

# Manuale utente Hub 2 Plus

Aggiornato il September 28, 2021



**Hub 2 Plus** è un dispositivo centrale nel sistema di sicurezza Ajax che controlla il funzionamento di tutti i dispositivi collegati e interagisce con l'utente e con l'Istituto di vigilanza.

L'hub segnala l'apertura di porte, la rottura di finestre, la minaccia di incendio o di inondazione e automatizza le azioni di routine utilizzando scenari. Se degli estranei entrano nella camera blindata, Hub 2 Plus invierà foto dei rilevatori di movimento [MotionCam](#) / [MotionCam Outdoor](#) e informerà una pattuglia dell'Istituto di vigilanza.



L'unità centrale Hub 2 Plus deve essere installata solo all'interno.

Hub 2 Plus ha bisogno di un accesso a Internet per connettersi al servizio Ajax Cloud. L'unità centrale è collegata a Internet via Ethernet, Wi-Fi e due schede SIM (2G/3G/4G).

La connessione ad Ajax Cloud è necessaria per la configurazione e la gestione del sistema attraverso le app Ajax, la trasmissione di notifiche di allarmi ed eventi, nonché per l'aggiornamento di OS Malevich. Tutti i dati su Ajax Cloud sono memorizzati con protezione multilivello; le informazioni vengono scambiate con l'hub tramite un canale crittografato.



Collegare tutti i canali di comunicazione per garantire una connessione più affidabile con Ajax Cloud e per garantire la sicurezza anche in caso di interruzioni degli operatori di telecomunicazioni.

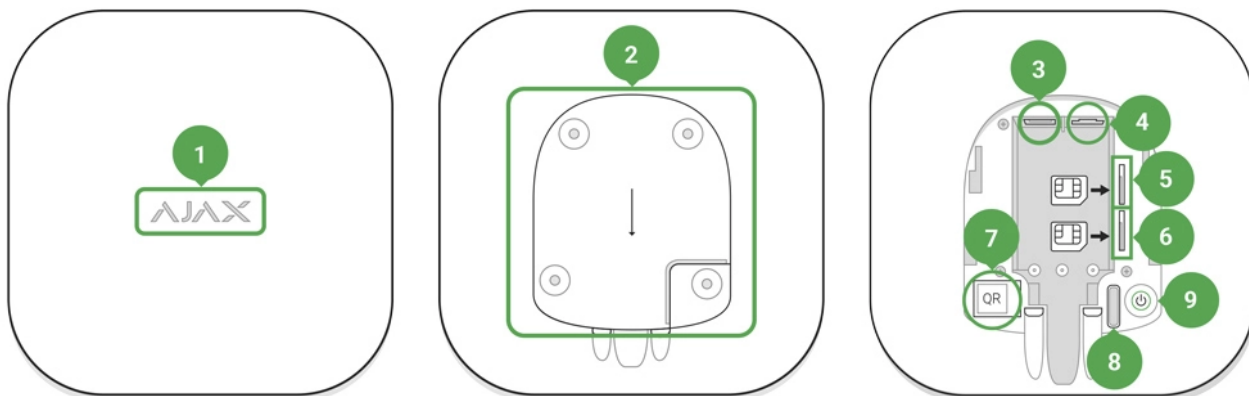
È possibile gestire il sistema di sicurezza e rispondere rapidamente ad allarmi e notifiche tramite app per iOS, Android, macOS e Windows. Il sistema permette di scegliere quali eventi notificare e come notificarli all'utente: tramite notifiche push, SMS o chiamate.

- Come configurare le notifiche push su iOS
- Come configurare le notifiche push su Android

Se il sistema è collegato ad un Istituto di vigilanza, gli eventi e gli allarmi saranno trasmessi alla stazione di monitoraggio – direttamente e/o tramite Ajax Cloud.

### Acquista l'unità centrale Hub 2 Plus

## Elementi funzionali



1. Logo Ajax con indicatore LED

2. Pannello di montaggio SmartBracket. Farlo scorrere verso il basso con forza per aprirlo



La parte perforata è necessaria per l'azionamento del dispositivo anti-manomissione in caso di tentativo di smontaggio dell'hub. Attenzione a non romperlo!

3. Presa cavo di alimentazione
4. Presa cavo Ethernet
5. Slot per micro SIM 2
6. Slot per micro SIM 1
7. Codice QR
8. Pulsante anti-manomissione
9. Pulsante di accensione

## Funzionamento

L'hub controlla il funzionamento del sistema di sicurezza comunicando con i dispositivi collegati tramite il Protocollo crittografato Jeweller. Il raggio d'azione della comunicazione è fino a 2.000 m in campo aperto (ad esempio pareti, porte, costruzioni interpiano). Se il rilevatore viene attivato, il sistema attiva l'allarme in 0,15 secondi, attiva le sirene e informa la stazione centrale di monitoraggio dell'organizzazione di sicurezza e gli utenti.

In caso di interferenze sulle frequenze operative o di tentativi di inibizione, Ajax passa a una frequenza radio libera e invia notifiche alla stazione centrale di monitoraggio dell'organizzazione di sicurezza e agli utenti del sistema.

### Che cos'è l'inibizione di un sistema di sicurezza wireless e come difendersi

Hub 2 Plus supporta fino a 200 dispositivi Ajax collegati, che proteggono da intrusioni, incendi e allagamenti, oltre a controllare gli apparecchi elettrici automaticamente in base agli scenari o manualmente da un'app.

Per inviare le foto dal rilevatore di movimento MotionCam / MotionCam Outdoor viene utilizzato un protocollo radio Wings separato e un'antenna dedicata. Ciò garantisce l'esecuzione della foto-verifica degli allarmi anche in presenza di un livello di segnale instabile e di interruzioni della comunicazione.

### Tutti i dispositivi Ajax

Hub 2 Plus funziona con un sistema operativo in tempo reale OS Malevich. Simili sistemi di controllo OS sono impiegati per veicoli spaziali, missili balistici e freni per auto. OS Malevich espande le capacità del sistema di sicurezza, aggiornandosi automaticamente per via aerea senza l'intervento dell'utente.

Utilizza degli scenari per automatizzare il sistema di sicurezza e ridurre il numero di azioni di routine. Regola il programma di sicurezza, programma le azioni dei dispositivi di automazione (Relay, WallSwitch, o Socket) in risposta a un allarme premendo il Button o secondo quanto pianificato. È possibile creare uno scenario in remoto tramite l'app Ajax.

### Come creare e configurare uno scenario nel sistema di sicurezza Ajax

## Indicatore LED



Il logo Ajax sulla parte anteriore dell'hub si illumina di rosso, bianco o verde a seconda dello stato dell'alimentazione e della connessione a Internet.

Evento	Indicatore LED
Almeno due canali di comunicazione – Wi-Fi, Ethernet o scheda SIM – sono collegati	Luce bianca
Un singolo canale di comunicazione è connesso	Luce verde
Hub non connesso a Internet o comunicazione con il server Ajax Cloud assente	Luce rossa
Alimentazione assente	Illuminato per 3 minuti, poi lampeggia ogni 10 secondi. Il colore dell'indicatore dipende dal numero dei canali di comunicazione collegati

## Account Ajax

Il sistema di sicurezza è configurato e controllato attraverso le [app Ajax](#). Le app Ajax sono disponibili per professionisti e utenti su iOS, Android, macOS e Windows.

