Hub manuale utente

Aggiornato il February 16, 2021

Hub è un dispositivo centrale che fa parte del sistema di sicurezza Ajax. Esso coordina il funzionamento dei dispositivi connessi, interagisce con l'utente e con l'istituto di vigilanza. Utilizzato negli spazi interni.

Per connettersi al server cloud Ajax Cloud, che consente di configurare il sistema, controllarlo da qualunque parte del mondo, trasmettere notifiche di eventi e aggiornamenti del software, Hub necessita di avere accesso a internet. I dati personali e i registri dettagliati delle operazioni di sistema sono archiviati con protezione multi-livello. Lo scambio di informazioni con Hub avviene tramite un canale criptato 24 ore su 24.

Per comunicare con Ajax Cloud, il sistema usa una connessione via cavo Ethernet e la rete GSM di un operatore mobile.

Se possibile, si prega di utilizzare entrambi i canali di connessione Internet. Ciò assicura una comunicazione più affidabile tra Hub e Ajax Cloud, evitando problemi causati da interruzioni del funzionamento di uno dei fornitori dei servizi di comunicazione.

Hub si controlla tramite **applicazione** per smartphone con sistema operativo iOS e Android. Le applicazioni per dispositivi mobili consentono di rispondere immediatamente a eventuali notifiche del sistema di sicurezza.

Per scaricare l'applicazione sul proprio smartphone, fare click su questo link:

Android

iOS

Su Hub, è possibile impostare gli eventi per i quali l'utente riceve una notifica e le modalità di notifica. Basta scegliere la modalità più conveniente: notifiche push, messaggi SMS, o chiamate telefoniche. Se il sistema Ajax passa in gestione a un istituto di vigilanza per la manutenzione, i segnali d'allarme vengono inviati direttamente all'istituto di vigilanza, bypassando il server.

Compra il pannello di sicurezza intelligente Hub

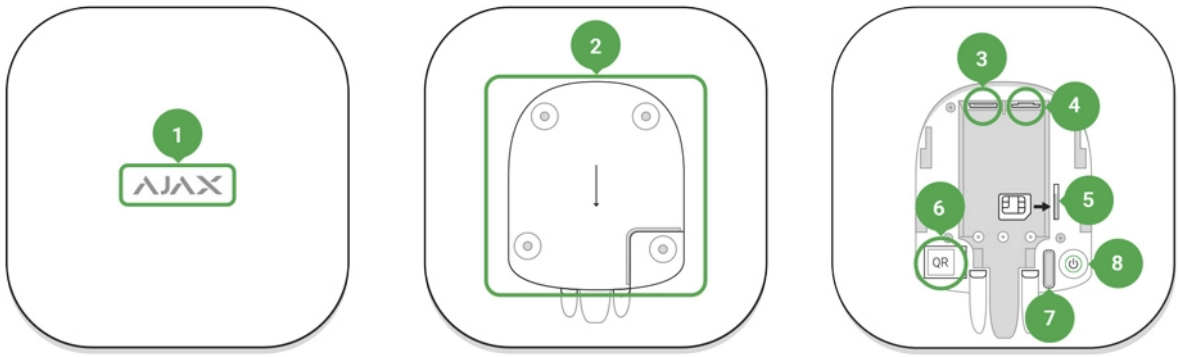
È possibile connettere fino a 100 dispositivi Ajax ad Hub. La comunicazione tra i dispositivi avviene tramite il protocollo protetto **Jeweller**, con raggio di copertura fino a 2 km in campo aperto.

