Hub 2 manuale utente

Aggiornato il March 24, 2021

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. Utilizzato negli spazi interni.

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.

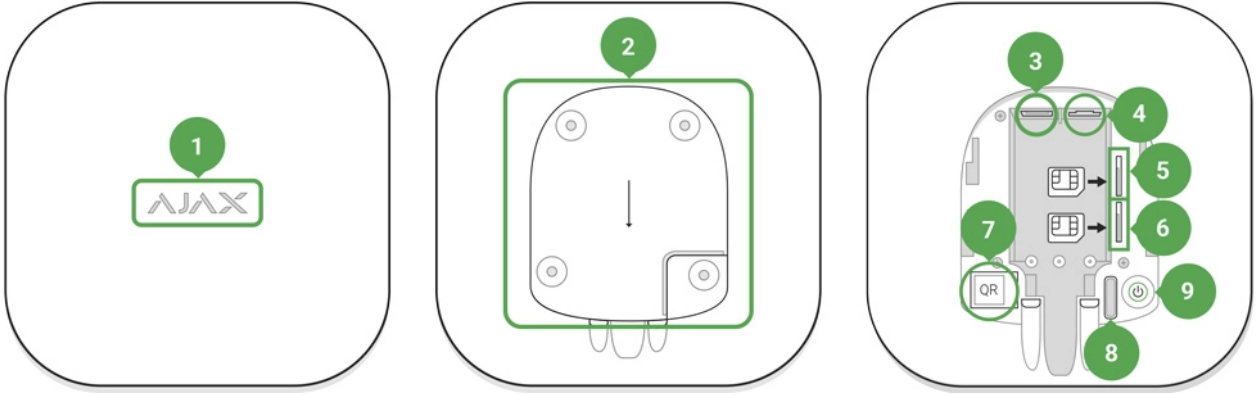
Gli utenti possono gestire il sistema di sicurezza e rispondere tempestivamente agli allarmi e alle notifiche usando le **app** per iPhone e gli smartphone basati su Android, macOS, e Windows. Il sistema avvisa l'utente in caso di allarmi e altri eventi tramite notifiche push, SMS e chiamate telefoniche.

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 10 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.

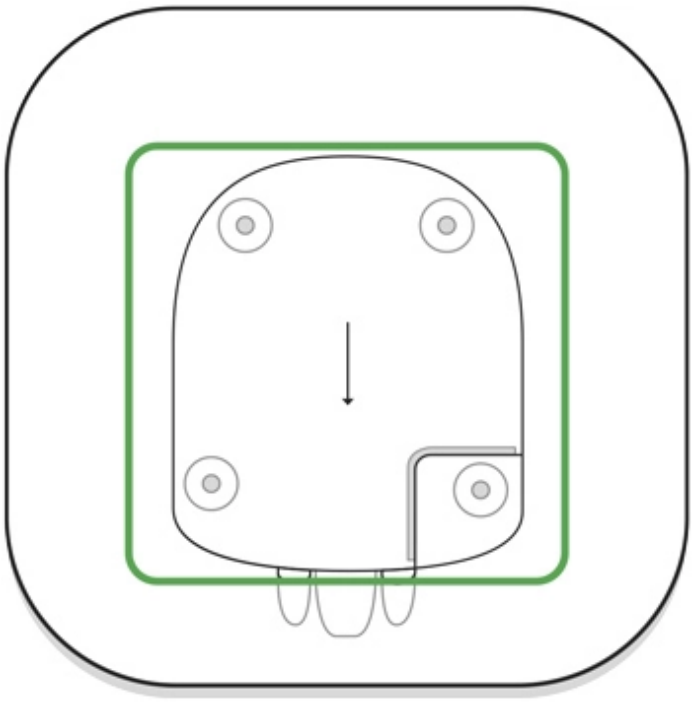
Requisiti di sicurezza

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.

