TELECAMERA DI RETE WEB

Manuale d'uso
firmware 5.0

V1.0.0

Introduzione

Generale

Questo manuale illustra le funzioni, la configurazione, l'utilizzo generale e la manutenzione della telecamera di rete.

Istruzioni di sicurezza

All'interno del manuale possono comparire i seguenti indicatori di pericolo, il cui significato è definito qui sotto.

Indicatori di pericolo	Significato
 AVVERTENZA	Indica una situazione a medio o basso rischio che, se non viene evitata, può causare lesioni di leggera o moderata entità.
 ATTENZIONE	Indica un rischio potenziale che, se non evitato, può causare danni alla proprietà, perdite di dati, un peggioramento delle prestazioni o effetti imprevedibili.
 CONSIGLI	Spiegano metodi utili per risolvere un problema o per aiutarvi a risparmiare tempo.
 NOTA	Fornisce informazioni aggiuntive che completano quelle riportate nel testo.

Cronologia delle revisioni

Versione	Contenuto della revisione	Data di rilascio
V1.0.0	Prima versione.	Ottobre 2020

Indicazioni sul manuale

Questo manuale serve solo come riferimento. In caso di discrepanza fra il manuale e il prodotto, quest'ultimo prevarrà.

Non ci riteniamo responsabili per eventuali perdite causate da un utilizzo non conforme a quanto esposto nel manuale.

Il manuale verrà aggiornato in base alle leggi e ai regolamenti più recenti delle relative giurisdizioni. Per informazioni dettagliate, fare riferimento al manuale cartaceo, al CD-ROM, al codice QR o al nostro sito web ufficiale. In caso di incongruenze tra il manuale cartaceo e la versione elettronica, quest'ultima prevarrà.

Grafiche e software sono soggetti a modifica senza preavviso. Gli aggiornamenti del prodotto possono generare delle differenze tra il prodotto effettivo e le informazioni contenute nel manuale. Contattare il servizio di assistenza per le procedure più recenti e la documentazione supplementare.

Potrebbero inoltre esserci delle differenze nei dati tecnici, nelle descrizioni di funzioni e operazioni, o errori di stampa. In caso di dubbi o vertenze, ci riserviamo il diritto di interpretazione finale.

Se non è possibile aprire il manuale in formato PDF, aggiornare il programma per la lettura dei file PDF o provarne un altro.

Tutti i marchi commerciali, i marchi registrati e i nomi di società presenti nel manuale sono di proprietà dei rispettivi titolari.

In caso di problemi nell'utilizzo del dispositivo, consigliamo di visitare il nostro sito web, contattare il fornitore o il servizio clienti.

In caso di dubbi o controversie, ci riserviamo il diritto di interpretazione finale.

Norme di sicurezza e avvertenze importanti

Sicurezza elettrica

Tutte le procedure di installazione e utilizzo devono rispettare le normative locali per la sicurezza elettrica.
La fonte di alimentazione deve rispettare lo standard SELV (bassissima tensione di sicurezza) e fornire corrente con tensione conforme alle fonti di alimentazione limitata descritte nello standard IEC60950-1. I requisiti di alimentazione sono indicati sull'etichetta del dispositivo.
Accertarsi che il tipo di alimentazione sia corretto prima di mettere in funzione il dispositivo.
Un dispositivo di disconnessione facilmente accessibile deve essere incorporato nel cablaggio dell'edificio di installazione.
Evitare che il cavo di alimentazione, e in particolar modo la spina, la presa di alimentazione e il raccordo che esce dal dispositivo, vengano calpestati o schiacciati.

Ambiente

Non mettere a fuoco il dispositivo quando è puntato in direzione di fonti di illuminazione intense, come le lampade o il sole, per evitare un'eccessiva luminosità o la formazione di macchie di luce. Questi fenomeni non dipendono da un malfunzionamento del dispositivo e riducono la longevità del sensore CMOS (Complementary Metal-Oxide Semiconductor).
Non collocare il dispositivo in ambienti umidi, polverosi, molto caldi o freddi, soggetti a forti radiazioni elettromagnetiche o caratterizzati da un'illuminazione insta bile.
Tenere il dispositivo lontano da qualsiasi tipo di liquidi per evitare danni ai componenti interni.
Tenere i dispositivi per interni al riparo dalla pioggia o dall'umidità per evitare incendi o danni causati dai fulmini.
Consentire una ventilazione adeguata per evitare il surriscaldamento.
Trasportare, utilizzare e stoccare il dispositivo entro i limiti consentiti per umidità e temperatura.
Durante il trasporto, la conservazione e l'installazione, il dispositivo non deve essere soggetto a sollecitazioni intense, forti vibrazioni o schizzi d'acqua.
Per il trasporto del dispositivo, utilizzare l'imballaggio originale o un imballaggio costituito da materiale simile.
Installare il dispositivo in un luogo accessibile solamente a professionisti esperti in protezioni e avvisi di sicurezza. È possibile che il personale non qualificato si ferisca accidentalmente accedendo all'area di installazione durante il normale funzionamento del dispositivo.

Funzionamento e manutenzione ordinaria

Non toccare il dissipatore di calore del dispositivo per evitare ustioni.
Seguire attentamente le istruzioni riportate sul manuale quando si esegue una qualsiasi operazione di smontaggio sul dispositivo; un intervento non professionale potrebbe causare infiltrazioni d'acqua o una cattiva qualità delle immagini. Quando l'essiccante diventa verde o se si trovano tracce di appannamento da condensa sull'obiettivo del dispositivo dopo averlo disimballato, contattare il servizio postvendita per la sostituzione dell'essiccante. (L'essicca nte non è incluso in tutti i modelli).
È consigliabile utilizzare il dispositivo insieme a uno scaricatore di sovratensione per migliorare la protezione dai fulmini.

È consigliabile collegare il dispositivo con messa a terra per migliorarne l'affidabilità.
Non toccare direttamente il sensore delle immagini (CMOS). Lo sporco e la polvere possono essere rimossi con aria compressa o passando delicatamente un panno morbido inumidito d'alcol.
È possibile pulire il corpo del dispositivo utilizzando un panno morbido e asciutto, con l'aggiunta di un po' di detergente delicato per le macchie più ostinate. Per evitare possibili danni al corpo del dispositivo e il conseguente peggioramento delle prestazioni, non pulirlo con solventi volatili come alcol, benzene, diluenti e sostanze simili o detergenti forti o abrasivi.
La cupola di rivestimento è un componente ottico: non toccarla o pulirla con le mani durante l'installazione o il funzionamento. Per rimuovere la polvere, il grasso o le impronte digitali, strofinare delicatamente con cotone privo di petrolio e inumidito con dietile o con un panno morbido e umido. È anche possibile rimuovere la polvere con dell'aria compressa.

AVVERTENZA

Per migliorare la protezione della rete, dei dati del dispositivo e delle informazioni personali, adottare misure di sicurezza che comprendano, in via esemplificativa ma non esaustiva, l'utilizzo e la modifica periodica di una password sicura, l'aggiornamento del firmware all'ultima versione e l'isolamento della rete. Su alcuni dispositiv i con vecchie versioni del firmware, la password ONVIF non verrà modificata automaticamente insieme alla password di sistema e sarà pertanto necessario cambiarla manualmente o aggiornare il firmware.
Utilizzare componenti o accessori standard forniti dal produttore e accertarsi che l'installazione e la manutenzione del dispositivo siano affidate a ingegneri professionisti.
In ambienti in cui vengono utilizzati dispositivi laser, la superficie del sensore per le immagini non deve essere esposta a radiazioni laser.
Se non specificato diversamente, non collegare il dispositivo a due o più fonti di alimentazione. Il mancato rispetto di questa indicazione potrebbe causare danni al dispositivo.

Indice

Introduzione I
Norme di sicurezza e avvertenze importanti III
1 Panoramica 1
1.1 Introduzione 1
1.2 Connessione di rete 1
1.3 Diagramma di configurazione 1
2 Inizializzazione del dispositivo 3
3 Accesso 7
3.1 Accesso al dispositivo 7
3.2 Reimpostazione della password 8
4 Live 10
4.1 Interfaccia live 10
4.2 Impostazione codifica 11
5 Impostazioni 12
5.1 Rete 12
5.1.1 TCP/IP 12
5.1.2 Porta 15
5.1.3 E-mail 17
5.1.4 Servizi di base 19
5.2 Evento 20
5.2.1 Impostazione ingresso allarme 21
5.2.2 Impostazione collegamento allarme 22
5.2.2.1 Aggiunta pianificazione 23
5.2.2.2 Collegamento registrazione 24
5.2.2.3 Collegamento istantanea 25
5.2.2.4 Collegamento uscita allarme 25
5.2.2.5 Collegamento e-mail 25
5.3 Sistema 26
5.3.1 Generale 26
5.3.1.1 Impostazioni di base 26
5.3.1.2 Data e ora 26
5.3.2 Account 28
5.3.2.1 Utente 28
5.3.2.1.1 Aggiunta utenti 28
5.3.2.1.2 Reimpostazione della password 30
5.3.2.2 Utente ONVIF 31
5.3.3 Responsabile 32

5.3.3.1 Requisiti 32
5.3.3.2 Manutenzione 33
5.3.3.3 Importazione/Esportazione 34
5.3.3.4 Predefinito 34
5.3.4 Aggiornamento 35
Appendice 1 Raccomandazioni sulla sicurezza informatica 36

1 Panoramica

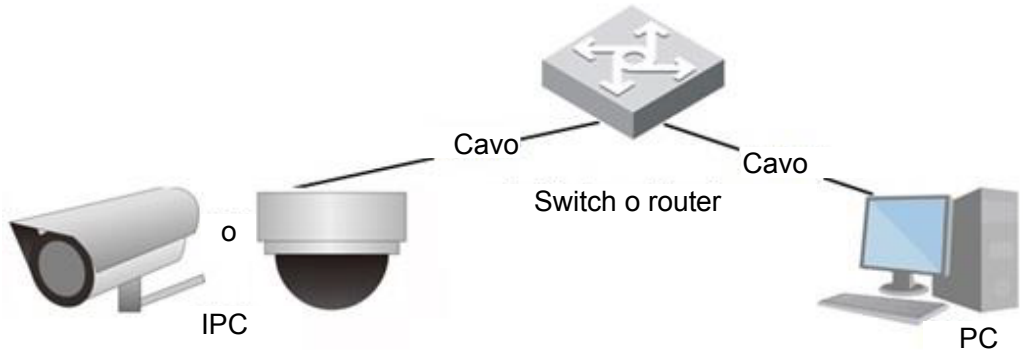
1.1 Introduzione

Le telecamere IP (Internet Protocol camera) sono telecamere digitali che ricevono dati di controllo e inviano dati relativi alle immagini via internet. Vengono comunemente utilizzate per la sorveglianza e necessitano solamente di una rete LAN, senza bisogno di un videoregistratore locale.
In base al numero di canali, le telecamere IP possono essere divise in modelli a canale singolo e modelli multicanale. Nelle telecamere multicanale è possibile impostare i parametri relativi a ogni canale.

1.2 Connessione di rete

Nella topologia di una rete IPC generica, la telecamera IP è connessa a un PC tramite switch o router.

Figura 1−1 Rete IPC generica



Una volta recuperato l'indirizzo IP con una ricerca su ConfigTool sarà possibile accedere alla telecamera via rete.

1.3 Diagramma di configurazione

Per il diagramma di configurazione del dispositivo, consultare la Figura 1−2. Per ulteriori informazioni, consultare la Tabella 1−1. Configurare il dispositivo in base alla situazione effettiva.

Figura 1-2 Diagramma di configurazione

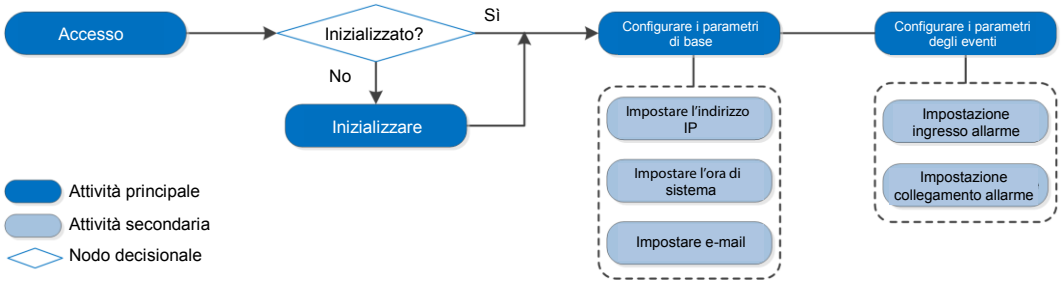


Tabella 1-1 Descrizione del diagramma

Configurazione		Descrizione	Riferimento
Accesso		Aprire il browser IE e inserire l'indirizzo IP per accedere all'interfaccia web. L'indirizzo IP predefinito della telecamera è 192.168.1.108.	"3 Accesso".
Inizializzazione		Inizializzare la telecamera quando la si utilizza per la prima volta.	"2 Inizializzazione del dispositivo"
Parametri di base	Indirizzo IP	Al primo utilizzo o quando si modificano le impostazioni di rete, cambiare l'indirizzo IP in base alla pianificazione della rete.	"5.1.1 TCP/IP"
	Data e ora	Impostare data e ora per garantire il corretto orario di registrazione.	"5.3.1.2 Data e ora"

2 Inizializzazione del dispositivo

La prima volta che si utilizza il dispositivo è necessario inizializzarlo. Questo manuale descrive le operazioni sull'interfaccia web. È anche possibile inizializzare il dispositivo utilizzando ConfigTool o un NVR.

