

kaspersky

Kaspersky Basic | Standard | Plus | Premium

© 2022 AO Kaspersky Lab

Sisu

[Andmete edastamine](#)

[Andmete edastamine lõppkasutaja litsentsilepingu alusel](#)

[Andmete edastamine lõppkasutaja litsentsilepingu alusel Euroopa Liidu, Ühendkuningriigi või Brasíilia territooriumil või California residentide poolt](#)

[Andmete edastamine Kaspersky Security Networki](#)

[Andmete salvestamine rakenduse tegevuse aruandesse](#)

[Andmete salvestamine tehnilise toe jaoks](#)

[Teave rakenduse kasutamise kohta Euroopa Liidus, Ühendkuningriigis, Brasíilias või California residentide poolt](#)

[Teave Kaspersky lahenduste kohta](#)

[Tellimusplaanide võrdlus](#)

[Riistvara- ja tarkvaranõuded](#)

[Ühilduvus teiste Kaspersky rakendustega](#)

[Mis on uut rakenduse uusimas versioonis?](#)

[Kuidas tellimus toimib](#)

[Tellimuse ostmine](#)

[Tellimuse tühistamiseks oma My Kaspersky kontol tehke järgmist.](#)

[Tellimuse tühistamine](#)

[Muu makseviisi määramine](#)

[Seadmes tellimuse aktiveerimine](#)

[Kui otsite tellimuse Kaspersky veebisaidilt](#)

[Kui otsite karbi või aktiveerimiskaardi](#)

[Tellimuse aktiveerimine, kui rakendus on seadmesse juba paigaldatud](#)

[Teie tellimus on aegunud](#)

[Tellimuse uuendamine varuaktiveerimiskoodiga](#)

[Proovitellimuselt tasulisele tellimusele üleminek](#)

[Rakenduse installimine või eemaldamine](#)

[Rakenduse paigaldamine](#)

[Paigaldamine teiste Kaspersky rakenduste peale](#)

[Brauserilaiend Kaspersky Kaitse](#)

[Rakenduse eemaldamine](#)

[Rakenduse uuendamine](#)

[Rohkemate seadmete kaitsmine](#)

[Rakenduse põhifunktsioonid](#)

[Arvutikaitse seisundi hindamine ja turvaprobleemide lahendamine](#)

[Arvuti turbeprobleemide lahendamine](#)

[Turvauudised](#)

[Teave turvauudiste kohta](#)

[Turvauudiste lubamine või keelamine](#)

[My Kasperskys turvauudiste saamise lubamine või keelamine](#)

[Rakenduse tegevuste logi ja üksikasjalik aruanne](#)

[Rakenduse kasutajaliidese seadistamine](#)

[Rakenduse teadete seadistamine](#)

[Rakenduse kujundusteema muutmine](#)

[Rakenduseikooni muutmine](#)

[Juurdepääsu rakenduse haldusfunktsioonidele kaitsmine parooliga](#)

[Rakenduse vaikeseadete taastamine](#)

[Rakenduse seadete rakendamine teises arvutis](#)

[Arvutikaitse peatamine ja jätkamine](#)

[Kaspersky rakenduse hindamine](#)

[Turvalisus](#)

[Arvuti kontrollimine](#)

[Kiirkontrolli käivitamine](#)

[Täiskontrolli käivitamine](#)

[Kohandatud kontrolli käivitamine](#)

[Irdkettakontrolli käivitamine](#)

[Faili või kausta kontekstimenüükontrolli käivitamine](#)

[Taustal toimuva kontrolli sisselülitamine või väljalülitamine](#)

[Kontrollimise ajakava loomine](#)

[Arvutisse paigaldatud rakenduste haavatavuste otsimine](#)

[Kindla faili, kausta või ohutüübi kontrollimisest välja jätmine](#)

[OneDrive'i pilvhoidlas failide kontrollimine](#)

[Viirusekaitse andmebaaside ja rakendusemoodulite uuendamine](#)

