

Ajax PRO: Tool for Engineers lietotne

Instalētāja lietotne: objekta izveide, centrāles un ierīču pievienošana, testi un nodošana klientam

Pamācība instalētājiem: kā izveidot PRO kontu, pievienot Ajax centrāli un ierīces lietotnē Ajax PRO: Tool for Engineers, pārbaudīt sistēmu, pieslēgt apsardzes centrāli un nodot objektu klientam.

1. PAR LIETOTNI

Ajax PRO: Tool for Engineers ir Ajax mobilā lietotne (iOS un Android) instalētājiem un apsardzes uzņēmumiem. Ar to izveido objektus (telpas, "space"), pievieno centrāles un ierīces, konfigurē sistēmu, veic testus objektā un attālināti apkalpo neierobežotu skaitu sistēmu.

Lietotni var lietot paralēli datora lietotnei Ajax PRO Desktop, un abas reāllaikā sinhronizējas caur mākonī. Ajax Superior ierīces uzstāda tikai ar Ajax PRO lietotni.

2. KAS NEPIECIEŠAMS

- Viedtālrunis ar lietotni Ajax PRO: Tool for Engineers. Objektu ("space") funkcijai vajag lietotnes versiju 2.0 vai jaunāku un centrāli ar OS Malevich 2.6 vai jaunāku.
- PRO konts. Lietotāja lietotnes Ajax Security System konts PRO lietotnē neder, tie ir atsevišķi konti (var izmantot to pašu e-pastu un tālruni).
- Centrāle, kas pieslēgta barošanai un internetam (Ethernet un/vai SIM karte), un ierīču QR kodi vai ID.
- Uzņēmuma konta izveidei: datora lietotne Ajax PRO Desktop.

Svarīgi: lai lietotne varētu rādīt trauksmes un notikumus, atļaujiet tai pieprasītās tālruņa funkcijas, arī paziņojumus.

3. PRO KONTA IZVEIDE

Individuāls PRO konts:

1. Atveriet lietotni un nospiediet "Create account".
2. Aizpildiet laukus, izvēlieties sistēmas e-pastu un SMS valodu, piekrītietai lietotāja līgumam, privātuma politikai un licences līgumam un nospiediet "Next". Vienam e-pastam vai tālruņa numuram var reģistrēt tikai vienu PRO kontu.
3. Ievadiet uzņēmuma datus un nospiediet "Next". Lauki "Company name" un "Website" nav obligāti, tos var izlaist ar "Skip".
4. Ievadiet divus apstiprinājuma kodus: vienu no SMS, otru no e-pasta, un nospiediet "Send". Kodus nevienam neizpaužiet.
5. Ja kāds kods nepienāk, nospiediet "Haven't received code yet?" un vēlreiz ievadiet e-pastu un tālruni; jums tiks atzvanīts. Atkarībā no valsts var būt jāievada pēdējie trīs vai seši zvanītāja numura cipari kopā ar e-pasta kodu. Ja tas nepalīdz, sazinieties ar Ajax atbalstu.
6. Pēc pārbaudes lietotne jūs pieslēdz automātiski.

Ja uzņēmums darbiniekiem izmanto vienoto pieteikšanos (SSO), konta izveide notiek citādi. Šāds darbinieka konts strādā tikai uzņēmuma vārdā, un to nevar uzaicināt objektā kā privātu instalētāju.

Uzņēmuma konts: uzņēmumu izveido tikai Ajax PRO Desktop (modulis "Company" > "Create company"; norāda nosaukumu, valsti un pakalpojuma veidu: apsardzes uzraudzība, uzstādīšana un apkope vai abi; apstiprinājuma kods pienāk īpašnieka e-pastā). PRO konts, kas izveidoja uzņēmumu, kļūst par tā īpašnieku ("Company owner"). Darbiniekus pievieno tikai tad, ja viņiem jau ir PRO konts. Vienu PRO kontu var piesaistīt neierobežotam skaitam uzņēmumu, un mobilajā lietotnē sistēmas var pārvaldīt gan no personīgā PRO konta, gan no uzņēmuma konta.

Konta drošībai var ieslēgt divfaktoru autentifikāciju (nav pieejama SSO darbinieku kontiem), sekot līdz aktīvajām sesijām citās ierīcēs un tās pārtraukt, kā arī aizsargāt lietotni ar 4 ciparu kodu un pēc izvēles ar pirkstu nospiedumu vai sejas atpazīšanu.

