su > per visualizzare le telecamere collegate al dispositivo e poi lo stato online/offline di ciascuna di esse.
- Fare clic su > per visualizzare le informazioni sul disco rigido del DVR, tra cui i risultati di valutazione del controllo automatico, i risultati di valutazione globale, lo stato operativo, il tempo di utilizzo, la temperatura del disco rigido le informazioni S.M.A.R.T.
- Spostare il cursore su 🐄 nella colonna Site per visualizzare le informazioni relative al proprietario della piattaforma e al suo responsabile, ad esempio il nome e il numero di telefono.
- Fare clic su <a>> nella colonna Operation per controllare manualmente il dispositivo di codifica selezionato.
- Fare clic su 🗈 nella colonna Operation e selezionare le telecamere per visualizzare i video in tempo reale.

- Se non si dispone delle autorizzazioni per la visualizzazione in tempo reale, è possibile richiederla all'utente finale. Per i dettagli, fare riferimento alla sezione *Richiesta dell'autorizzazione per un dispositivo*.
- Se una telecamera selezionata dispone di crittografia del flusso abilitata, è necessario inserire il codice di verifica del dispositivo prima di poterne visualizzare il video live.
- Il codice di verifica del dispositivo viene creato quando si connette il dispositivo al servizio Hik-Connect. Per i dettagli, fare riferimento alla sezione Aggiunta di dispositivi rilevati online.
- Se l'icona ① appare vicino al nome del dispositivo, significa che non si dispone dell'autorizzazione per configurarlo oppure l'indirizzo IP, il dominio o il DDNS impostato per il dispositivo non è valido. È possibile passare il cursore sull'icona, quindi richiedere l'autorizzazione all'utente finale, riconfigurare l'indirizzo IP/il dominio oppure il DDNS in base alle istruzioni visualizzate.

iNota

- Per i dettagli su come richiedere l'autorizzazione per la configurazione, fare riferimento alla sezione *Richiesta dell'autorizzazione per un dispositivo*.
- Per i dettagli su come configurare l'indirizzo IP/il dominio del dispositivo, fare riferimento alla sezione *Aggiunta di dispositivi tramite l'indirizzo IP*. Per i dettagli su come configurare il DDNS, fare riferimento alla sezione *Configurazione del DDNS dei dispositivi*.

Dispositivo di controllo degli accessi

È possibile visualizzare lo stato, tra cui lo stato di rete, il numero di porta, l'ora dell'ultimo controllo, ecc.

Sono disponibili le seguenti operazioni.

- Passare il cursore sul nome del dispositivo per visualizzarne tipo e versione.
- Fare clic su **Refresh** per controllare i dispositivi di controllo degli accessi.
- Selezionare **Abnormal Only** per visualizzare solo i dispositivi che presentano anomalie.
- Selezionare **Display Authorized Device Only** per visualizzare solo i dispositivi per cui è stata concessa l'autorizzazione alla configurazione.
- Spostare il cursore su 🐭 nella colonna Site per visualizzare le informazioni relative al proprietario della piattaforma e al suo responsabile, ad esempio il nome e il numero di telefono.
- Fare clic su <a>> nella colonna Operation per controllare manualmente il dispositivo di controllo degli accessi selezionato.
- Se l'icona 0 appare vicino al nome del dispositivo, significa che non si dispone dell'autorizzazione per configurarlo. È possibile richiedere l'autorizzazione all'utente finale.

Per i dettagli su come richiedere l'autorizzazione per la configurazione, fare riferimento alla sezione *Richiesta dell'autorizzazione per un dispositivo*.

Dispositivo di controllo della sicurezza

È possibile visualizzare i diversi stati tra cui stato di rete, batteria residua, ID ARC, numero di dispositivi che presentano anomalie, ecc.

iNota

La visualizzazione della batteria residua dei dispositivi non è supportata.

La seguente tabella contiene la descrizione di ciascuna icona di stato.

Tabella 10-2 Descrizione delle icone

lcona	Descrizione				
	energia residua della batteria sufficiente.				
	energia residua della batteria insufficiente.				
8	indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è normale.				
8	indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è media.				
•	indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è scarsa.				
0	indica un'anomalia della potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza.				
Ĭ	allarme attivato.				
*	manomissione dispositivo.				
.	esclusione di zona.				
4	eccezione di attivazione.				