[Andmebaaside ja rakendusemoodulite uuendamisest](#)

[Andmebaaside ja rakendusemoodulite uuenduse käivitamine](#)

[Sissetungitõrje](#)

[Sissetungitõrje kohta](#)

[Sissetungitõrje seadete muutmine](#)

[Rakenduse reputatsiooni kontrollimine](#)

[Nõrkade seadete kontroll](#)

[Teave operatsioonisüsteemi nõrkade seadete kohta](#)

[Kuidas leida ja parandada operatsioonisüsteemi nõrku seadeid](#)

[Kuidas lubada nõrkade seadete kontrollimist](#)

[Võrguseire](#)

[Nutikodu monitor](#)

[Komponent Nutikodu monitor](#)

[Nutikodu monitori sisse- ja väljalülitamine](#)

[Minu võrgus olevate seadmete vaatamine](#)

[Seadmele võrgujuurdepääsu keelamine](#)

[Loendist ühendusteta võrgu kustutamine](#)

[Märkuannete keelamine, kui seadmed ühenduvad minu võrguga](#)

[Nutikodu monitori kohta tagasiside saatmine](#)

[Kaspersky-eelne viiruse-eemaldus](#)

[Operatsioonisüsteemi taastamine pärast nakatumist](#)

[Operatsioonisüsteemi veaotsing Microsoft Windowsi veaotsingu nõustaja abil](#)

[Operatsioonisüsteemi avariitaaste](#)

[Kustutatud või desinfitseeritud faili taastamine](#)

[Meili kaitsmine](#)

[Meilide kaitse seadistamine](#)

[Soovimatute meilide \(rämpsmeili\) blokeerimine](#)

[Osalemine Kaspersky Security Networkis](#)

[Kaspersky Security Networkis osalemise lubamine ja keelamine](#)

[Kaspersky Security Networki ühenduse kontrollimine](#)

[Kaitse riistvara virtualiseerimise abil](#)

[Teave riistvara virtualiseerimist kasutava kaitse kohta](#)

[Riistvara virtualiseerimist kasutava kaitse sisselülitamine](#)

[Kaitse Antimalware Scan Interface'i \(AMSI\) abil](#)

[Teave Antimalware Scan Interface'i \(AMSI\) kaitse kohta](#)

[Antimalware Scan Interface'i kaitse lubamine](#)

[Antimalware Scan Interface'i kontrollist skripti väljajätmine](#)

[Arvutikaitse kaughaldus](#)

[Jõudlus](#)

[Kiirkäivitus](#)

[Arvuti kiirendamine](#)

[Rakenduseuuendaja](#)

[Teave rakenduseuuendaja kohta](#)

[Rakenduste uuenduste otsimine](#)

[Rakenduseuuendaja seadete muutmine](#)

[Uuenduste otsingu režiimi seadistamine](#)

[Rakenduseuuenduste loendi vaatamine](#)

[Uuenduse või rakenduse eemaldamine erandite loendist](#)

[Duplikaadid](#)

[Suured failid](#)

[Kasutamata rakendused](#)

[Kõvaketta seisundi jälgimisfunktsioon](#)

[Teave kõvaketta seisundi jälgimisfunktsiooni kohta](#)

[Kõvaketta seisundi jälgimisfunktsiooni sisse- või väljalülitamine](#)

[Kõvaketta seisundi kontrollimine](#)

[Andmete kopeerimine kahjustatud kõvakettalt](#)

[Kõvaketta seisundi jälgimisfunktsiooni piirangud](#)

[Varundamine ja taastamine](#)

[Teave varundamise ja taastamise kohta](#)

[Varundustegumi loomine](#)

[1. etapp. Failide valimine](#)

[2. etapp. Varundatavate kaustade valimine](#)

[3. etapp. Varundatavate failitüüpide valimine](#)

[4. etapp. Varuhoidla valimine](#)

[5. etapp. Varundamise ajakava loomine](#)

