

Hub 2 manuale utente

Aggiornato il July 3, 2020



Ajax è un sistema di sicurezza wireless che protegge da intrusioni, incendi e allagamenti; inoltre, consente agli utenti di controllare le apparecchiature elettriche direttamente da un'app per dispositivi mobili. Il sistema risponde immediatamente alle minacce, comunicando gli eventuali incidenti all'utente e all'istituto di vigilanza.



Hub 2 costituisce un pannello di controllo del sistema di sicurezza intelligente che supporta rilevatori con verifica fotografica delle intrusioni. In quanto

elemento chiave del sistema di sicurezza, controlla il funzionamento dei dispositivi Ajax e in caso di minaccia comunica immediatamente i segnali di allarme informando il proprietario e la centrale di monitoraggio degli incidenti.

Hub 2 necessita di una connessione Internet per accedere al servizio Ajax Cloud e configurare/gestire il sistema da qualsiasi luogo nel mondo tramite le applicazioni Ajax, nonché per comunicare allarmi ed eventi e aggiornare il firmware OS Malevich. Tutti i dati sono memorizzati in un sistema con sicurezza multilivello e lo scambio di informazioni con l'hub avviene tramite un canale crittografato.

Per comunicare con il servizio Ajax Cloud service, l'hub utilizza una connessione internet via cavo (Ethernet) e due SIM card 2G. È consigliabile fare uso di tutti i canali di comunicazione, in modo da garantire una connessione più affidabile con il servizio Ajax Cloud e prevenire il rischio di carenza di uno dei fornitori di servizi.

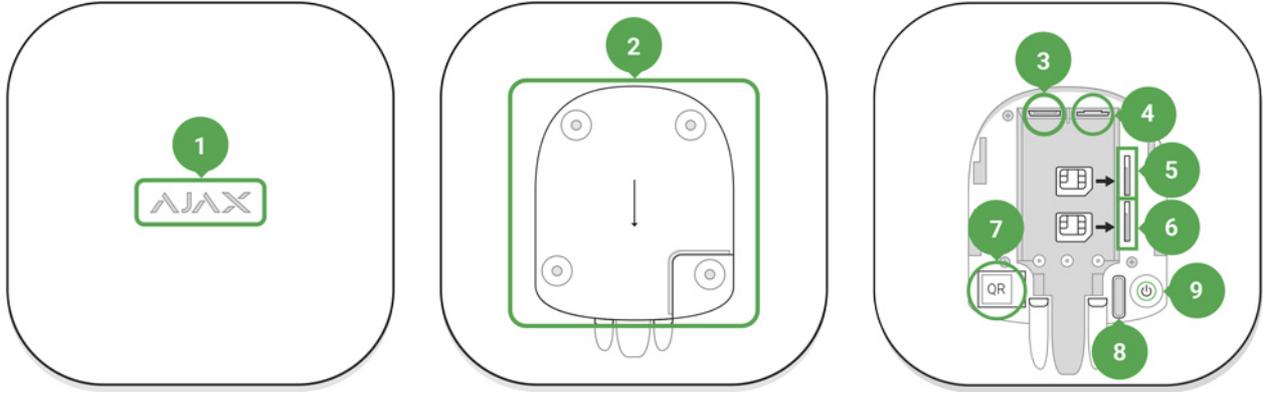
Gli utenti possono gestire il sistema di sicurezza e rispondere tempestivamente agli allarmi e alle notifiche usando le app per iPhone e gli smartphone basati su Android, macOS, e Windows. Il sistema avvisa l'utente in caso di allarmi e altri eventi tramite notifiche push, SMS e chiamate telefoniche.

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 Button o secondo quanto programmato. È possibile creare uno scenario in remoto tramite l'app Ajax.