Lista dei dispositivi Ajax

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

Prese e indicazioni di funzionamento di Hub



1. Logotipo con LED che fornisce informazioni sullo stato dell’Hub
2. Pannello di montaggio SmartBracket (la parte perforata è necessaria per l’attivazione del tamper in caso di qualsiasi tentativo di strappare l’Hub dalla superficie)
3. Presa per connettere un cavo di alimentazione
4. Presa per connettere un cavo Ethernet
5. Alloggiamento per installare la scheda di un operatore di servizi di telefonia (Micro SIM)
6. Codice QR
7. Pulsante tamper
8. Pulsante “On”

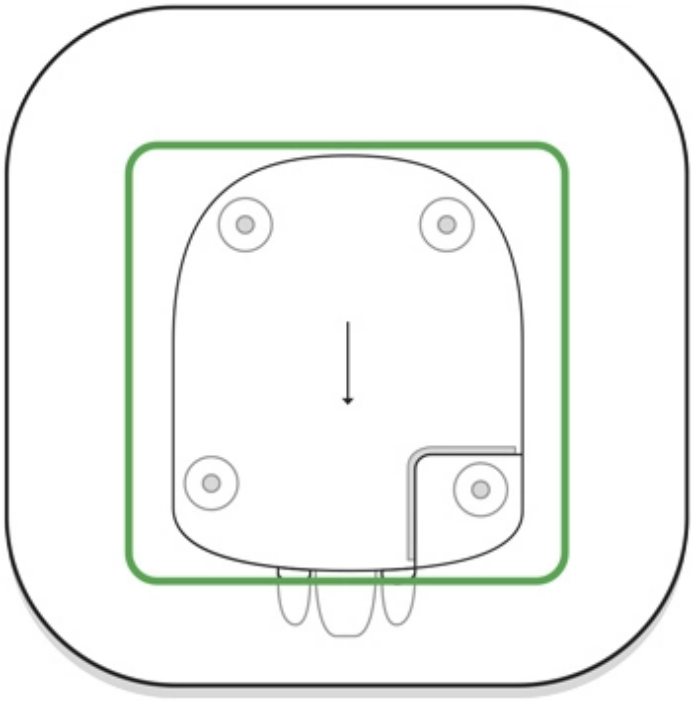
Indicatore LED sull’hub

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.