[6. etapp. Varukoopiade kaitsmiseks parooli seadmine](#)

[7. etapp. Failiversioonide hoidla seaded](#)

[8. etapp. Varundustegumi nime sisestamine](#)

[9. etapp. Nõustaja lõpuleviimine](#)

[Varundustegumi käivitamine](#)

[Varukoopiast andmete taastamine](#)

[Andmete taastamine FTP-hoidlast](#)

[Kaspersky taastevahendi abil varukoopiast andmete taastamine](#)

[Teave veebihoidla kohta](#)

[Veebihoidla aktiveerimine](#)

[Praegune tegevus](#)

[Režiim „Mitte segada“](#)

[Mängurežiim](#)

[Akusäästja](#)

[Operatsioonisüsteemi koormuse optimeerimine](#)

Privaatsus

[Kaspersky VPN](#)

[Andmelekkedekontroll](#)

[Teave andmelekkedekontrolli kohta](#)

[Andmelekkedekontrolli lubamine või keelamine](#)

[Kuidas kontrollida, kas teie andmed võivad muutuda avalikult kättesaadavaks](#)

[Kuidas luua automaatseks kontrollimiseks kontode loendit](#)

[Privaatne sirvimine](#)

[Teave privaatse sirvimise kohta](#)

[Andmete kogumise blokeerimine](#)

[Kõigil veebisaitidel andmete kogumise lubamine](#)

[Andmete kogumise lubamine erandina](#)

[Andmete internetist kogumise katsete aruande vaatamine](#)

[Veebilehitsejas privaatse sirvimise komponendi haldamine](#)

[Paroolihaldur](#)

[Paroolide kontrollimine ja turvaline säilitamine](#)

[Paroolide turvalisuse kontrollimine](#)

[Paroolide turvalisuse konfigureerimine](#)

[Turvalised maksed](#)

[Teave finantstehingute ja veebiostude kaitsmise kohta](#)

[Turvaliste maksete seadete muutmine](#)

[Kindla veebisaidi jaoks turvaliste maksete seadistamine](#)

[Turvaliste maksete kohta tagasiside saatmine](#)

[Veebikaamera ja mikrofoni kontroll](#)

[Teave rakenduse veebikaamerale ja mikrofoni juurdepääsu kohta](#)

[Rakenduse veebikaamerale või mikrofoni juurdepääsu seadete muutmine](#)

[Veebikaamerale juurdepääsu lubamine või blokeerimine üksiku rakenduse jaoks](#)

[Mikrofoni juurdepääsu lubamine või blokeerimine üksiku rakenduse jaoks](#)

[Nuhkvara tuvastamine](#)

[Ribareklaamifilter](#)

[Teave ribareklaamifiltri kohta](#)

[Ribareklaamifiltri komponendi sisselülitamine](#)

[Ribareklaamide blokeerimine](#)

[Ribareklaamide lubamine](#)

[Ribareklaamifiltri filtrite seadistamine](#)

[Ribareklaamifiltri haldamine veebilehitsejas](#)

[Soovimatute rakenduste installimise blokeerija](#)

[Rakendushalduri seadete muutmine](#)

[Reklaamprogrammide eemaldaja](#)

[Salahoidla](#)

[Teave salahoidla kohta](#)

[Failide teisaldamine salahoidlasse](#)

[Juurdepääs salahoidlas talletatavatele failidele](#)

[Failipurustaja](#)

[Privaatsete jälgede eemaldaja](#)

[Internetis isiklike andmete kaitsmine](#)

[Teave internetis isiklike andmete kaitsmise kohta](#)

[Teave ekraaniklaviatuuri kohta](#)

[Ekraaniklaviatuuri avamine](#)

[Ekraaniklaviatuuri ikooni kuvamise seadistamine](#)

[Teave arvuti klaviatuuri abil sisestatud andmete kaitse kohta](#)

[Arvuti klaviatuuri abil sisestatud andmete kaitse seadistamine](#)

[Veebisaidi ohutuse kontrollimine](#)

