

Ajax lietotnes

Lietošanas pamācības latviski: trīs atsevišķas lietotnes, katra ar savu pamācību

Lietotne	Kam paredzēta
Ajax lietotne	lietotājiem un mājas īpašniekiem (Ajax Security System)
Ajax PRO lietotne	montētājiem un uzstādītājiem (Ajax PRO: Tool for Engineers)
Ajax PRO Desktop	datora lietotne montētājiem un apsardzes centrālēm

SATURS

Ajax lietotne	2
Ajax PRO lietotne	6
Ajax PRO Desktop	11

LIETOŠANAS PAMĀCĪBA

Ajax lietotne

lietotājiem un mājas īpašniekiem (Ajax Security System)

Pamācība Ajax sistēmas lietotājiem: kā sākt lietot mobilo lietotni Ajax Security System, pievienot centrāli un ierīces, vadīt apsardzi, iestatīt paziņojumus, lietotājus, scenārijus un aizsargāt kontu.

1. PAR LIETOTNI

Ajax Security System ir bezmaksas lietotne Ajax sistēmas lietotājiem (iOS, Android, Apple Watch, Wear OS, Windows, macOS). Ar to vada apsardzi, saņem paziņojumus, pārvalda lietotājus, automatizāciju un video.

Viena objekta ierīces lietotnē apvieno "telpa" ("Space"), ko var izveidot arī bez centrāles. Lietotne pieejama arī latviešu valodā; izvēlnu nosaukumi šeit doti angļiski, kā ražotāja dokumentācijā.

2. KAS NEPIECIEŠAMS

- Ajax Security System lietotne no App Store vai Google Play (telpām versija 3.0 vai jaunāka).
- Ajax konts; vienai e-pasta adresei vai tālruņa numuram var būt tikai viens konts.
- Ajax centrāle (hub) apsardzes, ugunsdrošības, noplūdes un automatizācijas ierīcēm. Ajax kameras un NVR var pievienot arī bez tās.
- Lietotnei atļauta piekļuve visām funkcijām, īpaši paziņojumiem.

3. LEJUPIELĀDE UN KONTA IZVEIDE

1. Atveriet lietotni un nospiediet "Create account".
2. Aizpildiet laukus, piekrīti lietotāja līgumam, privātuma politikai un licences līgumam un vēlreiz nospiediet "Create account".
3. Ievadiet kodu no SMS un kodu no e-pasta, nospiediet "Send". Kodus nevienam neizpaužiet.
4. Ja kods nepienāk, nospiediet "Haven't received code yet?", vēlreiz ievadiet e-pastu un tālruni un sagaidiet zvanu. Dažās valstīs kopā ar e-pasta kodu jāievada zvanītāja numura pēdējie 3 vai 6 cipari. Ja nelīdz, rakstiet Ajax atbalstam.
5. Pēc pārbaudes lietotne jūs pieslēdz automātiski; turpmāk lietojiet e-pastu un paroli.

4. CENTRĀLES (HUB) PIEVIENOŠANA

Vispirms izveidojiet telpu: "Add Space" › nosaukums › "Add" (nākamās telpas: galvenā izvēlnē augšējā kreisajā stūrī › "Add Space"). Centrālei jābūt savienotai ar Ajax Cloud.

1. Atveriet lietotni, izvēlieties vai izveidojiet telpu.
2. Atveriet "Add Hub", izvēlieties pievienošanu manuāli vai ar soli pa solim norādījumiem.
3. Ievadiet centrāles nosaukumu un noskenējiet QR kodu zem SmartBracket paneļa (vai ievadiet ID).
4. Pagaidiet, līdz centrāle parādās lietotnē. Ja pieejami Ajax pakalpojumi, lietotne piedāvās tos aktivizēt.

Ja centrālei jau ir administrators, PRO ar pilnām tiesībām vai uzņēmums, nosūtiet pievienošanās pieprasījumu ("Send request"); pēc apstiprināšanas jūs pievienos esošajai telpai.