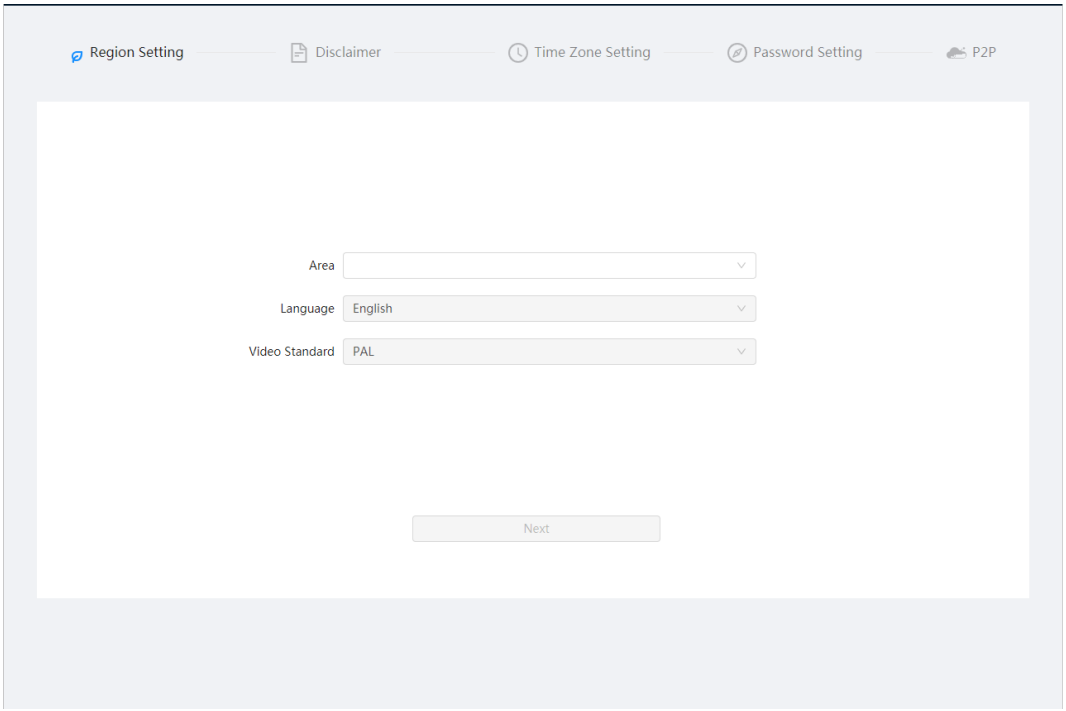
Per garantire la sicurezza del dispositivo, conservare con cura e modificare periodicamente la password di accesso.

Per l'inizializzazione del dispositivo, impostare l'indirizzo IP del PC e quello del dispositivo in modo che si trovino sulla stessa rete.

Fase 1: Aprire il browser Chrome, inserire l'indirizzo IP del dispositivo nella barra degli indirizzi e premere il tasto Invio.

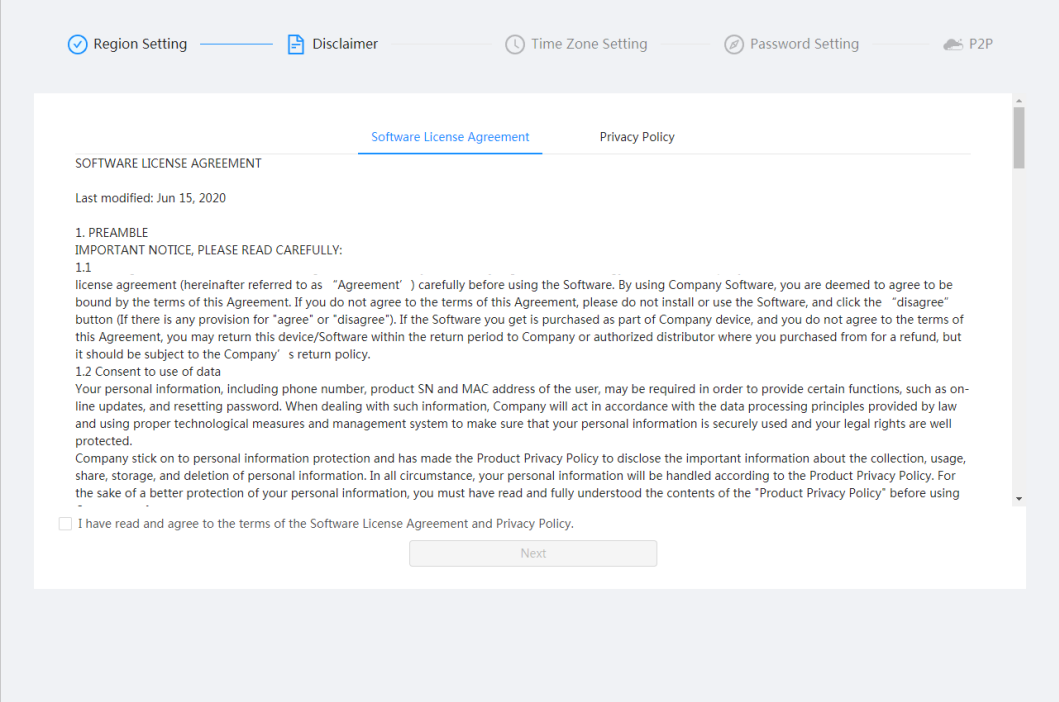
L'IP predefinito è 192.168.1.108.

Figura 2–1 Impostazioni regionali



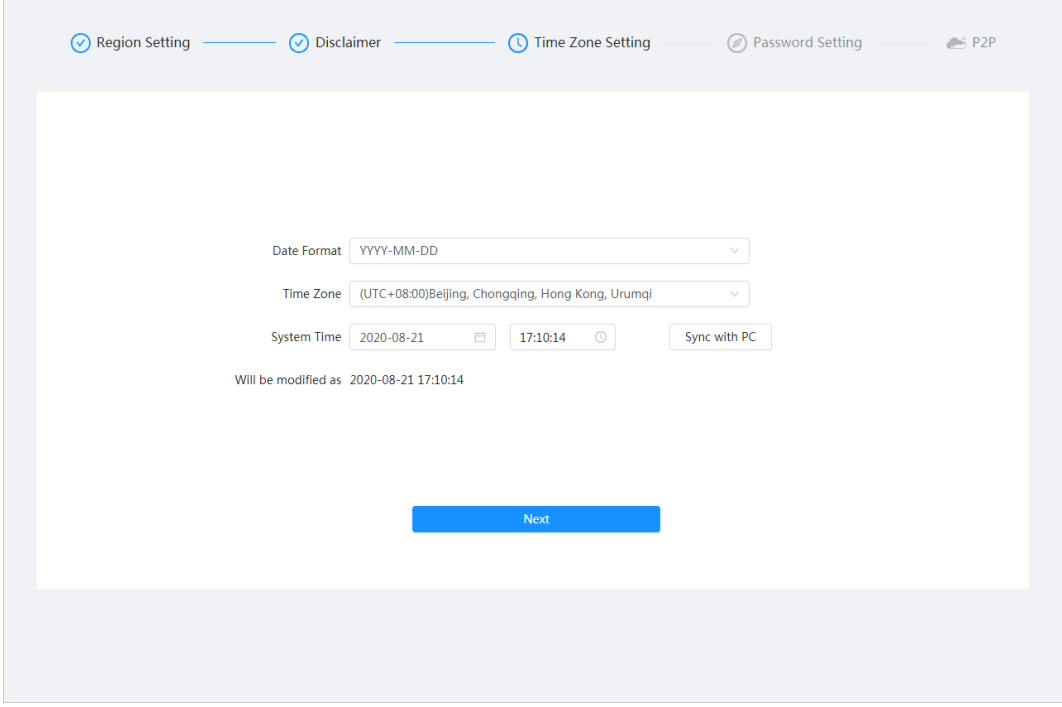
Fase 2: Selezionare l'area geografica, la lingua e lo standard video in base alle necessità e fare clic su **Avanti** (Next).

Figura 2-2 Dichiarazione di limitazione di responsabilità



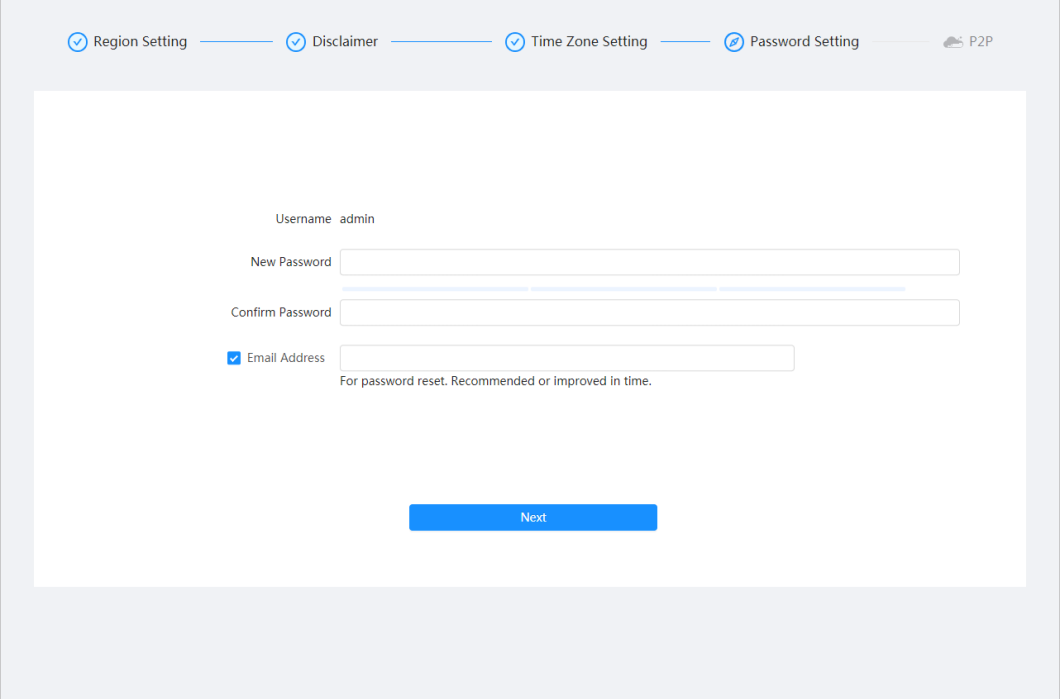
Fase 3: Selezionare la casella di spunta accanto alla scritta **Ho letto e accetto i termini** dell'Accordo di licenza del software e della Politica sulla privacy (I have read and agree to the terms of the Software License Agreement and Privacy Policy), quindi fare clic su **Avanti** (Next).

Figura 2-3 Impostazione del fuso orario



Fase 4: Configurare i parametri relativi all'ora e fare clic su **Avanti** (Next).

Figura 2-4 Impostazione della password



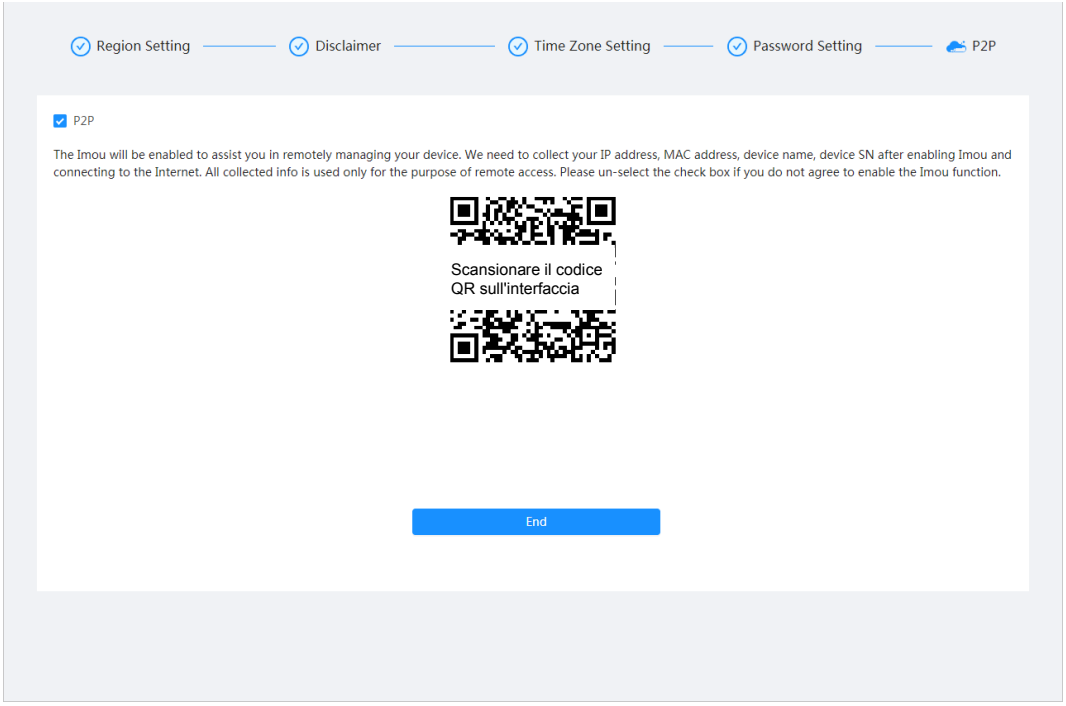
Fase 5: Impostare la password dell'account amministratore.

Tabella 2-1 Descrizione delle opzioni per la configurazione della password

Parametro	Descrizione
Nome utente	Il nome utente predefinito è admin.
Password	La password deve essere composta da 8-32 caratteri non spaziati e deve contenere almeno due tipi di caratteri tra maiuscole, minuscole, numeri e caratteri speciali (esclusi ' " ; : &). Scegliere una password con un livello di sicurezza elevato, secondo le indicazioni mostrate sull'interfaccia.
Conferma password	
E-mail riservata	Inserire un indirizzo e-mail per il ripristino della password. L'opzione è attiva per impostazione predefinita. Quando è necessario ripristinare la password dell'account amministratore, viene inviato un codice di sicurezza all'indirizzo e-mail riservato.

Fase 6: Fare clic su **Avanti** (Next) e il sistema mostrerà l'interfaccia **P2P**.

Figura 2-5 P2P



3 Accesso

3.1 Accesso al dispositivo

Questa sezione illustra come accedere all'interfaccia web e come uscirne. Il browser utilizzato nell'esempio è Chrome.

Prima di accedere all'interfaccia web è necessario inizializzare la telecamera. Per ulteriori informazioni, consultare la "2 Inizializzazione del dispositivo".

Per l'inizializzazione della telecamera, impostare l'indirizzo IP del PC e quello del dispositivo in modo che si trovino sulla stessa rete.

Seguire le istruzioni per scaricare e installare il plug-in al primo accesso.