Le impostazioni degli utenti del sistema di sicurezza Ajax e i parametri dei dispositivi collegati sono memorizzati localmente sull'hub e sono indissolubilmente legati ad esso. La modifica dell'amministratore dell'hub non azzera le impostazioni dei dispositivi collegati.

Per configurare il sistema, installare l'app Ajax e [creare un account](#). Un numero di telefono e un indirizzo e-mail possono essere utilizzati per creare un solo account Ajax! Non è necessario creare un nuovo account per ogni hub – un solo account può gestire più hub.



L'account può combinare due ruoli: l'amministratore di un hub e l'utente di un altro hub.

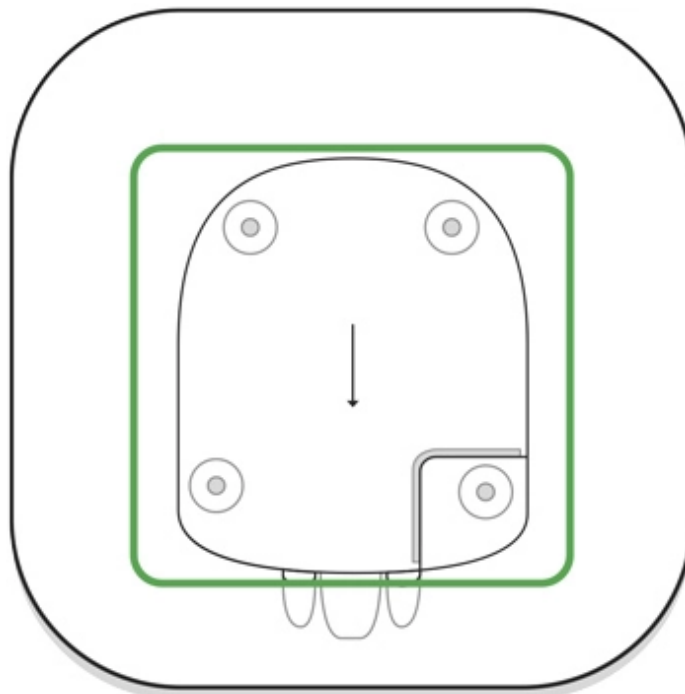
## Requisiti di sicurezza

Durante l'installazione e l'utilizzo di Hub 2 Plus, si raccomanda di seguire le norme generali di sicurezza relative ai dispositivi elettrici, oltre ai requisiti previsti dalle normative vigenti in materia di sicurezza elettrica.

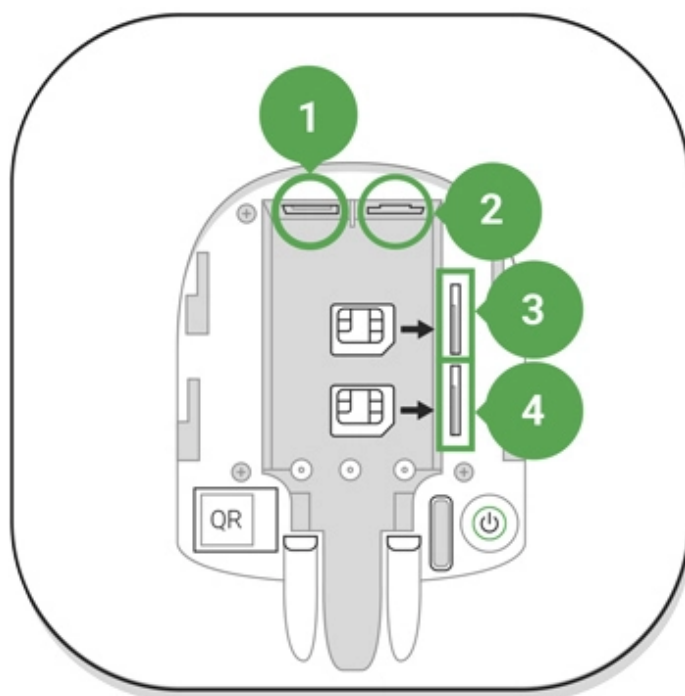
È severamente proibito smontare il dispositivo sotto tensione! Inoltre, non usare il dispositivo se il cavo di alimentazione risulta danneggiato.

# Connessione alla rete

1. Rimuovere il pannello di montaggio dello SmartBracket facendolo scorrere verso il basso con forza. Evitare di danneggiare la parte perforata – è essenziale per l'attivazione del dispositivo anti-manomissione in caso di smontaggio dell'hub!



2. Collegare l'alimentazione e i cavi Ethernet alle apposite prese, installare le schede SIM.



1 – Presa di alimentazione

2 – Presa Ethernet


3. Tenere premuto il pulsante di accensione per 3 secondi fino a quando il logo non si illumina. Ci vogliono circa 2 minuti prima che l'hub si aggiorni al firmware più recente e si connetta a Internet. Il colore del logo verde o bianco indica che l'hub è in funzione e collegato ad Ajax Cloud.



Se la connessione Ethernet non viene stabilita automaticamente, disattivare il filtraggio del proxy e dell'indirizzo MAC e attivare il DHCP nelle impostazioni del router. L'hub riceverà automaticamente un indirizzo IP. In seguito sarà possibile impostare un indirizzo IP statico dell'hub nell'app Ajax.

4. Per connettersi alla rete cellulare è necessaria una micro-SIM con richiesta di codice PIN disattivato (la si può disattivare con il cellulare) e fondi sufficienti sul conto per pagare i servizi alle tariffe del proprio operatore. Se l'hub non si connette alla rete cellulare, utilizzare Ethernet per configurare i parametri di rete: roaming, punto di accesso APN, nome utente e password. Contattare l'operatore di telecomunicazioni per ricevere assistenza per scoprire queste opzioni.

## Aggiungere un hub all'app di Ajax

1. Accendere l'hub e attendere che il logo Ajax diventi verde o bianco.
2. Aprire l'app di Ajax Dare accesso alle funzioni di sistema richieste per utilizzare appieno le capacità dell'app Ajax **e non perdere gli avvisi per gli allarmi o gli eventi**.
  - [Come impostare le notifiche su iOS](#)
  - [Come impostare le notifiche su Android](#)
3. Aprire il menu **Aggiungi hub** e selezionare la modalità di registrazione: manuale o la procedura guidata. Se si imposta il sistema per la prima volta, utilizzare una procedura guidata.
4. Specificare il nome dell'hub e scansionare il codice QR che si trova sotto il pannello di montaggio SmartBracket o immetterlo manualmente.
5. Attendere l'aggiunta dell'hub. Una volta collegato, l'hub sarà visibile nella scheda **Dispositivi** .

Dopo aver aggiunto un hub al proprio account, si diventa amministratori del dispositivo. Gli amministratori possono aggiungere altri utenti al sistema di sicurezza e determinare i loro diritti. L'unità centrale Hub 2 Plus può avere fino a 200 utenti.