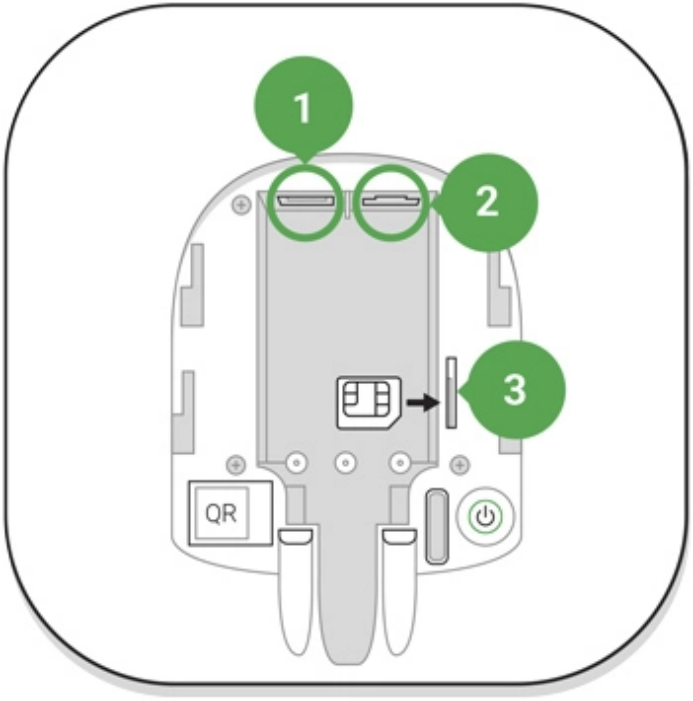
Connessione di Hub alla rete

1. Aprire il rivestimento di Hub spostandolo con forza verso il basso.



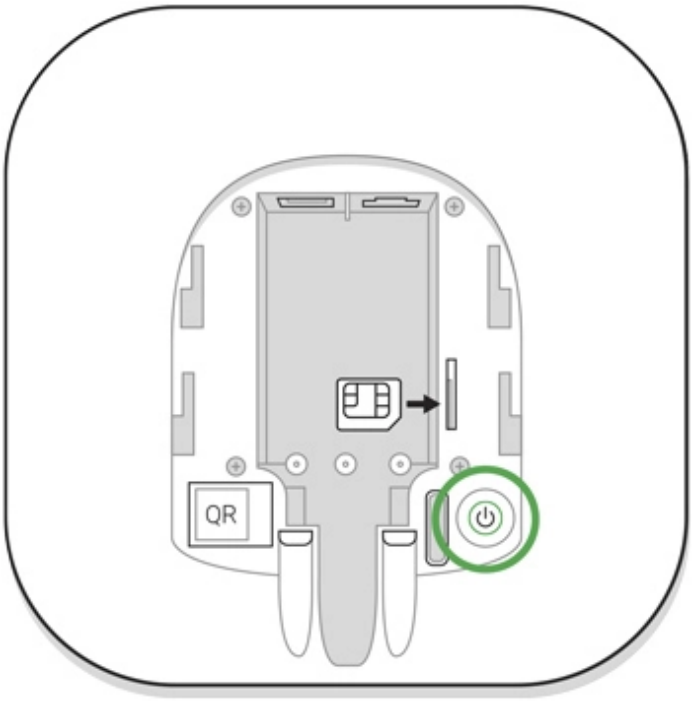
Fare attenzione a non danneggiare il tamper che protegge Hub dai tentativi di attacco!

2. Connettere i cavi di alimentazione e i cavi Ethernet alle rispettive prese.



1 — Porta di alimentazione
2 — Porta Ethernet
3 — Alloggiamenti schede SIM

3. Tenere premuto il pulsante “on” per 2 secondi fino a quando non si accende il logo. Hub impiega circa 2 minuti per identificare i canali di comunicazione disponibili.



Se il logo si illumina di verde acceso o di bianco, significa che Hub si è connesso al server

Se la connessione Ethernet non avviene automaticamente, disabilitare il server proxy e il filtraggio tramite indirizzi MAC e attivare il DHCP sulle impostazioni del router. Hub riceverà un indirizzo IP. Durante il processo di configurazione di Hub sull'**applicazione mobile**, sarà possibile preimpostare un indirizzo IP statico.

Per connettersi alla rete GSM, è necessaria la scheda di un operatore mobile in formato Micro-SIM, con richiesta di codice PIN disabilitata (è possibile disabilitare tale richiesta usando il proprio telefono cellulare) e credito sufficiente per utilizzare la rete GPRS, i servizi di SMS e per effettuare chiamate.

In alcune aree, Hub viene venduto con una scheda SIM in dotazione.

Se Hub non si connette ad Ajax Cloud tramite la rete GSM, utilizzare la connessione Ethernet per configurare i parametri della rete sull'applicazione mobile. Per impostare correttamente il punto d'accesso, il nome utente e la password si prega di contattare il servizio assistenza dell'operatore.

Account Ajax

Il sistema di sicurezza Ajax si imposta tramite l'applicazione a cui è connesso l'account dell'amministratore. L'account e le informazioni relative agli Hub aggiunti vengono salvate sul server cloud Ajax Cloud in forma criptata.

I parametri utente del sistema di sicurezza Ajax e dei dispositivi connessi sono archiviati localmente su Hub e sono strettamente connessi al dispositivo. Se cambia l'amministratore di Hub non si verifica alcun malfunzionamento delle impostazioni dei dispositivi ad esso connessi.