Svarīgi: telpu dzēš administrators vai instalētājs ar konfigurēšanas tiesībām, kad apsardze izslēgta (telpas iestatījumi › "Space Deletion"). Centrāle tiek atiestatīta uz rūpnīcas iestatījumiem, lietotāji zaudē piekļuvi.

5. IERĪČU PIEVIENOŠANA

Ierīces pievieno administrators vai PRO ar konfigurēšanas tiesībām, kamēr sistēma nav apsardzē. Vispirms izveidojiet istabu: "Rooms" > "Add room" > nosaukums > "Add" (bez centrāles līdz 50 istabām, ar centrāli pēc tās modeļa).

1. Cilnē "Rooms" atveriet istabu un izvēlieties "Add Device".
2. Ievadiet nosaukumu, noskenējiet QR kodu (vai ievadiet ID), izvēlieties istabu un turpiniet.
3. Kad sākas atpakaļskaitīšana, ieslēdziet ierīci: LED vienreiz nomirgos. Ierīcei jābūt centrāles bezvadu tīkla pārklājumā tajā pašā objektā.
4. Ja neizdodas, izslēdziet ierīci uz 5 sekundēm un mēģiniet vēlreiz.

6. APSARDZES REŽĪMI

Cilnē "Control" ir pogas "Arm", "Disarm", "Night mode" un trauksmes poga.

- Nakts režīmā apsargātas tikai izvēlētās ierīces (atvēršanas, stikla plīšanas, kustības detektori, kameras), lai mājās var brīvi pārvietoties. Ierīcei to ieslēdz: "Devices" > ierīce > iestatījumi > "Arm in Night mode" (pēc noklusējuma izslēgts). Bez grupu režīma apsardze aizstāj nakts režīmu un otrādi.
- Grupas: "Control" > iestatījumi > "Groups" > "Add group" (līdz 24 latīņu rakstzīmēm). Ierīce var būt tikai vienā grupā. Slēdzi "Group mode" ieslēdz administrators vai PRO ar administratora tiesībām, kad visas ierīces sadalītas. Grupu skaits: Hub un Hub 2 – 9, Hub 2 Plus – 25. Lietotājs bez administratora tiesībām vada tikai atļautās grupas.
- Trauksmes poga darbojas arī bez centrāles. Ar OS Malevich 2.9 vai jaunāku apsardzes uzņēmums saņem arī tālruņa koordinātas. Sirēnas tā ieslēdz, ja centrāles iestatījumos "Service" > "Sounds and alerts" aktivizēts "If in-app panic button is pressed".
- "Geofence" (telpas iestatījumos) pēc tālruņa GPS atgādina ieslēgt apsardzi, izejot no zonas, un izslēgt, ieejot.

7. PAZIŅOJUMI UN NOTIKUMI

Sistēma ziņo ar push paziņojumiem, SMS un zvaniem. Trauksmēm (ielaušanās, trauksmes poga, ugunsgrēks, noplūde, centrāles savienojuma zudums ar Ajax Cloud) pieejami visi trīs kanāli, un push var iestatīt kā parastu vai kritisku. Darbības traucējumiem, režīma maiņai, sistēmas notikumiem, gaisa kvalitātei un automatizācijai ir push un SMS. Visiem lietotājiem paziņojumus iestata administrators vai PRO ar konfigurēšanas tiesībām (telpas iestatījumi > "Users" > lietotājs > "Notification settings"), pārējie tikai savus push.

- iPhone: "Settings" > "Notifications" > Ajax, ieslēdziet "Allow Notifications" un "Allow Critical Alerts" (trauksmes skan arī klusuma un "Do Not Disturb" režīmā).
- Android: lietotnes izvēlne > "App settings" > "System settings" > "Critical alerts" > "To phone settings" > "Show notifications". Zemākajā skaļumā tālrunis tikai vibrē.
- Kritisko paziņojumu skaļumu maina "App Settings" > "System Settings"; pēc atkārtotas pieteikšanās tas atgriežas uz maksimālo.

Ja ieslēgta funkcija "Chime", par atvēršanas detektoru nostrādi bez apsardzes ziņo tikai sirēnas, ne lietotne.