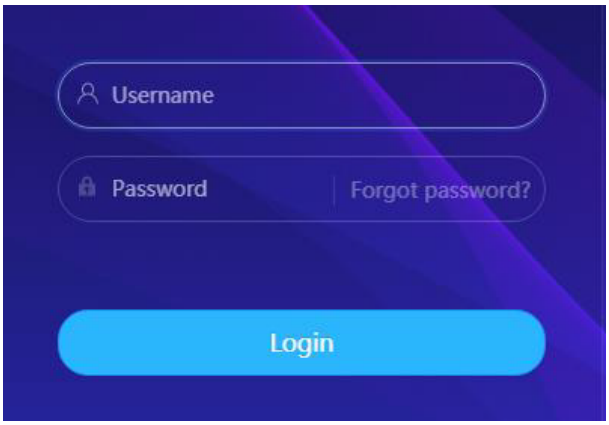
Fase 1: Aprire il browser Chrome, inserire l'indirizzo IP della telecamera (valore predefinito 192.168.1.108) nella barra degli indirizzi e premere Invio.

Fase 2: Inserire il nome utente e la password.

Il nome utente predefinito è admin.

Facendo clic su **Password dimenticata?** (Forgot password?) è possibile ripristinare la password usando l'indirizzo e-mail impostato in fase di inizializzazione. Per ulteriori informazioni, consultare la "3.2 Reimpostazione della password".

Figura 3-1 Accesso

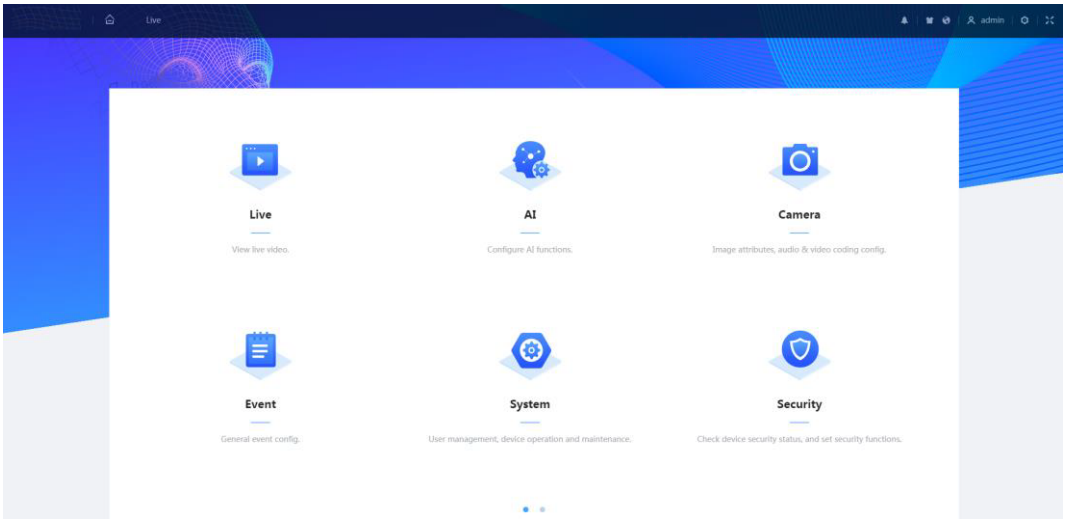


Fase 3: Fare clic su **Accedi** (Login).

Il sistema mostra l'interfaccia **Live**. Fare clic sull'icona nell'angolo in alto a sinistra per visualizzare l'interfaccia principale.

Quando si effettua il primo accesso, installare il plug-in seguendo le istruzioni a schermo.

Figura 3-2 Interfaccia principale



Live: visualizzazione dell'immagine di monitoraggio in tempo reale.
IA: configurazione delle funzioni IA della telecamera.
Telecamera: configurazione dei parametri della telecamera, come quelli relativi alle immagini, alla codifica e all'audio.
Evento: configurazione degli eventi generici, come quelli relativi alle eccezioni del collegamento dell'allarme, al rilevamento video e al rilevamento audio.
Sistema: configurazione dei parametri di sistema, come impostazioni generali, data e ora, account, sicurezza, impostazioni PTZ, impostazioni predefinite, importazione/esportazione, remoto, manutenzione automatica e aggiornamenti.
Sicurezza: verifica dello stato di sicurezza del dispositivo e impostazione delle funzioni di sicurezza.
Registrazione: riproduzione o scaricamento dei video registrati.
Immagine: riproduzione o scaricamento dei file delle immagini.
Report: ricerca dei report di sistema e relativi agli eventi IA.

3.2 Reimpostazione della password

Qualora sia necessario ripristinare la password dell'account amministratore, sarà inviato un codice di sicurezza all'indirizzo e -mail inserito.

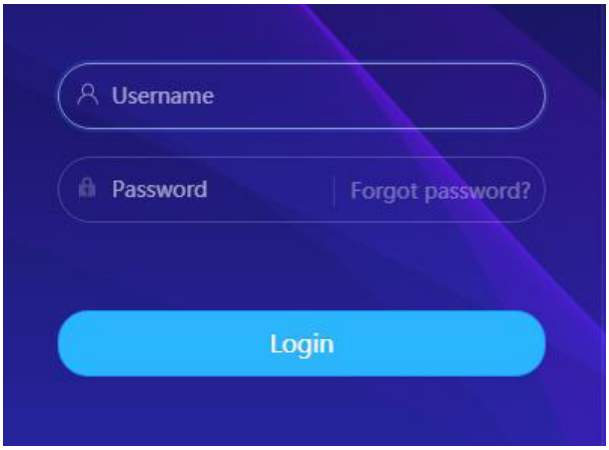
Prerequisiti

Attivazione del servizio di ripristino della password in > **Sistema** (System) > **Account** > **Utente** (User).

Procedura

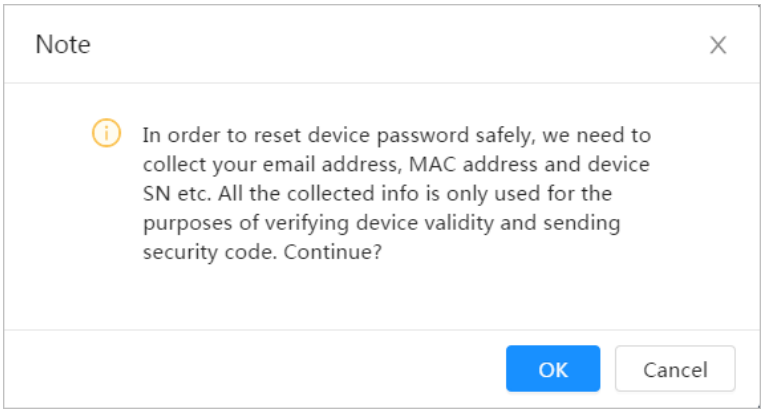
Fase 1: Aprire il browser Chrome, inserire l'indirizzo IP del dispositivo nella barra degli indirizzi e premere Invio.

Figura 3-3 Accesso



Fase 2: Facendo clic su **Password dimenticata?** (Forgot password?) è possibile ripristinare la password usando l'indirizzo e -mail impostato in fase di inizializzazione.

Figura 3-4 Accesso



4 Live

Questa sezione illustra il layout dell'interfaccia e la configurazione della funzione.

4.1 Interfaccia live

Accedere o fare clic sulla scheda **Live**.

L'interfaccia può variare in base al modello: in caso di discrepanze prevarrà il prodotto.

Figura 4–1 Interfaccia Live (canale singolo)

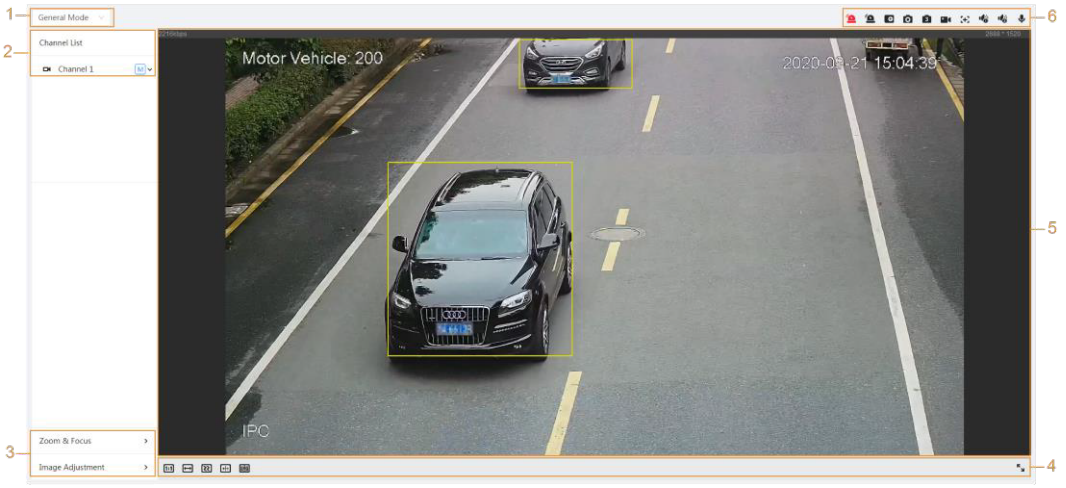


Figura 4–2 Interfaccia Live (multicanale)

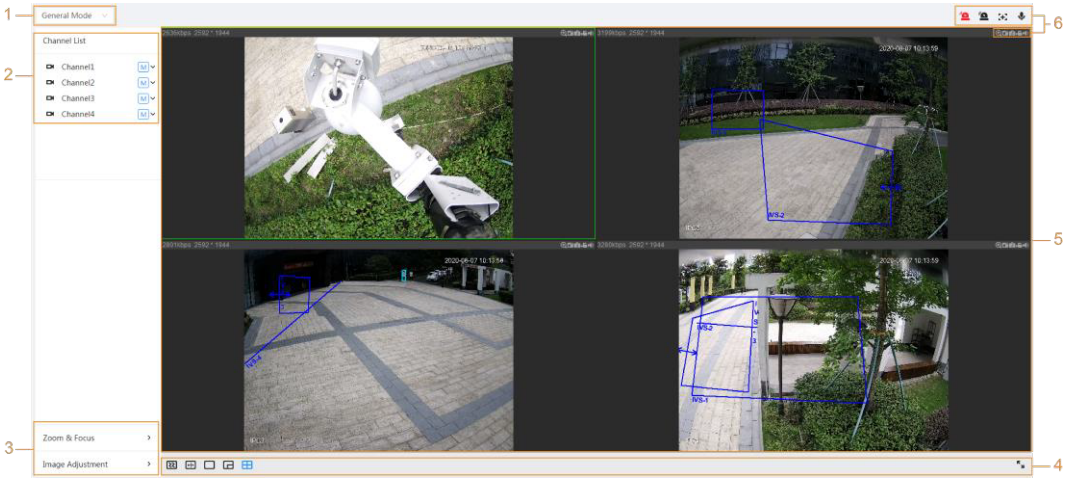


Tabella 4–1 Descrizione della barra delle funzioni

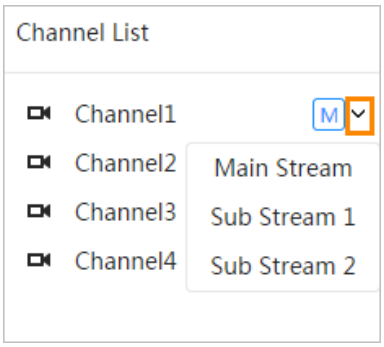
N.	Funzione	Descrizione
1	Modalità Visualizzazione	È possibile selezionare la modalità di visualizzazione dalle sezioni **Modalità generale** (General Mode) e **Modalità volto** (Face Mode).
2	Elenco dei canali	Mostra tutti i canali. È possibile selezionare il canale desiderato e impostare il tipo di flusso.

N.	Funzione	Descrizione
3	Regolazione dell'immagine	Funzioni di regolazione nella visualizzazione live.
4		
5	Visualizzazione live	Mostra l'immagine di monitoraggio in tempo reale.
6	Barra della funzione di visualizzazione live	Funzioni e comandi relativi alla visualizzazione live.

4.2 Impostazione codifica

Fare clic su ⌄ e selezionare il flusso desiderato.

Figura 4−3 Barra di codifica



Flusso principale: il valore del bitstream è alto e l'immagine è ad alta risoluzione, ma richiede una grande larghezza di banda. Questa opzione può essere utilizzata per l'archiviazione e il monitoraggio.

Flusso secondario: il valore del bitstream è basso, l'immagine è fluida e richiede una larghezza di banda inferiore. Questa opzione si usa generalmente per sostituire il flusso principale quando la larghezza di banda non è sufficiente.

L'icona M indica che è in uso il flusso principale; l'icona S1 indica che è in uso il flusso secondario 1; l'icona S2 indica che è in uso il flusso secondario 2.

5 Impostazioni

Questa sezione illustra le impostazioni di base della telecamera, fra cui quelle di rete, degli eventi, e di sistema.

5.1 Rete

Questa sezione illustra come configurare la rete.

5.1.1TCP/IP

È possibile configurare l'indirizzo IP, il server DNS (Domain Name System) e le altre impostazioni in base alla pianificazione della rete.

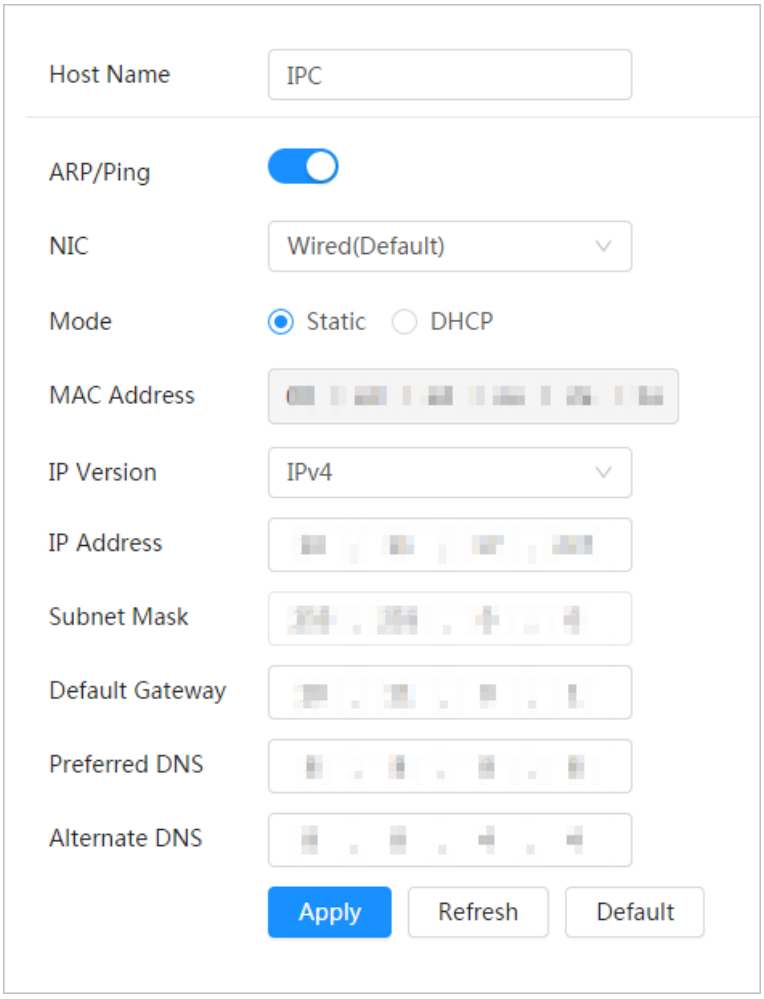
Prerequisiti

Connessione della telecamera alla rete.