[Krüptitud ühenduste seadete muutmine](#)

[Teave Wi-Fi-võrkudega turvalise ühenduse loomise kohta](#)

[Wi-Fi-võrkude haavatavuste kohta teadete seadistamine](#)

[Identiteet](#)

[Identiteeti kaitsev rahakott](#)

[Kaugjuurdepääsu tuvastamine](#)

[Tippklassi tugiteenused](#)

[Ühildumatute rakenduste eemaldamine](#)

[Rakenduse kasutamine käsuviiba abil](#)

[Tehnilise toega ühenduse võtmine](#)

[Tehnilise toe saamine](#)

[Tehnilise toe jaoks teabe kogumine](#)

[Teave teenuse andmefailide sisu ja talletamise kohta](#)

[Jälgimise sisselülitamine](#)

[Piirangud ja hoiatused](#)

[Muud teabeallikad rakenduse kohta](#)

[Välisteenuste ühenduse võrguseaded](#)

[Sõnastik](#)

[Andmepüügilinkide ja võltsitud krüptovaluutavahetuste andmebaas](#)

[Andmepüük](#)

[Arvatav rämpsmeil](#)

[Arvatavalt nakatunud objekt](#)

[Digiallkiri](#)

[Eksploit](#)

[Failimask](#)

[Haavatavus](#)

[Heuristiline analüüs](#)

[Hüperviisor](#)

[iCheckeri tehnoloogia](#)

[Jäljed](#)

[Kaitsekomponendid](#)

[Kaitstud veebilehitseja](#)

[Käivitusobjektid](#)

[Karantiin](#)

[Kaspersky Security Network \(KSN\)](#)

[Kaspersky uuendusserverid](#)

[Ketta alglaadimissektor](#)

[Klaviatuurinuhk](#)

[Liikluse kontrollimine](#)

[Nakatunud objekt](#)

[Objekti blokeerimine](#)

[Ohu tase](#)

[Pahatahtlike veebiaadresside andmebaas](#)

[Protokoll](#)
[Rakenduse aktiveerimine](#)
[Rakendusemoodulid](#)
[Rämpsmail](#)
[Rootkit](#)
[Salahoidla](#)
[Skript](#)
[Tegum](#)
[Tegumi seaded](#)
[Tihendatud fail](#)
[Tundmatu viirus](#)
[Turvatase](#)
[Ühildumatu rakendus](#)
[Usaldusgrupp](#)
[Usaldusväärne protsess](#)
[Uuendus](#)
[Uuenduspakett](#)
[Valehäire](#)
[Varundamine ja taastamine](#)
[Viirus](#)
[Viirusekaitse andmebaasid](#)
[Teave kolmanda osapoole koodi kohta](#)
[Kaubamärgiteated](#)

Andmete edastamine

See jaotis sisaldab teavet konkreetsete andmete kohta, mille Kasperskyle rakenduse kasutamise ajal edastate. Alamjaotis [Andmete salvestamine rakenduse tegevuse aruandesse](#) sisaldab andmeid, mis talletatakse teie arvutis kohapeal ja mida ei saadeta Kasperskyle.

Andmete edastamine lõppkasutaja litsentsilepingu alusel

See jaotis sisaldab teavet konkreetsete andmete kohta, mis edastatakse Kasperskyle, kui olete paigaldanud rakenduse versiooni, mis pole ette nähtud kasutamiseks Euroopa Liidus, Ühendkuningriigis, Brasiilias ega California residentidele.

[Plaani Kaspersky Basic andmed](#) 

[Plaani Kaspersky Standard andmed](#) 

[Plaanide Kaspersky Plus ja Kaspersky Premium andmed](#) 

Kaspersky kaitseb saadud infot vastavalt Kaspersky juriidilistele nõuetele ja kohaldatavatele reeglitele. Andmed edastatakse krüptitud kanalite kaudu.