4. CENTRĀLES PIEVIEŅOŠANA UN OBJEKTA IZVEIDE

1. Pieslēdziet centrālei barošanu un internetu (Ethernet un/vai SIM kartes). Ieslēdziet to un pagaidiet, līdz logotips iedegas zaļā vai baltā krāsā.
2. Atveriet lietotni un izvēlieties objektu vai izveidojiet jaunu: nospiediet "Add Space", ievadiet nosaukumu un nospiediet "Add".
3. Nospiediet "Add Hub".
4. Izvēlieties pievienošanas veidu: manuāli vai ar soli pa soli vedni. Pirmajai sistēmas iestatīšanai izmantojiet vedni.
5. Manuāli: ievadiet centrāles nosaukumu, noskenējiet tās QR kodu vai ievadiet ID un pagaidiet, līdz centrāle parādās cilnē "Devices". Ar vedni: sekojiet norādēm lietotnē.

Kad PRO konts pats izveido objektu un pievieno centrāli, tam ir neierobežots laiks sistēmas konfigurēšanai. Centrāles ID ir uz iepakojuma, plates un QR kodā zem SmartBracket vāciņa.

Ja centrāle jau pieder citam objektam un tai ir administrators, PRO ar pilnām tiesībām vai uzņēmums, lietotne piedāvā nosūtīt pievienošanās pieprasījumu ("Send request"). Pēc apstiprinājuma jūs tiekat pievienots esošajam objektam, jauns objekts netiek izveidots.

Svarīgi: dzēšot objektu ("Space Deletion" objekta iestatījumos, objektam jābūt noņemtam no apsardzes), tajā esošā centrāle tiek atiestatīta uz rūpnīcas iestatījumiem un lietotāji zaudē piekļuvi.

5. IERĪČU PIEVIEŅOŠANA UN KONFIGURĒŠANA

Bezvadu (Jeweller) ierīce:

1. Izvēlieties objektu un atveriet "Rooms" > telpa > "Add Device" vai cilni "Devices" > "Add Device".
2. Ievadiet ierīces nosaukumu, noskenējiet QR kodu vai ievadiet to manuāli, izvēlieties telpu (ja pievienojat no cilnes "Devices") un grupu (ja ieslēgts grupu režīms).
3. Nospiediet "Add"; sāksies atpakaļskaitīšana. Ieslēdziet ierīci pēc norādēm lietotnē.
4. Pievienošanas laikā ierīcei jāatrodas centrāles radio pārklājumā, tajā pašā aizsargājamajā objektā.

Vadu (Fibra) ierīces var pievienot pa vienai ar QR kodu vai visas reizē: "Add Device" > "Add All Fibra Devices" (arī centrāles iestatījumos "Lines"). Ierīci atpazīst divos veidos: pieskaroties tai sarakstā, tās LED sāk mirgot; vai ieslēdzot "Prioritize triggered devices" un izraisot nostrādi, ierīce uz 5 s pārvietojas saraksta augšā. Katrai ierīcei piešķiriet nosaukumu, telpu un grupu un nospiediet "Save".

Ierīces iestatījumi: "Devices" > ierīce > zobrata ikona. Visus iestatījumus apraksta konkrētās ierīces instrukcija. Vairākām ierīcēm vienlaikus var piemērot iestatījumu veidnes.

Signāla stipruma tests ("Jeweller Signal Strength Test", vadu ierīcēm "Fibra Signal Strength Test") ierīces iestatījumos sākas ne uzreiz, bet viena aptaujas perioda laikā (standarta iestatījumos 36 s). Rezultātu rāda lietotne un ierīces LED:

Signāls lietotnē	LED un nozīme
3 iedaļas	Deg gandrīz nepārtraukti ar īsu pārtraukumu ik pēc 1,5 s – teicams
2 iedaļas	Mirgo 5 reizes sekundē – apmierinošs
1 iedaļa	Mirgo 2 reizes sekundē – vājš
0 iedaļu	Īsi uzzibsnī ik pēc 1,5 s – nav savienojuma

Jeweller testu uzstādīšanas vietā veiciet vismaz 1 minūti; ierīci ieteicams uzstādīt vietā ar 2–3 iedaļām. Ja signāls vājš, pārvietojiet ierīci (jau 20 cm var būtiski uzlabot uztveršanu), un, ja tas nēlīdz, izmantojiet signāla pastiprinātāju. Fibra ierīcēm vājā signāla gadījumā vispirms pārbaudiet kabeļu pieslēgumu spailēm. Grade 3 ierīcēm un Superior Hub Hybrid (2G)/(4G) ar programmaparatūru 2.17 vai jaunāku ir arī signāla vājināšanas tests ("Signal Attenuation Test"): pēc signāla testa izvēlieties "Attenuation" un vismaz minūti pārbaudiet signālu; ja tas ir 2–3 iedaļas, vieta ir piemērota. Pēc testa obligāti atgrieziet "Auto", citādi baterija izlādēsies ātrāk.

