

Hub Lietotāja Instrukcija



Hub (Centrāle) ir centrālā Ajax drošības sistēmas ierīce, kura koordinē savienotās ierīces un mijiedarbojas ar lietotāju un apsardzes uzņēmumu. Paredzēts izmantošanai tikai iekštelpās.

Centrālei ir nepieciešama piekļuve internetam, lai sazinātos ar Ajax Cloud mākoņserveri - lai konfigurētu un kontrolētu no jebkuras vietas pasaulē, pārsūtītu paziņojumus par notikumiem un atjauninātu programmatūru. Personas datu un sistēmas darbības žurnāli tiek glabāti daudzlīmeņu aizsardzībā, un informācijas apmaiņa ar centrmezglu tiek veikta 24 stundas, izmantojot šifrētu kanālu.

Sazinoties ar Ajax Cloud, sistēma var izmantot Ethernet savienojumu un GSM tīklu.

Centrmezglu var kontrolēt, izmantojot iOS, Android, macOS vai Windows lietotni. Lietotne ļauj ātri reaģēt uz visiem drošības sistēmas paziņojumiem.

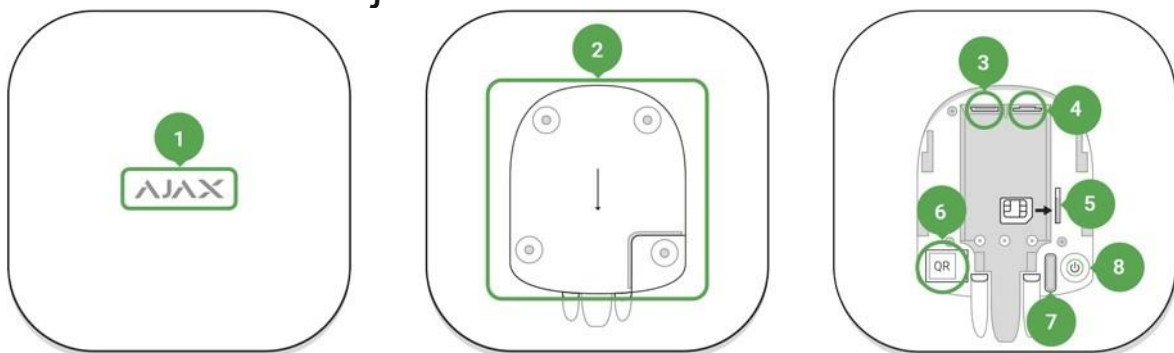
Centrāles iestatījumos lietotājs var pielāgot paziņojumus. Izvēlieties to, kas jums ērtāk: informatīvie paziņojumi, īsziņas vai zvani. Ja Ajax sistēma ir savienota ar centrālo uzraudzības staciju, trauksmes signāls tiks nosūtīts tieši

tai, apejot Ajax Cloud.

Centrālei var pievienot līdz 100 Ajax ierīcēm. Aizsargātais Jeweller radio protokols nodrošina drošu komunikāciju starp ierīcēm redzes līnijā līdz 2 km attālumā.

Izmantojiet scenārijus, lai automatizētu drošības sistēmu un samazinātu rutīnas darbību skaitu. Pielāgojiet apsardzes grafiku, automatizācijas iekārtu (Relejs, Sienas slēdzis vai Rozete) darbības, kuras reaģē uz trauksmi, pogas nospiešanu vai grafiku. Scenāriju var izveidot attālināti lietotnē Ajax.

Rozetes un indikācija



1. LED logo - sistēmas statusa indikācija
2. SmartBracket kronšteina stiprināšanas panelis (perforēta daļa ir nepieciešama, lai aktivizētu tamperu pie centrāles demontāžas mēģinājumb)
3. Kontaktligzda priekš barošanas kabeļa
4. Kontaktligzda Ethernet kabelis
5. micro SIM kartrs slots
6. QR kods
7. Tampera poga
8. Iesl./Izsl. poga

LED Indikācija



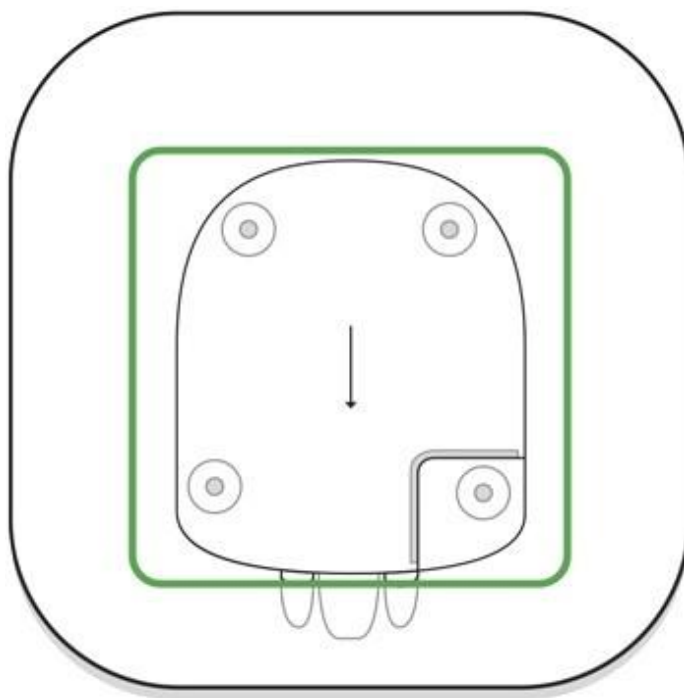
LED logo var iedegties sarkanā, baltā vai zaļā krāsā, atkarībā no iekārtas statusa.



Notikums	Gaismas indikators
Ethernet un vismaz viena SIM karte ir pievienota	Balts
Pievienots tikai viens komunikācijas kanāls	Zaļš
Centrāle nav pievienota pie interneta vai nav savienojuma ar Ajax Cloud	Sarkans
Nav barošanas	Iedegas uz 3 minūtēm, tad mirgo katras 10 sekundes. Indikators krāsa atkarīga no pievienoto komunikācijas kanālu skaita.