Come creare e configurare uno scenario nel sistema di sicurezza Ajax

Compra il pannello di sicurezza intelligente Hub 2

Elementi funzionali



1. Logo Ajax con indicatore luminoso
2. Pannello di montaggio SmartBracket (sfilare con decisione verso il basso per aprire; la sezione perforata è necessaria per il dispositivo anti-manomissione. Attenzione a non romperlo!)
3. Cavo di alimentazione
4. Connettore Ethernet
5. Slot per l'installazione di una micro-SIM
6. Slot per l'installazione di una micro-SIM
7. Codice QR
8. Pulsante anti-manomissione
9. Pulsante di accensione

Principi operativi di Hub 2

L'hub raccoglie informazioni in forma crittografata sul funzionamento dei dispositivi collegati, analizza i dati e, in caso di allarme, avverte del pericolo il proprietario del sistema in meno di un secondo e comunica l'allarme direttamente alla centrale di monitoraggio o all'istituto di vigilanza.

Per comunicare con i dispositivi, monitorare il loro funzionamento e rispondere rapidamente alle minacce, Hub 2 utilizza la tecnologia radio Jeweller. Per la trasmissione dei dati visivi, Hub 2 utilizza il protocollo radio Ajax Wings, un protocollo ad alta velocità basato sulla tecnologia Jeweller. Wings usa anche un'antenna specifica per aumentare l'affidabilità del canale.

[Tutti i dispositivi Ajax](#)

Indicatore LED sull'hub



Il logo con indicatore luminoso può assumere i colori rosso, bianco o verde secondo gli stati del dispositivo.

Evento	Indicatore luminoso
Ethernet e almeno una SIM collegate	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 20 secondi. Il colore dell'indicatore dipende dal numero dei canali di comunicazione collegati.

Account Ajax

Il sistema di sicurezza viene configurato e gestito mediante applicazioni Ajax progettate per iPhone e gli smartphone basati su Android, macOS e Windows.

Per configurare il sistema, installare l'[app Ajax](#) e registrare un account. Per gestire uno o più hub, si consiglia di utilizzare l'app del sistema di sicurezza Ajax. Se si prevede di gestire più di cento hub, è consigliabile utilizzare l'applicazione [Ajax PRO: Tool for Engineers](#) (per iPhone e smartphone basati su Android) o [Ajax PRO Desktop](#) (per computer fissi e portatili con sistemi operativi

Windows e macOS). La procedura richiede la conferma dell'indirizzo e-mail e del numero di telefono dell'utente. Nota bene: il proprio numero di telefono e l'indirizzo email sono utilizzabili per la creazione di un solo account Ajax! Non è necessario creare un nuovo account per ciascun hub: basta aggiungere i diversi hub a un singolo account.



Le informazioni concernenti gli hub aggiunti sull'account saranno caricate sul servizio cloud Ajax Cloud in forma crittografata.

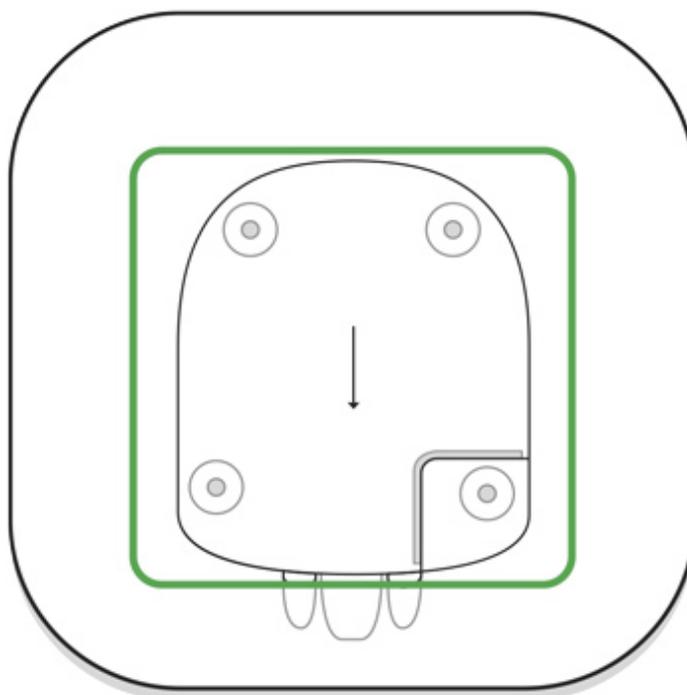
Requisiti di sicurezza

Durante l'installazione e l'utilizzo di Hub 2, 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.