La modifica o la rimozione dell'amministratore non comporta il ripristino delle impostazioni dell'hub o dei dispositivi collegati.

## Diritti dell'utente del sistema di sicurezza Ajax

## Stati dell'hub

### Icone

Le icone mostrano alcuni degli stati di Hub 2 Plus. È possibile vederli nell'applicazione Ajax, nel menu **Dispositivi** .


Icone	Valore
	Connesso a 2G
	Connesso a 3G
	Connesso a LTE
	La scheda SIM non è installata
	La scheda SIM è difettosa o ha un codice PIN
	Livello di carica della batteria di Hub 2 Plus. Visualizzati con incrementi del 5%
	Viene rilevato un malfunzionamento dell'Hub 2 Plus. L'elenco è disponibile nella lista degli stati hub
	L'hub è direttamente collegato alla stazione centrale di monitoraggio dell'organizzazione di sicurezza
	L'hub ha perso il collegamento con la stazione centrale di monitoraggio dell'organizzazione di sicurezza tramite connessione diretta

## Stati del dispositivo

Gli stati si trovano nell'app Ajax:

1. Accedere alla scheda **Dispositivi** .

2. Selezionare Hub 2 Plus dall'elenco.

Parametro	Significato
Malfunzionamento	<p>Fare clic su  per aprire la lista dei malfunzionamenti dell'Hub 2 Plus.</p> <p>Il campo appare solo se viene rilevato un malfunzionamento</p>
Intensità segnale cellulare	<p>Mostra l'Intensità segnale della rete di telefonia mobile per la scheda SIM attiva. Si consiglia di installare l'hub in luoghi con Intensità segnale pari a 2-3 barre. Se l'Intensità segnale è debole, l'hub non sarà in grado di comporre o inviare un SMS in merito a un evento o un allarme</p>
Livello batteria	<p>Livello di carica della batteria del dispositivi. Visualizzato in percentuale</p> <p><b><u>Come viene visualizzata la carica della batteria nelle app Ajax</u></b></p>
Stato coperchio	<p>Stato del dispositivo anti-manomissione che risponde allo smontaggio dell'hub:</p> <ul style="list-style-type: none"><li>• <b>Chiuso</b> – il coperchio dell'hub è chiuso</li><li>• <b>Aperto</b> – hub rimosso dal supporto SmartBracket</li></ul> <p><b><u>Cos'è una manomissione?</u></b></p>
Alimentazione esterna	<p>Stato di collegamento all'alimentazione esterna:</p> <ul style="list-style-type: none"><li>• <b>Collegato</b> – l'hub è collegato all'alimentazione esterna</li><li>• <b>Scollegato</b> – nessuna alimentazione esterna</li></ul>
Connessione	<p>Stato della connessione tra l'hub e Ajax Cloud:</p> <ul style="list-style-type: none"><li>• <b>Online</b> – l'hub è collegato ad Ajax Cloud</li></ul>

	<ul style="list-style-type: none"> <li>• <b>Offline</b> – l’hub non è collegato ad Ajax Cloud</li> </ul>
Cellulare	<p>Lo stato della connessione dell’hub a Internet mobile:</p> <ul style="list-style-type: none"> <li>• <b>Collegato</b> – l’hub è collegato ad Ajax Cloud tramite Internet mobile</li> <li>• <b>Scollegato</b> – l’hub non è collegato ad Ajax Cloud tramite Internet mobile</li> </ul> <p>Se l’hub dispone di fondi sufficienti sull’account o dispone di SMS/chiamate bonus, sarà in grado di effettuare chiamate e inviare SMS anche se in questo campo viene visualizzato lo stato <b>Scollegato</b></p>
Attivo	Visualizza la scheda SIM attiva: scheda SIM 1 o scheda SIM 2
SIM 1	Il numero della scheda SIM installata nel primo slot. Copiare il numero cliccandoci sopra
SIM 2	Il numero della scheda SIM installata nel secondo slot. Copiare il numero cliccandoci sopra
Wi-Fi	Stato della connessione Internet dell’hub tramite Wi-Fi. Per una maggiore affidabilità, si raccomanda di installare l’hub in luoghi con intensità segnale pari a 2-3 barre
Ethernet	<p>Stato della connessione Internet dell’hub tramite Ethernet.</p> <ul style="list-style-type: none"> <li>• <b>Collegato</b> – l’hub è collegato ad Ajax Cloud tramite Ethernet</li> <li>• <b>Scollegato</b> – l’hub non è collegato ad Ajax Cloud tramite Ethernet</li> </ul>
Rumore medio (dBm)	<p>Livello di potenza sonora nel sito di installazione dell’hub. I primi due valori mostrano il livello alle frequenze di Jeweller, e il terzo alle frequenze di Wings.</p> <p>Il valore accettabile è di -80 dBm o inferiore</p>
Centrale di sorveglianza	Lo stato del collegamento diretto dell’hub alla stazione centrale di monitoraggio


	<p>dell'organizzazione di sicurezza:</p> <ul style="list-style-type: none"> <li>• <b>Collegato</b> – l'hub è collegato direttamente alla stazione centrale di monitoraggio dell'organizzazione di sicurezza</li> <li>• <b>Scollegato</b> – l'hub non è collegato direttamente alla stazione centrale di monitoraggio dell'organizzazione di sicurezza</li> </ul> <p>Se questo campo viene visualizzato, l'istituto di vigilanza utilizza una connessione diretta per ricevere gli eventi e gli allarmi del sistema di sicurezza</p> <p><b><u>Cos'è un collegamento diretto?</u></b></p>
Modello di hub	Nome modello di hub
Versione hardware	Versione hardware. Impossibile aggiornare
Firmware	Versione firmware. Può essere aggiornato a distanza
ID	ID/numero di serie. Si trova anche sulla scatola del dispositivo, sul circuito stampato del dispositivo e nel codice QR sotto il pannello SmartBracket


## Stanze

Prima di collegare un rilevatore o un dispositivo ad un hub, creare almeno una stanza. Le stanze sono utilizzate per raggruppare rilevatori e dispositivi, nonché per aumentare il contenuto informativo delle notifiche. Il nome del dispositivo e della stanza verranno visualizzati nel testo dell'evento o dell'allarme del sistema di sicurezza.



### Per creare una stanza nell'app Ajax:

1. Andare alla scheda **Stanze** .
2. Fare clic su **Aggiungi stanza**.
3. Assegnare un nome alla stanza e, a scelta, allegare o scattare una foto: ciò aiuta a trovare rapidamente la stanza necessaria nella lista.
4. Fare clic su **Salva**.

Per cancellare la stanza o cambiare il suo avatar o il nome, andare alle **Impostazioni stanza** premendo .

## Connessione di rilevatori e dispositivi



L'hub non è compatibile con i moduli di integrazione [uartBridge](#) e [ocBridge Plus](#).

Quando si aggiunge un hub al proprio account utilizzando la procedura guidata, verrà richiesto di collegare i dispositivi all'hub. È possibile tuttavia saltare questo passaggio e ritornarvi in un secondo momento.