Pievienošana pie Tīkla

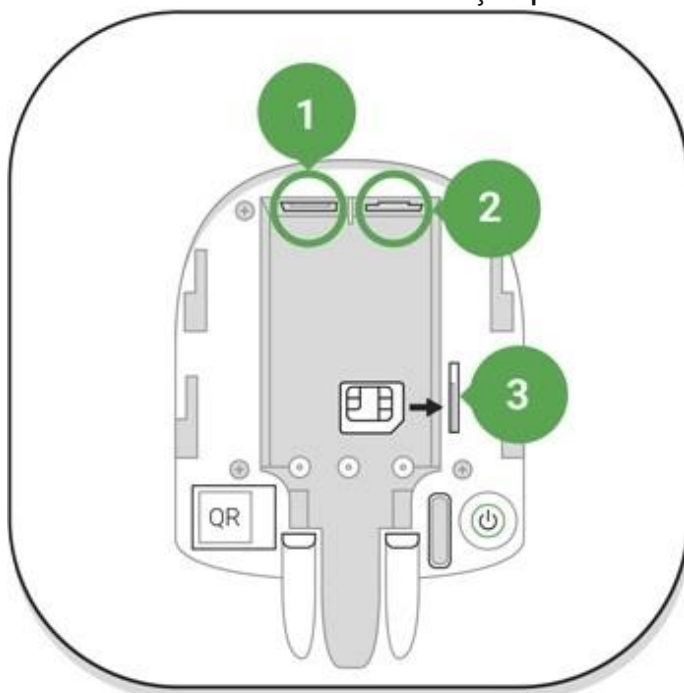
1. Atveriet centrāles vāku, pabīdot uz leju, pielietojot spēku.



Esiet uzmanīgi un nesabojājiet tamperu!

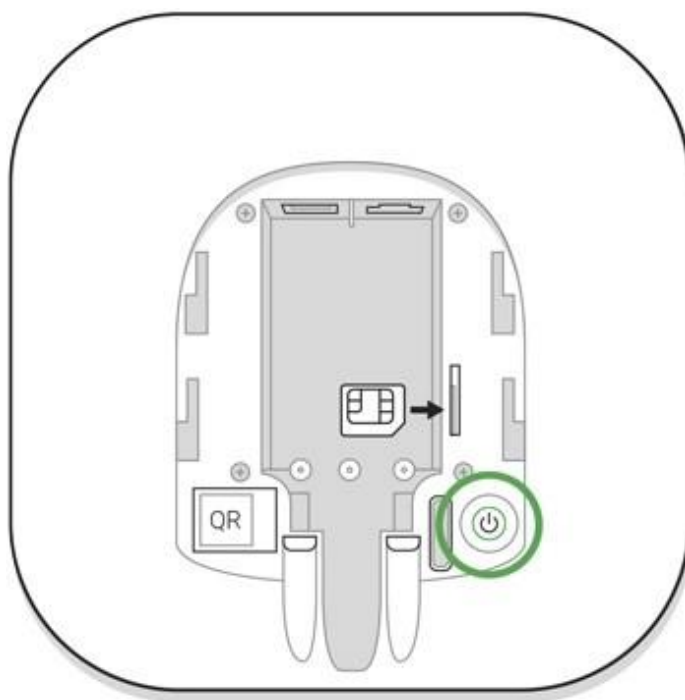


2. Pieslēdziet barošanas bloku un Ethernet kabeļus pie rozetēm.



- 1 – Barošanas ligzda
- 2 – Ethernet lidzga
- 3 – SIM kartes slots

3. Nospiediet un turiet nospiestu barošanas pogu 2 sekundes kamēr logo iedegsies. Centrālei nepieciešamas apmēram 2 minūtes, lai identificētu pieejamos komunikācijas kanālus.



Zaļā vai baltā indikatora krāsa norāda, ka centrāle ir pievienota pie Ajax Cloud.

Ja Ethernet savienojums neparādas automātiski, atslēdziet proxy, filtrēšanu pēc MAC adreses un aktivējiet DHCP iestatījumus rūtera iestatījumos: centrāle saņems IP adresi. Pie nākamās uzstādīšanas mobīlajā lietotnē, Jums būs iespēja uzstādīt IP adresi.

Lai pievienotu centrāli pie GSM tīkla, Jums nepieciešama-SIM karte ar atslēgtu PIN koda pieprasījumu (jūs varat atslēgt to, izmantojot mobīlo tālruni) un pie pietiekamas bilances kontā varat maksāt par GPRS, SMS pakalpojumiem uz zvaniem.

Ja centrāli nevar pievienot pie Ajax Cloud caur GSM, izmantojiet Ethernet, lai uzstādītu tīkla parametrus lietotnē. Korektiem piekļuves punkta, lietotājvārda un paroles iestatījumiem, sazinieties ar operatora atbalsta dienesta.

Ajax Lietotājkonts

Lietotājs ar administratora tiesībām var konfigurēt Ajax sistēmu lietotnē. The administrator account with the information about the added hubs is encrypted and placed on Ajax Cloud.



Visi Ajax apsardzes sistēmas parametri un pievienotas ierīces tiek glabātas lokāli centrālē. Šie parametri ir nesaraujami saistīti ar centrmezglu: centrmezgla administratora maiņa neietekmē pievienoto ierīču iestatījumus.



Vienu tālruņa numuru var pievienot tikai vienam Ajax lietotājkontam.

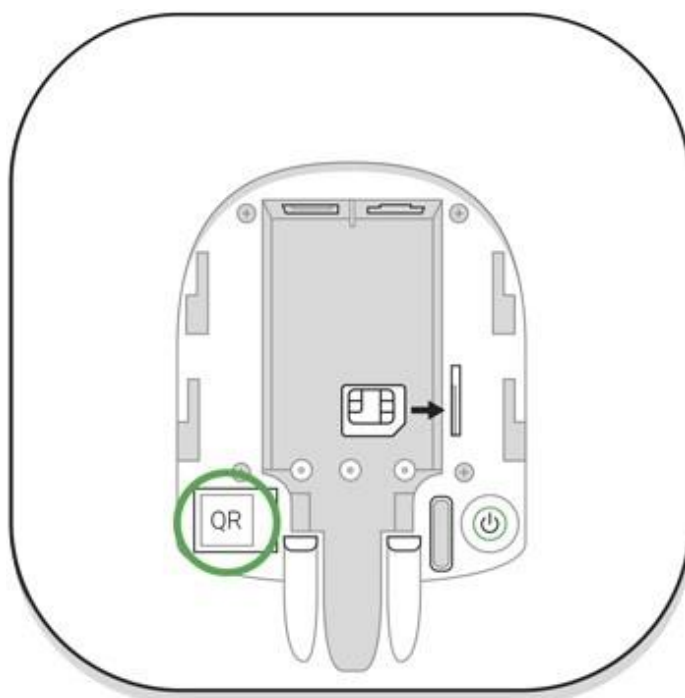
Izveidojiet Ajax lietotnē, sekojot instrukcijām. Jāapstiprina e-pasta adrese un tālruņa numurs.

Ajax konts ļauj apvienot lomas: jūs varat būt viena centrmezgla administrators, kā arī cita centrmezgla lietotājs.

Centrāles pievienošana Ajax lietotnei.

Piekļuves piešķiršana visām sistēmas funkcijām (jo īpaši, lai parādītu paziņojumus) ir obligāts nosacījums, lai kontrolētu Ajax drošības sistēmu, izmantojot viedtālruni.