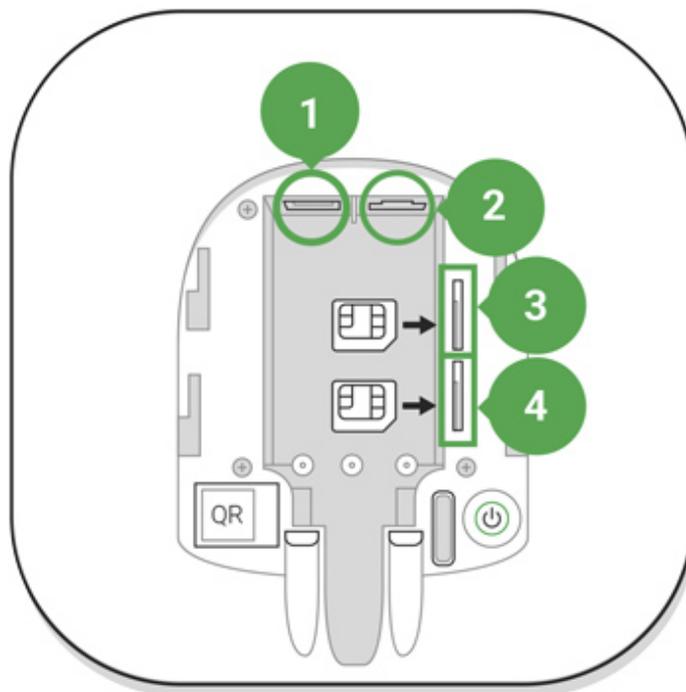
È severamente proibito smontare il dispositivo mentre è connesso a una fonte di alimentazione! Inoltre, non utilizzare il dispositivo se il cavo di alimentazione risulta danneggiato.

Connessione dell'hub

1. Rimuovere il coperchio dell'hub sfilandolo con decisione verso il basso. Non danneggiare la porzione perforata, la quale è necessaria per l'attivazione del dispositivo di allarme contro i tentativi di manomissione!



2. Collegare il cavo di alimentazione e il cavo Ethernet ai connettori corrispondenti.



- 1 – Connettore di alimentazione
- 2 – Connettore Ethernet
- 3, 4 – Slot per schede micro-SIM

3. Tenere premuto il pulsante di accensione per 3 secondi fino a quando il logo non si illumina. La procedura di aggiornamento alla versione firmware più recente e di accesso a internet può richiedere fino a 2 minuti. Il logo di colore verde o bianco indica che l'hub è in funzione ed è connesso al servizio Ajax Cloud.



Se la connessione Ethernet non viene stabilita automaticamente, disabilitare i filtri degli indirizzi proxy e MAC e attivare DHCP nelle impostazioni del router: l'hub riceverà automaticamente un indirizzo IP. Sarà poi possibile assegnare un indirizzo IP statico all'hub nell'applicazione Ajax.

4. Per connettersi via GSM, è necessaria una scheda micro-SIM di un operatore mobile con la richiesta del PIN disabilitata (è possibile disabilitarla utilizzando un telefono cellulare) e un saldo sul conto sufficiente per pagare i servizi dell'operatore di telefonia mobile. Se l'hub non è connesso via GSM, utilizzare Ethernet per configurare le impostazioni dell'operatore di rete (roaming, access point APN, nome utente, e

password). Per conoscere le impostazioni del proprio operatore di rete, contattare il servizio clienti del proprio provider.