Procedura

Fase 1: Selezionare > **Rete** (Network) > **TCP/IP**.

Figura 5-1 TCP/IP



Fase 2: Configurare i parametri TCP/IP.

Tabella 5-1 Descrizione dei parametri TCP/IP

Parametro	Descrizione
Nome host	Inserire il nome dell'host (lunghezza massima 15 caratteri).

Parametro	Descrizione
ARP/Ping	Fare clic su per attivare il servizio ARP/ping per impostare l'indirizzo IP. Recuperare l'indirizzo MAC della telecamera per poter modificare e configurare l'indirizzo IP del dispositivo con un comando ARP/ping. L'opzione è attiva per impostazione predefinita. Durante il riavvio, sarà possibile configurare l'indirizzo IP del dispositivo entro due minuti con un pacchetto ping di una lunghezza specifica. Il server si spegnerà al termine dei 2 minuti o immediatamente dopo la configurazione dell'indirizzo IP. Se l'opzione non è attiva, l'indirizzo IP non potrà essere configurato con un pacchetto ping. **Esempio di configurazione di un indirizzo IP tramite ARP/Ping.** 1. Verificare che la telecamera da configurare e il PC si trovino sulla stessa rete locale, quindi ottenere un indirizzo IP utilizzabile. 2. Recuperare l'indirizzo MAC della telecamera dall'etichetta del dispositivo. 3. Aprire il prompt dei comandi sul PC e digitare le seguenti istruzioni: Windows syntax arp –s <IP Address> <MAC> ping –l 480 –t <IP Address> Windows example arp -s 192.168.0.125 11-40-8c-18-10-11 ping -l 480 -t 192.168.0.125 UNIX/Linux/Mac syntax arp –s <IP Address> <MAC> ping –s 480 <IP Address> UNIX/Linux/Mac example arp -s 192.168.0.125 11-40-8c-18-10-11 ping -s 480 192.168.0.125 4. Riavviare la telecamera. 5. Verificare il prompt dei comandi del PC: se compare una scritta simile a Risposta da 192.168.0.125… (Reply from 192.168.0.125…), la configurazione è andata a buon fine ed è possibile spegnere la telecamera. 6. Scrivere http://(indirizzo IP) nella barra degli indirizzi del browser per eseguire l'accesso.
NIC	Selezionare la scheda Ethernet da configurare (l'impostazione predefinita è **Cablata** (Wired).

Parametro	Descrizione
Modalità	La modalità con cui la telecamera ottiene l'indirizzo IP: **Statica** Configurare le opzioni **Indirizzo IP** (IP Address), **Subnet Mask** e **Gateway predefinito** (Default Gateway) manualmente, quindi fare clic su **Salva** (Save). Il sistema mostra l'interfaccia di accesso con l'indirizzo IP impostato. **DHCP** Se è presente un server DHCP nella rete, selezionare l'opzione **DHCP** e la telecamera acquisirà automaticamente un indirizzo IP.
Indirizzo MAC	Mostra l'indirizzo MAC dell'host.
Versione IP	Selezionare **IPv4** o **IPv6**.
Indirizzo IP	Se si seleziona il valore **Statica** (Static) per l'opzione **Modalità** (Mode), inserire l'indirizzo IP e la subnet mask. Il protocollo IPv6 non ha una subnet mask. Il gateway predefinito deve trovarsi nello stesso segmento di rete dell'indirizzo IP.
Subnet mask	
Gateway predefinito	
DNS preferito	Indirizzo IP del DNS preferito
DNS alternativo	Indirizzo IP del DNS alternativo

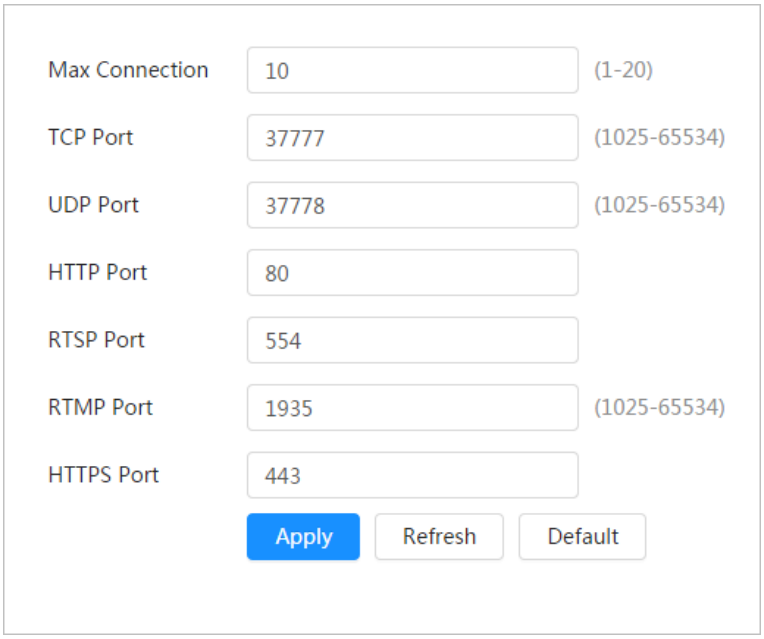
Fase 3: Fare clic su **Applica** (Apply).

5.1.2Porta

Configurare i numeri di porta e il numero massimo di utenti (comprendente l'interfaccia web, le piattaforme e i client mobili) che possono connettersi al dispositivo contemporaneamente.

Fase 1: Selezionare > **Rete** (Network) > **TCP/IP**.

Figura 5–2 Porte



Fase 2: Configurazione dei parametri delle porte.

I numeri di porta 0-1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780, -37880, 39999, 42323 sono già utilizzati per altri servizi.

Per la configurazione non è consigliabile utilizzare il valore predefinito già assegnato a un'altra porta.

Tabella 5–2 Descrizione dei parametri delle porte

Parametro	Descrizione
N. massimo connessioni	Il numero massimo di utenti (client web, piattaforme o client mobili) che possono collegarsi simultaneamente al dispositivo. Il valore predefinito è 10.
Porta TCP	La porta del protocollo di controllo della trasmissione. Il valore predefinito è 37777.
Porta UDP	La porta del protocollo UDP (User Datagram Protocol). Il valore predefinito è 37778.
Porta HTTP	Porta del protocollo hyper text transfer. Il valore predefinito è 80.

Parametro	Descrizione
Porta RTSP	La porta del protocollo RTSP (Real Time Streaming Protocol), il cui valore predefinito è 554. Per accedere alla visualizzazione live con QuickTime, VLC o smartphone Blackberry, è disponibile il formato URL indicato di seguito. Il formato dell'URL per la richiesta del servizio RSTP prevede l'indicazione del numero di canale e del tipo di flusso in bit. Il sistema può anche richiedere nome utente e password di accesso. Esempio del formato dell'URL: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 Valori presenti nell'URL: Nome utente: il nome utente, ad esempio admin. Password: la password, ad esempio admin. IP: l'indirizzo IP del dispositivo, ad esempio 192.168.1.112. Porta: non è necessario inserire alcun valore se si utilizza il valore predefinito 554. Canale: il numero del canale, a partire da 1. Ad esempio, se si utilizza il canale 2, sarà necessario scrivere canale=2. Tipo di bitstream: il tipo di bitstream: 0 indica il flusso principale (Subtype=0), 1 il flusso secondario (Subtype=1). Esempio: Pertanto, se si desiderasse richiedere il flusso secondario del canale 2 da un dispositivo, l'URL dovrebbe apparire come segue: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=21&=1 Se il nome utente e la password non fossero necessari, l'URL apparirebbe come segue: rtsp://ip:port/cam/realmonitor?channel=11&=0
Porta RTMP	Protocollo RTMP (Real Time Messaging Protocol). La porta che fornisce il servizio RTMP. Il valore predefinito è 1935.
Porta HTTPS	Porta di comunicazione HTTPS. Il valore predefinito è 443.

Fase 3: Fare clic su **Applica** (Apply).

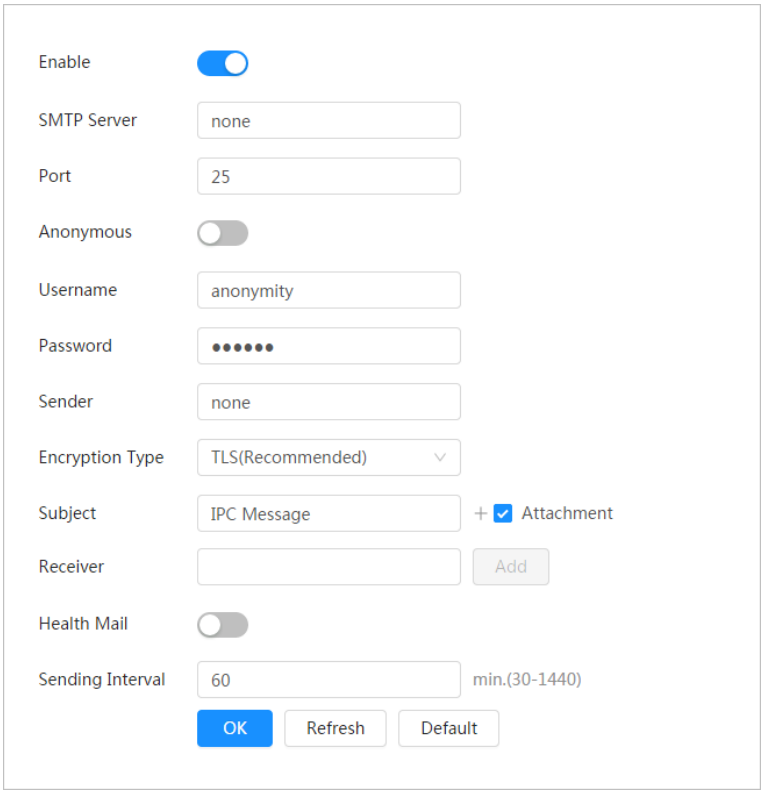
L'opzione **N. massimo di connessioni** (Max Connection) ha effetto immediatamente, le altre solo dopo un riavvio.

5.1.3E-mail

Configurare i parametri e-mail e attivare il collegamento e-mail. Il sistema invia un'e -mail all'indirizzo impostato quando si attiva l'allarme associato al servizio.

Fase 1: Selezionare > **Rete** (Network) > **E-mail** (Email).

Figura 5–3 E-mail



Fase 2: Fare clic su per attivare la funzione.

Fase 3: Configurare i parametri dell'opzione e -mail.

Tabella 5–3 Descrizione dei parametri dell'opzione e -mail

Parametro	Descrizione	
Server SMTP	Indirizzo del server SMTP	Per ulteriori informazioni, consultare la Tabella 5–4.
Porta	Il numero di porta del server SMTP.	
Nome utente	L'account del server SMTP.	
Password	La password del server SMTP.	
Anonimato	Facendo clic su , le informazioni del mittente non verranno mostrate nell'e -mail.	
Mittente	Indirizzo e-mail del mittente.	
Tipo di crittografia	Selezionare **Nessuna** (None), **SSL** o **TLS**. Per ulteriori informazioni, consultare la Tabella 5–4.	
Oggetto	Inserire un massimo di 63 caratteri comprendenti lettere dell'alfabeto cinese o inglese e numeri arabi. Fare clic su per selezionare il tipo di titolo, come **Nome dispositivo** (Device Name), **ID dispositivo** (Device ID) e **Tipo evento** (Event Type). È possibile impostare un massimo di due titoli.	
Allegato	Selezionare la casella di spunta per aggiungere allegati all'e -mail.	

Parametro	Descrizione
Destinatario	Indirizzo e-mail del destinatario. Sono supportati un massimo di 3 indirizzi. Una volta inserito l'indirizzo e -mail del destinatario, verrà mostrato il pulsante **Testa** (Test). Fare clic su **Testa** (Test) per verificare se è possibile inviare e ricevere e-mail correttamente.
E-mail di prova	Il sistema invia un'e-mail di prova per verificare che la connessione sia configurata correttamente. Fare clic su e configurare l'opzione **Intervallo di invio** (Sending Interval): il sistema invierà un'e-mail di prova in base all'intervallo impostato.

Per la configurazione delle caselle di posta gmail, consultare la Tabella 5-4.