Sono disponibili le seguenti operazioni.

- Passare il cursore sul nome del dispositivo per visualizzarne tipo e versione.
- Fare clic su 🕸 nella colonna Operation per configurare da remoto i parametri del dispositivo. Per i dettagli, consultare il manuale dell'utente del dispositivo.

iNota

La configurazione da remoto non è supportata se il dispositivo è inserito.

- Fare clic su **Refresh** per controllare i dispositivi di controllo degli accessi.
- Selezionare Abnormal Only per visualizzare solo i dispositivi che presentano anomalie.
- Selezionare **Display Authorized Device Only** per visualizzare solo i dispositivi per cui è stata concessa l'autorizzazione alla configurazione.
- Se l'icona ①appare vicino al nome del dispositivo, passare il cursore su tale simbolo, quindi fare clic su **Upgrade** nella finestra a comparsa per effettuare l'upgrade del dispositivo. Per i dettagli, fare riferimento alla sezione **Upgrade del firmware del dispositivo**.
- Se l'icona ① appare vicino al nome del dispositivo, significa che la modalità conforme a EN50131 è abilitata o che non si dispone dell'autorizzazione per configurarlo. Nel primo caso, passare il cursore sull'icona, quindi fare clic su Authenticate nella finestra a comparsa per effettuare l'autenticazione prima di visualizzare lo stato del dispositivo. Nel secondo caso, è possibile richiedere l'autorizzazione all'utente finale.

Per i dettagli su come richiedere l'autorizzazione per la configurazione, fare riferimento alla sezione *Richiesta dell'autorizzazione per un dispositivo*.

• Fare clic su > per visualizzare lo stato delle aree e dei dispositivi collegati al pannello di controllo di sicurezza.

È possibile passare il cursore su una zona specifica per visualizzarne le eccezioni.

- Spostare il cursore su ****** nella colonna Site per visualizzare le informazioni relative al proprietario della piattaforma e al suo responsabile, ad esempio il nome e il numero di telefono.
- Fare clic su <a>> nella colonna Operation per controllare manualmente il dispositivo di controllo degli accessi selezionato.

Dispositivo videocitofono

È possibile visualizzare gli stati quali lo stato di rete e l'ora dell'ultimo controllo. Sono disponibili le seguenti operazioni.

- Passare il cursore sul nome del dispositivo per visualizzarne tipo e versione.
- Fare clic su **Refresh** per controllare i videocitofoni.
- Fare clic su 🐵 nella colonna Operation per controllare manualmente il dispositivo selezionato.
- Se l'icona ① appare vicino al nome del dispositivo, significa che non si dispone dell'autorizzazione per configurarlo. È possibile richiedere l'autorizzazione all'utente finale.

iNota

Per i dettagli su come richiedere l'autorizzazione per la configurazione, fare riferimento alla sezione *Richiesta dell'autorizzazione per un dispositivo*.

Campanello

È possibile visualizzare le informazioni tra cui modello del dispositivo, stato di rete, stato della scheda SD, orario dell'ultimo controllo, ecc.

Sono disponibili le seguenti operazioni.

- Passare il cursore sul nome del dispositivo per visualizzarne tipo e versione.
- Fare clic su **Refresh** per controllare i dispositivi di controllo degli accessi
- Selezionare Abnormal Only per visualizzare solo i dispositivi che presentano anomalie.
- Selezionare **Display Authorized Device Only** per visualizzare i dispositivi la cui autorizzazione alla configurazione è stata concessa solo all'installatore.
- Fare clic su 🐵 nella colonna Operation per configurare da remoto i parametri del dispositivo. Per i dettagli, consultare il manuale d'uso del dispositivo.
- Fare clic su <a>> nella colonna Operation per controllare manualmente il dispositivo di codifica selezionato.
- Fare clic su 🖾 nella colonna Operation e selezionare le telecamere per visualizzare i video in tempo reale.