Aggiungere un hub all'app di Ajax

1. Accedere all'app di Ajax. Assicurarsi di concedere all'app l'accesso a tutte le funzioni di sistema richieste e, in particolare, alle autorizzazioni per la visualizzazione di notifiche. Se si usa uno smartphone Android, è consigliabile utilizzare le [istruzioni di configurazione delle notifiche push](#).
2. Accedere al proprio account e fare clic su **Aggiungi un hub**. Scegliere se utilizzare il metodo manuale o la guida passo-passo. Quando si configura il sistema per la prima volta, è consigliabile utilizzare la guida passo-passo.
3. Specificare il nome dell'hub e scansionare il codice QR che si trova sotto il coperchio o immetterlo manualmente.
4. Attendere che il processo di aggiunta sia completato. Una volta collegato, l'hub sarà visibile nella scheda **Dispositivi**. .

Utenti del sistema di sicurezza

Quando si aggiunge un Hub al proprio account, l'utente diventa l'amministratore del dispositivo. Un solo hub può avere fino a 50 utenti/amministratori. Gli amministratori possono aggiungere utenti al sistema di sicurezza e assegnare loro i relativi diritti.

Il cambiamento o la rimozione di un amministratore del sistema di sicurezza non causano il reset dei dispositivi ad esso collegati.

Diritti dell'utente del sistema di sicurezza Ajax

Aggiungere stanze

Prima di collegare il dispositivo all'hub, creare almeno una stanza.

La descrizione di un evento del dispositivo indicherà la stanza in cui esso si trova:



Per creare una stanza, andare alla scheda **Stanze**  e fare clic su **Aggiungi Stanza**. Assegnarle un nome e, se necessario, allegare (o scattare) una foto per facilitare l'identificazione della stanza nella lista.

Per cancellare una stanza o modificarne il nome o l'avatar, fare clic sull'icona a forma di ingranaggio  e accedere alle impostazioni della stanza.

Connessione di rilevatori e dispositivi

Quando si aggiunge un hub seguendo la guida passo-passo, verrà richiesto di aggiungere i dispositivi che proteggeranno gli ambienti. È possibile saltare questo passaggio e ritornarvi in un secondo momento.

Per assegnare un dispositivo all'hub:

1. Nell'applicazione Ajax, aprire la stanza e selezionare **Aggiungi dispositivo**.
2. Attribuire un nome al dispositivo, immettere il suo codice QR inquadrandolo (o inserendolo manualmente) e assegnare un gruppo (se la modalità gruppo è abilitata).
3. Fare clic su **Aggiungi** per attivare il conto alla rovescia per l'aggiunta del dispositivo.
4. Accendere il dispositivo durante il conto alla rovescia; il LED del dispositivo lampeggia una volta. Perché sia possibile collegarlo, il dispositivo deve trovarsi entro la portata delle comunicazioni radio dell'hub (nello stesso ambiente protetto).

Se la connessione non riesce, spegnere il dispositivo per 5 secondi e riprovare.

Videosorveglianza

È possibile collegare telecamere di terze parti al sistema di sicurezza: è stata implementata un'integrazione completa con le telecamere IP e i videoregistratori Dahua, Hikvision e Safire e si possono anche collegare telecamere di terze parti che supportano il protocollo RTSP. È possibile collegare al sistema fino a 25 dispositivi di videosorveglianza.

Aggiunta di una telecamera o di un videoregistratore Dahua all'hub

Aggiunta di una telecamera o di un videoregistratore Hikvision/Safire all'hub

Impostazioni dell'hub

Per accedere alle impostazioni dell'hub, selezionare quest'ultimo nella lista dei dispositivi e fare clic sull'icona ingranaggio .