Tabella 5-4 Descrizione della configurazione della casella di posta

Casella di posta	Server SMTP	Autenticazione	Porta	Descrizione
gmail	smtp.gmail.com	SSL	465	È necessario attivare il servizio SMTP sulla propria casella di posta. È richiesto il codice di autenticazione, mentre la password dell'account e-mail non è applicabile. Codice di autenticazione: il codice ricevuto all'attivazione del servizio SMTP.
		TLS	587	

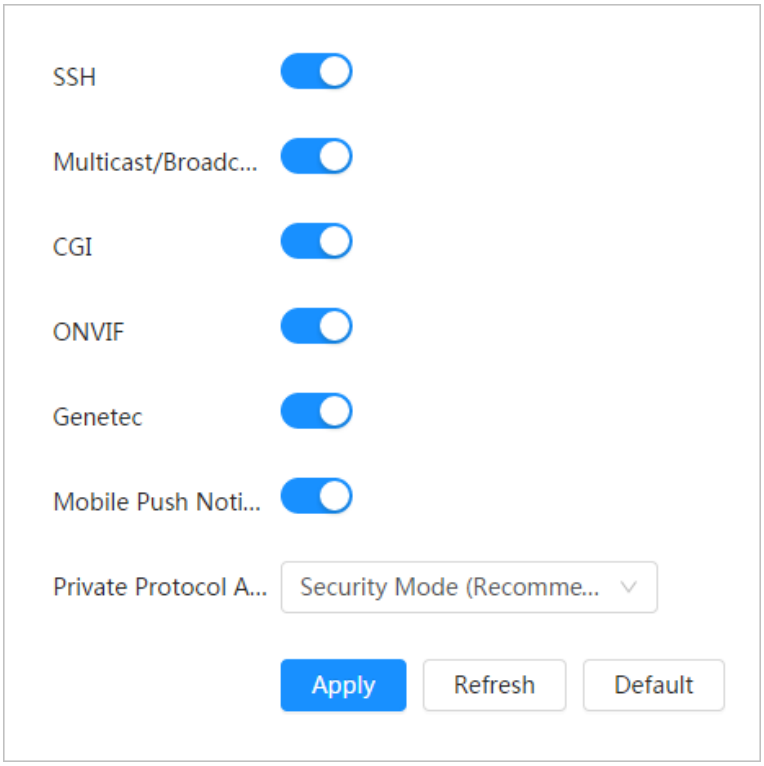
Fase 4: Fare clic su **Applica** (Apply).

5.1.4Servizi di base

Configurare i servizi di base per migliorare la sicurezza della rete e dei dati.

Fase 1: Selezionare > **Rete** (Network) > **Servizi di base** (Basic Service).

Figura 5-4 Servizi di base



Fase 2: Attivare i servizi di base in base alle necessità effettive.

Tabella 5-5 Descrizione dei parametri dei servizi di base

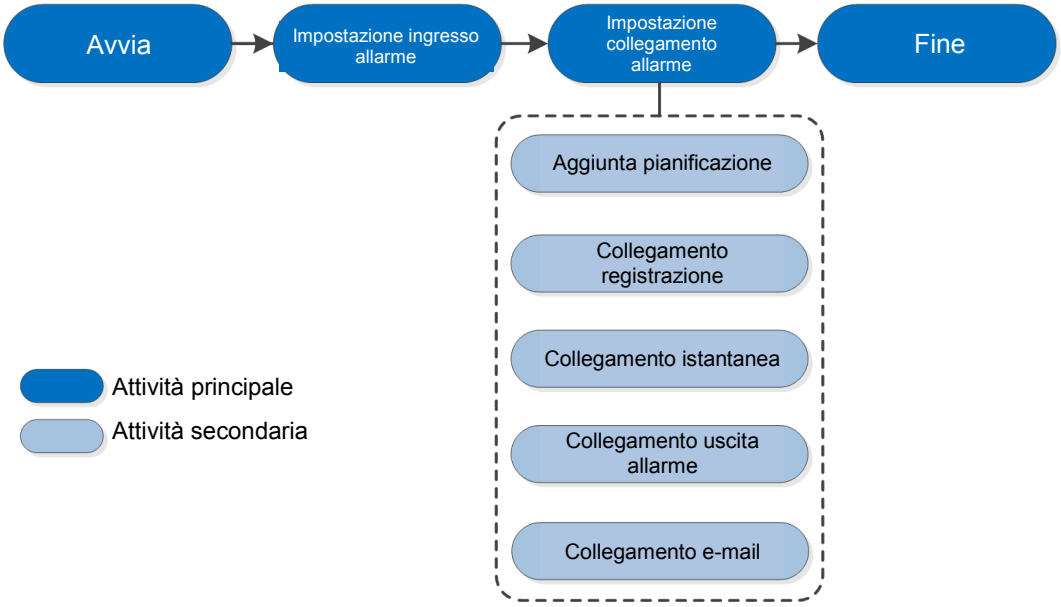
Funzione	Descrizione
SSH	È possibile attivare l'autenticazione SSH per eseguire operazioni di amministrazione in sicurezza.
Ricerca multicast/broadcast	Attivando questa funzione, più utenti che visualizzano contemporaneamente l'immagine video tramite la rete possono trovare il dispositivo utilizzando il protocollo multicast/broadcast.
CGI	Attivando la funzione, altri dispositivi potranno accedere utilizzando questo servizio. La funzione è attiva per impostazione predefinita.
ONVIF	
Genetec	
Notifiche push mobili	Attivando questa funzione, il sistema invierà al telefono l'istantanea scattata quando si attiva l'allarme. L'opzione è attiva per impostazione predefinita.
Modalità di autenticazione protocollo privato	Selezionare un'opzione di autenticazione fra **Modalità sicura** (Security Mode) e **Modalità compatibile** (Compatible Mode). È consigliabile l'utilizzo della modalità sicura.

Fase 3: Fare clic su **Applica** (Apply).

5.2 Evento

Questa sezione utilizza l'ingresso allarme come esempio per illustrare la configurazione del collegamento degli allarmi.

Figura 5-5 Configurazione degli eventi di allarme



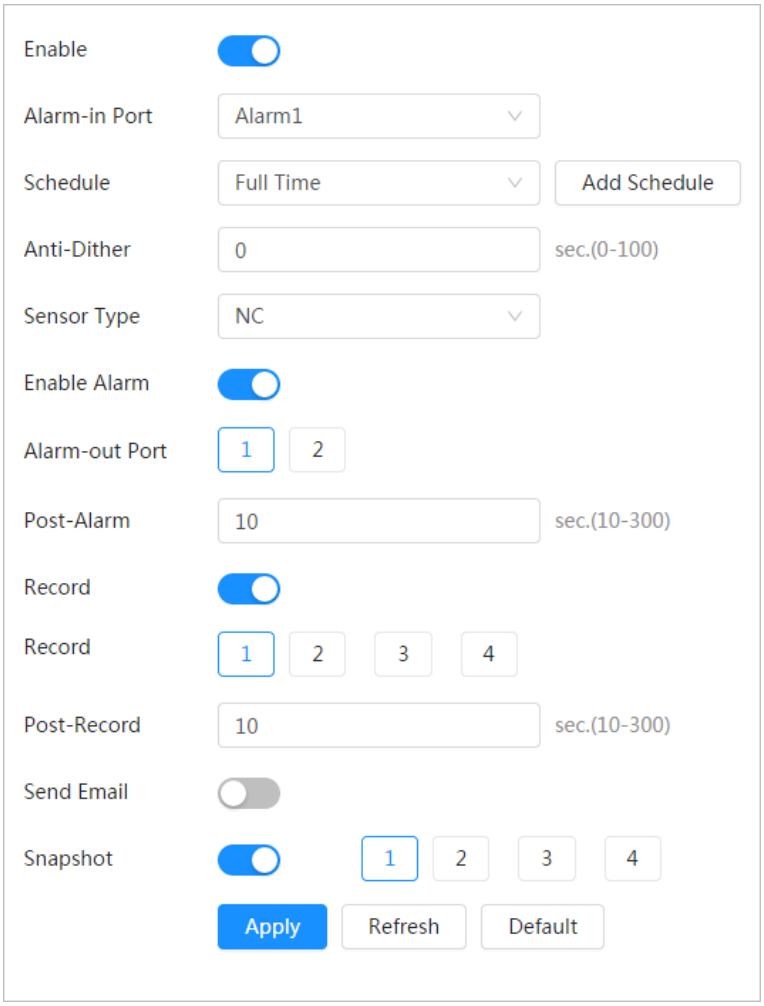
5.2.1 Impostazione ingresso allarme

Quando si attiva un allarme dal dispositivo connesso alla porta di ingresso dell'allarme, il sistema attiva il relativo collegamento.

Fase 1: Selezionare > **Evento** > **Allarme** (Event > Alarm).

Fase 2: Fare clic su accanto alla voce **Abilita** (Enable) per attivare il collegamento dell'allarme.

Figura 5-6 Collegamento allarme



Fase 3: Selezionare una porta di ingresso allarme e un tipo di sensore.

Tipo di sensore: NA o NC.

Anti-dithering: viene registrato un solo evento di allarme durante il periodo di anti-dithering.

Fase 4: selezionare le fasce orarie di pianificazione e inserimento e l'azione di collegamento allarme. Per ulteriori informazioni, consultare la "5.2.2 Impostazione collegamento allarme". Se le pianificazioni esistenti non rispondono ai requisiti dello scenario, è possibile fare clic su **Aggiungi pianificazione** (Add Schedule) per aggiungere una nuova pianificazione. Per ulteriori informazioni, consultare la "5.2.2.1 Aggiunta pianificazione".

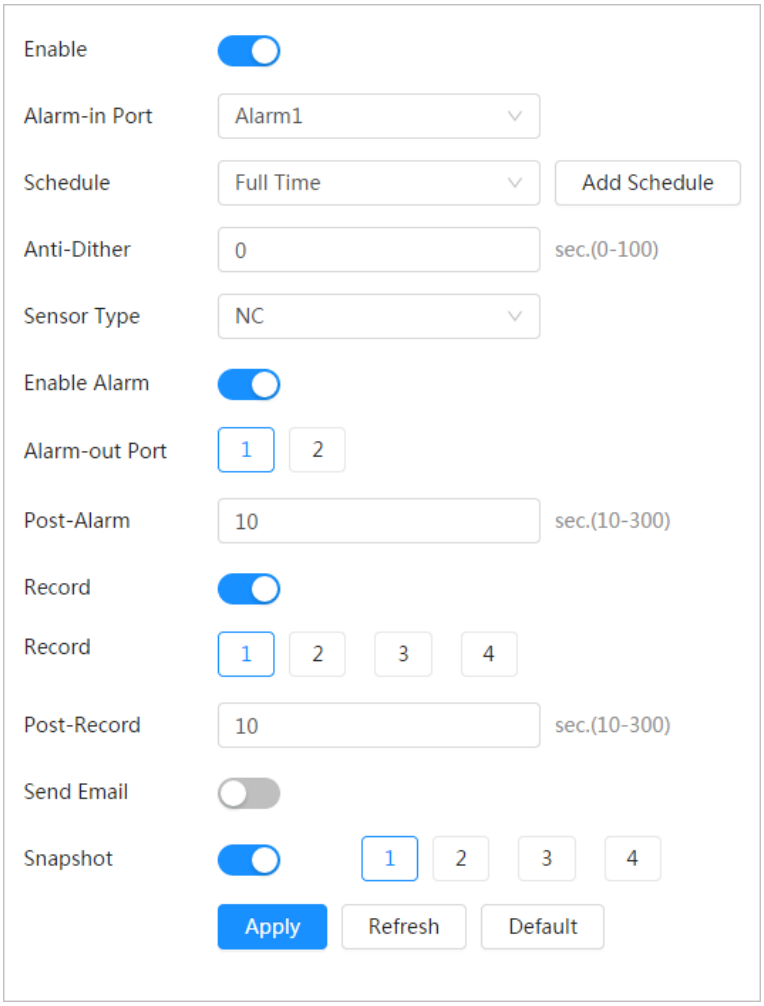
Fase 5: Fare clic su **Applica** (Apply).

5.2.2Impostazione collegamento allarme

Quando si configurano gli eventi di allarme, selezionare i relativi collegamenti (ad esempio registrazione o istantanea). Quando scatta l'allarme corrispondente nel periodo di inserimento configurato, il sistema attiva il collegamento.

Selezionare > **Evento** > **Allarme** (Event > Alarm), quindi fare clic su accanto alla voce **Abilita** (Enable) per attivare il collegamento dell'allarme.

Figura 5-7 Collegamento allarme

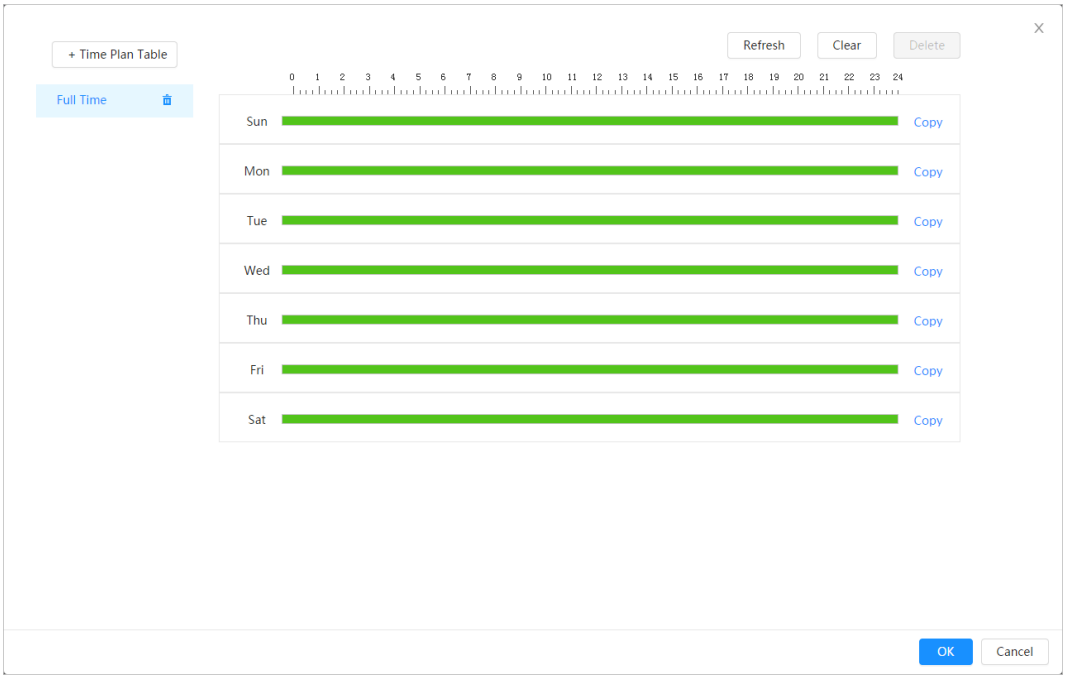


5.2.2.1 Aggiunta pianificazione

Impostare le fasce orarie di inserimento. Il sistema esegue le azioni di collegamento corrispondenti solamente nei periodi di tempo configurati.

Fase 1: Fare clic su **Aggiungi pianificazione** (Add Schedule) accanto alla voce **Pianificazione** (Schedule).

Figura 5-8 Pianificazione



Fase 2: Tenere premuto il pulsante sinistro del mouse sulla timeline per impostare le fasce orarie di inserimento. Gli allarmi saranno attivati in corrispondenza delle fasce orarie evidenziate in verde sulla timeline.