8. LIETOTĀJI UN PIEKĻUVES TIESĪBAS

Kas telpu pievieno savam kontam, kļūst par tās administratoru. Telpā var būt līdz 200 lietotājiem, PRO un uzņēmumiem (ar centrāli pēc tās modeļa). Uzaicina administrators, PRO ar konfigurēšanas tiesībām vai instalēšanas uzņēmums.

1. Cilnē "Control" atveriet telpas iestatījumus > "Users" > "Send invites".
2. Ievadiet e-pastu vai izvēlieties "Add from contacts", nospiediet "Continue".
3. Ja personai ir Ajax konts, tā parādās sadaļā "Active users". Ja nav, tā reģistrējas ar šo e-pastu; līdz tam redzama sadaļā "Pending invites".

Loma	Ko var darīt
Administrators ar pilnām tiesībām	Pilna vadība un konfigurēšana, lietotāju un PRO pārvaldība.
Administrators bez konfigurēšanas tiesībām	Vada režīmus, maina paziņojumus, uzaicina lietotājus; sistēmas iestatījumus nemaina.
Lietotājs	Apsardzes ieslēgšana un izslēgšana, trauksmes poga, trauksmju paziņojumi.
PRO (instalētājs, apsardzes uzņēmums)	Ar pilnām tiesībām konfigurē sistēmu. Piekļuvi var dot bez termiņa vai uz 1, 2, 4 vai 8 stundām.

Tiesības maina, pieskaroties lietotājam sarakstā. Ar OS Malevich 2.38 un lietotni 3.43 vai jaunāku sadaļā "Permissions" var dot atsevišķas tiesības (piem., iestatījumi, uzaicināšana, scenāriji, kameras, grupas).

Svarīgi: nedodiet pilnas administratora tiesības trešajām personām pat uz laiku un vienmēr paturiet tās sev. Ajax Systems nevar atjaunot neuzmanības dēļ zaudētu piekļuvi.

9. SCENĀRIJI UN AUTOMATIZĀCIJA

Scenāriji pēc trauksmes, grafika, apsardzes maiņas, temperatūras vai pogas nospiešanas vada automatizācijas ierīces (releji, slēdži, rozetes, WaterStop) vai apsardzi. Tos veido tikai PRO vai lietotājs ar administratora tiesībām.

1. Cilnē "Devices" atveriet automatizācijas ierīces iestatījumus (zobrats) › "Scenarios".
2. Nospiediet "Create scenario" (pirmajam) vai "Add scenario", izvēlieties veidu (piem., "By alarm") un iestatiet nosacījumus un darbību.
3. Nospiediet "Save". Labo vai dzēš, pieskaroties scenārijam sarakstā.

Apsardzi pēc grafika iestata "Control" › telpas iestatījumi › "Scenarios and schedule" › "Security schedule". Pirms tam iestatiet pareizo "Time zone".

- Scenāriju skaits: Hub – 5, Hub 2 – 32, Hub 2 Plus – 64, Superior MegaHub – 100. Katrai ierīcei var būt tikai viena reakcija uz apsardzes maiņu; tā limitā neietilpst.
- Bezsaistē esoša ierīce (piem., strāvas pārrāvumā) nokavēto scenāriju neizpilda arī vēlāk.

10. VIDEO NOVĒROŠANA

- Ajax kameras un NVR var pievienot telpai bez centrāles, katru tikai vienai telpai. Citu ražotāju kamerām vajag centrāli; tās dod tikai RTSP straumi bez arhīva (atbalstīts arī ONVIF).
- Tiesības uz tiešraidi, arhīvu un foto pēc pieprasījuma piešķir telpas iestatījumos "Privacy".

Fragmenta lejupielāde (vajag arhīva tiesības; NVR jābūt diskam; tikai notikumu vai pastāvīgā ieraksta fragmenti):

1. Izvēlieties centrāli, kameru vai NVR kanālu un atveriet arhīvu.
2. Nospiediet "Download", atzīmējiet "Start Here" un "End Here" (3 sekundes līdz 15 minūtes).
3. Nospiediet "Request File". Gatavais fails pieejams 24 stundas.