iNota

- Se non si dispone delle autorizzazioni per la visualizzazione in tempo reale, è possibile richiederla all'utente finale. Per i dettagli, fare riferimento alla sezione *Richiesta dell'autorizzazione per un dispositivo*.
- Se una telecamera selezionata dispone di crittografia del flusso abilitata, è necessario inserire il codice di verifica del dispositivo prima di poterne visualizzare il video live.
- Il codice di verifica del dispositivo viene creato quando si connette il dispositivo al servizio Hik-Connect. Per i dettagli, fare riferimento alla sezione *Aggiunta di dispositivi rilevati online*.
- Se l'icona ① appare vicino al nome del dispositivo, significa che non si dispone dell'autorizzazione per configurarlo. È possibile richiedere l'autorizzazione all'utente finale.

iNota

Per i dettagli su come richiedere l'autorizzazione per la configurazione, fare riferimento alla sezione *Richiesta dell'autorizzazione per un dispositivo*.

• Se l'icona ①appare vicino al nome del dispositivo, passare il cursore su tale simbolo, quindi fare clic su **Upgrade** nella finestra a comparsa per effettuare l'upgrade del dispositivo. Per i dettagli, fare riferimento alla sezione **Upgrade del firmware del dispositivo**.

Hik-ProConnect Box

È possibile visualizzare lo stato della rete di Hik-ProConnect Box, il numero di canali offline (telecamere) aggiunti ad esso e l'ultima volta in cui è stato controllato il dispositivo.

È inoltre possibile fare clic su >> per visualizzare le informazioni di base (ad esempio, il numero di serie e il modello del dispositivo) e l'elenco dettagliato dei canali online e offline (telecamere). Inoltre, sono disponibili le operazioni seguenti:

- Fare clic su 🕸 nella colonna Operation per configurare da remoto i parametri del dispositivo. Per i dettagli, consultare il manuale d'uso del dispositivo.
- Fare clic su 🞯 nella colonna Operation per controllare manualmente il dispositivo selezionato.

Switch

È possibile visualizzare lo stato della rete dello switch (online/offline), il numero di porte online dello switch e l'ultima volta in cui è stato controllato il dispositivo. Inoltre, sono disponibili le operazioni seguenti:

- Fare clic su 🐵 nella colonna Operation per controllare manualmente il dispositivo selezionato.
- Fare clic su 💿 nella colonna Operation per riavviare da remoto lo switch.
- Fare clic su 🕆 nella colonna Operation per visualizzare la topologia di questo switch. Per i dettagli sulla topologia, fare riferimento alla sezione **Topologia di rete**.

Fare clic su >> per visualizzare le informazioni dettagliate sullo switch, tra cui l'utilizzo della memoria e della CPU, lo stato della porta (Alarm, Normal, Not Connected), ecc.

Basic Information					
Site Name:	v	Device Serial No.: E86	5	Device Model: DS-3E1	
Device Status					
Memory Usage: 💻	42%				
CPU Usage: 💻	14%				
Port Status					
n RJ45 Port St	FP Port			Alarn	n 💻 Normal 🔳 Not Connect
				20 22 24	
Port Name	Status	Bit Rate	Bandwidth Usage	Peer Device	Operation
Gel	Not Connected	1 0 1 0	0 1 0 1		
Ge2	Not Connected	10	0 1		•••

Figura 10-1 Dettagli relativi allo switch

Spostare il cursore sull'icona dello switch per visualizzare l'immagine ingrandita delle porte. Fare clic su $\cdots \rightarrow$ **Restart Port** per riavviare la porta.

Se una porta dispone dell'allarme e si desidera eliminarlo, fare clic su Clear Alarm.

10.2 Visualizzazione dello stato dei dispositivi in piattaforme specifiche

È possibile visualizzare lo stato dei dispositivi in una piattaforma specifica assegnata.

Passaggi

- 1. Fare clic su **Health Monitoring** → **Health Status** nel pannello Navigation per accedere alla pagina Health Status.
- 2. Selezionare una piattaforma specifica dall'elenco relativo. Verrà visualizzato lo stato dei dispositivi nella piattaforma.
- 3. Opzionale: È possibile effettuare le seguenti operazioni.