Fare clic sull'opzione **Copia** (Copy) accanto a un giorno e, nell'interfaccia di avviso, selezionare i giorni sui quali si desidera copiare la pianificazione. Selezionare la casella di spunta **Seleziona tutti** (Select All) per copiare la configurazione su tutti i giorni.

È possibile impostare 6 fasce orarie per ogni giorno.

Fase 3: Fare clic su **Applica** (Apply).

Fase 4: (Opzionale) fare clic su **Tabella di pianificazione oraria** (Time Plan Table) per aggiungere una nuova tabella di pianificazione oraria.

È possibile:

fare doppio clic sul nome della tabella per modificarlo;

fare clic su per eliminare la tabella.

5.2.2.2Collegamento registrazione

Il sistema può collegare un canale di registrazione quando si verifica un evento di allarme. Dopo l'attivazione dell'allarme, il sistema smette di registrare una volta trascorso il periodo di tempo impostato nell'opzione **Post-registrazione** (Post-Record).

Prerequisiti

Una volta abilitato il tipo di allarme corrispondente (**Normale** (Normal), **Movimento** (Motion) o **Allarme** (Alarm)), viene attivato il collegamento al canale di registrazione.

Attivare la modalità di registrazione automatica affinché il collegamento alla registrazione diventi effettivo.

Impostazione del collegamento alla registrazione

Sull'interfaccia **Allarme** (Alarm), fare clic su per attivare il collegamento alla registrazione, quindi selezionare il canale desiderato e impostare l'opzione **Post-registrazione**

(Post-Record) per configurare il collegamento dell'allarme e il ritardo della registrazione.
Una volta configurata l'opzione **Post-registrazione** (Post-Record), dopo la fine dell'allarme la registrazione proseguirà per il periodo di tempo impostato.

Figura 5–9 Collegamento alla registrazione

5.2.2.3Collegamento istantanea

Una volta configurato il collegamento alle istantanee, il sistema sarà in grado di scattare istantanee quando si attiva un allarme.

Prerequisiti

Una volta abilitato il tipo di allarme corrispondente (**Normale** (Normal), **Movimento** (Motion) o **Allarme** (Alarm)), viene attivato il collegamento al canale di acquisizione delle istantanee.

Impostazione del collegamento alla registrazione

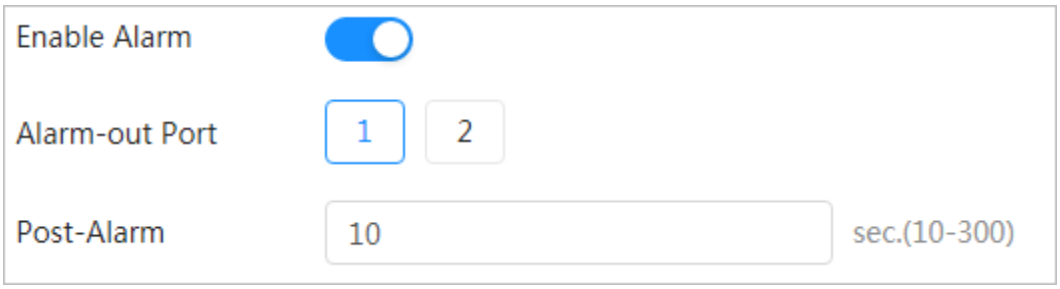
Sull'interfaccia **Allarme** (Alarm), fare clic su per attivare il collegamento alle istantanee e selezionare il canale desiderato.

Figura 5–10 Collegamento alle istantanee

5.2.2.4Collegamento uscita allarme

Quando si attiva un allarme, il sistema è in grado di collegarsi automaticamente all'uscita allarme del dispositivo.
Sull'interfaccia **Allarme** (Alarm), fare clic su per attivare il collegamento all'uscita allarme, selezionare il canale desiderato e configurare l'opzione **Post-allarme** (Post alarm).
Quando viene configurato il ritardo dell'allarme, l'allarme prosegue, dopo la sua cessazione, per il periodo di tempo impostato.

Figura 5–11 Collegamento uscita allarme



5.2.2.5Collegamento e-mail

Quando viene attivato un allarme, il sistema invia automaticamente un'e -mail agli utenti.

Il collegamento e-mail ha effetto solamente una volta configurato il servizio SMTP. Per ulteriori informazioni, consultare la "5.1.3 E-mail".

Figura 5-12 Collegamento e-mail

5.3 Sistema

Questa sezione illustra la configurazione dei parametri di sistema, come impostazioni generali, data e ora, account, sicurezza, impostazioni PTZ, impostazioni predefinite, importazione/esportazione, remoto, manutenzione automatica e aggiornamenti.

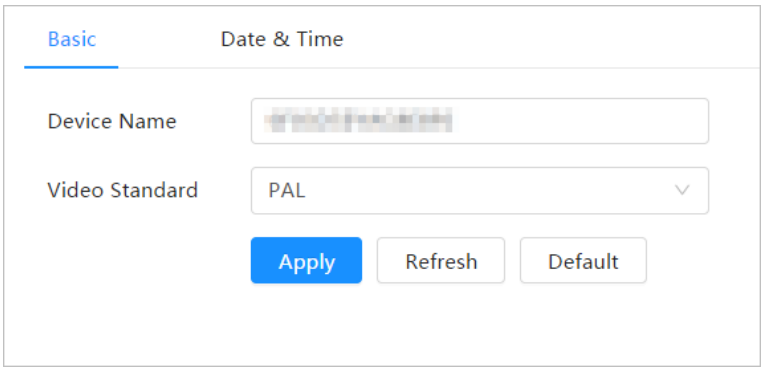
5.3.1 Generale

5.3.1.1 Impostazioni di base

È possibile configurare il nome del dispositivo, la lingua e lo standard video.

Fase 1: Selezionare > **Sistema** (System) > **Generali** (General) > **Imp. di base** (Basic).

Figura 5-13 Impostazioni di base



Fase 2: Configurare i parametri dell'interfaccia Generali.

Tabella 5-6 Descrizione dei parametri generali

Parametro	Descrizione
Nome	Inserire il nome del dispositivo.
Standard video	Selezionare uno standard video fra **PAL** e **NTSC**.

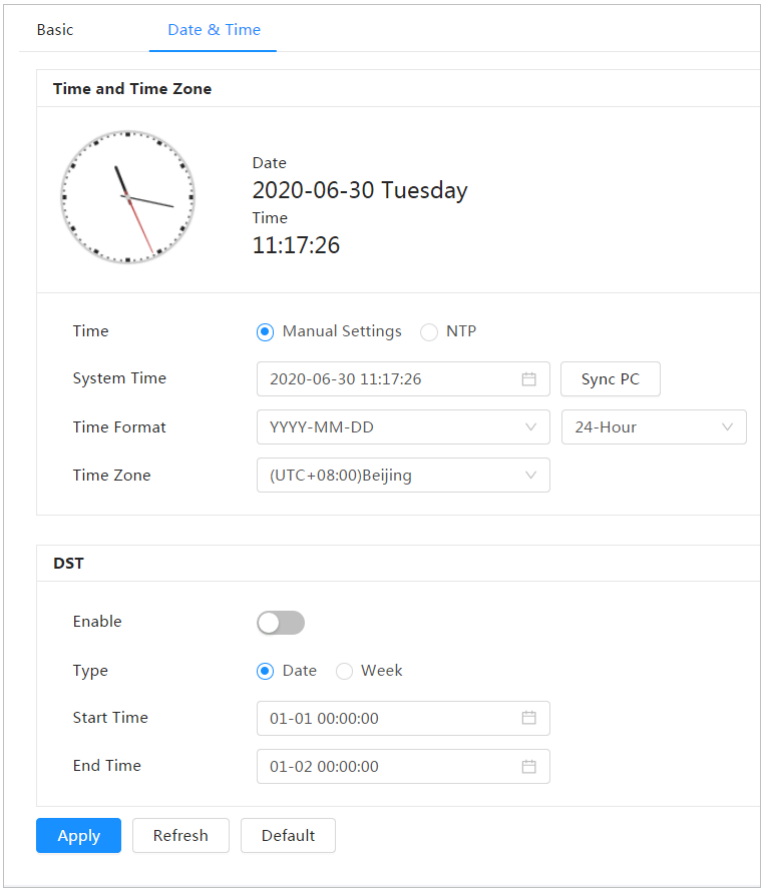
Fase 3: Fare clic su **Applica** (Apply).

5.3.1.2 Data e ora

È possibile configurare il formato della data e dell'ora, il fuso orario, l'ora, l'ora legale o il server NTP.

Fase 1: Selezionare > **Sistema** (System) > **Generali** (General) > **Data e ora** (Date & Time).

Figura 5–14 Data e ora



Fase 2: Configurare i parametri relativi alla data e all'ora.

Tabella 5–7 Descrizione dei parametri relativi alla data e all'ora

Parametro	Descrizione
Formato data	Configurazione del formato della data.
Ora	**Impostazione manuale:** configurazione manuale dei parametri. **NTP:** selezionando l'opzione NTP, il sistema sincronizzerà l'ora in tempo reale con il server Internet. Per utilizzare la funzione è anche possibile inserire l'indirizzo IP, il fuso orario, la porta e l'intervallo di un PC che abbia installato un server NTP.
Formato ora	Configurazione del formato dell'ora. È possibile scegliere fra le opzioni **12 ore** (12-Hour) o **24 ore** (24-Hour).
Fuso orario	Configurazione del fuso orario del luogo in cui si trova il dispositivo.
Ora corrente	Configurare l'ora di sistema. Fare clic su **Sincronizza PC** (Sync PC) per modificare l'ora di sistema sincronizzandola con quella del PC.
Ora legale	Attivare l'ora legale se necessario. Fare clic su , e configurare l'ora di inizio e quella di fine dell'ora legale tramite le opzioni **Data** (Date) o **Settimana** (Week).

Fase 3: Fare clic su **Applica** (Apply).

5.3.2Account

È possibile gestire gli utenti, ad esempio aggiungendoli, eliminandoli o modificandoli. Esistono utenti admin, utenti aggiunti e utenti ONVIF.

La gestione degli utenti e dei gruppi è riservata agli amministratori.

I nomi degli utenti e dei gruppi possono essere composti da un massimo di 31 caratteri, scelti fra numeri, lettere, trattini bassi, lineette, punti e simboli @.

La password deve essere composta da 8-32 caratteri non spaziati e deve contenere almeno due tipi di caratteri tra maiuscole, minuscole, numeri e caratteri speciali (esclusi ' " ; : &).

È possibile avere un massimo di 18 utenti e 8 gruppi.

È possibile gestire gli utenti individualmente o come gruppi. Non sono consentiti nomi utente o nomi di gruppi uguali. Un utente può far parte di un solo gruppo alla volta e gli utenti di un gruppo possono disporre di autorizzazioni entro i limiti dei permessi del gruppo.

Gli utenti online non possono modificare le proprie autorizzazioni.

Esiste un amministratore predefinito che possiede le autorizzazioni di livello più alto.

Selezionando **Accesso anonimo** (Anonymous Login) è possibile accedere solamente con l'indirizzo IP, senza bisogno di inserire nome utente e password. Gli utenti anonimi hanno solo i permessi per visualizzare le anteprime. Quando si accede come utenti anonimi, è possibile fare clic su **Esci** (Logout) e accedere nuovamente con un nome utente diverso.

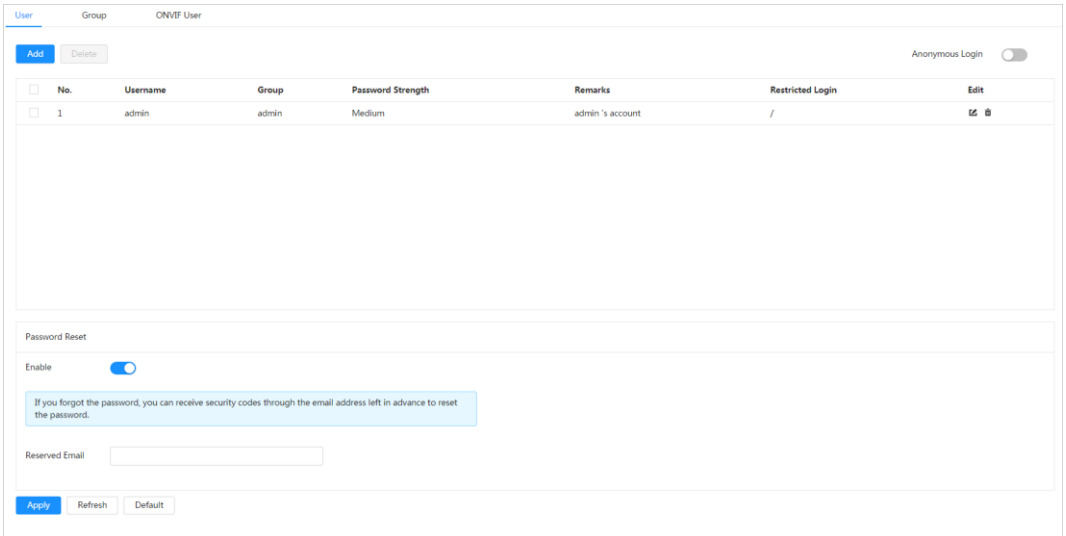
5.3.2.1Utente

5.3.2.1.1 Aggiunta utenti

L'utente predefinito è l'utente amministratore, che può aggiungere utenti e configurare le autorizzazioni.

Fase 1: Selezionare > **Sistema** (System) > **Account** (Account) > **Utente** (User).

Figura 5–15 Utente



Fase 2: Fare clic su **Aggiungi** (Add).