Un numero di telefono può essere usato per creare un solo account Ajax

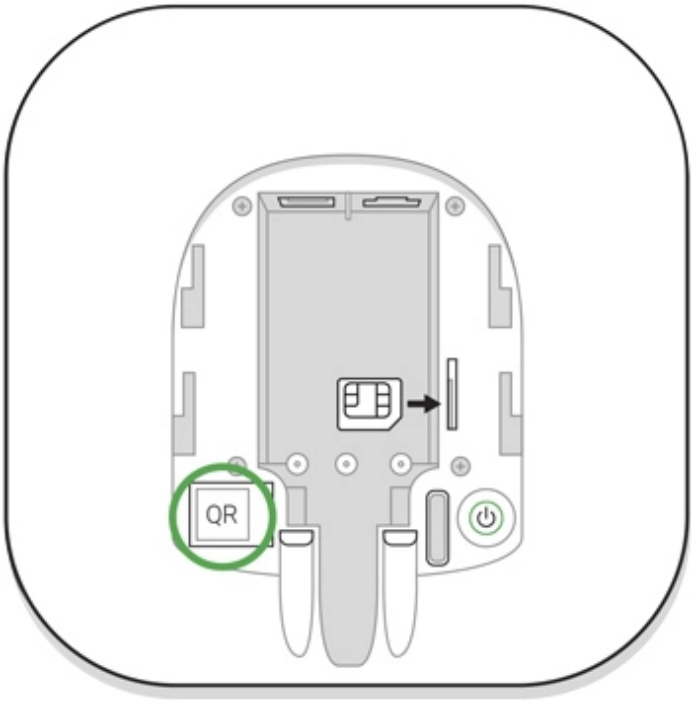
Per creare un account sul sistema Ajax tramite applicazione mobile, seguire la procedura guidata. La procedura richiede di confermare la propria email e il proprio numero di telefono cellulare.

L’account permette di unire diversi ruoli — amministratore di un Hub, utente di un altro Hub.

Aggiungere Hub all’applicazione del sistema di sicurezza Ajax

È necessario permettere all’applicazione di accedere a tutte le funzioni di sistema (in particolare, per visualizzare le notifiche)! È una conditio sine qua non per controllare il sistema di sicurezza Ajax da uno smartphone.

1. Accedere al proprio account.
2. Accedere al menu “**Aggiungere Hub**” e selezionare il metodo desiderato — manuale o procedura guidata.
3. Durante la fase di registrazione, specificare il nome di Hub e scansionare il codice QR che si trova sotto alla custodia (o inserire manualmente una chiave di registrazione).



4. Attendere fino all’avvenuta registrazione di Hub. Un nuovo dispositivo comparirà sul desktop dell’applicazione.

Installazione di Hub

Prima di procedere all’installazione di Hub, assicurarsi di aver selezionato il luogo di

installazione ideale: la ricezione della scheda SIM è regolare, la comunicazione radio di tutti i dispositivi è stata testata e Hub è nascosto alla vista.

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

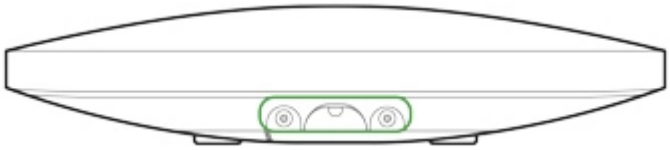
Hub deve essere fissato stabilmente alla superficie (in verticale o in orizzontale). Si sconsiglia vivamente di usare del nastro biadesivo in quanto non garantisce il fissaggio stabile del dispositivo e ne facilita lo smontaggio.

Non posizionare 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 scarso segnale GSM;
- 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.

Installare l'hub:

1. Fissare il rivestimento di Hub alla superficie usando le viti in dotazione. Se si usano altri metodi di fissaggio, si prega di assicurarsi che non danneggino o deformino il rivestimento di Hub.
2. Posizionare Hub all'interno del rivestimento e fissarlo 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.

Fissando il rivestimento di Hub con delle viti si evitano spostamenti accidentali e si riduce il rischio di furto spontaneo del dispositivo.

Se Hub è fissato in maniera stabile, il tamper anti-manomissione si attiva quando la custodia del dispositivo viene rimossa dalla superficie e si riceverà una notifica.

Stanze sull’applicazione del sistema di sicurezza Ajax

Le stanze consentono di unire i dispositivi connessi. L’applicazione permette di creare fino a 50 stanze, con un dispositivo per stanza.