Parametri regolabili:

Utenti – impostazioni del sistema di sicurezza per gli utenti. Determina chi ha accesso al sistema di sicurezza, i diritti assegnati agli utenti e in che modo il sistema di sicurezza li informa sugli eventi.

In che modo il sistema di sicurezza Ajax segnala gli eventi

Come aggiungere nuovi utenti all'hub

Ethernet – impostazioni per la connessione internet via cavo.

GSM – attiva/disattiva la connessione alla rete cellulare, imposta la connessione e permette di controllare il proprio saldo.

Geofence – configurazione dei promemoria per inserire/disinserire il sistema di sicurezza quando si superano i confini di una certa zona. La posizione dell'utente viene determinata usando il modulo GPS dello smartphone.

Cosa sono i Geofence e come funzionano

Aree – configurazione della modalità gruppo.

La modalità gruppo fornisce le seguenti funzionalità:

- Gestione della sicurezza di locali singoli o di gruppi di rilevatori.
L'ufficio è protetto mentre l'addetto alle pulizie lavora in cucina.
- Differenziazione dell'accesso agli strumenti di amministrazione delle modalità di sicurezza.
I dipendenti del reparto marketing non possono entrare nell'ufficio legale.

Hub OS Malevich 2.6: nuovo livello di sicurezza

Programma di sicurezza – inserimento / disinserimento del sistema di sicurezza come programmato.

Come creare e configurare uno scenario nel sistema di sicurezza

Ajax

Prova zona rilevazione – test della zona di rilevamento dei rilevatori connessi all’hub. Il test consente di determinare la distanza massima di attivazione degli allarmi dei rilevatori.

Cos’è una prova zona di rilevazione

Jeweller – configurazione del periodo di polling per l’hub e i dispositivi collegati. Queste impostazioni determinano la frequenza di scambio dei dati tra l’hub e i dispositivi, nonché la velocità di identificazione delle perdite di comunicazione.

- **Lunghezza frame (sec)** – frequenza di polling dei dispositivi connessi all’hub, impostata in una gamma tra 12 e 300 s (default: 36 s).
- **Perdite prima di segnare sensore come perso** – conteggio dei pacchetti di comunicazioni non consegnati (default: 30 pacchetti).

Il tempo che precede l’invio di un messaggio relativo alla perdita della comunicazione tra l’hub e il dispositivo viene calcolato utilizzando la formula:

*Intervallo di Polling * (numero di pacchetti non consegnati + 1 pacchetto di correzione)*

Più breve è il periodo di polling, più è rapida la ricezione delle informazioni sugli eventi dai dispositivi connessi all’hub e la comunicazione dei comandi dall’hub ai dispositivi; tuttavia, ciò riduce la durata utile delle batterie in dotazione dei dispositivi. Allo stesso tempo, le informazioni su un allarme o una manomissione vengono sempre comunicate istantaneamente.

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 o più	100 dispositivi

Il numero massimo di sirene connesse è 10 con qualsiasi impostazione!

Manutenzione – un gruppo di impostazioni di servizio dell’hub.

Impostazioni di connessione per l’Hub e il servizio Ajax Cloud:

- **Intervallo di ping Hub-Server (sec).** La frequenza di polling del servizio Ajax Cloud da parte dell’hub, impostata tra 10 e 300 s. Il valore raccomandato e di default è 60 s.
- **Aumento ritardo allarme quando hub non è in linea (sec).** Questo ritardo è necessario per ridurre i rischi di falso allarme associati alla perdita di connessione con il servizio 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 e di default è 300 s.