1. Ielogojieties savā lietotājkontā.
2. Atveriet Centrāles pievienošanas izvēlni uz izvēlieties reģistrācijas veidu: manuāli vai soli pa solim.
3. Reģistrācijas posmā ierakstiet centrāles nosaukumu un skenējiet QR kodu, kas atrodas zem vāka (vai manuāli ievadiet reģistrācijas atslēgu).



4. Sagaidiet, kamēr centrāle tiks pierēģistrēta.

Uzstādīšana



Pirms centrmezgla uzstādīšanas pārliedzinieties, vai esat izvēlējies optimālo atrašanās vietu: SIM karte parāda konsekventu uztveršanu, visām ierīcēm ir pārbaudīts radio savienojums un centrmezgls ir paslēpts no tieša skata.

Centrālei jābūt cieši piestiprinātai pie virsmas (vertikāli vai horizontāli). Mēs nerekomendējam izmantot divpusējo līmlenti, jo tas negarantē drošu stiprinājumu un vienkāršo iekārtas izņemšanas iespēju.

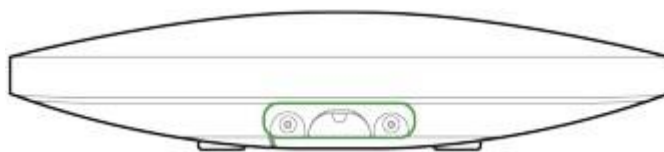
Neizvietojiet centrāli:

- Ārtelpās;
- metāla priekšmetu tuvumā vai iekšpusē, kas izraisa radio signāla vājināšanu un aizsegšanu;
- vietās ar vāju GSM signālu;
- tuvu radio traucējumu avotiem: mazāk nekā 1 metrs no maršrutētāja un strāvas kabeļiem;
- telpās, kur temperatūra un mitrums pārsniedz pieļaujamās robežas.

Centrāles uzstādīšana:



1. Nostipriniet centrāles vāku uz virsmas, izmantojot komplektā esošās skrūves. Izmantojot citus fiksējošos piederumus, pārliecinieties, ka tie nesabojā un nedeformē centrāles vāku.
2. Uzlieciet centrāli uz vāka un nostipriniet to ar komplektā iekļautajām skrūvēm.



Neapgrieziet centrāli, pievienojot to vertikāli (piemēram, pie sienas).
Pie pareizās uzstādīšanas, Ajax logotipu var nolasīt horizontāli.



Centrāles piestiprināšana pie vāka ar skrūvēm novērš nejaušu centrāles nobīdīšanos un samazina ierīces zādzības risku.

Ja centrāle ir pilnībā fiksēta, mēģinājums to noraut izraisa traucējumu, un sistēma nosūta paziņojumu.



Istabas Ajax lietotnē

Virtuālas istabas izmantotas, lai grupētu, pievienotas iekārtas. Lietotājs var izveidot līdz 50 istabām, izvietojot katru iekārtu tikai vienā istabā.



Ja neizveidosiet istabu, nevarēsiet pievienot iekārtas Ajax lietotnē!

Istabas izveidošana un konfigurācija

Istabu veido, izmantojot **Add Room** izvēlni.

Izveidojiet nosaukumu istabai un pēc izvēles, piesaistiet vai uztaisiet fotogrāfiju: tas palīdz atrast nepieciešamo istabu ātrāk.

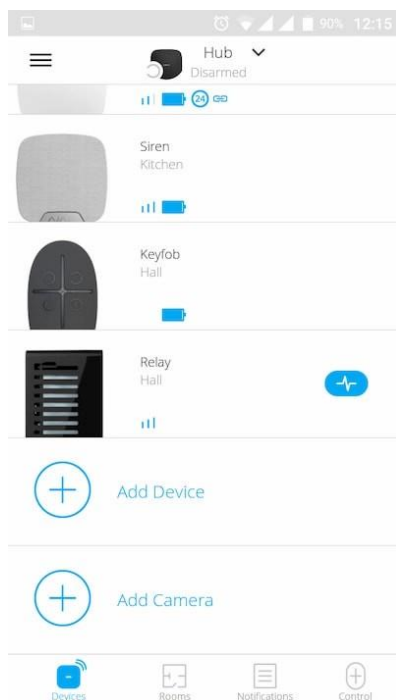
Nospiežot pogu  atvēršies iestatījumu izvēlne.

Lai izdzēstu istabu, pārvietojiet visas iekārtas uz citām istabām, izmantojot iekārtas iestatījumu izvēlni. Izdzēšot istabu, tiks izdzēsti arī visi tās iestatījumi.

Iekārtu pieslēgšana



Centrāle neatbalsta [uartBridge](#) un [ocBridge Plus](#) integrācijas moduļus.



Pirmās centrāles reģistrācijas laikā lietotnē jums tiks lūgts pievienot ierīces telpas apsargāšanai. Tomēr jūs varat atteikties un atgriezties pie šī soļa vēlāk.



Lietotājs ierīci var pievienot tikai tad, kad drošības sistēma ir izslēgta!



1. Lietotnē atveriet istabu un atlasiet opciju **Pievienot ierīci**.
2. Nosauciet ierīci, noskenējiet **QR kodu** (vai ievadiet ID manuāli), izvēlieties istabu un ejiet uz nākamo soli.
3. Kad lietotne sāk meklēt un sāk atpakaļskaitīšanu, ieslēdziet ierīci: tās gaismas diode mirgos vienreiz. Lai notiktu noteikšana un savienošana pārī, ierīcei jāatrodas centrāles bezvadu tīkla pārklājuma zonā (pie viena aizsargāta objekta).




Savienojuma pieprasījums tiek pārsūtīts uz īsu brīdi ierīces ieslēgšanas brīdī.








Ja savienojums neizdodas pirmajā mēģinājumā, izslēdziet ierīci uz 5 sekundēm un mēģiniet vēlreiz. Pie centrāles var pieslēgt līdz 10 kamerām vai DVR, kas atbalsta RTSP protokolu.

Kā konfigurēt un savienot IP kameru ar Ajax drošības sistēmu

Centrāles stāvokļi


Ikonas



Ikonas atspoguļo centrāles stāvokļus. Tos var redzēt Ajax lietotnes leriču izvēlnē .