Se non si crea una stanza, non è possibile aggiungere dispositivi all’applicazione del sistema di sicurezza Ajax!

Creare e impostare una stanza

È possibile creare una stanza tramite applicazione mobile, tramite il menu “**Aggiungi stanza**“.

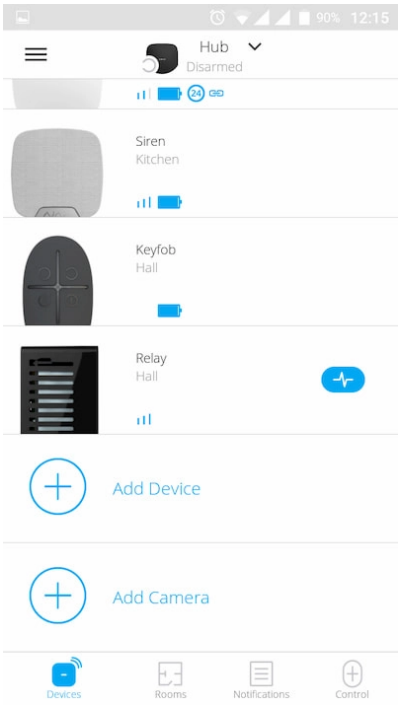
Assegnare un nome alla stanza e, se si desidera, allegare (o scattare) una foto per identificare più facilmente la stanza all’interno della lista.

Accedere al menu di impostazioni della stanza premendo l’icona con la ruota dentata ⚙.

Per eliminare una stanza, spostare tutti i dispositivi assegnati alla stanza che si vuole eliminare in altre stanze attraverso il menu impostazioni del dispositivo. Eliminando la stanza, si annullano tutte le relative impostazioni.

Connettere dispositivi a Hub

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



Quando si registra per la prima volta Hub sull'applicazione mobile, viene richiesto di aggiungere dispositivi per inserire una stanza. È possibile saltare questo passaggio e ritornarvi in un secondo momento.

Il dispositivo può essere aggiunto solo se il sistema è disinserito!

1. Aprire una stanza sull'applicazione mobile e selezionare l'opzione "**Aggiungere dispositivo**".
2. Dare un nome personalizzato al dispositivo, scansionare il **codice QR** (o inserire manualmente il codice identificativo), selezionare la stanza dove è localizzato e andare al passaggio successivo.
3. Quando l'applicazione inizia la ricerca dispositivi e lancia il conto alla rovescia, accendere il dispositivo. Il LED lampeggia una volta. Per avviare il processo di rilevamento e interfacciamento, il dispositivo deve essere localizzato all'interno dell'area di copertura della rete wireless dell'hub (in un unico locale protetto).

La richiesta di connessione all'hub viene trasmessa per un breve periodo di tempo appena si accede il dispositivo

Se il primo tentativo di connessione a Hub fallisce, spegnere il dispositivo per 5 secondi e ripetere il tentativo di connessione.

È possibile collegare all'hub Ajax fino a 10 telecamere o NVR con supporto del protocollo RTSP.

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

Stati dell'hub

Icone

Le icone mostrano alcuni degli stati di Hub. 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. Visualizzati con incrementi del 5%
	Viene rilevato un malfunzionamento dell'Hub. 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 dall'elenco.

Parametro	Significato
Malfunzionamento	Fare clic su ⓘ per aprire la lista dei malfunzionamenti dell'Hub. 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**
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)	Il livello di potenza sonora sulle frequenze Jeweller nel luogo dove è installato l’hub. Il valore accettabile è di -80dbm o meno
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

Configurare Hub

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

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

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 secondi	39 dispositivi
24 secondi	79 dispositivi
36 secondi 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*

- **Disattivare gli allarmi quando la connessione al server è 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 Plus 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.

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.