### Per aggiungere un dispositivo all'hub, nell'app Ajax:

1. Aprire la camera e selezionare **Aggiungi dispositivo**.
2. Attribuire un nome al dispositivo, scansionare il suo codice QR (o inserirlo manualmente) e assegnare un gruppo (se la modalità gruppo è abilitata).
3. Fare clic su **Aggiungi**: inizierà il conto alla rovescia per l'aggiunta di un dispositivo.
4. Seguire le istruzioni dell'app per collegare il dispositivo.

Si prega di notare che, per potersi collegare all'hub, il dispositivo deve essere posizionato all'interno del raggio di comunicazione radio dell'hub (sullo stesso oggetto protetto).

## Impostazioni dell'hub

Le impostazioni possono essere modificate nell'app Ajax:

1. Accedere alla scheda **Dispositivi** .
2. Selezionare Hub 2 Plus dall'elenco.
3. Recarsi a **Impostazioni** facendo clic sull'icona .



Si noti che, dopo aver modificato le impostazioni, si dovrà fare clic sul pulsante **Indietro** per salvarle.


**Avatar** è un'immagine del titolo personalizzata per il sistema di sicurezza Ajax. Viene visualizzato nel menu di selezione degli hub e aiuta ad identificare l'oggetto richiesto.

Per modificare o impostare un avatar, fare clic sull'icona della fotocamera e impostare l'immagine desiderata.

**Nome hub.** Viene visualizzato nel testo di notifica SMS e push. Il nome può contenere fino a 12 caratteri cirillici o fino a 24 caratteri latini.

Per modificarlo, fare clic sull'icona della matita e inserire il nome dell'hub desiderato.

**Utenti** – impostazioni dell'utente per un sistema di sicurezza: quali diritti sono concessi agli utenti e in che modo il sistema di sicurezza notifica eventi e allarmi.

Per modificare le impostazioni dell'utente, fare clic su  di fronte al nome dell'utente.

[In che modo il sistema di sicurezza Ajax notifica gli avvisi agli utenti](#)

[Come aggiungere nuovi utenti all'hub](#)

**Ethernet** – impostazioni per la connessione internet via cavo.

- Ethernet – consente di abilitare e disabilitare Ethernet sull'hub
- DHCP/Statico – selezione del tipo di indirizzo IP dell'hub per ricevere: dinamico o statico
- Indirizzo IP – Indirizzo IP dell'hub
- Subnet mask – maschera di sottorete in cui opera l'hub
- Router – gateway utilizzato dall'hub
- DNS – DNS dell'hub

**Wi-Fi** – impostazioni per la connessione Internet Wi-Fi. L'elenco generale mostra tutte le reti disponibili per l'hub.

- Wi-Fi – consente di attivare e disattivare il Wi-Fi sull’hub. Dopo aver premuto il pulsante [i], le impostazioni di rete vengono aperte:
  - DHCP/Statico – selezione del tipo di indirizzo IP dell’hub per ricevere: dinamico o statico
  - Indirizzo IP – Indirizzo IP dell’hub
  - Subnet mask – maschera di sottorete in cui opera l’hub
  - Router – gateway utilizzato dall’hub
  - DNS – DNS dell’hub
  - Dimentica questa rete – dopo averlo premuto, l’hub cancella le impostazioni della rete e non si collega più ad essa

**Cellulare** – abilita/disabilita la comunicazione cellulare, configura le connessioni e verifica l’account.

- Cellulare – disabilita e abilita le schede SIM sull’hub
- Roaming – se attivato, le schede SIM installate nell’hub possono funzionare in roaming
- Ignora errore di registrazione della rete – quando questa impostazione è attivata, l’hub ignora gli errori quando tenta di connettersi tramite una scheda SIM. Attivare questa opzione se la scheda SIM non può connettersi alla rete
- Disattiva il ping prima della connessione – quando questa impostazione è attivata, l’hub ignora gli errori di comunicazione dell’operatore. Attivare questa opzione se la scheda SIM non può connettersi alla rete
- Scheda SIM 1 – visualizza il numero della scheda SIM installata. Fare clic sul campo per andare alle impostazioni della scheda SIM
- Scheda SIM 2 – visualizza il numero della scheda SIM installata. Fare clic sul campo per andare alle impostazioni della scheda SIM

# Impostazioni della scheda SIM

## Impostazioni di connessione

- **APN, nome utente e Password** – impostazioni per la connessione a Internet tramite una scheda SIM. Per conoscere le impostazioni dell'operatore di telefonia mobile, contattare il servizio di assistenza del proprio provider.

### Come impostare o modificare le impostazioni APN nell'hub

## Utilizzo di dati mobili

- **In arrivo** – la quantità di dati ricevuti dall'hub. Visualizzata in KB o MB.
- **In uscita** – la quantità di dati inviati dall'hub. Visualizzata in KB o MB.



Tenere presente che i dati dipendono dall'hub e possono differire dalle statistiche dell'operatore.

**Ripristina statistiche** – azzera le statistiche del traffico in entrata e in uscita.

## Verifica saldo

- **Codice USSD** – inserire il codice che viene utilizzato per controllare il saldo in questo campo. Per esempio, \*111#. Dopo di ciò, fare clic su **Controlla credito residuo** per inviare una richiesta. Il risultato sarà visualizzato sotto il pulsante.

**Geofence** – configurare i promemoria per inserire/disinserire il sistema di sicurezza quando si attraversa una determinata area. La posizione dell'utente viene determinata utilizzando il modulo GPS dello smartphone.

### Cosa sono i Geofence e come funzionano

**Aree** – configurazione della modalità gruppo. Ciò consente di fare quanto segue:

- Gestire le modalità di sicurezza per locali separati o gruppi di rilevatori. Per esempio, l'ufficio è inserito mentre l'addetto alle pulizie lavora in cucina.
- Delimitare l'accesso al controllo delle modalità di sicurezza. Ad esempio, i dipendenti del reparto marketing non hanno accesso allo studio legale.

[Come attivare e configurare la modalità aree nel sistema di sicurezza Ajax](#)

**Programma di sicurezza** – inserire/disinserire il sistema di sicurezza secondo la pianificazione.

[Come creare e configurare uno scenario nel sistema di sicurezza Ajax](#)

**Test zona di rilevamento** – eseguire il test della zona di rilevamento per i rilevatori collegati. Il test determina la distanza sufficiente per consentire ai rilevatori di registrare gli allarmi.

[Che cos'è il test della zona di rilevamento](#)

**Jeweller** – configurazione dell'intervallo di ping del rilevatore dell'hub. Le impostazioni determinano la frequenza con cui l'hub comunica con i dispositivi e la rapidità con cui viene rilevata la perdita di connessione.

### Maggiori informazioni

- **Intervallo di ping del rilevatore** – la frequenza di interrogazione dei dispositivi collegati da parte dell'hub è impostata nell'intervallo da 12 a 300 s (36 s per default)
- **Numero di pacchetti non consegnati per determinare la perdita della connessione** – un contatore dei pacchetti di comunicazioni non consegnati (default: 8 pacchetti).