Filtraggio dati	Selezionare Abnormal Only per visualizzare solo i dispositivi che presentano anomalie. Selezionare Display Authorized Device Only per visualizzare i dispositivi la cui autorizzazione alla configurazione è stata concessa solo all'installatore.
Aggiornamento del firmware del dispositivo	Se sono presenti upgrade disponibili per i pannelli di controllo di sicurezza, viene visualizzato un numero rosso su Upgrade che indica i dispositivi aggiornabili. In questo caso, è possibile fare clic su Upgrade e selezionare i dispositivi aggiornabili e poi selezionare Upgrade per aggiornare quelli selezionati.
	i Nota
	Per i dettagli, fare riferimento alla sezione Upgrade del firmware del dispositivo.
Diagnostica dei dispositivi della piattaforma	Fare clic su Health Check per aprire la finestra di controllo dello stato, quindi fare clic su Check now per eseguire la diagnosi dei dispositivi presenti sulla piattaforma. Una volta completata la diagnostica, è possibile visualizzare lo stato di ciascun dispositivo presente nella piattaforma. Per il pannello di controllo di sicurezza di AX Pro, NVR e DVR è inoltre possibile fare clic su View Report per esportare il report di diagnostica come file PDF sul computer locale.
Visualizzazione delle informazioni sul proprietario della piattaforma	Fare clic su Site Owner per visualizzare le informazioni sul proprietario della piattaforma, tra cui il nome, l'indirizzo e-mail e il numero di telefono.

Visualizzazione delle informazioni sul responsabile della piattaforma	Fare clic su Site Manager per visualizzare le informazioni sul responsabile della piattaforma, tra cui il nome, l'indirizzo e-mail e il numero di telefono.		
Controllo dei dispositivi nelle piattaforme	Fare clic su Refresh per controllare tutti i dispositivi presenti nella piattaforma.		
Configurazione da remoto	Selezionare un dispositivo e fare clic su Remote Configuration per configurare da remoto i parametri del dispositivo.		
	i Nota		
	• Per poter eseguire la configurazione, è necessario che il dispositivo sia online.		
	• Per i dettagli, consultare il manuale d'uso del dispositivo.		
Controllo di un solo dispositivo	Selezionare un dispositivo e fare clic su 🧐 per controllarlo.		
Riconfigurazione dell'IP/del dominio del dispositivo di codifica	Spostare il cursore su ⁽¹⁾ , quindi fare clic su Edit IP/Domain per riconfigurare l'IP/il dominio del dispositivo. Per i dettagli su come riconfigurare l'IP/il dominio, fare riferimento alla sezione <i>Aggiunta di dispositivi tramite l'indirizzo IP o il nome di dominio</i> .		
Riconfigurazione del DDNS	Spostare il cursore su ⁽¹⁾ , quindi fare clic su Configure DDNS per riconfigurare il DDNS del dispositivo. Per i dettagli su come configurare il DDNS, fare riferimento alla sezione Configurazione del DDNS dei dispositivi .		
Visualizzazione dei dettagli del dispositivo di codifica	È possibile visualizzare lo stato di rete, lo stato dell'archivio, l'uso del disco rigido, lo stato di registrazione sovrascritta, ecc. Inoltre, è possibile fare clic sul dispositivo di codifica per visualizzarne i dettagli, tra cui le informazioni di base (ad esempio, il tipo di dispositivo e il numero di serie), e lo stato di rete di ciascuna telecamera collegata ad esso (è possibile fare clic su e selezionare le telecamere collegate, quindi fare clic su e visualizzare i video in tempo reale). Se il dispositivo di codifica è un DVR, è inoltre possibile visualizzare le informazioni relative al suo disco rigido, tra cui i risultati di valutazione del controllo automatico, lo stato operativo, il tempo di utilizzo, la temperatura del disco rigido e le informazioni S.M.A.R.T. È possibile controllare la perdita del segnale video delle telecamere analogiche.		