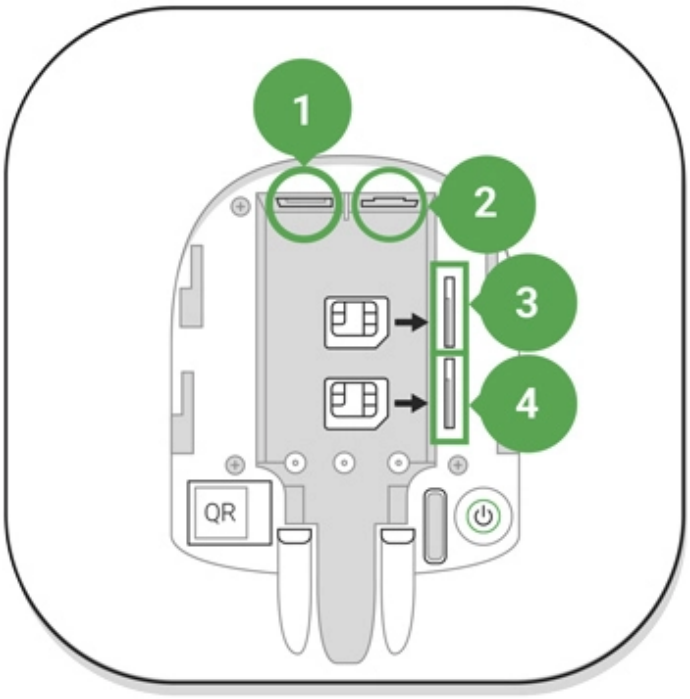
È severamente proibito smontare il dispositivo mentre è connesso a una fonte di alimentazione! Inoltre, non utilizzare il dispositivo se il cavo di alimentazione risulta danneggiato.

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

Stati dell'hub

Icone

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

Icone	Valore
	Connesso a 2G
	La scheda SIM non è installata
	La scheda SIM è difettosa o ha un codice PIN
	Livello di carica della batteria di Hub 2. Visualizzati con incrementi del 5%
	Viene rilevato un malfunzionamento dell'Hub 2. 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 dall'elenco.

Parametro	Significato
Malfunzionamento	Fare clic su  per aprire la lista dei malfunzionamenti dell'Hub 2. Il campo appare solo se viene rilevato un malfunzionamento
Intensità segnale cellulare	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
Livello batteria	Livello di carica della batteria del dispositivi. Visualizzato in percentuale **Come viene visualizzata la carica della batteria nelle app Ajax**

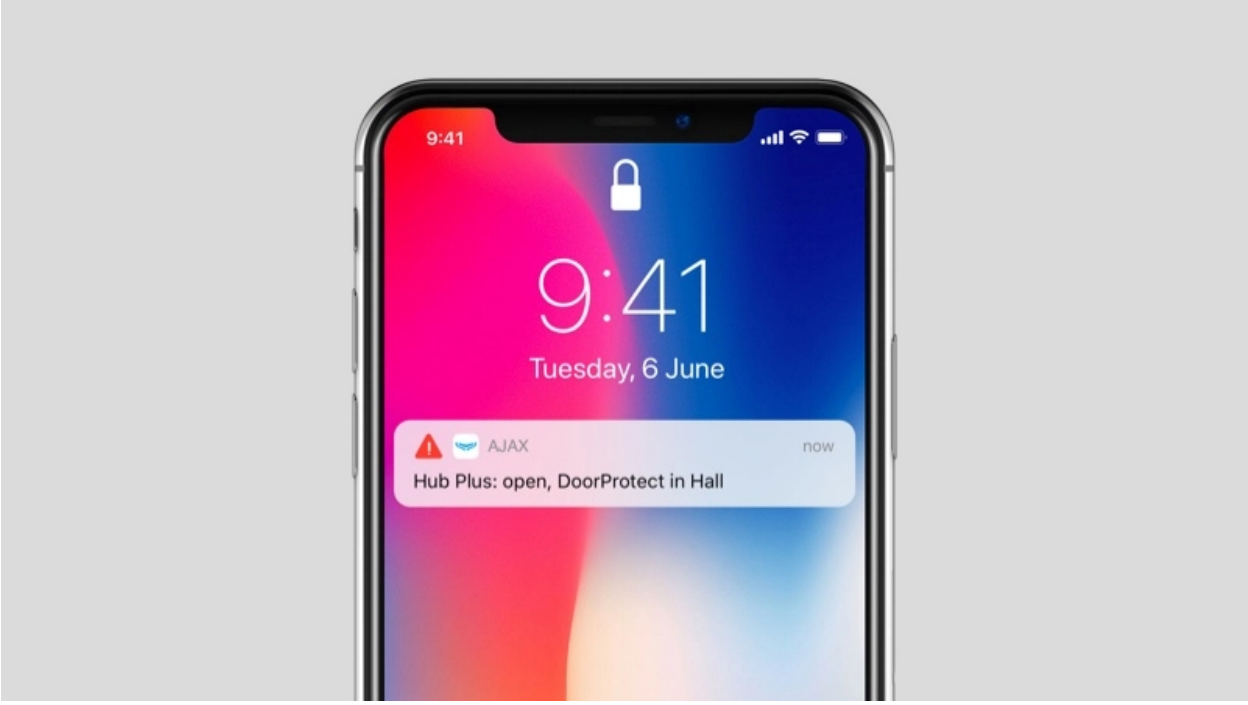
Stato coperchio	Stato del dispositivo anti-manomissione che risponde allo smontaggio dell'hub: • **Chiuso** — il coperchio dell'hub è chiuso • **Aperto** — hub rimosso dal supporto SmartBracket **Cos'è una manomissione?**
Alimentazione esterna	Stato di collegamento all'alimentazione esterna: • **Collegato** — l'hub è collegato all'alimentazione esterna • **Scollegato** — nessuna alimentazione esterna
Connessione	Stato della connessione tra l'hub e Ajax Cloud: • **Online** — l'hub è collegato ad Ajax Cloud • **Offline** — l'hub non è collegato ad Ajax Cloud
Cellulare	Lo stato della connessione dell'hub a Internet mobile: • **Collegato** — l'hub è collegato ad Ajax Cloud tramite Internet mobile • **Scollegato** — l'hub non è collegato ad Ajax Cloud tramite Internet mobile 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 **Scollegato**
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
Ethernet	Stato della connessione Internet dell'hub