**Il tempo che trascorre prima di dare l'allarme per la perdita di comunicazione tra l'hub e il dispositivo viene calcolato con la seguente formula:**

$$\text{Intervallo di ping} * (\text{numero di pacchetti non consegnati} + 1 \text{ pacchetto di correzione})$$

Un intervallo di ping più breve (in secondi) significa una più rapida trasmissione degli eventi tra l'hub e i dispositivi collegati; tuttavia, un breve intervallo di ping riduce la durata della batteria. Allo stesso tempo, gli allarmi vengono trasmessi immediatamente a prescindere dall'intervallo di ping.

**Si sconsiglia di ridurre le impostazioni predefinite del periodo e dell'intervallo di ping.**

Si noti che l'intervallo limita il numero massimo di dispositivi collegati:

Intervallo	Limite di connessione
12 s	39 dispositivi
24 s	79 dispositivi
36 s	119 dispositivi
48 s	159 dispositivi



Indipendentemente dalle impostazioni, l'hub supporta al massimo 10 sirene collegate!

**Servizio** è un gruppo di impostazioni di servizio dell'hub. Queste sono divisi in 2 gruppi: impostazioni generali e impostazioni avanzate.

## Impostazioni generali

### Fuso orario

Selezionare il fuso orario in cui opera l'hub. Viene utilizzato per gli scenari in base al programma. Pertanto, prima di creare scenari, impostare il fuso orario corretto.

### [Maggiori informazioni sugli scenari](#)

### Luminosità dei LED

Regolazione della luminosità della retroilluminazione a LED del logo dell'hub. Impostato nell'intervallo da 1 a 10. Il valore predefinito è 10.

## Aggiornamento automatico firmware

Configurazione degli aggiornamenti automatici del firmware OS Malevich.

- **Se abilitato**, il firmware viene aggiornato automaticamente quando è disponibile una nuova versione, quando il sistema non è inserito e l'alimentazione esterna è collegata.
- **Se disattivato**, il sistema non si aggiorna automaticamente. Se è disponibile una nuova versione del firmware, l'app chiederà di aggiornare il sistema operativo OS Malevich.

## Come aggiornare OS Malevich

### Log dell'hub



I log sono file contenenti informazioni sul funzionamento del sistema. Possono aiutare a risolvere il problema in caso di errori o guasti.

L'impostazione permette di selezionare il canale di trasmissione per i log degli hub o di disabilitare la loro registrazione:

- Ethernet
- Wi-Fi
- No – log disattivati



La disattivazione dei registri è sconsigliata poiché le informazioni possono essere utili in caso di errori nel funzionamento del sistema!

## Come inviare un rapporto di errore

### Impostazioni avanzate

L'elenco delle impostazioni avanzate degli hub dipende dal tipo di applicazione: standard o PRO.

Ajax Security System	Ajax PRO
Connessione al server Impostazioni delle sirene Impostazioni rilevatori antincendio Verifica dell'integrità del sistema	PD 6662 Impostazione guidata Connessione al server Impostazioni delle sirene Impostazioni rilevatori antincendio Verifica dell'integrità del sistema Conferma dell'allarme Ripristina dopo l'allarme Processo d'inserimento/disinserimento Disattivazione automatica dei dispositivi

Apri una guida passo-passo su come impostare il sistema per conformarsi allo standard di sicurezza britannico PD 6662:2017.

### Ulteriori informazioni su PD 6662:2017

### Come configurare il sistema in conformità con PD 6662:2017

#### Connessione al server

Il menu contiene le impostazioni per la comunicazione tra l'hub e l'Ajax Cloud:

- **Intervallo di polling server hub, sec.** Frequenza di invio dei ping dall'hub al server Ajax Cloud. È impostato nell'intervallo da 10 a 300 s. Il valore raccomandato di default è 60 s.
- **Ritardo dell'allarme di errore di connessione al server, sec.** Si tratta di un ritardo per ridurre il rischio di un falso allarme associato alla perdita di connessione del server Ajax Cloud. L'allarme viene attivato dopo 3 richieste di comunicazioni non riuscite. Il ritardo è impostabile nell'intervallo compreso tra 30 e 600 s. Il valore raccomandato di default è 300 s.

Il tempo per generare un messaggio relativo alla perdita di comunicazione tra l'hub e il server Ajax Cloud viene calcolato con la seguente formula:

$$(Intervallo\ di\ ping * 4) + tempo\ di\ ritardo$$

Con le impostazioni predefinite, Ajax Cloud segnala all'hub una perdita di comunicazione dopo 9 minuti:

$$(60\ s * 4) + 300\ s = 9\ min$$

- **Ricevi eventi di perdita di connessione al server senza allarme.** Le applicazioni Ajax possono notificare la perdita di comunicazione hub-server in due modi: con un segnale standard di notifica push o con il suono di una sirena (abilitata per default). Quando l'opzione è attiva, la notifica viene fornita con un segnale standard di notifica push.

- **Notifica de perdita di connessione su canali.** Il sistema di sicurezza Ajax può notificare sia agli utenti che alla società di sicurezza la perdita di connessione anche attraverso uno dei canali di connessione.

In questo menu, è possibile scegliere la perdita di connessione di quali canali sarà segnalata dal sistema, nonché il ritardo per l'invio di tali notifiche:

- Ethernet
  - Cellulare
  - Wi-Fi
- **Ritardo notifica di perdita, min** – tempo del ritardo prima di inviare la notifica di perdita di connessione tramite uno dei canali di comunicazione. Impostare nell'intervallo da 3 a 30 minuti.

Il tempo di invio di una notifica sulla perdita di connessione attraverso uno dei canali di comunicazione è calcolato con la formula:

*(Intervallo di polling \* 4) + Filtro di tempo + Ritardo notifica di perdita*

## Impostazioni delle sirene


Il menu contiene due gruppi di impostazioni della sirena: i parametri di attivazione della sirena e l'indicazione della sirena dopo l'allarme.

### Parametri di attivazione della sirena

**Se l'hub o il coperchio del rilevatore è aperto.** Quando abilitato, l'hub attiva le sirene collegate se la custodia dell'hub, il rilevatore o qualsiasi altro dispositivo Ajax è aperto.

**Se nell'app viene premuto il pulsante di antipanico.** Quando la funzione è attiva, l'hub attiva le sirene collegate se nell'app Ajax è stato premuto il pulsante emergenza.



È possibile disattivare la reazione delle sirene quando si preme il pulsante emergenza sul telecomando SpaceControl nelle impostazioni dei tasti del telecomando (Dispositivi → SpaceControl → Impostazioni .

## Impostazioni dell'indicazione della sirena dopo l'allarme



Questa impostazione è disponibile solo nelle [app PRO Ajax](#)

La sirena può informare sugli inneschi in un sistema inserito per mezzo di un'indicazione a LED. Grazie a questa funzione, gli utenti del sistema e le pattuglie dell'Istituto di vigilanza possono vedere che il sistema è stato attivato.

### Implementazione delle funzionalità in HomeSiren

### Implementazione delle funzionalità in StreetSiren

### Implementazione delle funzionalità in StreetSiren DoubleDeck

## Impostazioni rilevatori antincendio

Menu di impostazione dei rilevatori d'incendio FireProtect e FireProtect Plus. Permette di configurare gli allarmi FireProtect interconnessi dei rilevatori d'incendio.