Il tempo necessario per l’invio di un messaggio relativo alla perdita della comunicazione tra l’hub e il dispositivo viene calcolato utilizzando la formula:

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

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

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

Rapidità di rilevamento della perdita di connessione tra l’hub e il servizio Ajax Cloud

- **Luminosità dei LED.** Regolazione della luminosità dei LED nel logo dell'hub. Impostabile in una gamma tra 1 e 10 (default: 10).
- **Controllo dell'integrità del sistema.** Una volta abilitata la funzione, l'hub controlla lo stato di tutti i dispositivi prima di inserire: carica delle batterie, anti-manomissione, connessione. Se viene rilevato un problema quando si inserisce il sistema, l'hub non attiva la modalità inserita e invia un avviso.
- **Permesso di inserimento** (l'opzione è attivabile solo dopo l'abilitazione del **Controllo di integrità del sistema**). Quando la funzione è attiva, il sistema di sicurezza può essere inserito anche quando è presente un malfunzionamento.

Per inserire il sistema di sicurezza malfunzionante mediante l'applicazione Ajax:

1. Attivare la modalità inserita – si riceverà il relativo avviso con l'elenco dei malfunzionamenti.
2. Confermare l'attivazione dello stato inserito del sistema di sicurezza premendo **Inserire**.

Per confermare l'attivazione della modalità inserita del sistema di sicurezza con malfunzionamenti quando si usa la tastiera del KeyPad o un telecomando SpaceControl:

1. Attivare la modalità inserita – sarà comunicato un rifiuto.
2. Confermare la modalità inserita del sistema ripetendo l'attivazione della modalità inserita entro 30 s.

Che cos'è la verifica di integrità del sistema?

- **Aggiornamento automatico firmware.** Configurazione degli aggiornamenti automatici del firmware OS Malevich. Il firmware dell'hub si aggiorna automaticamente all'accensione se è disponibile una nuova versione.

Come si aggiorna OS Malevich

Configurazione dei rilevatori d'incendi FireProtect e FireProtect Plus

- **Interconnessione allarmi FireProtect.** La funzione attiva le sirene incorporate di tutti i rilevatori d'incendi, se almeno uno di essi rileva una minaccia.



Gli Interconnessione allarmi sono supportati dai rilevatori FireProtect e FireProtect Plus con versioni firmware 3.42 e superiori. Si prega di notare che quando si attivano gli Allarmi interconnessi, non è possibile impostare l'intervallo di ping del rilevatore di hub (impostazioni Jeweller) a più di 48 secondi.

Cosa sono gli allarmi FireProtect interconnessi?

- **Ignora il primo allarme.** Funzionalità di ripetizione allarmi per verificare la presenza di fumo.

Questa opzione funziona come segue:

1. Un rilevatore rileva presenza di fumo.
2. Si attiva un timer di 30 s incorporato all'interno del rilevatore.
3. Se il rilevatore rileva ancora una minaccia dopo 30 s, l'allarme viene comunicato all'hub.

Questa impostazione è raccomandata se ci sono possibili fonti di falsi allarmi all'interno dei locali; ad esempio, se il rilevatore è installato in una posizione in cui possono esserci correnti d'aria.

Impostazioni per la raccolta e la memorizzazione dei rapporti del Sistema di sicurezza Ajax

- **Log dell'hub.** È possibile disattivare i log o selezionare un canale di trasmissione:
 - Ethernet
 - Wi-Fi (solo in Hub Plus)

- No – log disattivati



La disattivazione dei log è sconsigliata poiché le informazioni possono essere utili in caso di errori di azionamento del sistema!

Impostazioni di attivazione della sirena

- **Se l'hub o la custodia del rilevatore sono aperti.** Quando questa funzione è attiva, l'hub aziona le sirene connesse se la custodia dell'hub, il rilevatore o qualsiasi altro dispositivo Ajax viene aperto.
- **Se viene premuto il pulsante allarme nell'applicazione.** Quando questa funzione è attiva, l'hub aziona le sirene connesse se il pulsante antipanico dell'app di Ajax viene premuto.



Disabilitare la risposta della sirena premendo il pulsante antipanico sul telecomando SpaceControl nelle impostazioni del telecomando (**Dispositivi** 
> **SpaceContol** > **Impostazioni** )

Società di sicurezza – impostazioni per la connessione diretta alla stazione di monitoraggio centrale dell'istituto di vigilanza.