Ikona	Nozīme
	2G savienojums
	SIM karte nav ievietota
	SIM karte ir defektīva vai tai uzstādīts PIN kods
	Hub battery charge level. Displayed in 5% increments
	Hub malfunction is detected. The list is available in hub states list
	The hub is directly connected to the central monitoring station of the security organization
	The hub have lost connection with the central monitoring station of the security organization via direct connection

Stāvokļi



Stāvokļus var atrast [Ajax lietotnē](#):

1. Ejiet uz [Iekārtas cilni](#) .
2. Izvēlieties centrāli no saraksta.

Parametrs	Nozīme
Nepareiza darbība	<p>Uzklīkšķiniet uz  lai atvērtu centrāles nepareizo darbību sarakstu.</p> <p>Lauks parādas tikai ja notiek nepareizā darbība.</p>
Cellular signal strength	<p>Parāda aktīvās SIM kartes mobilā tīkla signāla līmeni. Centrāli ieteicams uzstādīt vietās, kur signāla stiprums ir 2-3 iedalījumi. Ja signāla līmenis ir vājš, centrāle nevarēs iezvanīt vai nosūtīt īsziņu par notikumu vai trauksmi</p>
Baterijas uzlāde	<p>Baterijas līmenis. Norāda procentos.</p> <p>Baterijas uzlāde tiek atspoguļota Ajax lietotnē.</p>
Vāks	<p>Tampera stāvoklis atbild uz centrāles demontāžu:</p> <p style="padding-left: 40px;">Aizvērts - centrāles vāks ir aizvērts.</p> <p style="padding-left: 40px;">Atvērts - centrāle izņemta no SmartBracket turētāja</p>
Ārēja barošana	<div style="display: flex; align-items: center;">  <div> <p>Ārējās barošanas savienojuma stāvoklis:</p> <p style="padding-left: 40px;">Savienots - centrāle ir pieslēgta pie ārējā barošanas bloka</p> <p style="padding-left: 40px;">Atvienots - nav ārējā barošanas bloka</p> </div> </div>
Savienojums	<p>Savienojuma stāvoklis starp centrāli un Ajax Cloud:</p> <p style="padding-left: 40px;">Tiešsaitē - centrāle pievienota pie Ajax Cloud</p> <p style="padding-left: 40px;">Bezsaitē - centrāle nav pieslēgta pie Ajax Cloud</p>
Mobīlais internets	<p>Centrāles savienojuma stāvoklis pie mobila tīkla:</p> <p>Centrāles savienojuma statuss ar mobilo internetu:</p> <p style="padding-left: 40px;">Savienots - centrāle ir savienota ar Ajax Cloud, izmantojot mobilo internetu</p> <p style="padding-left: 40px;">Atvienots - centrāle nav savienota ar Ajax Cloud, izmantojot mobilo internetu</p> <p style="padding-left: 40px;">Ja centrālē kontā ir pietiekami daudz līdzekļu vai ir bonusa SMS / zvani, tas varēs veikt zvanus un nosūtīt īsziņas pat tad, ja šajā laukā tiek parādīts statuss Nav savienots.</p>

Ethernet	<p>Centrāles interneta savienojuma stāvoklis caur Ethernet:</p> <p>Savienots – centrāle pieslēgta pie Ajax Cloud, izmantojot Ethernet</p> <p>Atvienots – centrāle nav pievienota pie Ajax Cloud caur Ethernet</p>
Vidējie trokšņi (dBm)	<p>Trokšņa jaudas līmenis Jeweller frekvencēs centrāles uzstādīšanas vietā.</p> <p>Pieņemamā vērtība ir -80 dBm vai mazāka</p>
Uzraudzības Stacija	<p>Centrāles tiešā savienojuma stāvoklis pie apsardzes uzņēmuma centrālās uzraudzības stacijas:</p> <p>Savienots – centrāle pieslēgta pie apsardzes uzņēmuma centrālās uzraudzības stacijas</p> <p>Atvienots – centrāle nav tieši pieslēgta pie apsardzes uzņēmuma centrālās uzraudzības stacijas</p> <p>Ja šis lauks ir atspoguļots, apsardzes uzņēmums izmanto tiešo savienojumu, lai saņemtu notikumus un apsardzes sistēmas trauksmes.</p>
Centrāles modelis	Centrāles modeļa nosaukums
Aparatūras versija	Aparatūras versija. Nevar atjaunināt.
Programmnodrošinājums	Programmnodrošinājuma versija. Var atjaunināt attālināti.
ID	ID / sērijas numurs. Atrodas arī ierīces kastē, ierīces shēmā un QR kodā zem SmartBracket paneļa

Iestatījumus var mainīt Ajax lietotnē:

1. Ejiet uz **lekārtas cilni** .
2. Izvēlieties centrāli no saraksta.
3. Ejiet uz **iestatījumiem**, noklikšķinot uz ikonas .



Ņemiet vērā, ka pēc iestatījumu maiņas, lai tos saglabātu, noklikšķiniet uz pogas **Atpakaļ**.

Avatar ir pielāgots nosaukuma attēls Ajax drošības sistēmai. Tas tiek parādīts centrāles izvēles izvēlnē un palīdz noteikt nepieciešamo objektu.

Lai mainītu vai iestatītu Avatar, noklikšķiniet uz kameras ikonas un iestatiet vajadzīgo



Centrāles nosaukums. Tiek parādīts SMS un push paziņojuma tekstā. Nosaukumā var būt līdz 12 kirilicas rakstzīmēm vai līdz 24 latīņu rakstzīmēm.

Lai to izmainītu, noklikšķiniet uz zīmuļa ikonas un ievadiet vajadzīgo centrāles nosaukumu.

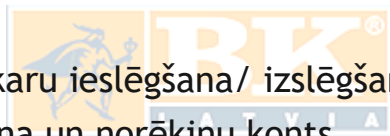
Lietotāji – drošības sistēmas lietotāja iestatījumi: kādas tiesības tiek piešķirtas lietotājiem un kā drošības sistēma viņus informē par notikumiem un traucsmēm.

Lai izmantotu iestatījumus, noklikšķiniet 



Ethernet – iestatījuma vada Interneta savienojumam.

- ◆ Ethernet – ļauj ieslēgt un izslēgt Ethernet centrālē.
- ◆ DHCP / Static – centrāles IP adreses izvēles veids: dinamiska vai statiska
- ◆ IP Adrese – centrāles IP Adrese
- ◆ Apakštīkla maska – Apakštīkla maska, kur centrāle darbojas
- ◆ Maršrutētājs – vārti (gateway), kuru izmanto centrāle
- ◆ DNS – centrāles DNS



Mobilie dati – mobilo sakaru ieslēgšana/ izslēgšana, savienojumu konfigurēšana un norēķinu konts.