Aptveršanas zonas tests ("Detection zone test") pārbauda, vai detektors izvēlētajā vietā pareizi reaģē. To palaiž ierīces iestatījumos vai centrāles iestatījumos vairākām ierīcēm reizē. Testa laikā ierīces LED deg nepārtraukti un nodziest nostrādes brīdī; jaunākās versijās lietotnē parādās arī paziņojums. Atvēšanas detektoram atveriet un aizveriet durvis vai logu; kustības detektoram staigājiet tā redzeslokā; stikla plīšanas detektoram piesitiet ar dūri stiklam (to nesaplēšot), tad 1,5 s laikā uzmetiet cietai virsmai metāla priekšmetu, piemēram, karoti; detektoram abas reizes jāreaģē ar LED nodzišanu. Ja detektors nereaģē katru reizi, uzstādiet to citur. Ja testa laikā nostrādā korpusa sensors, paziņojumu saņem visi lietotāji un apsardzes centrāle.

6. LIETOTĀJU UZAICINĀŠANA UN TIESĪBAS

1. Izvēlieties objektu un atveriet tā iestatījumus.
2. Atveriet "Users" un nospiediet "Send invites".
3. Ievadiet e-pasta adresi vai izvēlieties kontaktu ("Add from contacts") un nospiediet "Continue".

Ja personai jau ir Ajax konts, objekts parādās tās lietotnē un sadaļā "Active users". Ja konta nav, tā jāizveido lietotnē Ajax Security System ar to pašu e-pastu; līdz tam persona redzama sadaļā "Pending invites".

Loma	Ko drīkst
Administrators ar pilnām tiesībām	Konfigurē sistēmu, testē ierīces, pārvalda lietotājus, instalētājus un uzņēmumus, piešķir un atsauc PRO piekļuvi.
Administrators bez konfigurēšanas tiesībām	Vada apsardzes režīmus, maina paziņojumu veidus, uzaicina lietotājus, var piešķirt PRO piekļuvi iestatījumiem.
Lietotājs	Ieslēdz un izslēdz apsardzi, lieto trauksmes pogu, saņem trauksmju paziņojumus.
PRO ar pilnām tiesībām	Konfigurē un testē sistēmu, pārvalda lietotājus un PRO kontus.
PRO bez piekļuves iestatījumiem	Sistēmas iestatījumiem piekļuves nav.

Administrators var dot PRO kontam pastāvīgu vai pagaidu piekļuvi uz 1, 2, 4 vai 8 stundām; pēc tam tiesības tiek atsauktas automātiski. Lietotāju skaits atkarīgs no centrāles modeļa; katrs PRO konts un pieslēgts uzņēmums aizņem vienu lietotāja vietu. Privātuma iestatījumus (foto pēc pieprasījuma) PRO lietotnēs pārvaldīt nevar.

7. GRUPAS UN APSARDZES REŽĪMI

Telpas ("Rooms") tikai sakārto ierīces, un bez tām ierīci pievienot nevar. Grupas ļauj ieslēgt apsardzi atsevišķām ierīcēm vai zonām un piesaistīt tām sirēnas, pultis, tastatūras un automatizācijas ierīces. Grupu režīmu konfigurē administrators vai PRO ar administratora tiesībām; maksimālais grupu skaits atkarīgs no centrāles (piem., Hub 2 – 9, Hub 2 Plus – 25, Superior MegaHub – 100).

1. Atveriet "Control" > iestatījumi > "Groups" un nospiediet "Add group"; ievadiet nosaukumu (līdz 24 latīņu vai 12 kirilicas rakstzīmēm) un nospiediet "Add".
2. Grupā atveriet "Devices" > "Edit", atzīmējiet ierīces un nospiediet "Save". Ierīce var būt tikai vienā grupā.
3. Kad visas ierīces sadalītas, sadaļā "Groups" ieslēdziet "Group mode" un saglabāji ar "Back".
4. Grupā atveriet "Users" > "Edit", atzīmējiet lietotājus, kas drīkst to vadīt, un nospiediet "Save"; administratoriem vienmēr ir piekļuve visām grupām.
5. Pēc vajadzības grupā nospiediet "Edit", iestatiet "Arm if system armed", "Disarm if system disarmed" un "Followed groups" un nospiediet "Save".