Figura 5-16 Aggiungi utente (sistema)

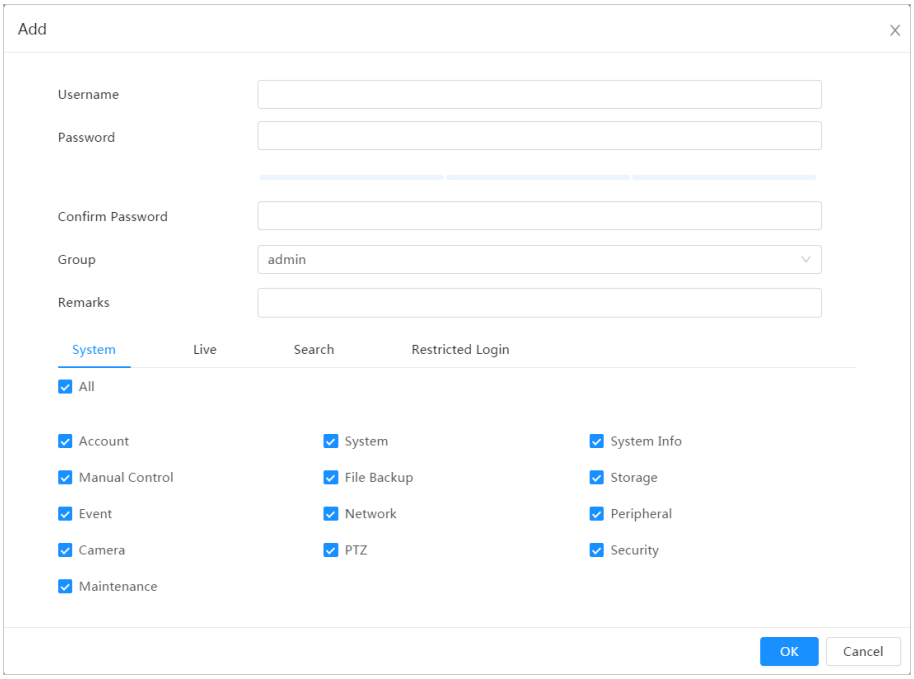
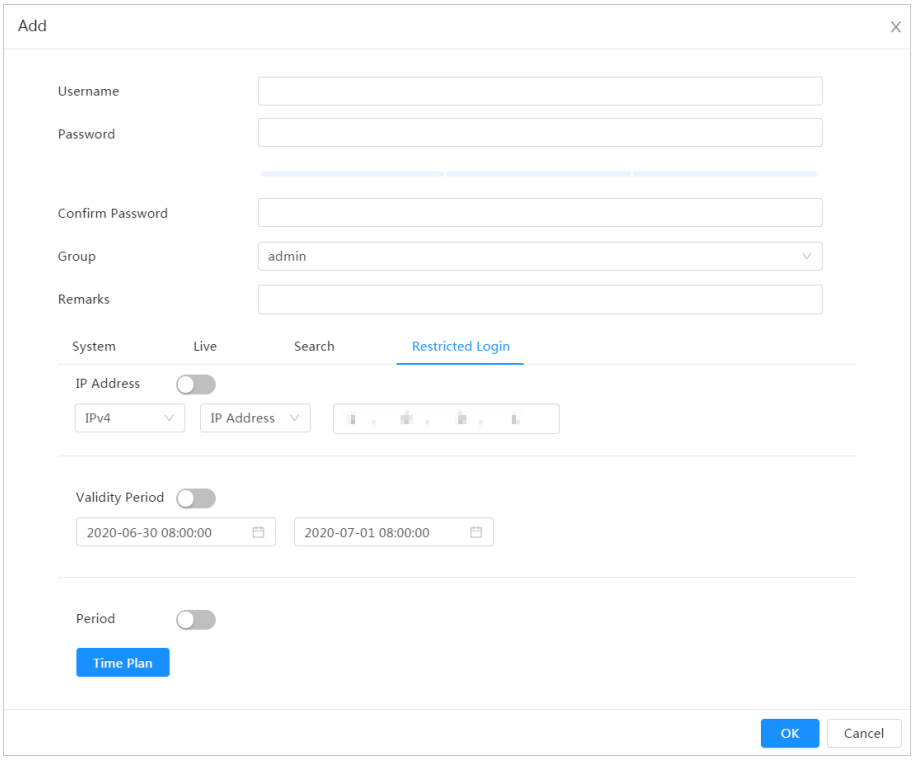


Figura 5-17 Aggiungi utente (accesso limitato)



Fase 3: Configurare i parametri dell'utente.

Tabella 5-8 Descrizione dei parametri dell'utente (1)

Parametro	Descrizione
Nome utente	Identificativo unico dell'utente. Non è possibile adoperare un nome utente già in uso.
Password	Inserire la password e confermarla nuovamente.

Parametro	Descrizione
Conferma password	La password deve essere composta da 8-32 caratteri non spaziati e deve contenere almeno due tipi di caratteri tra maiuscole, minuscole, numeri e caratteri speciali (esclusi ' " ; : &).
Gruppo	Il gruppo a cui appartiene l'utente. Ogni gruppo ha autorizzazioni diverse.
Annotazioni	Descrizione dell'utente.
Sistema	Selezionare le autorizzazioni in base alle proprie esigenze. È consigliabile assegnare meno autorizzazioni agli utenti normali rispetto a quelli premium.
Live	Assegnazione dell'autorizzazione per la visualizzazione live all'utente da aggiungere.
Ricerca	Assegnazione dell'autorizzazione per la ricerca all'utente da aggiungere.
Accesso limitato	Impostazione dell'indirizzo del PC tramite il quale l'utente selezionato può accedere alla telecamera, il periodo di validità e la fascia oraria. L'utente potrà accedere all'interfaccia web con l'IP configurato, nella fascia oraria e per il periodo di validità stabiliti. Indirizzo IP: è possibile accedere all'interfaccia web tramite il PC con questo indirizzo IP. Periodo di validità: è possibile accedere all'interfaccia web per il periodo impostato. Fascia oraria: è possibile accedere all'interfaccia web du rante la fascia oraria impostata. Impostare le opzioni come segue 1. Indirizzo IP: inserire l'indirizzo IP dell'host da aggiungere. 2. Segmento IP: inserire l'indirizzo iniziale e finale dell'host da aggiungere.

Fase 4: Fare clic su **Applica** (Apply).

L'utente appena aggiunto viene visualizzato nell'elenco dei nomi utente.

Operazioni collegate

Fare clic su per modificare la password, il gruppo, la descrizione o le autorizzazioni.

L'unico parametro modificabile dell'account amministratore è la password.

Fare clic su per eliminare gli utenti aggiunti. L'utente amministratore non può essere eliminato.

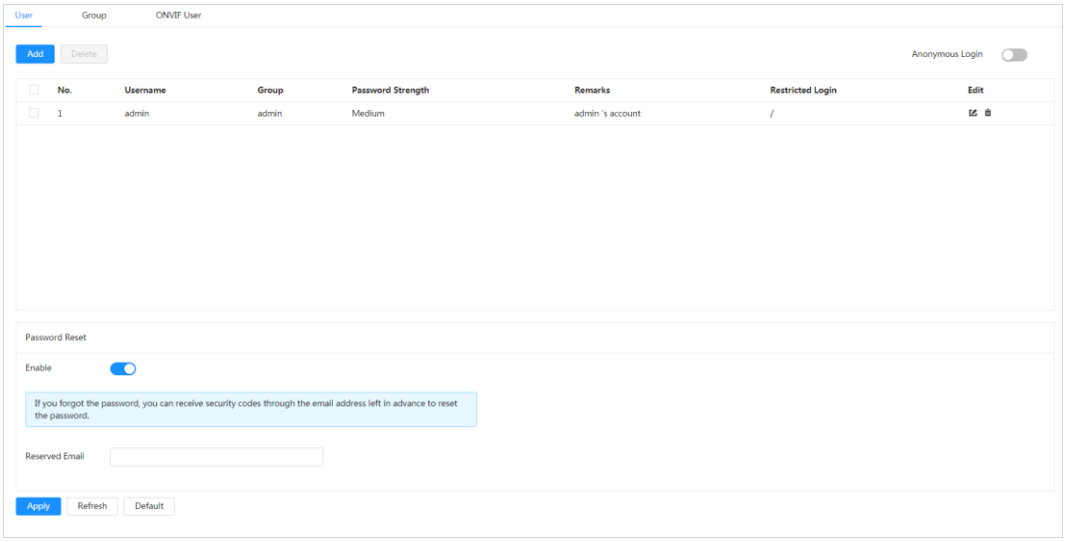
L'account amministratore non può essere eliminato.

5.3.2.1.2 Reimpostazione della password

Attivando questa funzione sarà possibile ripristinare la password facendo clic su **Password dimenticata?** (Forget password?) nell'interfaccia di accesso. Per ulteriori informazioni, consultare la "3.2 Reimpostazione della password".

Fase 1: Selezionare > **Sistema** (System) > **Account** (Account) > **Utente** (User).

Figura 5-18 Utente



Fase 2: Fare clic su accanto alla voce **Abilita** (Enable) nella sezione **Ripristino password** (Password Reset).

Se la funzione non è attiva, è possibile ripristinare la password solamente resettando la telecamera.

Fase 3: Inserire l'indirizzo e-mail riservato.

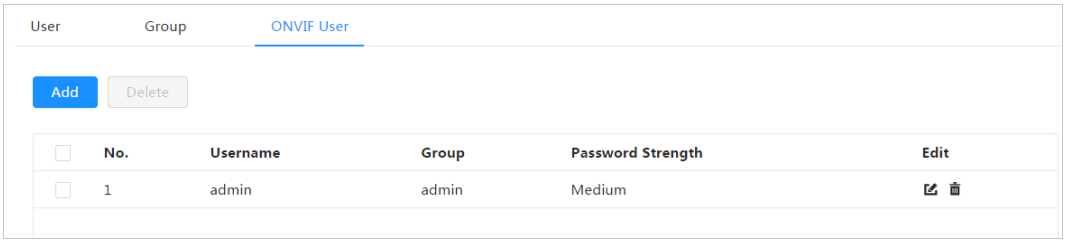
Fase 4: Fare clic su **Applica** (Apply).

5.3.2.2Utente ONVIF

È possibile aggiungere ed eliminare un utente ONVIF, nonché modificarne la password.

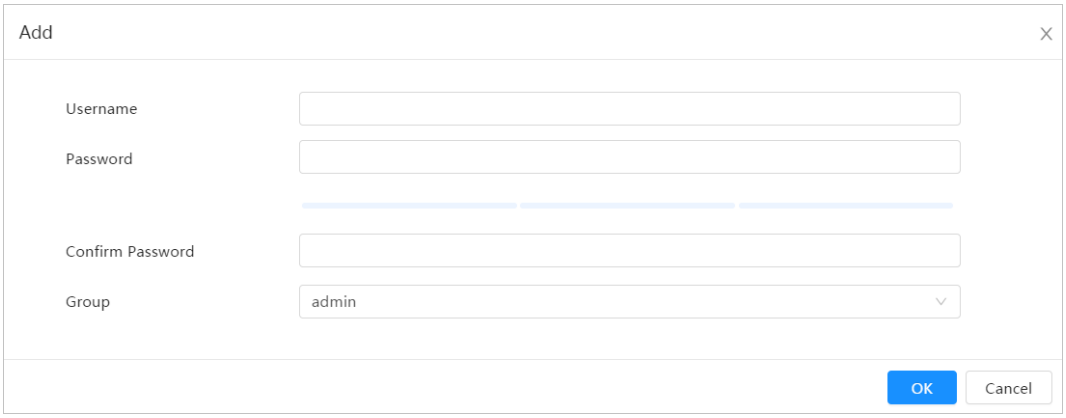
Fase 1: Selezionare > **Sistema** (System) > **Account** > **Utente ONVIF** (User ONVIF).

Figura 5-19 Utente ONVIF



Fase 2: Fare clic su **Aggiungi** (Add).

Figura 5-20 Aggiunta utente ONVIF



Fase 3: Configurare i parametri dell'utente.

Tabella 5-9 Descrizione dei parametri per gli utenti ONVIF

Parametro	Descrizione
Nome utente	Identificativo unico dell'utente. Non è possibile adoperare un nome utente già in uso.
Password	Inserire la password e confermarla nuovamente. La password deve essere composta da 8-32 caratteri non spaziati e deve contenere almeno due tipi di caratteri tra maiuscole, minuscole, numeri e caratteri speciali (esclusi ' " ; : &).
Conferma password	
Nome gruppo	Il gruppo a cui appartiene l'utente. Ogni gruppo ha autorizzazioni diverse.

Fase 4: Fare clic su **OK**.

L'utente appena aggiunto viene visualizzato nell'elenco dei nomi utente.

Operazioni collegate

Fare clic su per modificare la password, il gruppo, la descrizione o le autorizzazioni.

L'unico parametro modificabile dell'account amministratore è la password.

Fare clic su per eliminare gli utenti aggiunti. L'utente amministratore non può essere eliminato.

L'account amministratore non può essere eliminato.

5.3.3 Responsabile

5.3.3.1 Requisiti

Per accertarsi che il sistema funzioni normalmente, eseguire le seguenti operazioni di manutenzione:

Controllare periodicamente la qualità delle immagini di sorveglianza.

Cancellare periodicamente le informazioni degli utenti e dei gruppi che vengono usati raramente.

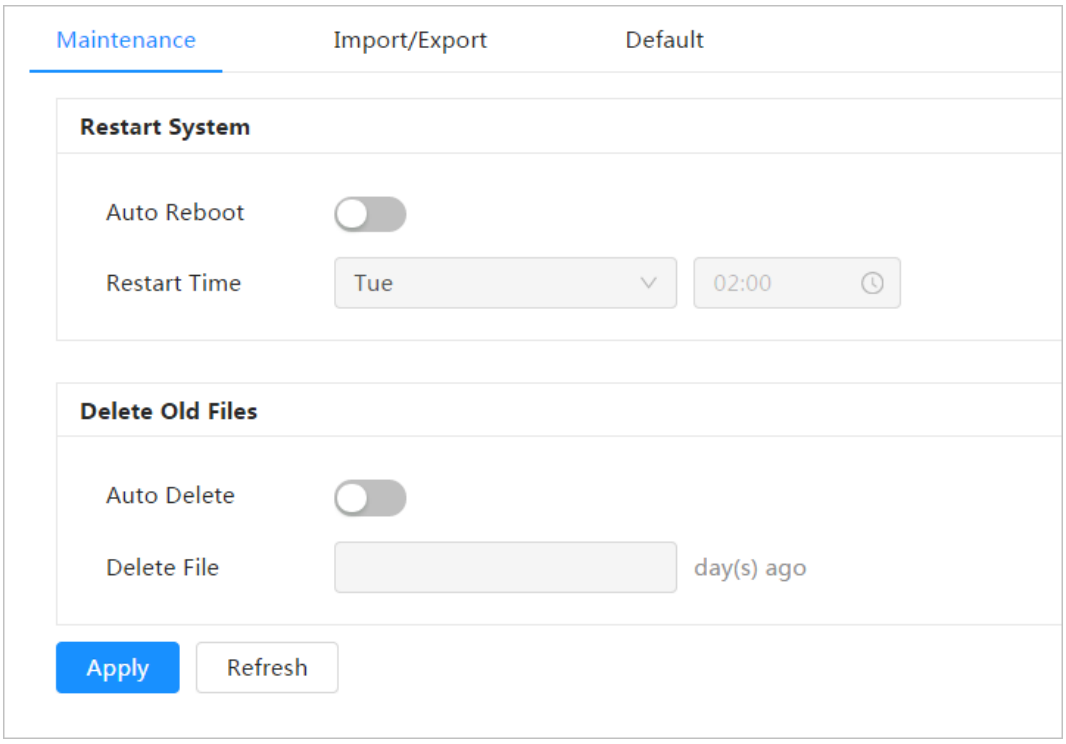
Modificare la password ogni tre mesi. Per ulteriori informazioni, consultare la "5.3.2 Account".
Consultare i registri di sistema, analizzarli e correggere le anomalie per tempo.
Eseguire backup regolari della configurazione di sistema.
Riavviare il dispositivo ed eliminare i vecchi file periodicamente.
Aggiornare tempestivamente il firmware.