Gli eventi e gli allarmi possono essere comunicati alla stazione di monitoraggio centrale o all'Istituto di vigilanza senza queste impostazioni

Cos'è la Società di sicurezza

PRO – impostazioni per gli utenti PRO (installatori e rappresentanti degli istituti di vigilanza) del sistema di sicurezza. Determina chi ha accesso al sistema di sicurezza, i diritti assegnati agli utenti e in che modo il sistema di sicurezza li informa sugli eventi.

Centrale di sorveglianza – 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.

Guida utente – apre la guida utente di Hub 2.

Disaccoppia hub – rimuovi il tuo account dall'hub. Nel frattempo tutte le impostazioni e i rilevatori collegati vengono salvati.

Resetta le impostazioni dell'hub

Riporta l'hub alle impostazioni di fabbrica:

1. Accende 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.

Avvisi sugli eventi e gli allarmi

Il Sistema di sicurezza Ajax informa l'utente su avvisi ed eventi utilizzando tre tipi di notifiche: notifiche push, SMS e chiamate telefoniche. Le impostazioni di avviso possono essere modificate solo dagli utenti registrati.

Tipi di eventi	Scopo	Tipi di notifiche
Malfunzionamenti	<ul style="list-style-type: none"> • Perdita di connessione tra il dispositivo e l'hub • Inibizione • Carica batteria bassa nel dispositivo o nell'hub • Mascheramento • Manomissione dell'involucro del rilevatore 	<p>Notifiche push</p> <p>SMS</p>
Allarme	<ul style="list-style-type: none"> • Intrusione • Incendio • Allagamento • L'hub ha perso la connessione con il servizio Ajax Cloud 	<p>Chiamate</p> <p>Notifiche push</p> <p>SMS</p>
Eventi	<ul style="list-style-type: none"> • Accendi/Spegni <u>WallSwitch</u>, <u>Relay</u>, <u>Socket</u> 	<p>Notifiche push</p> <p>SMS</p>
Inserire/disinserire	<ul style="list-style-type: none"> • Inserire/disinserire locali interi o gruppi • Attivazione della modalità Notte 	<p>Notifiche push</p> <p>SMS</p>

In che modo Ajax comunica gli allarmi agli utenti

Connessione a una centrale di sorveglianza

L'elenco delle organizzazioni che collegano il sistema alle stazioni di monitoraggio centrali delle organizzazioni si trova nel menu **Centrale di sorveglianza (Dispositivi  > Hub > Impostazioni  > Centrale di sorveglianza)**.

Si prega di contattare i rappresentanti di uno degli istituti che forniscono tali servizi nella propria città per impostare la connessione.

La connessione alla Centrale Ricezione Allarmi (CRA) si effettua tramite Contact ID o protocollo SIA.

Fissaggio

Prima di installare l'hub, assicurarsi che la posizione scelta sia ottimale e conforme ai requisiti di queste istruzioni! È consigliabile installare l'hub in un luogo al riparo dagli sguardi indiscreti.

Accertarsi che l'hub disponga di un'intensità di segnale stabile con tutti i dispositivi connessi. Se l'intensità del segnale è bassa (una sola tacca) non possiamo garantire un funzionamento stabile del sistema di sicurezza. Adottare ogni possibile misura 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 di segnale bassa o instabile, usare un ripetitore ReX del segnale radio.

Durante l'installazione 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.

Installazione dell'hub:

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



L'uso di nastro biadesivo per l'installazione è sconsigliato. Esso può causare la caduta dell'hub e il malfunzionamento del dispositivo a causa dell'urto.

2. Fissare l'hub al pannello di montaggio. Dopo l'installazione, verificare lo stato dell'anti-manomissione nell'applicazione Ajax e la saldezza del fissaggio del pannello.
3. Per garantire una maggiore tenuta, fissare l'hub alla piastra con le viti in dotazione.