	 Se non si dispone delle autorizzazioni per la visualizzazione live, è possibile richiederla all'utente finale. Per i dettagli, fare riferimento alla sezione <i>Richiesta dell'autorizzazione per un dispositivo</i>. Se una telecamera dispone di crittografia del flusso abilitata, è necessario inserire il codice di verifica del dispositivo nella finestra a comparsa prima di poterne visualizzare il video live. Il codice di verifica del dispositivo viene creato quando si connette la telecamera al servizio Hik-Connect. Per i dettagli, fare riferimento alla sezione <i>Aggiunta di dispositivi rilevati online</i>. 			
Visualizzazione dei dettagli relativi al dispositivo di controllo degli accessi	Fare clic sul dispositivo di controllo degli accessi per visualizzarne i dettagli tra cui informazioni di base come tipo di dispositivo, numero di serie, stato del dispositivo, stato di rete e numero di porte collegate.			
Visualizzazione dei dettagli del pannello di controllo di sicurezza	 Fare clic su un pannello di controllo di sicurezza per visualizzarne i dettagli, tra cui le informazioni di base e lo stato delle aree, le telecamere e i dispositivi collegati. L'elenco seguente mostra la descrizione di ciascuna icona di stato. energia residua della batteria sufficiente. energia residua della batteria insufficiente. energia residua della batteria insufficiente. indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è normale. indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è scarsa. indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è scarsa. indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è scarsa. indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è scarsa. indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è scarsa. indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è scarsa. indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è scarsa. indica che la potenza dei segnali di comunicazione tra il dispositivo e il pannello di controllo di sicurezza è scarsa. 			
Visualizzazione dei dettagli del videocitofono	Fare clic su un videocitofono per visualizzarne le informazioni di base e lo stato di rete.			
Visualizzazione dei dettagli relativi al campanello	Fare clic su un campanello per visualizzarne le informazioni di base (tra cui, il modello, il tipo e il numero di serie del dispositivo). Se le telecamere sono collegate al campanello, è inoltre possibile fare clic su una di esse per visualizzare il video in tempo reale.			

Visualizzazione dei	Fare clic su Hik-ProConnect Box per visualizzarne le informazioni di
dettagli relativi a	base e i canali aggiunti ad esso.
Hik-ProConnect Box	È inoltre possibile visualizzare lo stato online dei canali aggiunti.
Visualizzazione dei dettagli relativi allo switch	 Gli switch vengono visualizzati per scheda. Fare clic su uno switch per visualizzarne le informazioni, tra cui il modello, il tipo e il numero di serie del dispositivo, l'ora dell'ultimo controllo, lo stato della rete, l'utilizzo della memoria e della CPU, lo stato della porta (Alarm, Normal, Not Connected). Spostare il cursore sull'icona dello switch per visualizzare la relativa immagine ingrandita. Fare clic su ··· → Restart Port per riavviare la porta. Fare clic su ··· → Restart Port per riavviare la porta. Fare clic su ··· → Restart Port per riavviare della pagina per visualizzare la topologia di questo switch. Per i dettagli sulla topologia, fare riferimento alla sezione <i>Topologia di rete</i>. Fare clic su ··· → nella colonna Operation per controllare manualmente il dispositivo selezionato. Se una porta dispone dell'allarme e si desidera eliminarlo, fare clic su Clear Alarm.

10.3 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.

iNota

- 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 alla configurazione, fare riferimento alla sezione **Richiesta dell'autorizzazione per un dispositivo**.
- Se non è stato attivato il servizio di monitoraggio dello stato per lo switch, alcune funzioni della topologia (ad esempio, la visualizzazione dello stato del dispositivo sulla topologia) non sono disponibili. Per i dettagli su come attivare il servizio di monitoraggio dello stato sui dispositivi, fare riferimento alla sezione *Impostazione dei dispositivi coperti dal pacchetto di monitoraggio dello stato*.

È possibile accedere alla pagina Network Topology nei modi seguenti:

• Nel pannello di navigazione, fare clic su **Site**, quindi selezionare il nome di una piattaforma per accedere alla pagina dei relativi dettagli. Dopodiché fare clic su **View Topology**.

Se NON è stato attivato il servizio di monitoraggio dello stato sullo switch, è possibile accedere alla pagina Network Topology solo in questo modo.

- Nel pannello di navigazione, fare clic su Health Monitoring → Health Status, selezionare All Sites dall'elenco delle piattaforme, quindi scegliere Network Switch e poi fare clic su nella colonna Operation dell'elenco degli switch.
- Nel pannello di navigazione, fare clic su **Health Monitoring** → **Health Status**, selezionare una piattaforma dall'elenco per accedere alla pagina dei relativi dettagli, quindi scegliere **Topology**.