Annullare le impostazioni di Hub

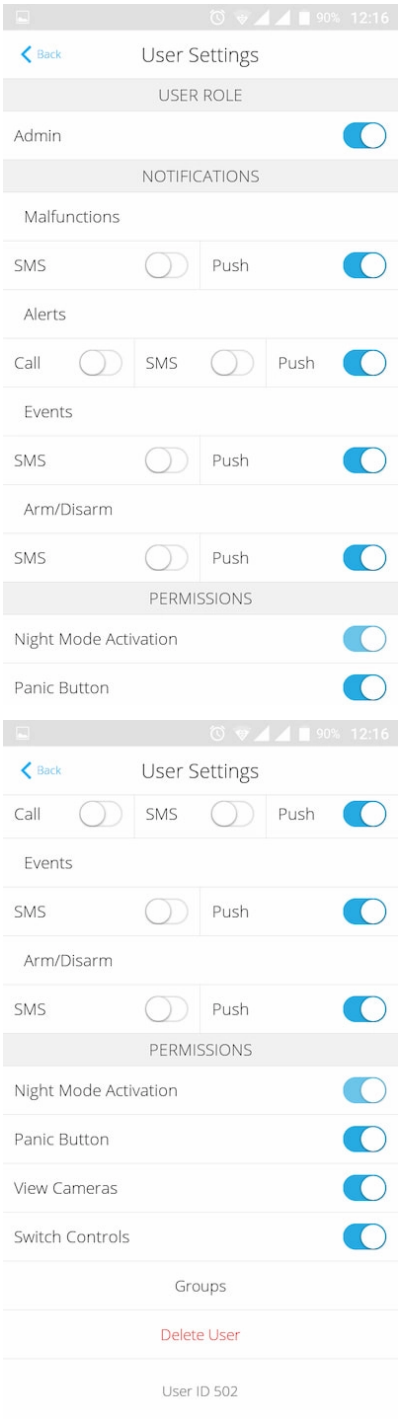
Per tornare alle impostazioni predefinite di Hub, accendere il dispositivo e tenere premuto il pulsante "on" per 30 secondi (il logo inizia a lampeggiare con luce rossa).

In questo modo, le impostazioni di tutti i rilevatori connessi, delle stanze e le impostazioni utenti verranno annullate. I profili utenti rimarranno connessi al sistema.

Utenti del sistema di sicurezza

Dopo aver aggiunto Hub al proprio account, si diventa amministratori del dispositivo. Un Hub può avere fino a 50 utenti/amministratori. Gli amministratori possono aggiungere utenti al sistema di sicurezza e determinare i loro diritti.

Notifiche di eventi e allarmi



Hub invia notifiche all'utente usando tre metodi: notifiche push su dispositivo mobile, SMS e chiamate telefoniche.

Le notifiche possono essere configurate dal menu "**Utenti**":

Tipi di eventi	Per cosa si usano	Tipi di notifiche
Inserire/disinserire	Si ricevono notifiche dopo aver inserito/disinserito il sistema	• SMS • Notifiche push
Allarme	Notifiche di intrusione, incendio, allagamento	• SMS • Notifiche push • Chiamata
Eventi	Notifiche degli eventi relativi al dispositivo WallSwitch, Relay	• SMS • Notifiche push
Guasti	Notifiche relative alla perdita della comunicazione, inibizione, batteria quasi scarica o apertura della custodia del rilevatore	• SMS • Notifiche push

- **Notifiche push** — inviate dal server Ajax Cloud all'applicazione del sistema di sicurezza Ajax, se la connessione internet è disponibile.
- **SMS** — inviati al numero di telefono indicato dall'utente durante il processo di registrazione dell'account di Ajax.
- In caso di **chiamate telefoniche**, l'hub chiama il numero di telefono specificato tra i dati dell'account dell'app di Ajax.