La funzionalità è raccomandata dalle norme europee in materia di incendi, che richiedono, in caso di incendio, una potenza del segnale di avvertimento di almeno 85 dB a 3 metri dalla sorgente sonora. Una tale potenza sonora sveglia anche una persona che dorme profondamente durante un incendio. E si possono disattivare rapidamente i rilevatori d'incendi attivati utilizzando l'app Ajax, Button o KeyPad/KeyPad Plus.

### Maggiori informazioni

## Verifica dell'integrità del sistema

Il **Verifica dell'integrità del sistema** è un parametro che ha la responsabilità di controllare lo stato di tutti i rilevatori e dispositivi di sicurezza prima dell'attivazione. Per impostazione predefinita è disabilitato.

### Maggiori informazioni

## Conferma dell'allarme



Questa impostazione è disponibile solo nelle [app PRO Ajax](#)

La **Conferma dell'allarme** è un evento speciale che l'hub invia al CRA e agli utenti del sistema se determinati dispositivi diversi si sono attivati in un determinato periodo di tempo. Rispondendo solo agli allarmi confermati, l'istituto di vigilanza e le forze di Pubblica Sicurezza potranno ridurre il numero di visite per rispondere ai falsi allarmi.

### [Maggiori informazioni](#)

## Ripristina dopo l'allarme



Questa impostazione è disponibile solo nelle [app PRO Ajax](#)

La funzione non consente di inserire il sistema se in precedenza è stato registrato un allarme. Per l'inserimento, il sistema deve essere ripristinato da un utente autorizzato o da un utente PRO. Le tipologie di allarmi che richiedono il ripristino del sistema vengono definite al momento della configurazione della funzionalità.

La funzione elimina le situazioni in cui l'utente inserisce il sistema con rilevatori che generano falsi allarmi.

### [Maggiori informazioni](#)

## Processo d'inserimento/disinserimento



Questa impostazione è disponibile solo nelle [app PRO Ajax](#)

Il menu permette di abilitare l'inserimento in due fasi, nonché di impostare il ritardo di trasmissione dell'allarme per il processo di disinserimento del sistema di sicurezza.

### Cos'è l'inserimento a due stadi e perché è necessario

### Cos'è il ritardo di trasmissione dell'allarme e perché è necessario

## Disattivazione automatica dei dispositivi



Questa impostazione è disponibile solo nelle [app PRO Ajax](#)

Il sistema di sicurezza Ajax può ignorare gli allarmi o altri eventi dei dispositivi senza rimuoverli dal sistema. In determinate impostazioni, le notifiche sugli eventi di un determinato dispositivo non saranno inviate agli utenti del CRA e del sistema di sicurezza.

Esistono due tipi di **disattivazione automatica dei dispositivi**: da parte del timer e in base al numero di allarmi.

### Cos'è la disattivazione automatica dei dispositivi

È anche possibile disattivare manualmente un dispositivo specifico. Per saperne di più sulla disattivazione manuale dei dispositivi, vedere [qui](#).

## Cancello storico notifiche

Facendo clic sul pulsante si cancellano tutte le notifiche nel feed degli eventi dell'hub.

**Centrale di sorveglianza** – impostazioni per la connessione diretta alla stazione di monitoraggio centrale dell'istituto di vigilanza. I parametri sono impostati dagli ingegneri dell'Istituto di vigilanza. Tenere presente che gli

eventi e gli allarmi possono essere inviati alla stazione di monitoraggio centrale dell'Istituto di vigilanza anche senza queste impostazioni.

### Scheda "Stazione di monitoraggio": cos'è?

- **Protocollo** – la scelta del protocollo utilizzato dall'hub per l'invio degli allarmi alla stazione centrale di monitoraggio dell'Istituto di vigilanza tramite un collegamento diretto. Protocolli disponibili: Ajax Translator (Contact-ID) e SIA.
- **Connessione su richiesta.** Attivare questa opzione se è necessario collegarsi alla Centrale Ricezione Allarmi (CRA) solo quando si trasmette un evento. Se l'opzione è disattivata, il collegamento viene mantenuto ininterrottamente. L'opzione è disponibile solo per il protocollo SIA.
- **Numero oggetto** – il numero di un oggetto nella stazione di monitoraggio (hub).

### **Indirizzo IP primario**

- **Indirizzo IP e Porta** sono le impostazioni dell'indirizzo IP primario e della porta del server dell'Istituto di vigilanza a cui vengono inviati gli eventi e gli allarmi.

### **Indirizzo IP secondario**

- **Indirizzo IP e Porta** sono le impostazioni dell'indirizzo IP secondario e della porta del server dell'Istituto di vigilanza a cui vengono inviati gli eventi e gli allarmi.

### **Canali di invio dell'allarme**

In questo menu vengono selezionati i canali per l'invio di allarmi ed eventi alla stazione centrale di monitoraggio dell'Istituto di vigilanza. Hub 2 Plus può inviare allarmi ed eventi alla stazione di monitoraggio centrale tramite **Ethernet, UMTS/LTE e Wi-Fi**. Raccomandiamo di utilizzare tutti i canali di comunicazione allo stesso momento, così da aumentare l'affidabilità della trasmissione e restare al sicuro contro i guasti che interessano gli operatori di telecomunicazioni.

- **Ethernet** – consente la trasmissione di eventi e allarmi tramite Ethernet.
- **Cellulare** – consente la trasmissione di eventi e allarmi tramite Internet mobile.
- **Wi-Fi** – consente la trasmissione di eventi e allarmi tramite Wi-Fi.
- **Prova periodica** – se abilitato, l’hub invia i rapporti di prova con un determinato periodo di tempo alla Centrale Ricezione Allarmi (CRA) per un ulteriore monitoraggio della connessione dell’oggetto.
- **Intervallo di monitoraggio della stazione di sorveglianza** – imposta il periodo per l’invio dei messaggi di prova: da 1 minuto a 24 ore.

### **Sistema di crittografia**

Impostazioni di crittografia della trasmissione degli eventi nel protocollo SIA. Viene utilizzata la crittografia AES a 128 bit.

- **Crittografia** – se abilitata, gli eventi e gli allarmi trasmessi alla stazione centrale di monitoraggio in formato SIA sono criptati.
- **Chiave di codifica** – chiave di cifratura degli eventi e degli allarmi trasmessi. Deve corrispondere al valore sulla Stazione Centrale di Monitoraggio.

### **Coordinate del pulsante di emergenza**

- **Invia coordinate** – se abilitato, la pressione di un pulsante di emergenza nell’app invia alla stazione centrale di monitoraggio le coordinate del dispositivo su cui è installata l’app e su cui il pulsante di emergenza viene premuto.

### **Ripristino allarme su CRA**

L'impostazione permette di selezionare quando l’evento di ripristino dell’allarme verrà inviato al CRA: ripristino immediato/al ripristino del rilevatore (per default) o al disinserimento.

[Maggiori informazioni](#)

**PRO** – Impostazioni degli utenti PRO (installatori e rappresentanti dell'Istituto di vigilanza) del sistema di sicurezza. Determina chi ha accesso al sistema di sicurezza, i diritti assegnati agli utenti PRO e in che modo il sistema di sicurezza li informa in merito agli eventi.