Figura 10-2 Pagina Network Topology

La tabella seguente illustra le descrizioni delle operazioni disponibili nella pagina Network Topology.

Tabella	10-3	Operazioni	disponibili
---------	------	------------	-------------

Operazione	Descrizione				
	È possibile fare clic su 😻 vicino a More per visualizzare le legende (vedere la figura qui sotto).				
Visualizza legenda	Device Type Remove Laber Cypical note — rooman — buy — albuce () forcometeree Device Type Remove Switch Remove Network Switch III Video Intercom Device Remove Control Device () Thermal Cemera () Speed Dome () Network Cem Remove Control Panel () Doorbell Remove Hik-ProConnect Box () DVR/NVR () Unknown Device Type				
	Device Status	1000 Xe-10000000000-10000 2001/001/001	211 0 Xi-1000000000-1000 10010012001200		
	Normal	Abnormal	Offline	Devices not Under the Site	
	Figura 10-3 Legenda				

Operazione	Descrizione			
	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 spostare il cursore sul nodo principale corrente e fare clic su i per impostare uno switch come tale.			
Modifica nodo principale	Figura 10-4 Modifica nodo principale			
	Fare clic su Refresh per aggiornare la struttura della topologia.			
	i Nota			
Aggiorna topologia	Lo stato del dispositivo non viene aggiornato.			
Visualizza nelle schede	Per visualizzare altre informazioni sullo stato del dispositivo in una panoramica di tutti quelli collegati agli switch, fare clic su Display in Cards per vedere i dettagli del dispositivo nelle schede.			
Sposta topologia di rete	Trascinare la topologia di rete per spostarla.			
Ingrandisci/riduci zoom	È possibile fare clic su +/ – nell'angolo in alto a sinistra per ingrandire/ridurre la topologia.			
Regola dimensione della	È possibile fare clic su 🔅 nell'angolo in alto a sinistra per adattare la dimensione della topologia alla finestra di visualizzazione.			
τομοιοβία	È possibile fare clic su 👯 nell'angolo in alto a sinistra per visualizzare la topologia nella modalità a schermo intero.			
Visualizza miniatura	Se la topologia è stata ingrandita, è possibile fare clic su <a> per visualizzare la miniatura che indica la posizione corrente del cursore sulla topologia.			

Operazione	Descrizione				
Cerca dispositivi nella topologia	È possibile inserire una parola chiave di un dispositivo per cercarlo nella topologia. Una volta individuato, la topologia esegue automaticamente la panoramica e lo zoom per visualizzarlo.				
	È possibile visualizzare le informazioni di collegamento in base alle legende indicate nella seguente immagine.				
Visualizza informazioni di collegamento	Network Cable Optical Fiber Normal Busy Blocked 🚫 Disconned				
	Figura 10-5 Legenda delle informazioni di collegamento				
Visualizza dettagli della piattaforma	È possibile spostare il cursore su un collegamento specifico per visualizzarne i dettagli, ad esempio l'upstream, il downstream, il nome e lo stato della porta.				
	Se non si dispone dell'autorizzazione per configurare un dispositivo, viene visualizzato un messaggio che invita a richiederla. Per farlo, è possibile fare clic su Apply for Permission .				
Richiedi autorizzazione alla configurazione	i Nota				
	In assenza dell'autorizzazione, la posizione del dispositivo nella topologia di rete potrebbe essere errata.				
	È possibile selezionare uno switch sulla topologia per visualizzare le relative informazioni, tra cui quelle di base, lo stato del dispositivo e lo stato della porta.				
Visualizza i dettagli dello switch e controllalo	È inoltre possibile eseguire alcune operazioni, quali il riavvio dello switch e della porta. Per ulteriori informazioni, fare riferimento alla sezione <i>SwitchVisualizzazione dello stato dei</i> <i>dispositivi in piattaforme specifiche</i> .				
	i Nota				
	Non è possibile visualizzare i dettagli di uno switch virtuale.				