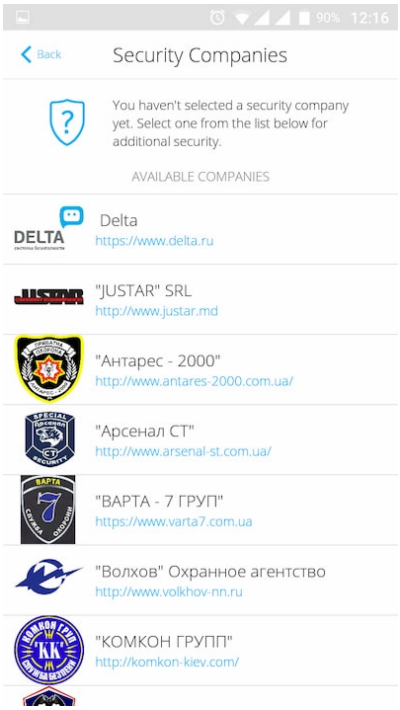
Le chiamate telefoniche vengono effettuate solo in caso di allarme, per attirare l'attenzione e ridurre il rischio di perdersi un allarme critico. Si consiglia di abilitare questo tipo di notifica. L'hub chiama uno dopo l'altro tutti gli utenti che hanno abilitato questo tipo di notifica, nell'ordine specificato nelle Impostazioni utenti. Se si verifica un secondo allarme, l'hub effettua nuovamente una chiamata, non più di una volta ogni 2 minuti.

La chiamata si disconnette automaticamente non appena si risponde al telefono. Si

consiglia di salvare il numero di telefono associato alla scheda SIM dell'hub nella propria lista di contatti.

Le impostazioni delle notifiche possono essere modificate solo per gli utenti registrati.

Collegare il sistema Ajax a un istituto di vigilanza



La lista delle organizzazioni per connettere il sistema Ajax a una centrale ricezione allarmi è disponibile sul menu "**Istituti di vigilanza**" nelle impostazioni di Hub:

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

La connessione alla centrale ricezione allarmi (CRA) si effettua tramite i protocolli Contact ID o SIA.

Manutenzione del sistema Ajax

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.

Per pulire l'hub, evitare l'uso di sostanze contenenti alcol, acetone, benzina o altri solventi attivi.

Come sostituire la batteria del hub

Set completo di Hub

1. Ajax Hub
2. Panello per il montaggio SmartBracket
3. Cavo di alimentazione
4. Cavo Ethernet
5. Kit di installazione
6. SIM card *
7. Manuale utente

* Disponibile solo in alcuni paesi.

Requisiti di sicurezza

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

Specifiche tecniche

Numero massimo di dispositivi connessi	100
Numero massimo di gruppi	9
Numero massimo di utenti dell'hub	50

Videosorveglianza	Fino a 10 telecamere o DVR
Numero massimo di stanze	50
Numero massimo di scenari	5
ReX (ripetitori)	1
Alimentazione	110 – 240 V AC, 50/60 Hz
Batteria	Li-Ion 2 A·h (fino a 15 ore di funzionamento autonomo*)
Consumo energetico	10 W
Tamper anti-sabotaggio	Si
Banda di frequenza	868.0 – 868.6 MHz o 868.7 – 869.2 MHz, in base al luogo di acquisto
Potenza irradiata equivalente	8.20 dBm / 6.60 mW (limite 25 mW)
Modulazione del segnale radio	GFSK
Raggio del segnale radio	Fino a 2.000 m (in campo aperto)
Canali di comunicazione	GSM (850/900/1800/1900 MHz), Ethernet
Istallazione	Interni
Temperature di funzionamento	Da -10°C a +40°C
Umidità di funzionamento	Fino al 75%
Dimensioni totali	163 × 163 × 36 mm
Peso	350 g
Certificazione	Grado di sicurezza 2, classe ambientale II SP2 (GSM-SMS), SP5 (LAN) DP3 in conformità ai requisiti degli standard EN 50131-1, EN 50131-3, EN 50136-2, EN 50131-10, EN 50136-1, EN 50131-6, EN 50131-5-3

* in caso di connessione Ethernet inattiva

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**