Mobilie dati – ieslēdz un izslēdz SIM karti centrālē

Viesabonēšana - ja tā ir aktivizēta, centrālē instalētās SIM kartes var darboties viesabonēšanas laikā

Ignorēt tīkla reģistrācijas kļūdu - kad šis iestatījums ir aktivizēts, centrāle ignorēs kļūdas, mēģinot izveidot savienojumu, izmantojot SIM karti. Aktivizējiet šo opciju, ja SIM karte nevar izveidot savienojumu ar tīklu

Atspējot Ping pirms savienojuma izveidošanas - kad šis iestatījums ir aktivizēts, centrāle ignorē operatora sakaru kļūdas. Aktivizējiet šo opciju, ja SIM karte nevar izveidot savienojumu ar tīklu

SIM karte 1 - parāda instalētās SIM kartes numuru. Noklikšķiniet uz lauka, lai pārietu uz SIM kartes iestatījumiem

SIM kartes iestatījumi

Savienojuma iestatījumi

APN, Lietotājsvārds un Parole – iestatījumi Interneta savienojumam caur SIM karti. Lai uzzinātu sava mobilā operatora iestatījumus, sazinieties ar pakalpojumu sniedzēja atbalsta dienestu.

Mobilā datu izmantošana

Ieejošie – centrāles saņemto datu apjoms. Atspoguļots KB vai MB.

Izejošie – centrāles nosūtīto datu apjoms. Atspoguļots KB vai MB.

Atiestatīt statistiku - atiestata statistiku par ienākošo un izejošo trafiku.

Bilances pārbaude

USSD kods – ievadiet kodu, kas tiek izmantots, lai pārbaudītu atlikumu šajā laikā. Piemēram, * 111 #. Pēc tam noklikšķiniet uz Pārbaudīt atlikumu, lai nosūtītu pieprasījumu. Rezultāts tiks parādīts zem pogas.

Ģeožogs – atgādinājumu konfigurēšana apsardzes sistēmas ieslēgšanai / izslēgšanai šķērsojot noteikto zonu. Lietotāja atrašanās vieta tiek noteikta, izmantojot viedtālruna GPS moduli.

Grupas - grupas režīma konfigurēšana. Tas ļauj:

Pārvaldiet atsevišķu telpu vai detektoru grupu drošības režīmus.
Piemēram, birojs ir apbruņots, kamēr apkopēja strādā virtuvē.

Norobežojiet piekļuvi drošības režīmu kontrolei.
Piemēram, mārketinga nodaļas darbiniekiem nav pieejas juridiskās nodaļas birojam.

Apsardzes grafiks – apbruņošana/atbruņošana pēc grafika

Uztveršanas Zonas testēšana - uztveršanas zonas tests savienotajiem detektoriem. Tests nosaka attālumu, kad tiks uztveta trauksme.

Jeweller – centrāles un detektora ping intervāla konfigurēšana.
Iestatījumi nosaka, cik bieži centrāle sazinās ar ierīcēm un cik ātri tiek konstatēts savienojuma zudums.

Detektora ping intervāls - centrāles savienoto iekārtu poll (aptaujas) frekvence tiek iestatīta diapazonā no 12 līdz 300 s (pēc noklusējuma - 36 s)

Nepiegādāto pakešu skaits, lai noteiktu savienojuma kļūme - nepiegādāto pakešu skaitītājs (pēc noklusējuma 8 paketes).

Laiks pirms trauksmes paziņošanas sakarā ar sakaru zudumu starp centrāli un ierīci tiek aprēķināts pēc šādas formulas:

*Ping intervāls * (nepiegādāto pakešu skaits + 1 korekcijas pakete).*

Īsāks ping intervāls (sekundēs) nozīmē ātrāku notikumu piegādi starp centrāli un pievienotajām ierīcēm; tomēr īss ping intervāls samazina akumulatora darbības laiku. Tajā pašā laikā trauksmes signāli tiek pārraidīti nekavējoties neatkarīgi no ping intervāla.

Mēs neiesakām samazināt ping perioda un intervāla noklusējuma iestatījumus.

Ņemiet vērā, ka intervāls ierobežo maksimālo pievienoto ierīču skaitu:

Intervāls	Savienojuma limits
12 sek.	39 iekārtas
24 sek.	79 iekārtas
36 un vairāk sek.	100 iekārtas

Centrāle atbalsta maksimāli 10 sirēnas!

Service ir centrāles pakalpojumu iestatījumu grupa. Tie ir sadalīti 2 grupās: vispārīgie iestatījumi un papildu iestatījumi.

Galvenie iestatījumi

Laika zona

Laika joslas izvēle, kurā centrāle darbojas. To izmanto scenārijiem pēc grafika. Tāpēc pirms scenāriju izveidošanas iestatiet pareizo laika joslu.



LED Spilgtums

Centrāles logotipa spilgtuma regulēšana. Diapazons no 1 līdz 10. Pēc noklusējuma 10.

Automātiskās OS Malevich programmnodrošinājuma atjaunināšanas iestatīšana.

- **Ja ieslēgts**, programmnodrošinājums tiek automātiski atjaunināts, kad pieejama jauna versija, sistēma nav apbruņota un ir pieslēgta ārējā barošana.
- **Ja izslēgts**, sistēma neatjaunināsies automātiski. Ja jauna versija nav pieejama, lietotne piedāvās atjaunināt OS Malevich.

Centrāles Sistēmas Žurnāli



Žurnāli ir faili, kas satur informāciju par sistēmas darbību. Tie var palīdzēt atrisināt problēmu kļūdu vai kļūmju gadījumā.

Šis iestatījums ļauj izvēlēties centrāles žurnālu pārraides kanālu vai izslēgt to ierakstīšanu:

- ♦ Ethernet
- ♦ Nē - žurnāli ir izslēgti





Mēs neiesakām atspējot žurnālus, jo šī informācija var būt noderīga sistēmas darbības kļūdu gadījumā!

Papildus iestatījumi

Papildus centrāles iestatījumi atkarīgi no lietotnes tipa: standarta vai PRO.

Ajax Security System	Ajax PRO
Servera savienojums Sirēnas iestatījumi Ugunsdrošības detektoru iestatījumi Sistēmas integritātes iestatījumi	PD 6662 Iestatījumi Servera Savienojums Sirēnas Iestatījumi Ugunsdrošības detektoru iestatījumi Sistēmas integritātes pārbaude Trauksmes Apstiprināšana Restoration After Alarm Apbruņošanas/Atbruņošanas Process Iekārtas Auto Deaktivācija

Servera Savienojums

Izvēlne satur komunikācijas iestatījumus starp centrāli un Ajax Cloud:

- Servera Ping Intervāls (sek.) Pingu nosūtīšanas frekvence no centrāles uz Ajax mākoņserveri. Tas ir uzstādīts diapazonā no 10 līdz 300s. Rekomendēta vērtība pēc noklusējuma ir 60s.

- **Savienojuma Kļūdas Trauksmes Aizkāve (sek.)** Tā ir aizkāve, lai samazinātu viltus trauksmju risku, kuras saistītas ar Ajax Cloud servera savienojuma zudumu. Tas ir aktivēts pēc 3 neveiksmīgām centrāles-servera aptaujām. Aizkāve ir uzstādīta diapazonā no 30 līdz 600s. Rekomendēta vērtība ir 300s.