Operazione	Descrizione				
Visualizza i dettagli di un altro dispositivo e configuralo	Se un dispositivo online è connesso allo switch e si trova sulla stessa piattaforma di quest'ultimo, vengono visualizzati l'icona e il numero di serie del dispositivo, che sono selezionabili per vedere le relative informazioni, incluse quelle di base (ad esempio, il modello del dispositivo) e lo stato del dispositivo (ad esempio, lo stato della rete). È inoltre possibile fare clic su <a>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>				
	 In dispositivo sconosciuto (ad esempio, un computer) connesso allo switch viene visualizzato come e non è possibile visualizzare le relative informazioni. Se un dispositivo online è connesso allo switch ma NON si trova sulla stessa piattaforma di quest'ultimo, viene visualizzato un numero di serie virtuale generato casualmente per il dispositivo e non è possibile visualizzare le relative informazioni. 				

10.4 Centro eccezioni

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

- 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*.

Fare clic su **Health Monitoring** \rightarrow **Exception Center** per accedere alla pagina Exception Center come illustrato di seguito.

iNota

Search Q	Last 7 Days	✓ All Exceptions	~		Auto-Update	Export 🛛 Open in New Window
	Time ‡	Site Name 🗘	Source ‡	Exception Type 🗘	Site Owner 🗘	Received by \$
V S All Sites	2019/12/24 10:26:03	This site is for test only	D - Camera 1	Offline		
This site is for test only	2019/12/23 20:52:10	This site is for test only	2 9	Offline		🖾 📕 🔯
	2019/12/23 20:52:09	This site is for test only	2 - Camera 1	Offline		1 II II
	2019/12/23 17:50:36	This site is for test only	E 3- Camera 1	Offline		e.
	2019/12/23 17:50:34	This site is for test only	D 3- Camera 1	Offline		ē
	2019/12/23 16:20:39	This site is for test only	D 8- Camera 1	Offline		e
	2019/12/23 14:55:53	This site is for test only	D 3	Offline		e
	2019/12/21 17:12:05	This site is for test only	E 9- Camera 1	Offline		Q.
	2019/12/21 17:12:04	This site is for test only	D 9	Offline		e
	2019/12/21 17:12:01	This site is for test only	E 3	Offline		. C
	2019/12/20 19:12:05	This site is for test only	D	Offline		Q. C.
	2019/12/20 19:12:04	This site is for test only	D - Camera 1	Offline		Q 8
	2019/12/20 17:28:14	This site is for test only	E ?- Camera 1	Offline		Q +
	2019/12/20 17:28:13	This site is for test only	D 3- Camera 1	Offline		e
	2019/12/20 15:27:12	This site is for test only	D 3- Camera 1	Offline		ē
	Total 26 Record(s) 100	~				1 > 1 /1 Go

Figura 10-6 Exception Center

Verifica dei dettagli dell'eccezione

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

- 1. Selezionare una piattaforma nel relativo elenco per visualizzare le eccezioni dei dispositivi presenti in tale piattaforma. Inoltre è possibile selezionare un dispositivo o un canale per visualizzare le eccezioni che si sono verificate sul dispositivo o sul canale.
- 2. Impostare il periodo di tempo. Vengono visualizzate le eccezioni ricevute durante questo periodo.
- 3. Selezionare i tipi di eccezione da verificare. I tipi di eccezione includono l'eccezione del dispositivo e l'eccezione del canale.

È possibile attivare il pulsante **Auto-Update** in modo che nella tabella vengano visualizzate in tempo reale le eccezioni più recenti ricevute dal Portale.

iNota

L'aggiornamento automatico non sarà valido durante la visualizzazione dei registri della cronologia (inclusi i registri dopo pagina 1 e quelli ricevuti fino a oggi).

Esportazione di registrazioni delle eccezioni

Una volta filtrate le eccezioni, fare clic su **Export** e selezionare il formato del file con cui esportare i record relativi alle eccezioni sul computer locale.

iNota

Al momento, i formati supportati del file esportato sono: CSV, Excel e PDF

Apri in nuova finestra

Fare clic su **Open in New Window** nell'angolo in alto a destra per aprire una nuova finestra del browser e visualizzare il Centro eccezioni. Con questa funzione è possibile visualizzare simultaneamente il Centro eccezioni e altre pagine.