5.3.3.2Manutenzione

È possibile riavviare il sistema manualmente e impostare un orario per l'esecuzione automatica del riavvio e dell'eliminazione dei file. Questa funzione è disabilitata per impostazio ne predefinita.

Fase 1: Selezionare > **Sistema** (System) > **Responsabile** (Manager) > **Manutenzione** (Maintenance).

Figura 5–21 Manutenzione



Fase 2: Configurare i parametri per la manutenzione automatica.

Fare clic su accanto alla voce **Riavvio automatico** (Auto Reboot) in **Riavvia sistema** (Restart System) e impostare l'orario del riavvio: il sistema si riavvierà automaticamente ogni settimana all'ora impostata.

Fare clic su accanto alla voce **Eliminazione automatica** (Auto Delete) in **Elimina vecchi file** (Delete Old Files) e impostare un valore: il sistema eliminerà automaticamente i file dopo il numero di giorni impostato. Il valore selezionabile varia da 1 a 31 giorni.

Attivando e confermando la funzione **Eliminazione automatica** (Auto Delete), i file eliminati non potranno più essere ripristinati. Usare la funzione con cautela.

Fase 3: Fare clic su **Applica** (Apply).

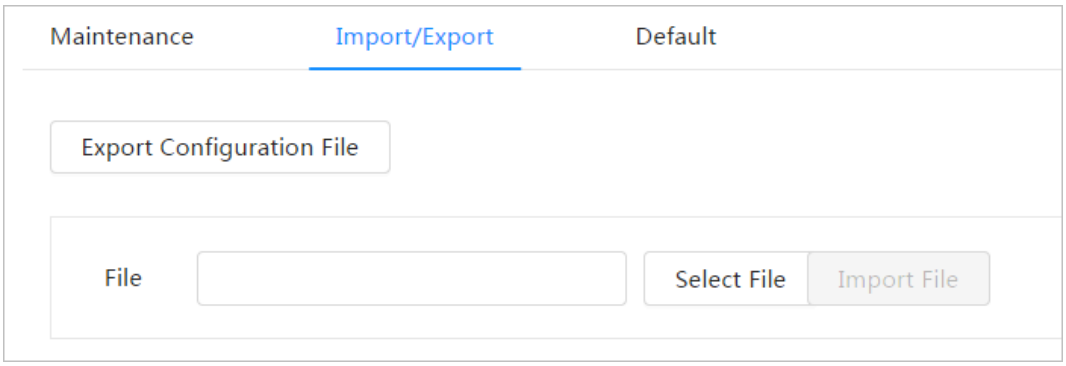
5.3.3.3Importazione/Esportazione

Esportare il file di configurazione di sistema per effettuarne un backup.

Importare il file di configurazione di sistema per eseguire una configurazione rapida o per ripristinare le impostazioni.

Fase 1: Selezionare > **Sistema** (System) > **Responsabile** (Manager) > **Importazione/esportazione** (Import/Export).

Figura 5-22 Importazione/esportazione



Fase 2: Importazione ed esportazione.

Importazione: selezionare il file di configurazione locale e fare clic su **Importa file** (Import File) per importare il file di configurazione di sistema locale.

Esportazione: fare clic su **Esporta file di configurazione** (Export Configuration file) per esportare il file di configurazione di sistema su una periferica di archiviazione locale.

5.3.3.4Predefinito

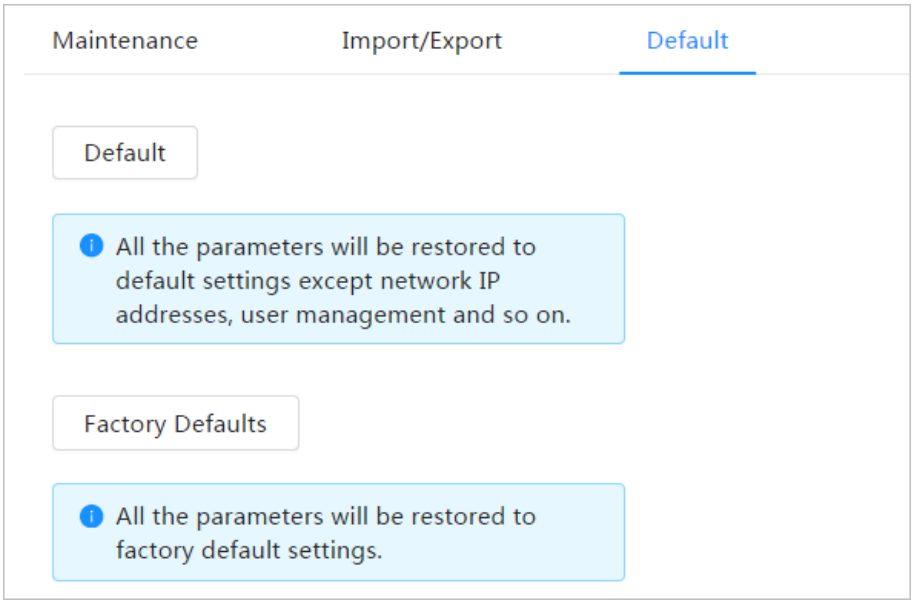
Ripristino della configurazione predefinita o delle impostazioni di fabbrica del dispositivo. Questa funzione ripristina la configurazione o le impostazioni di fabbrica predefinite del dispositivo.

Selezionare > **Sistema** (System) > **Gestione** (Manager) > **Impostazioni predefinite** (Default).

Fare clic su **Impostazioni predefinite** (Default) per ripristinare i valori predefiniti di tutte le configurazioni tranne l'indirizzo IP e l'account.

Fare clic su **Impostazioni di fabbrica predefinite** (Factory Default) per ripristinare i valori di fabbrica di tutte le configurazioni.

Figura 5-23 Impostazioni predefinite



5.3.4 Aggiornamento

Aggiornare il sistema alla versione più recente consente di migliorare le funzioni e la stabilità della telecamera.

Se è stato utilizzato un file di aggiornamento errato, riavviare il dispositivo per evitare malfunzionamenti.

Fase 1: Selezionare > **Sistema** (System) > **Aggiornamento** (Upgrade).

Figura 5-24 Aggiornamento

Fase 2: Fare clic su **Sfoglia** (Browse) e caricare il file di aggiornamento.

Questo file deve avere l'estensione .bin.

Fase 3: Fare clic su **Aggiornamento** (Upgrade).

Inizia la procedura di aggiornamento.

Appendice 1 Raccomandazioni sulla sicurezza informatica

La sicurezza informatica non è solamente una parola di moda: è qualcosa che ha a che fare con tutti i dispositivi collegati a Internet. La sorveglianza video IP non è immune ai rischi informatici, ma adottare semplici misure di protezione e rafforzamento delle reti e dei dispositivi di rete rende questi ultimi meno suscettibili agli attacchi. Di seguito sono forniti alcuni consigli e raccomandazioni su come creare un sistema di sorveglianza più sicuro.

Azioni obbligatorie da intraprendere per la sicurezza di rete di base dei dispositivi:

1. **Utilizzare password sicure**

   Seguire queste raccomandazioni quando si impostano le password:

   la lunghezza non deve essere inferiore a 8 caratteri;

   utilizzare almeno due tipi di caratteri diversi scelti fra lettere maiuscole e minuscole, numeri e simboli;

   le password non devono contenere il nome dell'account o il nome dell'account al contrario;

   non utilizzare caratteri in sequenza, come 123, abc ecc.;

   non utilizzare caratteri ripetuti, come 111, aaa ecc.;

2. **Aggiornare il firmware e il software del client regolarmente**

   Per assicurare che il sistema sia sempre protetto dalle patch e dagli aggiornamenti di sicurezza più recenti, è consigliabile mantenere aggiornati i firmware dei propri dispositivi (come NVR, DVR, telecamere IP ecc), come previsto dagli standard del settore tecnologico. Quando i dispositivi sono collegati a una rete pubblica, è consigliabile attivare la funzione Verifica automaticamente la presenza di aggiornamenti (auto-check for updates) per ottenere informazioni regolari sugli aggiornamenti del firmware rilasciati dai produttori.

   È consigliabile scaricare e utilizzare l'ultima versione del software del client.

Raccomandazioni facoltative ma consigliate per migliorare la sicurezza di rete dei dispositivi:

1. **Protezione fisica**

   È consigliabile proteggere fisicamente le apparecchiature, specialmente i dispositivi di archiviazione. Ad esempio, posizionare le apparecchiature all'interno di un armadio in una stanza dei computer e implementare misure per il controllo degli accessi e la gestione delle chiavi adatte a evitare che il personale non autorizzato possa danneggiare l'hardware, collegare senza permesso dispositivi rimovibili (come chiavette USB e porte seriali) ecc.

2. **Modificare le password con regolarità**

   È consigliabile modificare le password regolarmente per ridurre il rischio che vengano scoperte o violate.

3. **Impostare e aggiornare tempestivamente le informazioni per il ripristino delle password**

   Il dispositivo supporta la funzione di ripristino della password. Configurare per tempo le informazioni relative al ripristino della password, compreso l'indirizzo e -mail dell'utente finale e le domande di sicurezza. Se le informazioni cambiano, modificarle tempestivamente. Quando si impostano le domande di sicurezza per il ripristino della password, è consigliabile non utilizzare domande le cui risposte possono essere facilmente indovinate.

4. Attivare il blocco dell'account
   La funzione di blocco dell'account è attiva per impostazione predefinita ed è consigliabile non disattivarla per garantire la sicurezza dell'account. Se un malintenzionato cerca di accedere ripetutamente con una password errata, l'account corrispondente e l'indirizzo IP utilizzato verranno bloccati.
5. **Modificare i valori predefiniti delle porte HTTP e relative agli altri servizi**
   Per ridurre il rischio che venga scoperto il numero di porta utilizzato, è consigliabile modificare i valori predefiniti delle porte HTTP e relative agli altri servizi scegliendo una qualsiasi combinazione di numeri compresa fra 1024 e 65535.
6. **Attivare il protocollo HTTPS**
   È consigliabile attivare il protocollo HTTPS, così da poter accedere al servizio web tramite un canale di comunicazione sicuro.
7. Associare l'indirizzo MAC
   È consigliabile associare gli indirizzi IP e MAC del gateway alle apparecchiature per ridurre il rischio di spoofing ARP.
8. **Assegnare account e autorizzazioni in modo ragionevole**
   Aggiungere gli utenti con ragionevolezza e assegnare loro il minimo set di permessi in base alle esigenze lavorative e di gestione.
9. **Disattivare i servizi non necessari e scegliere modalità sicure**
   Per ridurre i rischi, è consigliabile disattivare servizi come SNMP, SMTP, UPnP ecc quando non sono necessari.

   Se sono necessari, è vivamente consigliato utilizzare le modalità sicure per i servizi che seguono (l'elenco non è esaustivo):
   SNMP: scegliere SNMPv3 e impostare password crittografiche e di autenticazione sicure.
   SMTP: scegliere TLS per accedere al server e-mail.
   FTP: scegliere SFTP e impostare password sicure.
   Hotspot AP: scegliere la crittografia WPA2-PSK e impostare password sicure.
10. **Utilizzare la trasmissione crittografata di audio e video**
    Se i contenuti audio e video sono molto importanti o sensibili, è consigliabili utilizzare la funzione di trasmissione crittografata per ridurre il rischio che i dati vengano rubati.

    Nota: la trasmissione crittografata rende la trasmissione meno efficiente.
11. **Verifiche di sicurezza**
    Verifica degli utenti online: è consigliabile verificare regolarmente gli utenti online per vedere se qualcuno ha eseguito l'accesso al dispositivo senza autorizzazione.
    Verifica dei registri delle apparecchiature: controllando i registri, è possibile conoscere gli indirizzi IP utilizzati per accedere ai propri dispositivi e alle operazioni chiave.
12. **Registro di rete**
    A causa della limitata capacità di archiviazione delle apparecchiature, il registro salvato è limitato. Se è necessario archiviare il registro per un tempo maggiore, è consigliabile attivare il registro di rete per assicurarsi che i registri critici siano sincronizzati con il server del registro di rete, garantendo una tracciatura efficiente.
13. **Costruire un ambiente di rete sicuro**
    Per garantire la sicurezza delle apparecchiature e ridurre i rischi informatici potenziali, è consigliabile:

disattivare la funzione di mappatura delle porte del router per evitare l'accesso diretto ai dispositivi intranet da una rete esterna;
la rete deve essere suddivisa e isolata in base alle effettive esigenze di rete. in assenza di requisiti di comunicazione fra due sottoreti, è consigliabile utilizzare tecnologie come VLAN, GAP e altre per suddividere la rete e isolarla.
Utilizzare il sistema di autenticazione degli accessi 802.1x per ridurre il rischio di accessi non autorizzati alle reti private.
Attivare la funzione di filtraggio degli indirizzi IP/MAC per limitare il numero di host che possono accedere al dispositivo.

Hiltron Land S.r.l.
Strada Provinciale di Caserta, 218 - 80144 - Napoli
t: +39 081 185 39 000
www.hiltronsecurity.net