Nakts režīms ("Night mode") ieslēdz apsardzi tikai ierīcēm, kurām iestatījumos ieslēgts "Arm in Night mode"; pēc noklusējuma tas ir izslēgts. Grupu dzēšot, vispirms pārvietojiet tās ierīces uz citu grupu; pēdējo grupu var dzēst tikai pēc grupu režīma izslēgšanas.

8. SAVIENOJUMS AR APSARDZES CENTRĀLI

Uzraudzības pieprasījumu apsardzes uzņēmumam sūta objekta administrators vai PRO ar konfigurēšanas tiesībām:

1. Izvēlieties objektu, atveriet cilni "Control" un objekta iestatījumus.
2. Atveriet "Security companies", izvēlieties uzņēmumu un nospiediet "Apply". Ja zināt uzņēmuma e-pastu, izmantojiet "Invite by email".
3. Uzņēmums pieprasījumu pieņem Ajax PRO Desktop un izveido objekta karti ar numuru.

Uzstādīšanas un apkopes uzņēmumu pievieno sadaļā "Installers/Companies" > "Invite" ar uzņēmuma e-pastu; apstiprinājums nav vajadzīgs, un uzņēmumam ir 8 stundas iestatījumu maiņai. Ja vajag abus pakalpojumus, sūtiet abus pieprasījumus.

Papildus uzraudzībai caur Ajax Cloud apsardzes uzņēmums var izmantot tiešo savienojumu: centrāles iestatījumos "Monitoring Station" norāda IP adresi un portu, un centrāle sūta notikumus tieši (Contact ID vai SIA protokolā). Šī savienojuma stāvoklis redzams centrālās stāvokļos. Atsevišķām ierīcēm ziņošanu uz uzraudzības programmatūru var izslēgt to iestatījumu sadaļā "Monitoring".

9. SISTĒMAS PĀRBAUDES

Staigāšanas tests ("Walk test") pārbauda visas apsardzes un ugunsdrošības ierīces bez trauksmes: sistēma nerada trauksmi, neieslēdz sirēnas un nesūta paziņojumus lietotnēm un centrālei, bet reģistrē katras ierīces pēdējo nostrādi. Vajag centrāli ar OS Malevich 2.35 vai jaunāku (izņemot Hub (2G) Jeweller) un vismaz vienu apsardzes vai ugunsdrošības ierīci.

1. Pārliecinieties, ka sistēma nav apsardzē un nenotiek atjauninājumi vai citi testi.
 2. Cilnē "Devices" izvēlieties centrāli > iestatījumi > "Walk test" > "Start". Pāreja testa režīmā var ilgt līdz 5 minūtēm.
 3. Izraisiet katras ierīces nostrādi; jaunākā nostrāde parādās saraksta augšā.
 4. Beidziet ar "Stop" vai sagaidiet automātisko iziešanu.
- Tests aptver ielašanās detektorus un to maskēšanas sensorus, trauksmes pogas un ugunsdrošības ierīces (izņemot manuālos trauksmes punktus un EN54 Line ierīces).
 - Testa laikā korpusa atvēršanas trauksmes un bojājumi joprojām tiek sūtīti lietotnēm un centrālei; centrāle saņem kodus E607/TS (sākums) un R607/TE (beigas).
 - Testa laikā nevar ieslēgt apsardzi, atjaunināt programmaparatūru, pievienot vai dzēst ierīces un skenēt Fibra līnijas. Ja grafiks paredz apsardzi, sistēma iziet no testa un ieslēdz apsardzi.
 - Bojātu vai nepareizi uzstādītu ierīci var deaktivizēt, to nedzēšot: ierīces iestatījumi > "Permanent deactivation" ("Entirely" vai "Lid only") > "Save"; to var tikai administrators vai PRO, sistēmai jābūt bez apsardzes. Tas var ietekmēt atbilstību EN 50131.