Selleks, et tõsta turbetaadlikkust uute ohtudest ja nende allikate kohta ning parandada teie seadme kaitsetaset ja toote toimimist, on õiguste valdajal teie nõusolekul, mis on sõnaselgelt kinnitatud Kaspersky Security Networki andmete kogumise avalduses, selgesõnaline õigus sellist teavet saada. Kaspersky Security Networki teenuse saab installimise ajal deaktiveerida. Samuti saab Kaspersky Security Networki teenuse tarkvara seadete aknas igal ajal aktiveerida või inaktiveerida.

Lisaks tunnistate ja nõustute, et õiguste valdaja kogutud teavet võib kasutada turvariskide suundumuste jälgimiseks ja avaldamiseks õiguste valdaja ainuisikulise äranägemise järgi.

Kui te ei soovi, et tarkvara poolt kogutud teave saadetakse õiguste valdajale, ei tohi te Kaspersky Security Networki teenust aktiveerida ja/või inaktiveerida.

Andmete edastamine lõppkasutaja litsentsilepingu alusel Euroopa Liidu, Ühendkuningriigi või Brasiilia territooriumil või California residentide poolt

See jaotis sisaldab teavet konkreetsete andmete kohta, mis edastatakse Kasperskyle, kui olete paigaldanud rakenduse versiooni, mis on ette nähtud kasutamiseks Euroopa Liidus, Ühendkuningriigis, Brasiilias või California residentidele. **Selles jaotises nimetatud teave ei sisalda kasutaja isiklikke andmeid ja on vajalik õiguse valdaja tarkvara kasutamiseks, kui pole selgelt öeldud teisiti.**

Reaalajas kaitse kvaliteedi parandamiseks, tarkvara töö kvaliteedi parandamiseks ning vastavalt kasutajate arvule tarkvara paigaldamise, eemaldamise ja uuendamise mehhanismiga seotud tõrgete kiireks tuvastamiseks ja lahendamiseks nõustute rakenduse kasutamise ajal esitama Kasperskyle automaatselt järgmised andmed.

[Plaanide Kaspersky Basic ja Kaspersky Standard andmed](#) 

[Plaanide Kaspersky Plus ja Kaspersky Premium andmed](#) 

Internetis maksetehinguid tegeva kasutaja kaitse kvaliteedi parandamiseks nõustute esitama finantsveebisaidile automaatselt teabe tarkvara nime ja versiooni ning tarkvara kohandamiseseade, finantsveebisaidi avamiseks kasutatud veebilehitseja tarkvaralisandmooduli ID ning turvalise veebilehitseja või tavaveebilehitseja kasutamist tähistava ID kohta.


Õiguse valdaja kaitseb saadud teavet seaduses ettenähtud viisil ja see teave on vajalik litsentsi alusel kasutamiseks kättesaadavaks tehtud tarkvara toimimiseks.

Kaspersky võib saadud teabe põhjal hangitud statistilisi andmeid kasutada arvutiturbeohtude arengusuundade jälgimiseks ja nende ohtude kohta aruannete avaldamiseks.

Andmete edastamine Kaspersky Security Networki

Kaspersky Security Networki edastatavate andmete ulatust on kirjeldatud Kaspersky Security Networki avalduses.

Kaspersky Security Networki avalduse vaatamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake rakenduse akna allosas nuppu .
Avatakse aken **Seaded**.
3. Valige **Turvaseaded** → **Kaspersky Security Network**.
Avaneb aken **Kaspersky Security Network**, milles kuvatakse Kaspersky Security Networki üksikasjad ja Kaspersky Security Networkis osalemise seaded.
4. Kaspersky Security Networki avalduse teksti avamiseks klõpsake linki **Kaspersky Security Networki avaldus**.

Andmete salvestamine rakenduse tegevuse aruandesse

Aruandefailid võivad sisaldada isikuandmeid, mis on saadud kaitsekomponentide (nt Failide kaitse, Meilide kaitse, Turvaline sirvimine ja Rämpseilifilter) töö käigus.