Capitolo 11 Ricerca dei registri operativi

Tutte le informazioni sulle operazioni (tra cui operatore, tempo di attività, piattaforma, target e risultato dell'operazione, ecc.) eseguite dai dipendenti (in riferimento all'amministratore di installazione e agli installatori) saranno registrate in modo da poter essere ricercate nei registri operativi di ciascun dipendente, al fine di verificare l'origine di eventuali problemi delle piattaforme.

Fare clic su **Company** \rightarrow **Operation Log** per visualizzare l'elenco dei dipendenti e tutti i registri operativi. È possibile cercare i registri per dipendente, piattaforma e ora.

iNota

- I registri di tutti gli account sono disponibili per gli account dotati di autorizzazione alla gestione di account e ruolo. Gli account privi di autorizzazione per la gestione di account e ruoli, possono visualizzare solo i propri registri.
- I registri di tutte le piattaforme sono disponibili per gli account dotati di autorizzazione alla gestione di tutte le piattaforme. Gli account che non dispongono di tale autorizzazione possono solo visualizzare i registri della piattaforma assegnata.

Employee	Name ‡	Employee's Email 🗘	Client	Site ‡	Operation Target 🗘	Operation Content 🗘	Schedule ‡
IIA 👤 🖌	lulu	.81@qq.com	Portal			Login Succeeded	7, Nov, 2020 10:57:45
🖂 👤 de	ddc	itest1@sina.com	Portal			Login Succeeded	7. Nov. 2020 10:51:30
 L 	p h	-75@qq.com	Portal	hucong	1260	Adding Device Succeeded	7. Nov. 2020 10:35:35
	p h	.75@qq.com	Portal			Login Succeeded	7, Nov, 2020 10:32:17
	lulu	.81@qq.com	Portal			Login Succeeded	6. Nov. 2020 23:55:57
₩ 1 P	lulu	.81@qq.com	Portal			Login Succeeded	6, Nov, 2020 23:35:56
 ✓ ▲ ° ✓ ▲ st 	lulu	81@qq.com	Portal	B3	D418	Remove Device from Health Monitoring Package Succeeded	6. Nov. 2020 21:41:26
🖌 💄 sh	lulu	.81@qq.com	Portal	83	D418	Deleting Device Succeeded	6. Nov. 2020 21:41:25
✓ ▲ sc	lulu	.81@qq.com	Portal	83	D418	Adding Device Succeeded	6, Nov, 2020 21:40:58
Sites	lulu	81@qq.com	Portal			Login Succeeded	6. Nov. 2020 21:39:36
All Logs 🗸 🗸	huha	81@aa.com	Portal			Login Succeeded	6. Nov. 2020 20:48:08
Schedule							
Last 30 Days 🗸 🗸	lulu	81@qq.com	Portal	83	D418	Deleting Device Succeeded	6, Nov, 2020 20:43:49
a sure de la constante de la co	Tulu	.81@qq.com	Portal	83	D418	Adding Device Succeeded	6. Nov. 2020 20:43:12
Search	Total 5976 Recor	rd(s) 20 ~			< 1 2 3 4	5 6 299 > 1	/ 299 Go

Figura 11-1 Ricerca dei registri operativi

Capitolo 12 Strumenti

Hik-ProConnect fornisce strumenti, come il calcolatore del disco e il calcolatore del canale NVR, che aiutano a migliorare l'efficienza del lavoro.

Nella schermata principale, fare clic su **Tools** o **Tools** per accedere alla pagina degli strumenti.

Calcolatore del disco

Questo strumento serve a calcolare il tempo e lo spazio di registrazione impostando i relativi parametri.

Calcolatore del canale NVR

Questo strumento serve a calcolare il numero di telecamere di rete che possono essere collegate all'NVR impostando i relativi parametri.

Calcolatore della lunghezza focale

Questo strumento serve a calcolare la lunghezza focale e la distanza dell'oggetto impostando i relativi parametri, ad esempio le dimensioni del sensore. È possibile visualizzare i dati consigliati dallo strumento.

Calcolatore della larghezza di banda

Questo strumento serve a calcolare la larghezza di banda necessaria per una telecamera di rete o un NVR impostando parametri quali il numero del canale e la risoluzione.