[Come aggiungere un PRO all'hub](#)

**Istituti di vigilanza** – un elenco di istituti di vigilanza nella zona dell'utente. La zona è determinata in base ai dati GPS o alle impostazioni regionali dello smartphone.

**Manuale utente** – apre la guida utente di Hub 2 Plus.

**Importazione dati** – un menu per il trasferimento automatico di dispositivi e impostazioni da un altro hub. **Notare che ci si trova nelle impostazioni dell'hub sul quale si desidera importare i dati.**

[Maggiori informazioni sull'importazione dei dati](#)

**Disaccoppia hub** – rimuove l'account dall'hub. Indipendentemente da ciò, tutte le impostazioni e i rilevatori collegati rimangono memorizzati.

**Reset delle impostazioni**

Riportare l'hub alle impostazioni di fabbrica:

1. Accendere l'hub se è spento.
2. Rimuovere tutti gli utenti e gli installatori dall'hub.
3. Tenere premuto il pulsante di accensione per 30 s – il logo Ajax sull'hub inizierà a lampeggiare con luce rossa.
4. Rimuovere l'hub dal proprio account.



Il reset dell'hub non cancella gli utenti collegati!

## Notifiche di eventi e allarmi

Il sistema di sicurezza Ajax informa l'utente su allarmi ed eventi in tre modi: notifiche push, SMS e telefonate. Le impostazioni di notifica possono essere modificate solo dagli utenti registrati.

Tipi di eventi	Scopo	Tipi di notifiche
Malfunzionamenti	<ul style="list-style-type: none"><li>• Perdita di connessione tra il dispositivo e l'hub</li><li>• Inibizione</li><li>• Carica batteria bassa nel dispositivo o nell'hub</li><li>• Mascheramento</li><li>• Allarme in caso di manomissione</li></ul>	Notifiche push SMS
Allarme	<ul style="list-style-type: none"><li>• Intrusione</li><li>• Incendio</li><li>• Inondazione</li><li>• Perdita di connessione tra l'hub e il server Ajax Cloud</li></ul>	Chiamate Notifiche push SMS

Eventi	<ul style="list-style-type: none"> <li>Attivazione di <b><u>WallSwitch, Relay, Socket</u></b></li> </ul>	<p>Notifiche push</p> <p>SMS</p>
Inserire/disinserire	<ul style="list-style-type: none"> <li>Inserire/disinserire gruppi o oggetti interi</li> <li>Attivazione della <b><u>modalità Notte</u></b></li> </ul>	<p>Notifiche push</p> <p>SMS</p>

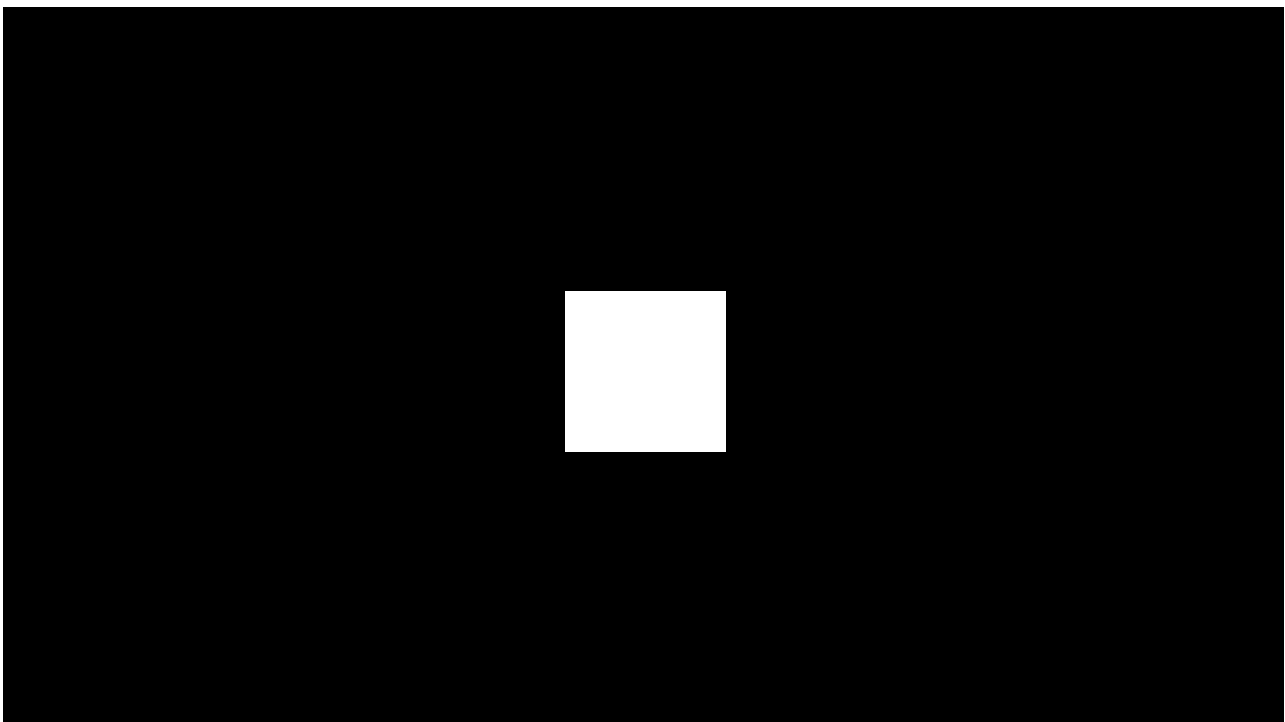
### In che modo Ajax invia le notifiche degli avvisi agli utenti



L'hub non notifica agli utenti i rilevatori di apertura che si attivano in modalità disinserita quando la funzione Campanello è abilitata e configurata. Solo le sirene collegate al sistema avvertono dell'apertura.

[Che cosa sono la funzione Campanello](#)

## Videosorveglianza



00:00



00:10

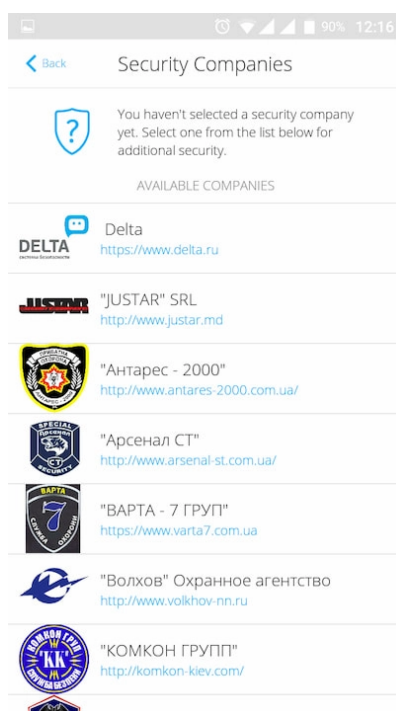
È possibile collegare telecamere di terze parti al sistema di sicurezza: è stata implementata la perfetta integrazione con le telecamere IP e i videoregistratori

Dahua, Hikvision e Safire. È inoltre possibile collegare telecamere di terze parti che supportano il protocollo RTSP. È possibile collegare al sistema fino a 100 dispositivi di videosorveglianza.