11. DROŠĪBAS IESTATĪJUMI

Visi iestatījumi: galvenā izvēlne (augšējais kreisais stūris) › "App settings".

Iestatījums	Ko tas dara
"Sessions"	Ierīces, kurās lietots kods. Sesiju beidz, pavelkot pa kreisi › "Terminate", vai visas citas ar "Terminate all other sessions".
"System settings" › "Passcode Lock"	4 ciparu kods (pēc izvēles biometrija) lietotnes atvēršanai.
"Edit account" › "Password"	Paroles maiņa: lielie un mazie burti, cipari, simboli.

1. Divfaktoru autentifikācijai instalējiet autentifikatoru (piem., Google Authenticator, Duo Mobile, Tofu).
2. "App settings" › "Account protection" › "Two-Factor Authentication" › "Enable".

3. Pievienojiet kontu autentifikatoram, ievadiet 6 ciparu kodu (derīgs 30 sekundes) un nospiediet "Verify".

Pēc ieslēgšanas konts citās ierīcēs tiek izrakstīts. Tālruņa laikam jābūt automātiskam, citādi kods tiek noraidīts. Atjauniniet lietotni visās ierīcēs.

12. BIEŽĀKĀS PROBLĒMAS

Problēma	Risinājums
Aizmirsta parole	"Log in" > "Forgot password", ievadiet abus kodus un jauno paroli. Bez piekļuves e-pastam vai tālrunim rakstiet Ajax atbalstam.
Nepienāk push paziņojumi	Pārbaudiet tālruņa atļaujas un lietotāja piekļuvi notikumu plūsmai; trauksmēm ieslēdziet arī SMS un zvanus.
Aizdomas par uzlaušanu	Beidziet pārējās sesijas, nomainiet paroli, ieslēdziet divfaktoru autentifikāciju.

Pilnā ražotāja lietošanas instrukcija: <https://ajax.systems/support/posts/how-to-configure-a-space/>

LIETOŠANAS PAMĀCĪBA

Ajax PRO lietotne

montētājiem un uzstādītājiem (Ajax PRO: Tool for Engineers)

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, piekrītieta 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 līdzi 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 solim 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 saglabājat 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 pārnēst tikai uz tādu pašu vai jaudīgāku modeli. Visi jaunās centrāles dati tiek aizstāti ar vecās datiem. Uzraudzības kanālu iestatījumi netiek pārnēsti; 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/>

LIETOŠANAS PAMĀCĪBA

Ajax PRO Desktop

datora lietotne montētājiem un apsardzes centrālēm

Īss ceļvedis instalatoriem, servisa un monitoringa uzņēmumiem: programmas instalēšana, uzņēmuma un darbinieku pārvaldība, objektu pievienošana un trauksmju apstrāde.

1. PAR LIETOTNI

Ajax PRO Desktop ir Windows un macOS programma neierobežota skaita Ajax sistēmu konfigurēšanai, testēšanai, lietotāju piekļuves pārvaldībai un notikumu uzraudzībai. Monitoringa uzņēmumi ar to organizē centrālo uzraudzības staciju (CMS).

Ierīces un sistēmu var iestatīt arī mobilajā lietotnē Ajax PRO: Tool for Engineers, bet uzņēmumu, darbiniekus, viņu tiesības un monitoringu pārvalda tikai datorprogrammā.

- Objektam (space) pieslēgts uzņēmums skaitās kā viens lietotājs neatkarīgi no darbinieku skaita.
- Vienu PRO kontu var pieslēgt neierobežotam uzņēmumu skaitam, katrā ar citu lomu.