10. ATJAUNINĀJUMI

Centrālās iestatījumu sadaļā "Service" opcija "Firmware auto-update" pēc noklusējuma ir ieslēgta: OS Malevich atjauninās automātiski, kad sistēma nav apsardzē un pieslēgta ārējā barošana. Ja opcija izslēgta, lietotne piedāvā atjauninājumu, kad tas pieejams. Manuāli atjauninājumu pārbauda ar "Firmware update" > "Check for new version". Centrāle pārbauda atjauninājumus ik pēc 5 minūtēm; lejupielāde notiek fonā (tikai centrālei 10–20 min, ar pastiprinājumiem ilgāk).

Ja centrālās programmaparatūra ir novecojusi, ierīces pievienošanā var rasties kļūda; tad lietotne aicina atvērt "Firmware update" un pārbaudīt jaunu versiju. Ierīces programmaparatūras versija redzama tās stāvokļu saraksta apakšā.

11. OBJEKTA NODOŠANA KLIENTAM

1. Pabeidziet konfigurēšanu un pārbaudes.
2. Objekta iestatījumos "Users" uzaiciniet klientu un piešķiriet viņam administratora tiesības.
3. Kad objektam pievienots administrators, PRO konts zaudē pastāvīgās tiesības; konfigurēšana vēl pieejama 8 stundas.
4. Vēlāk piekļuvi pieprasiet ar "Access rights" (ikona augšējā labajā stūrī) > "Request access", izvēloties tiesības un laiku > "Send request". Administrators saņem paziņojumu, un apstiprinātais pieprasījums stājas spēkā minūtes laikā.

Ja objektā vairs nav neviena administratora, PRO konts automātiski saņem pastāvīgu piekļuvi iestatījumiem.

Svarīgi: Ajax neiesaka klientam piešķirt trešajām personām pilnas administratora tiesības, pat uz laiku. Ja tiesības nolaidības dēļ zaudētas, Ajax Systems piekļuvi centrālei atjaunot nevar.

Centrāles nomaiņai izmantojiet datu pārnēsi: vecās centrāles iestatījumos "Transfer settings to another hub" noskenējiet jaunās centrāles QR kodu, pārbaudiet sarakstu, nospiediet "Next", izslēdziet veco centrāli un nospiediet "Start". Objektam jābūt bez apsardzes, centrālēm nedrīkst notikt atjaunināšana, un datus var pārnest tikai uz tādu pašu vai jaudīgāku modeli. Visi jaunās centrāles dati tiek aizstāti ar vecās datiem. Uzraudzības kanālu iestatījumi netiek pārnesti; ja jaunā centrāle pieslēgta apsardzes centrālei, vispirms apturiet uzraudzību. Pogas un pultis pārnēs, divreiz nospiežot jebkuru to pogu jaunās centrāles pārklājumā.

12. BIEŽĀKĀS PROBLĒMAS

Problēma	Risinājums
Nevar pieteikties ar Ajax Security System kontu	PRO lietotnei vajag atsevišķu PRO kontu.
Nepienāk reģistrācijas kods	"Haven't received code yet?" un atzvana kods; ja nepalīdz, Ajax atbalsts.
Centrāle jau piesaistīta citam kontam	Nosūtiet pievienošanās pieprasījumu vai lūdziet administratoram uzaicināt jūsu PRO kontu; administratoru palīdz noskaidrot Ajax atbalsts.
Piekļuve iestatījumiem beigusies	Pēc 8 stundām pieprasiet piekļuvi atkārtoti ar "Request access".
Vājš signāls (0–1 iedaļa)	Pārvietojiet ierīci vai centrāli, izmantojiet pastiprinātāju; Fibra ierīcēm pārbaudiet kabelus un līnijas noslodzi.
Detektors aptveršanas testā nereaģē katru reizi	Uzstādiet to citā vietā.
"Walk test" nesākas	Noņemiet apsardzi, pagaidiet atjauninājumu vai cita testa beigas, izslēdziet akumulatora taupīšanas režīmu.

Pilnā ražotāja lietošanas instrukcija: <https://ajax.systems/ajax-pro-tool-for-engineers/>

Šī ir Sareme Latvia SIA sagatavota īsa lietošanas pamācība latviešu valodā, kas balstīta uz ražotāja oficiālo instrukciju (dati uz 16.10.2026). Pilnīgu un saistošu informāciju, tostarp visus drošības norādījumus, skatiet ražotāja instrukcijā. Ražotājs var mainīt produktu un instrukciju bez iepriekšēja brīdinājuma.