## Come aggiungere una telecamera al sistema di sicurezza Ajax

### Connessione a un istituto di vigilanza

L'elenco delle aziende che accettano il sistema alla stazione centrale di monitoraggio si trova nel menu **Istituto di vigilanza (Dispositivi**  **→ Hub** **→ Impostazioni**  **→ Istituti di vigilanza)**:



Selezionare un Istituto di vigilanza e fare clic su **Invia richiesta di monitoraggio**. L'Istituto di vigilanza contatterà l'utente per discutere le condizioni di connessione. In alternativa, è possibile contattare un Istituto di vigilanza (i contatti sono disponibili nell'app) per concordare una connessione.

La connessione alla Centrale Ricezione Allarmi (CRA) è implementata tramite il protocollo Contact ID o SIA.

### Installazione

Prima di installare l'hub, assicurarsi che la posizione scelta sia ottimale e conforme ai requisiti di questo manuale! È consigliabile installare l'hub in un luogo nascosto alla vista.

Assicurarsi che la comunicazione tra l'hub e tutti i dispositivi collegati sia stabile. Se l'intensità del segnale è bassa (una sola tacca) non possiamo garantire un funzionamento stabile del sistema di sicurezza. Attuare tutte le misure possibili per migliorare la qualità del segnale! Come minimo, provare a spostare il dispositivo: uno spostamento di soli 20 cm può migliorare notevolmente la qualità della ricezione.

Se dopo lo spostamento viene rilevata un'intensità segnale bassa o instabile, usare il [ripetitore ReX del segnale radio](#).

Durante l'installazione e l'utilizzo del dispositivo, si raccomanda di seguire le norme generali di sicurezza relative ai dispositivi elettrici, oltre ai requisiti previsti dalle normative vigenti in materia di sicurezza elettrica. È severamente proibito smontare il dispositivo sotto tensione! Non usare il dispositivo se il cavo di alimentazione risulta danneggiato.

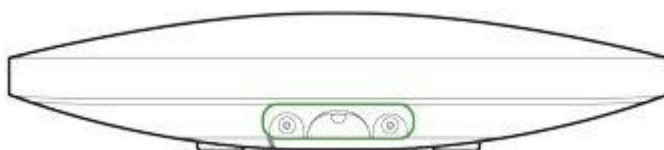
### Installazione dell'hub:

1. Fissare il pannello di montaggio SmartBracket usando le viti in dotazione. Se si usano altri metodi di fissaggio, assicurarsi che non danneggino o deformino il pannello.



Si sconsiglia l'uso di nastro biadesivo per l'installazione: ciò può causare la caduta di un hub in caso di urto.

2. Fissare l'hub al pannello di montaggio. Dopo l'installazione, verificare lo stato dell'anti-manomissione sull'app di Ajax e la tenuta del pannello. Se viene rilevato un tentativo di rimuovere il ripetitore dalla superficie o dal pannello di montaggio, verrà inviata una notifica.
3. Fissare l'hub sul pannello SmartBracket con le viti in dotazione.



Non capovolgere l'hub quando lo si attacca in posizione verticale (ad esempio, su una parete). Se fissato correttamente, il logo Ajax può essere letto orizzontalmente.



## Non collocare l'hub:

- Fuori dai locali protetti (all'esterno).
- Vicino o dentro a oggetti in metallo o specchi, in quanto potrebbero attenuare o bloccare il segnale.
- In luoghi con alti livelli di interferenze radio.
- Vicino a fonti di interferenza radio: a meno di 1 metro dal router e dai cavi di alimentazione.
- All'interno di locali la cui temperatura e umidità superano i limiti indicati nelle specifiche.

## Manutenzione

Verificare regolarmente la capacità operativa del sistema di sicurezza Ajax. Mantenere pulita la custodia dell'hub rimuovendo immediatamente polvere, ragnatele e altre impurità. Utilizzare una salvietta morbida e asciutta per le operazioni di manutenzione dell'apparecchiatura.

Non utilizzare sostanze contenenti alcool, acetone, benzina e altri solventi attivi per la pulizia dell'hub.

### Come sostituire la batteria dell'hub

## La confezione include

1. Hub 2 Plus
2. Pannello di montaggio SmartBracket

3. Cavo di alimentazione
4. Cavo Ethernet
5. Kit di installazione
6. Starter pack – non disponibile in tutti i Paesi
7. Guida rapida

## Specifiche tecniche

Classificazione	Pannello di controllo del sistema di sicurezza con supporto Ethernet, Wi-Fi e doppia scheda SIM
Supporto dei rilevatori con verifica fotografica degli allarmi	Disponibile
Numero di dispositivi connessi	Fino a 200
Numero di ReX connessi	Fino a 5
Numero di sirene collegate	fino a 10
Numero di gruppi di sicurezza	Fino a 25
Numero di utenti	Fino a 200
Videosorveglianza	Fino a 100 telecamere o DVR
Numero di stanze	Fino a 50
Numero di scenari	Fino a 64 <a href="#"><u>Maggiori informazioni</u></a>
Protocolli di comunicazione con la Stazione di monitoraggio centrale	Contact ID, SIA (DC-09) <a href="#"><u>Software per CRA con supporto per la foto-verifica degli allarmi</u></a>
Alimentatore	110-240 V con la batteria preinstallata 6 V con un alimentatore alternativo <a href="#"><u>6V PSU</u></a> Consumo energetico – 10 W
Batteria di backup integrata	Li-Ion 3 A·h Fornisce fino a 15 ore di durata della batteria con una scheda SIM

Consumo di energia dalla rete	Fino a 10 W
Protezione dalle manomissioni	Disponibile, anti-manomissione
Banda di frequenza operativa	868,0–868,6 MHz o 868,7–869,2 MHz, in base al luogo di acquisto
Potenza di uscita RF	10,4 mW (limite 25 mW)
Raggio del segnale radio	Fino a 2.000 m
Canali di comunicazione	<p>2 Schede SIM</p> <ul style="list-style-type: none"> <li>• 2G (GSM900/DCS1800 (B3/B8))</li> <li>• 3G (WCDMA 850/900/2100 (B1/B5/B8))</li> <li>• LTE (FDD B1/B3/B5/B7/B8/B20/B28)</li> </ul> <p>Wi-Fi (802.11 b/g/n)</p> <p>Ethernet</p>
Temperature di funzionamento	Da -10°C a +40°C
Umidità di funzionamento	Fino al 75%
Dimensioni	163 × 163 × 36 mm
Peso	367 g
Vita utile	10 anni

### Conformità agli standard

## Garanzia

La garanzia per i prodotti “AJAX SYSTEMS MANUFACTURING”, LIMITED LIABILITY COMPANY, è valida per 2 anni a partire dalla data di acquisto e non vale per la batteria pre-installata.

Se il dispositivo non funziona correttamente, si prega di contattare il servizio di supporto. Nella metà dei casi si riesce a risolvere i problemi tecnici a distanza!

### Obblighi di garanzia

### Contratto con l'utente finale

Supporto tecnico: [support@ajax.systems](mailto:support@ajax.systems)