Non capovolgere l'hub in posizione verticale (ad esempio su una parete). Con una corretta fissazione, il logo Ajax leggerà in orizzontale.

Se viene rilevato un tentativo di rimuovere il ripetitore dalla superficie o dal pannello di montaggio, verrà inviata una notifica.



È severamente proibito smontare il dispositivo mentre è connesso a una fonte di alimentazione! Non usare il dispositivo se il cordone di alimentazione risulta danneggiato.

Non smontare o modificare il dispositivo ReX o i suoi singoli componenti. Ciò potrebbe interferire con il normale funzionamento del dispositivo o causarne il guasto.

Non collocare l'hub:

- fuori dal locale (all'esterno);
- vicino a oggetti in metallo e specchi che potrebbero attenuare o bloccare i segnali radio;
- in luoghi con un segnale GSM debole;
- vicino a fonti di interferenza radio: a meno di 1 metro dal router e dai cavi di alimentazione;
- in ambienti con elevata umidità e temperature superiori a limiti ammessi.

Manutenzione del sistema Ajax

Verificare regolarmente il funzionamento del sistema di sicurezza Ajax.
Mantenere pulita la custodia rimuovendo immediatamente polvere, ragnatele e altre impurità. Utilizzare una salvietta morbida e asciutta adatta alla manutenzione dell'apparecchiatura.

Non usare sostanze contenenti alcol, acetone, benzina o altri solventi attivi.

Come sostituire la batteria del hub

La confezione include

1. Hub 2
2. Cavo di alimentazione
3. Cavo Ethernet
4. Kit di installazione
5. Kit startup GSM – non disponibile in tutti i paesi
6. Guida rapida

Specifiche tecniche

Classificazione	Pannello di controllo del sistema di sicurezza intelligente con supporto Ethernet e di due SIM card
Numero massimo di dispositivi collegabili	Fino a 100
ReX (ripetitori)	Fino a 5
Gruppi di sicurezza	Fino a 9
Utenti del sistema di sicurezza	Fino a 50
Videosorveglianza	Fino a 25 telecamere o DVR
Stanze	Fino a 50
Escenarios	Fino a 32 (Le reazioni al cambiamento della modalità di sicurezza non sono prese in considerazione nel limite generale degli scenari hub)

Protocolli di comunicazione con la Stazione di monitoraggio centrale	Contact ID, SIA
Alimentatore	110–240 V CA, 50/60 Hz
Batteria ricaricabile incorporata	Li-Ion 2 A·h (fino a 16 ore di durata della batteria quando le connessioni Ethernet e Wi-Fi sono disattivate)
Consumo energetico	10 W
Protezione dalle manomissioni	Disponibile, anti-manomissione
Banda di frequenza operativa	868.0 – 868.6 MHz or 868.7 – 869.2 MHz, secondo l'area di vendita
Potenza di uscita RF	8.20 dBm / 6.60 mW (limite 25 mW)
Modulazione del segnale radio	GFSK
Portata del segnale radio	Fino a 2.000 m (in campo aperto)
Canali di comunicazione	<ul style="list-style-type: none"> • 2 SIM card (GSM 850/900/1800/1900 MHz GPRS) • Ethernet
Temperature di funzionamento	Da -10°C a +40°C
Umidità di funzionamento	Fino al 75%
Dimensioni	163 × 163 × 36 mm
Peso	362 g

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 si applica alla 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!

[Testo integrale della garanzia](#)

[Contratto con l'utente finale](#)



Serve aiuto?

In questa sezione troverai dei manuali dettagliati e dei video didattici su tutte le funzioni di Ajax. Nel caso tu abbia bisogno dell'aiuto di un tecnico specializzato, siamo disponibili per te H24.

[Invia una richiesta](#)