Laiks, lai uzģenerētu ziņojumu par komunikācijas zudumu starp centrāli un Ajax Cloud serveri ir saskaitīts, izmantojot formulu:

$$(Ping\ intervāls * 4) + Laiks\ filtrs$$

Ar noklusējuma iestatījumiem, Ajax Cloud atskaitās par centrāles zudumu 9 minūtes:

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

- ♦ Izslēgt trauksmes, kad savienojums ar serveri ir pazudis. Ajax lietotnes var paziņot par centrāles-servera komunikācijas zudumu divos veidos: ar standarta push paziņojumu vai ar sirēnas skaņas signālu (pēc noklusējuma ieslēgts). Kad opcija ir aktīva, paziņojums nāk ar standarta push signālu.

Sirēnas iestatījumi

Izvēlne satur divas sirēnas iestatījumu grupas: sirēnas aktivācijas parametrus un sirēnas pēc trauksmes indikāciju.

Sirēnas aktivācijas parametri

Ja centrāles vai detektora vāks ir atvērts. Ja tas ir ieslēgts, centrāle aktivizē pievienotās sirēnas, ja centrāles korpuss, detektors vai jebkura cita Ajax ierīce ir atvērta. Ja tiek nospiesta lietotnes trauksmes poga. Kad funkcija ir aktīva, centrāle aktivizē pievienotās sirēnas, ja Ajax lietotnē tika nospiesta trauksmes poga.



Jūs varat izslēgt sirēnas atbildes reakciju, nospiežot trauksmes pogu uz SpaceControl breloka iestatījumos (Iekārtas → SpaceControl → Iestatījumi



Sirēnas pēc-trauksmes paziņojumi



Pieejams tikai lietotnēs Ajax PRO

Sirēna var informēt par trauksmēm sistēmā, izmantojot LED indikāciju. Pateicoties šai funkcijai, sistēmas lietotāji un garāmbraucošo drošības uzņēmumu patruļas var redzēt, ka sistēma tika iedarbināta.

Ugunsdrošības detektora iestatījumi

FireProtect un FireProtect Plus ugunsdrošības detektoru izvēlnes iestatījumi ļauj konfigurēt savstarpēji savienotus uguns detektoru trauksmes signālus.

Šo funkciju iesaka Eiropas ugunsdrošības standarti, kas ugunsgrēka gadījumā 3 metru attālumā no skaņas avota prasa brīdinājuma signāla jaudu vismaz 85 dB. Šāda skaņas jauda ugunsgrēka laikā modina pat cieši gulošu cilvēku. Izmantojot Ajax lietotni, Button vai Keypad, varat ātri atspējot aktivizētos uguns detektorus.



Sistēmas integritātes pārbaude

Sistēmas integritātes pārbaude ir parametrs, kas ir atbildīgs par visu drošības detektoru un ierīču stāvokļa pārbaudi pirms ieslēgšanas. Pārbaude pēc noklusējuma ir atspējota.

Trauksmes Apstiprināšana



Iestatījums pieejams tikai Ajax Pro lietotnē

Trauksmes apstiprināšana ir speciāls notikums, kuru centrāle nosūta CMS sistēmai un lietotājiem, ja noteiktā laika posmā ir iedarbinājušās vairākas noteiktas ierīces. Reagējot tikai uz apstiprinātām trauksmēm, apsardzes uzņēmums un policija samazina viltus trausmju apmeklējumu skaitu.

Atjaunošana pēc trauksmes



Iestatījums pieejams tikai Ajax Pro lietotnē

Šī funkcija neļauj sistēmu ieslēgt, ja trauksme ir reģistrēta iepriekš. Apbruņošanai sistēma jāatjauno pilnvarotam lietotājam vai PRO lietotājam. Konfigurējot funkciju, tiek noteikti trauksmes veidi, kuriem nepieciešama sistēmas atjaunošana.

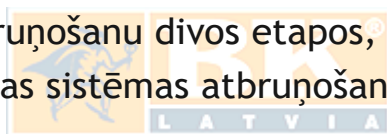
Funkcija novērš situācijas, kad lietotājs apbruņo sistēmu ar detektoriem, kas rada viltus trauksmes signālus.

Apbruņošanas/atbruņošanas Process



Iestatījums pieejams tikai Ajax Pro lietotnē

Izvēlnē ļauj ieslēgt apbruņošanu divos etapos, kā arī Trauksmes Pārraidē Aizkāvi drošības sistēmas atbruņošanas procesam.



Iekārtu Auto Deaktivācija



Iestatījums pieejams tikai Ajax Pro lietotnē

Ajax drošības sistēma var ignorēt trauksmes vai citus ierīču notikumus, tos neizņemot no sistēmas. Saskaņā ar noteiktiem iestatījumiem paziņojumi par konkrētās ierīces notikumiem netiks nosūtīti CMS un drošības sistēmas lietotājiem.

Ir divu veidu ierīču automātiskā deaktivizācija: pēc taimera un pēc trauksmju skaita.

Notīrīt paziņojumu vēsturi

Noklikšķinot uz pogas, centrāles notikumu žurnālā tiks izdzēsti visi paziņojumi.

Uzraudzības stacija – iestatījumi tiešam savienojumam ar apsardzes uzņēmuma centrālo uzraudzības staciju. Parametrus nosaka apsardzes firmas inženieri. Paturiet prātā, ka notikumus un trauksmes signālus var nosūtīt uz apsardzes uzņēmuma centrālo uzraudzības staciju arī bez šiem iestatījumiem.

Protokols - protokola izvēle, ko centrāle izmanto, lai nosūtītu trauksmes signālus uz apsardzes uzņēmuma centrālo uzraudzības staciju, izmantojot tiešu savienojumu. Pieejamie protokoli: Ajax Translator (Contact-ID) un SIA.



Savienojums pēc pieprasījuma. Iespējojiet šo opciju, ja jums ir nepieciešams izveidot savienojumu ar CMS (centrālo uzraudzības staciju) tikai tad, kad pārraida notikumu. Ja opcija ir atspējota, savienojums tiek uzturēts nepārtraukti. Opcija ir pieejama tikai SIA protokolam.

Objekta numurs –uzraudzības stacijas (centrāles) objekta numurs.

Noklusējuma IP adrese

- ♦ **IP adrese un Ports** ir noklusējuma IP adreses iestatījumi un ports ir apsardzes kompānijas serveris, uz kuru trauksmes un notikumi tiek nosūtīti.

Sekundārā IP adrese

- ♦ **IP adrese un Ports** ir sekundāras IP adreses iestatījumi un ports ir apsardzes kompānijas serveris, uz kuru trauksmes un notikumi tiek nosūtīti.