2. SISTĒMAS PRASĪBAS

Parametrs	Windows (minimums / ieteicams)	macOS (minimums / ieteicams)
Operētājsistēma	Windows 10 64 bitu / Windows 11 64 bitu vai jaunāka	macOS Big Sur 11.6 / macOS 15 Sequoia vai jaunāka
Procesors	Intel Core i3 (8. paaudze) vai AMD Ryzen 3 (1000. sērija) / Intel Core i5 (12. paaudze) vai AMD Ryzen 5 (5000. sērija), vai līdzvērtīgs	M1 / M3
Operatīvā atmiņa	8 GB / 16 GB	8 GB / 16 GB
Videokarte	Draiveris ar OpenGL 2.1 vai jaunāku atbalstu	—
Brīva vieta diskā	2 GB / 8 GB	2 GB / 8 GB
Ekrāna izšķirtspēja	1600×900 / 1920×1080	1440×900 / 2560×1600

Svarīgi: kopš 2025. gada jūnija jaunās versijas neatbalsta Windows 7, Windows 8, 32 bitu Windows un macOS Catalina. Šīm sistēmām pēdējā saderīgā versija ir 4.24, tās lejupielādes saiti izsniedz Ajax atbalsta dienests. Ražotājs iesaka operētājsistēmu atjaunināt.

3. INSTALĒŠANA UN PIETEIKŠANĀS

1. Lejupielādējiet instalācijas failu, atveriet to un instalējiet programmu.
2. Ja jums ir PRO konts, ievadiet e-pastu un paroli un nospiediet "Login".
3. Ja konta nav, nospiediet "Create PRO account" un sekojiet norādēm. Kontu var izveidot arī lietotnē Ajax PRO: Tool for Engineers.

Svarīgi: Ajax Security System (gala lietotāja) konts PRO programmā neder. PRO kontam drīkst izmantot to pašu e-pastu un tālruni, tomēr tas būs atsevišķs konts.

Sākuma ekrānā vienmēr redzama poga "Log in with SSO". Vienoto pieteikšanos (SAML) no versijas 5.30 iestata tikai uzņēmuma īpašnieks izvēlnē "Single sign-on (SSO)".

4. SASKARNE UN KONTA DROŠĪBA

- Ir divi kontu veidi: personīgais PRO konts (pieslēgšanās uzņēmumiem un piesaistīto sistēmu iestatīšana) un uzņēmuma konts (monitorings, apkope, uzstādīšana). Programma atver pēdējo izmantoto uzņēmumu; pārslēgties var izvēlnē ar uzņēmuma logotipu vai iniciāļiem.
 - Indikators augšējā labajā stūrī rāda saiti ar Ajax Cloud: zaļš nozīmē, ka savienojums ir, sarkans ar uzrakstu "No Connection" nozīmē, ka tā nav.
 - Moduļi augšējā kreisajā stūrī: "Company", "Objects", "Monitoring", "Journal" un "Services" (piem. Ajax SIM aktivizēšana). Redzami moduļi atkarīgi no lomas.
1. Noklikšķiniet uz PRO konta ikonas, atveriet "Profile Settings" un cilni "Account Security".
 2. Ieslēdziet "Two-factor authentication" un pēc ekrāna norādēm pievienojiet autentifikatoru, piem. Google Authenticator.
 3. Sadaļā "Sessions" pārbaudiet citas ierīces. Svešu sesiju beidziet ar "Terminate" vai "Terminate all other sessions", pēc tam nomainiet paroli un ieslēdziet divfaktoru autentifikāciju.

5. DARBS PERSONĪGAJĀ PRO KONTĀ

Pēc pieteikšanās redzams piesaistīto objektu (spaces) saraksts ar bojājumu skaitītāju. Jaunu objektu piesaista ar "Add Space". Objekti darbojas ar centrālēm, kurām ir OS Malevich 2.6 vai jaunāka, un Ajax PRO Desktop 4.0 vai jaunāku.

- Objekta iestatījumi: izvēlieties objektu un atveriet "Settings" (zobrats).
- Centrāle vai ierīce: izvēlne "Devices" > ierīce > "Settings". Katra iestatījuma nozīme aprakstīta ierīces instrukcijā.
- Lietotāji: objekta iestatījumos izvēlne "Users"; PRO konti un uzņēmumi: izvēlne "Installers/Companies". Abās var pievienot, mainīt tiesības un dzēst.
- Piekļuvi iestatījumiem un kameru video var pieprasīt uz laiku vai pastāvīgi, noklikšķinot uz piekļuves lauka objekta augšējā labajā stūrī. Pieprasījumu apstiprina objekta administrators. Apsardzes režīmus un panikas pogu PRO var lietot, ja administrators to atļāvis.