Aruandefailid võivad sisaldada järgmisi isiklikke andmeid.

- Kasutaja seadme IP-aadress
- Veebisirvimisajalugu
- Blokeeritud lingid
- Sõnumite ajalugu suhtlusvõrkudes
- Veebilehitseja ja operatsioonisüsteemi versioonid
- Küpsiste ja muude failide nimed ning nende teed
- Meiliaadress, saatja, sõnumi teema, sõnumi tekst, kasutajanimed ja kontaktide loend

Kui kasutate komponenti Laste kaitse, Nutikodu monitor või Turvauudised, esitate järgmised andmed.

- Wi-Fi-võrgu ID, Wi-Fi-võrgu olek, seadme ID, seadme MAC-aadressi räsi, seadme olek;
- teave külastatud veebisaitide kohta;
- teave faili arvutis käivitamise kordade arvu kohta (faili populaarsus).

Aruandefaile talletatakse arvutis kohapeal ja neid ei edastata Kasperskyle. Aruandefailide tee: %allusersprofile%\Kaspersky Lab\AVP21.8\Report\Database.

Aruanded salvestatakse järgmistesse failidesse.

- reports.db
- reports.db-wal
- reports.db-shm (ei sisalda isiklike andmeid)

Aruandefailid on volitamata juurdepääsu eest kaitstud, kui Enesekaitse on Kasperskys sisse lülitatud. Kui enesekaitse on keelatud, pole aruandefailid kaitstud.

Andmete salvestamine tehnilise toe jaoks

Rakendus töötleb ja talletab tehnilisel toel täpsema analüüsi tegemise võimaldamiseks järgmisi isiklike andmeid.

- Rakenduse kasutajaliideses kuvatavad andmed.
 - My Kasperskyga ühenduse loomiseks kasutatud meiliaadress
 - Eranditesse lisatud veebisaidiaadressid (kuvatatakse ohutu sirvimise, ribareklaamifiltri, privaatsuse sirvimise ja võrgu komponentides ning aknas „Aruanded“)
 - Litsentsi andmed

Need andmed salvestatakse kohapeal muutmata kujul ja neid saab vaadata arvuti igal kasutajakontol.

- Andmed rakenduse protsesside süsteemimälu kohta mäluühendamise loomishetkel.
- Jäljejälituse lubamise korral kogutavad andmed.

Need andmed salvestatakse kohapeal muudetud kujul ja neid saab vaadata arvuti igal kasutajakontol. Need andmed edastatakse Kasperskyle ainult teie nõusolekul, kui võtate ühendust tehnilise toega. Andmete kohta lisateabe saamiseks klõpsake aknas **Kasutajatoe tööriistad** linki **Tehnilise toe avaldus**.

Teave rakenduse kasutamise kohta Euroopa Liidus, Ühendkuningriigis, Brasiilias või California residentide poolt

Rakenduse versioonid, mida Kaspersky ja meie partnerid levitavad Euroopa Liidus, Ühendkuningriigis, Brasiilias (samuti versioonid, mis on mõeldud kasutamiseks California residentidele), vastavad nendes piirkondades kehtestatud isiklike andmete kogumist ja töötlemist reguleerivate õigusaktide nõuetele.

Rakenduse paigaldamiseks peate nõustuma lõppkasutaja litsentsilepingu ja privaatsuspoliitika tingimustega.

Lisaks palub paigaldusnõustaja teil nõustuda järgmiste lepingutega teie isiklike andmete töötlemise kohta.

- Kaspersky Security Networki avaldus. See avaldus võimaldab Kaspersky ekspertidel teie kaitse parandamiseks saada kiiresti teavet teie arvutis tuvastatud ohtude kohta, käitatavate rakenduste ja allalaaditavate allkirjastatud rakenduste kohta, samuti teavet operatsioonisüsteemi kohta.
- Turundamise jaoks andmete töötlemise avaldus. See avaldus võimaldab meil luua teie jaoks väärtuslikumaid pakkumisi.
- Rämpseilifiltri kasutamisel andmete töötlemise avaldus. See avaldus võimaldab Kaspersky ekspertidel võtta vastu andmeid, mis aitavad täiustada rämpsseilifiltri komponenti.