Trauksmes sūtīšanas kanāli

Šajā izvēlnē, trauksmju un notikumu sūtīšanas kanāli uz centrālo uzraudzības staciju ir izvēlēti. Hub 2 Plus var sūtīt trauksmes un notikumus uz centrālo uzraudzības staciju caur **Ethernet** vai **EDGE**. Mēs iesakām izmantot visus sakaru kanālus vienlaikus - tas palielinās pārraides uzticamību un pasargās no kļūmēm telekomunikāciju operatoru pusē.

- ♦ **Ethernet** –notikumu un trauksmes pārraide, izmantojot Ethernet.
- ♦ **GSM** – notikumu un trauksmes pārraide, izmantojot mobilo internetu.
- ♦ **Periodiskās pārbaudes atskaite** – ja ieslēgta, centrāle sūta testa ziņojumus ar noteiktu periodu CMS (centrālajai monitoringa stacijai) objekta savienojuma papildu uzraudzībai.
- ♦ **Uzraudzības stacijas pinga intervāls** – uzstāda testa ziņojumu nosūtīšanas periodu: no 1 minūtes līdz 24 stundām.

Šifrēšana

Notikumu pārraides šifrēšanas iestatījumi SIA protokolā. Tiek izmantota AES 128 bitu šifrēšana.

Šifrēšana – Ja ieslēgts, notikumi un trauksmes tiks pārraidīti uz centrālu uzraudzības staciju SIA formātā šifrētā veidā.

Šifrēšanas atslēga – pārsūtīto notikumu un trauksmes šifrēšanas atslēga. Jāatbilst centrālās uzraudzības stacijas vērtībai.

Trauksmes pogas koordinātas

Nosūtīt koordinātas – ja ieslēgts, trauksmes pogas nospiešana lietotnē nosūtīs iekārtas koordinātas, kur lietotne ir uzstādīta un trauksmes poga nospiesta, uz centrālo uzraudzības staciju.

Apsardzes kompānijas – Apsardzes kompāniju saraksts jūsu reģionā. Reģionu nosaka Jūsu viedtālruņa GPS datu iestatījumi.



Datu Imports – izvēlne automātiskai iekārtu un iestatījumu pārvešanai uz citu centrāli.

Iestatījumu Atiestatīšana

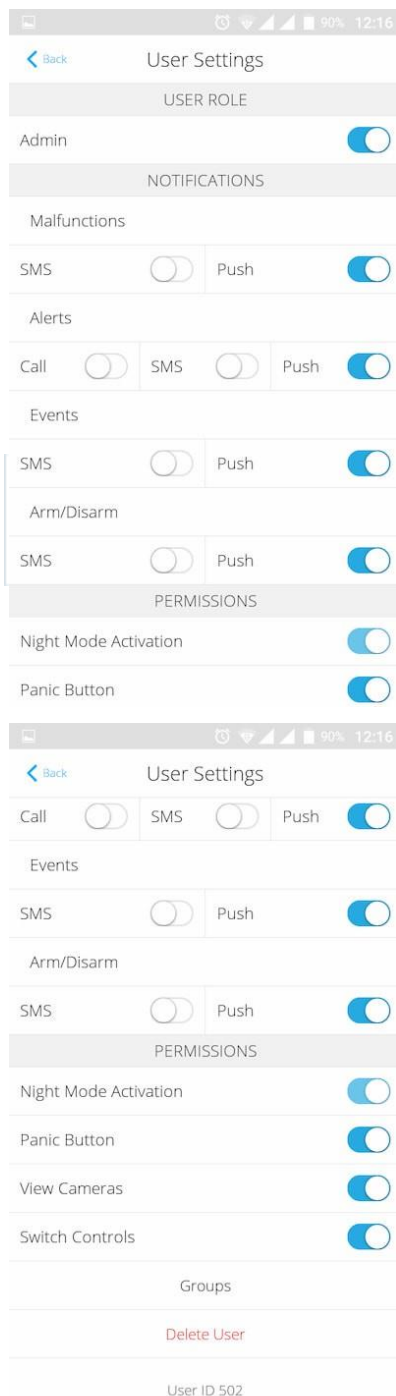
Lai atgrieztu centrālei rūpnīcas noklusējuma iestatījumus, ieslēdziet to un pēc tam 30 sekundes turiet ieslēgšanas / izslēgšanas pogu (logotips sāks mirgot sarkanā krāsā).

Tajā pašā laikā visi pievienotie detektori, telpas iestatījumi un lietotāja iestatījumi tiks izdzēsti. Lietotāja profili paliks savienoti ar sistēmu.

Lietotāji

Pēc centrāles pievienošanas lietotājkontam, jūs kļūsit par iekārtas administratoru. Vienai centrālei var būt 50 lietotāji/administratori. Administrators var uzaicināt lietotājus uz drošības sistēmu un noteikt viņu tiesības.

Notikumu un trauksmes paziņojumi



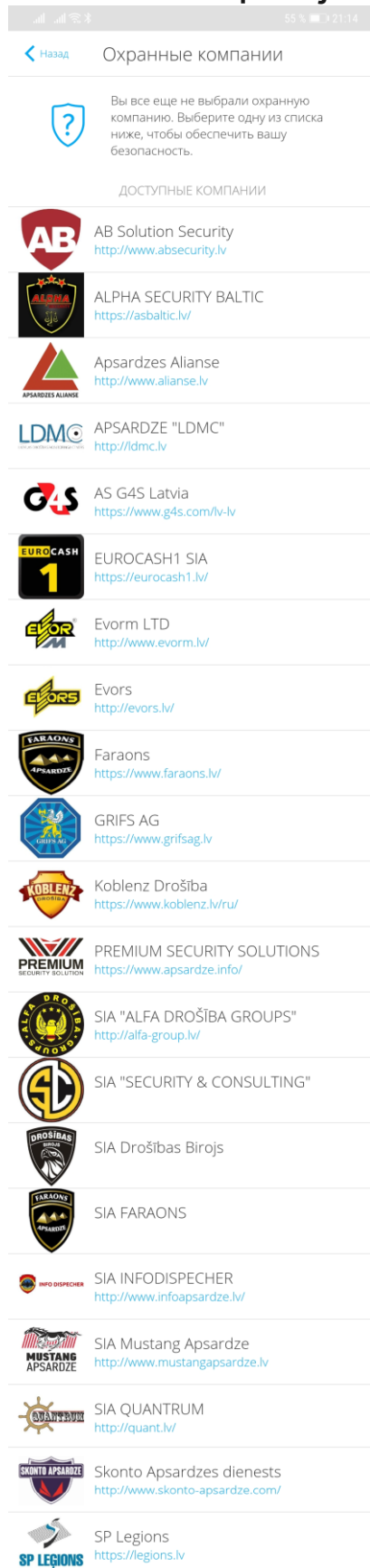
Centrāle paziņo lietotājiem par notikumiem trijos veidos: push paziņojumi, SMS vai zvani.