6. UZŅĒMUMS UN DARBINIEKI

1. Personīgajā PRO kontā atveriet moduli "Company" un nospiediet "Create company".
2. Ievadiet nosaukumu, apkalpošanas valsti un pakalpojuma veidu: "Alarm monitoring", "Installation and maintenance" vai abus. Īpašnieks veidu var mainīt jebkurā laikā, saskarē tam pielāgojas.
3. Norādiet strādājošu e-pastu un pēdējā solī ievadiet uz to atsūtīto kodu. Pēc apstiprināšanas uzņēmums ir gatavs.

Izveidotājs kļūst par "Company owner"; šī loma var būt tikai vienam kontam. Nosaukumu maina tikai ar Ajax atbalsta dienesta palīdzību.

Pakalpojuma veids	Lomas
Alarm monitoring	Company owner, Senior CMS Engineer, Engineer, Head of operators, Operator, Senior Ajax services manager, Ajax services manager
Installation and maintenance	Company owner, Head of installers, Installer
Abi	Visas lomas

- Darbinieku pievieno ar "Company" > "Employees" > "Add employee": ievadiet viņa PRO konta e-pastu, izvēlieties lomu, nospiediet "Add". Bez PRO konta pievienot nevar.
- Īpašumtiesības monitoringa vai uzstādīšanas un monitoringa uzņēmumā nodod tikai pašreizējais īpašnieks (no 5.42): "Employees" > darbinieks > "More" > "Edit" > "Company owner" > "Save". Abi tiek izrakstīti.
- Izvēlnē "Access rights" tiesības piešķir visai lomai. Viedslēdžu vadību, apkopes atskaites un datu eksportu var atļaut tikai īpašnieks.
- Reaģēšanas vienības pievieno ar "Add RRU"; tās incidentus saņem lietotnē Ajax Response.

7. OBJEKTI

1. Modulī "Objects" nospiediet "Add object".
2. Ievadiet objekta numuru, nosaukumu un 20 zīmju centrāles ID (zem QR koda uz centrāles vai iepakojuma). Numurs un ID obligāti ir tikai monitoringa uzņēmuma CMS inženierim.
3. Nospiediet "Add Object" un aizpildiet objekta kartīti.
 - Ar ID pievieno, ja centrāle ir tiešsaistē, objektā nav administratoru vai PRO un centrāle nav piesaistīta citam uzstādīšanas uzņēmumam vai bloķēta citam monitoringa uzņēmumam. Tukšu objektu (tikai nosaukums) var izveidot tikai Installer vai Head of installers.
 - Monitoringa pieprasījumu sūta objekta administrators vai PRO ar iestatīšanas tiesībām Ajax lietotnē: "Control" > objekta iestatījumi > "Security companies". Programmā atveriet "Monitoring requests (from end-users)" vai "(from installers)", nospiediet "Accept request", ievadiet numuru un nosaukumu, saglabāji.
 - Uzstādīšanas pieprasījums nāk caur "Installers/Companies" > "Invite" un nav jāapstiprina. Uzņēmumam ir 8 stundas iestatījumu maiņai, ierīču pievienošanai un lietotāju uzaicināšanai.
 - Ja pilna piekļuve objektiem izslēgta, instalators objektu redz tikai pēc tam, kad Head of installers to piešķir: objektā "Installers" > "Assign" vai "Employees" > darbinieks > "Assigned objects" > "Assign". Instalatora tiesības nevar pārsniegt uzņēmuma tiesības.
 - Laika pagarinājumu (1, 2, 4 vai 8 stundas vai pastāvīgi) instalators pieprasa no Head of installers, kurš to apstiprina tikai Ajax PRO Desktop; ja uzņēmumam tiesību nepietiek, piekļuvi pieprasa objekta administratoram.
 - "Stop monitoring" pārvieto objektu uz "Withdrawn from monitoring", kur to 7 dienas var atjaunot ar "Restore objects" (nav iespējams, ja ir atvērti incidenti). "Stop maintenance" objektu dzēš neatgriezeniski.