	tramite Ethernet. • **Collegato** — l'hub è collegato ad Ajax Cloud tramite Ethernet • **Scollegato** — l'hub non è collegato ad Ajax Cloud tramite Ethernet
Rumore medio (dBm)	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. Il valore accettabile è di -80 dBm o inferiore
Centrale di sorveglianza	Lo stato del collegamento diretto dell'hub alla stazione centrale di monitoraggio dell'organizzazione di sicurezza: • **Collegato** — l'hub è collegato direttamente alla stazione centrale di monitoraggio dell'organizzazione di sicurezza • **Scollegato** — l'hub non è collegato direttamente alla stazione centrale di monitoraggio dell'organizzazione di sicurezza Se questo campo viene visualizzato, l'istituto di vigilanza utilizza una connessione diretta per ricevere gli eventi e gli allarmi del sistema di sicurezza **Cos'è un collegamento diretto?**
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

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

L'hub non è compatibile con i moduli di integrazione uartBridge e ocBridge Plus.

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.

Configurazione e connessione di una telecamera IP al sistema di sicurezza Ajax

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

Le impostazioni possono essere modificate nell’**app Ajax**:

1. Accedere alla scheda **Dispositivi**.
2. Selezionare Hub 2 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

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.

> **OS Malevich 2.6: un nuovo livello di sicurezza**

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:

*Intervallo di ping * (numero di pacchetti non consegnati + 1 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 o più	100 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
- 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

PD 6662 Impostazione guidata

Apre 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 ping del server (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.
- **Aumento ritardo allarme quando hub non è in linea (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*

- **Disattiva gli allarmi quando la connessione al server é interrotta**. 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.

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 → SpaceContol → 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.

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**.

Cancella 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 può inviare allarmi ed eventi alla stazione di monitoraggio centrale tramite **Ethernet** e **EDGE**. 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.
- **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.

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.

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	• Perdita di connessione tra il dispositivo e l'hub • Inibizione • Carica batteria bassa nel dispositivo o nell'hub • Mascheramento • Manomissione dell'involucro del rilevatore	Notifiche push SMS
Allarme	• Intrusione • Incendio • Allagamento	Chiamate Notifiche push SMS

	• L'hub ha perso la connessione con il servizio Ajax Cloud	
Eventi	• Accendi/Spegni **WallSwitch**, **Relay**, **Socket**	Notifiche push SMS
Inserire/disinserire	• Inserire/disinserire locali interi o gruppi • Attivazione della **modalità Notte**	Notifiche push SMS

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.

Il dispositivo è destinato esclusivamente all'installazione negli spazi interni.

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 (DC-09) **Software per CRA con supporto per la foto-verifica degli allarmi**
Alimentatore	110-240 V con la batteria preinstallata 12 V con un alimentatore alternativo **12V PSU** 6 V con un alimentatore alternativo **6V PSU**Consumo energetico — 10 W
Batteria di backup integrata	Li-Ion 2 A·h Fornisce fino a 16 ore di durata della batteria con una scheda SIM
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	• 2 SIM card (GSM 850/900/1800/1900 MHz GPRS) • Ethernet
Istallazione	Interni
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

Supporto tecnico: **support@ajax.systems**