Paziņojumus uzstāda lietotāju izvēlnē:

Notikumu tipi	Kādam nolūkam izmanto	Paziņojumu tipi
Apbruņošana / Atbruņošana	Paziņojumi tiek saņemti pēc apbruņošanas / atbruņošanas	SMS, Push-paziņojumi
Trauksme	Paziņojumi par ielaušanos, ugunsgrēku, noplūdi	SMS, Push paziņojumi, zvani
Notikumi	Paziņo par notikumiem, saistītiem ar Ajax WallSwitch, Releja kontroli	SMS, Push-paziņojumi
Nepareiza darbība	Paziņojumi par sakaru zudumu, traucēšanu, zemu akumulatora baterijas līmeni vai detektora korpusa atvēršanu	SMS, Push-paziņojumi

- Push paziņojumu Ajax Cloud nosūta Ajax Security sistēmas lietotnei, ja ir pieejams interneta savienojums.
- SMS tiek nosūtīts uz tālruņa numuru, kuru lietotājs norāda, reģistrējot Ajax kontu.
- Tālruņa zvans nozīmē, ka centrmezgls zvana uz Ajax kontā norādīto numuru.






















Pieslēgšana pie Apsardzes Kompānijas



← Назад Охранные компании

Вы все еще не выбрали охранную компанию. Выберите одну из списка ниже, чтобы обеспечить вашу безопасность.

ДОСТУПНЫЕ КОМПАНИИ

-  AB Solution Security
<http://www.absecurity.lv>
-  ALPHA SECURITY BALTIC
<https://asbaltic.lv>
-  Apsardzes Alianse
<http://www.alianse.lv>
-  APSARDZE "LDMC"
<http://dmc.lv>
-  AS G4S Latvia
<https://www.g4s.com/lv-lv>
-  EUROCASH 1 SIA
<https://eurocash1.lv>
-  Evorm LTD
<http://www.evorm.lv>
-  Evors
<http://evors.lv>
-  Faraons
<https://www.faraons.lv>
-  GRIFS AG
<https://www.grifsag.lv>
-  Koblenz Drošība
<https://www.koblenz.lv/ru/>
-  PREMIUM SECURITY SOLUTIONS
<https://www.apsardze.info/>
-  SIA "ALFA DROŠĪBA GROUPS"
<http://alfa-group.lv/>
-  SIA "SECURITY & CONSULTING"
-  SIA Drošības Birojs
-  SIA FARAONS
-  SIA INFODISPECHER
<http://www.infoapsardze.lv/>
-  SIA Mustang Apsardze
<http://www.mustangapsardze.lv>
-  SIA QUANTRUM
<http://quant.lv/>
-  Skonto Apsardzes dienests
<http://www.skonto-apsardze.com/>
-  SP LEGIONS
<https://legions.lv>

Organizāciju saraksts, kas pieslēdz Ajax sistēmu ar centrālo uzraudzības staciju, ir pieejams centrālās iestatījumu izvēlnē **Drošības uzņēmumi**:

Sazinieties ar uzņēmuma pārstāvjiem, kas sniedz pakalpojumus jūsu pilsētā, un vienojieties par savienojumu.

Savienojums ar centrālo uzraudzības staciju (CMS) ir iespējams, izmantojot Contact ID vai SIA protokolus.

Apkope

Regulāri pārbaudiet drošības sistēmas Ajax darbību.

Notīriet centrāles korpusu no putekļiem, zirnekļa tīkliem un citiem piesārņojumiem, kad tie parādās. Izmantojiet mīkstu sausu salveti, kas piemērota aprīkojuma apkopei.

Centrāles tīrīšanai neizmantojiet vielas, kas satur spirtu, acetonu, benzīnu un citus aktīvos šķīdinātājus.

Komplekts

1. Ajax Hub Centrāle
2. SmartBracket stiprinājuma panelis
3. Barošanas kabelis
4. Ethernet kabelis
5. Instalācijas komplekts
6. GSM sākuma pakete (pieejama ne visās valstīs)
7. Rokasgrāmata

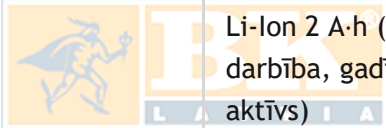


Drošības prasības

Centrāles uzstādīšanas un lietošanas laikā jāievēro vispārējie elektrisko ierīču lietošanas noteikumi elektrodrošības jomā, kā arī normatīvo aktu prasības par elektrodrošību.

Stingri aizliegts izjaukt ierīci zem sprieguma! Nelietojiet ierīci ar bojātu strāvas kabeli.

Tehniskie parametri

Iekārtas	Līdz 100
Grupas	Līdz 9
Lietotāji	Līdz 50
Videonovērošana	Līdz kamerām vai DVR
Istabas	Līdz 50
Scenāriji	Līdz 5 (Scenāriji ar apbruņošanu / atbruņošanu nav iekļauti scenāriju vispārējā ierobežojumā)
Savienots ReX	1
Barošana	110 – 240 V AC, 50/60 Hz
Akumulatora vienība	 Li-Ion 2 A·h (Līdz 15 stundām autonoma darbība, gadījumā, ja Ethernet savienojums nav aktīvs)
Enerģijas patēriņš	10 W
Tampera aizsardzība	Jā
Frekvences josla	868.0 – 868.6 MHz vai 868.7 – 869.2 MHz Atkarīgs no jūsu reģiona
Efektīva jauda	8.20 dBm / 6.60 mW (robeža 25 mW)
Radio signāla modulācija	GFSK
Radio signāla diapazons	Līdz 2,000 m

Komunikācijas kanāli	GSM 850/900/1800/1900 MHz GPRS, Ethernet
Uzstādīšana	Iekšējās
Darbības temperatūras diapazons	No -10°C līdz +40°C
Darbības mitrums	Līdz 75%
Izmēri	163 × 163 × 36 mm
Svars	350 g
Sertifikācija	Security Grade 2, Environmental Class II SP2 (GSM-SMS), SP5 (LAN) DP3 in conformity with the requirements of EN 50131-1, EN 50131-3, EN 50136-2, EN 50131-10, EN 50136-1, EN 50131-6, EN 50131-5-3



Garantija

Garantija “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY produktiem ir spēkā 2 gadus no pirkuma dienas un neattiecas uz akumulatoru.

Ja ierīce nedarbojas pareizi, vispirms sazinieties ar atbalsta dienestu - pusē gadījumu tehniskās problēmas var atrisināt attālināti!

Tehniskais atbalsts: info@bklatvia.lv