8. NOTIKUMU MONITORINGS

Modulis "Monitoring" pieejams lomām Company owner, Senior CMS Engineer, Head of operators un Operator. Jauni incidenti cilnē "New" skan ar sirēnu, līdz tos sāk izskatīt. Incidentu rada trauksmes, korpusa atvēršana, traucēšana, savienojuma vai ārējās barošanas zudums un citi bojājumi.

1. Atveriet incidentu: redzams laiks, ierīce, telpa, foto verifikācija un objekta dati.
2. Nospiediet "Start processing"; incidents pāriet uz cilni "Processing".
3. Noskaidrojiet cēloni: zvaniet atbildīgajām personām ar ārēju programmu (Ajax PRO Desktop tām nezvana), atzīmējiet "Accepted" vai "Not responding" un pārskatiet foto cilnē "MotionCam".
4. Ja trauksme ir patiesa vai cēlonis nav skaidrs, nosūtiet RRU un sekojiet statusam "Dispatched", "Arrived" vai "Unavailable".
5. Žurnāla augšā izvēlieties cēloni (viltus trauksmei "False alarm" vai "No incident"), pēc vajadzības pievienojiet komentāru un pabeidziet. Slēgtu incidentu atvērt atkārtoti nevar.
 - "Sleep Mode" uz 1, 5, 15 vai 30 minūtēm (vai 1–300 minūtēm pēc izvēles) ignorē objekta trauksmes, tās tikai ieraksta žurnālā.
 - "Voice Connect" (no 5.29, centrāle ar OS Malevich 2.33 un SpeakerPhone Jeweller): ieslēdziet lomai "Make and receive calls using voice module" un centrāles "Telephony settings" iestatiet "Allow communication via voice module" ar "Ajax server".

9. VIDEO UN PRIVĀTUMS

- "Video wall" rāda vairāku kameru tiešraidi un arhīvu (ja kamerai vai Ajax NVR ir atmiņa). Atveriet "Video wall" pie objekta nosaukuma un ieslēdziet "Open Video wall widget". No 5.35 vienā sienā var apvienot dažādu objektu kameras.
- Objekta administrators nosaka, kad uzņēmums var skatīt foto un video: jebkurā laikā, tikai tad, kad kopīgotās ierīces ir apsardzē, vai noteiktu laiku pēc trauksmes. Instalators var pieprasīt pagaidu piekļuvi video.
- Mediju glabāšanas periodu (7, 30, 90, 180 dienas, 1 vai 2 gadi) nosaka īpašnieks. Izmaiņas attiecas tikai uz jauniem failiem, periodam jāatbilst vietējiem likumiem.

10. ATSKAITES UN ŽURNĀLS

Apkopes atskaites ir PDF faili par objekta ierīču stāvokli, tikai objektiem ar centrāli. Funkciju ieslēdz īpašnieks, tiesības piešķir izvēlnē "Access rights".

1. "Maintenance reports" cilnē "Objects" atzīmējiet objektus un nospiediet "Create report" > "Create" (regulārai sūtīšanai "Schedule report").
2. Cilnē "Archive" atzīmējiet atskaites un nospiediet "Download selected". Glabājas pēdējās 5 atskaites katram objektam.

Faila prefikss	Nozīme
p	Pārbaude izturēta, bojājumu nav.
pw	Izturēta, bet ir bojājumi; ieteicams inženiera apmeklējums.
f	Nav izturēta; ieteicams inženiera apmeklējums.

- "Export data" izveido CSV: "Object report" vai "Device report". Atļauju dod tikai īpašnieks.
- Modulī "Journal" ir visu objektu notikumi ar filtriem un atskaites "Hubs availability" un "Operators availability". Eksports CSV līdz 1000 notikumiem.

Pilnā ražotāja lietošanas instrukcija: <https://ajax.systems/support/manuals/pro-desktop/>

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.