Kaspersky Security Networki avaldusega ja turundamise jaoks andmete töötlemise avaldusega saate igal ajal nõustuda või neist keelduda aknas **Seaded** → **Turvaseaded** → **Kaspersky Security Network**.

Teave Kaspersky lahenduste kohta

Meie uued lahendused kajastavad meie visiooni moodsast küberturvalisusest. Lisaks uutele nimedele leiame uue kasutajaliidese ja palju uusi funktsioone.

Lahendused on esitatud mitme plaaniga. Plaanid erinevad kaitsetaseme ning kasutajatele pakutavate funktsioonide ja teenuste arvu poolest. Plaanid sisaldavad nii uusi kui ka järeleproovitud funktsioone, mis jagunevad kolme kategooriasse.

Tutvuge igas kategoorias saadaolevate funktsioonidega:

- [Turvalisus](#)
- [Jõudlus](#)
- [Privaatsus](#)

Tellimusplaanide võrdlus

Rakendus pakub nelja tellimusplaani. Järgmises tabelis on loetletud iga tellimusplaaniga saadaolevad rakenduse funktsioonid.

Tellimusplaanid

Funktsioon	Basic	Standard	Plus	Premium
My Kaspersky	✓	✓	✓	✓
Turvalisus				
Kiirkontroll	✓	✓	✓	✓
Täiskontroll	✓	✓	✓	✓
Valikuline kontroll	✓	✓	✓	✓
Irdkettakontroll	✓	✓	✓	✓
Taustal toimuv kontroll	✓	✓	✓	✓
Haavatavuste kontroll	✓	✓	✓	✓
Failide kaitse	✓	✓	✓	✓
Turvaline sirvimine	✓	✓	✓	✓
Meilide kaitse	✓	✓	✓	✓
Andmebaaside ja rakendusemoodulite uuendus	✓	✓	✓	✓
Aruanded	✓	✓	✓	✓
Karantiin	✓	✓	✓	✓
Microsoft Windowsi veaotsing	✓	✓	✓	✓
Hädaabitaaste	✓	✓	✓	✓
Eksploitide tõkestus	✓	✓	✓	✓
Süsteemiseire	✓	✓	✓	✓

Nõrkade seadete kontroll	✓	✓	✓	✓
Võrgurünnakute tõrje	✓	✓	✓	✓
URL-i nõustaja	✓	✓	✓	✓
Laiend Kaspersky Kaitse	✓	✓	✓	✓
Sissetungitõrje		✓	✓	✓
Tulemüür		✓	✓	✓
Võrguseire		✓	✓	✓
Nutikodu monitor			✓	✓
Andmepüügivastane kaitse		✓	✓	✓
Turvauudised		✓	✓	✓
Jõudlus				
Kiirkäivitus		✓	✓	✓
Arvuti kiirendamine		✓	✓	✓
Duplikaadid		✓	✓	✓
Suured failid		✓	✓	✓
Kasutamata rakendused		✓	✓	✓
Rakenduse värskendusprogramm		✓	✓	✓
Praegune tegevus		✓	✓	✓
Mängurežiim		✓	✓	✓
Režiim Ära sega		✓	✓	✓
Akusäästja		✓	✓	✓
Kõvaketta seisundi jälgimisfunktsioon			✓	✓
Varundamine ja taastamine			✓	✓
Privaatsus				
Andmelekkekontroll	üks konto	üks konto	✓	✓
Privaatne sirvimine		✓	✓	✓
Turvalised maksed		✓	✓	✓
Veebikaamera ja mikrofoni kontroll		✓	✓	✓
Mobiilnuhkvara tuvastus		✓	✓	✓
Soovimatute rakenduste installimise blokeerija		✓	✓	✓
Reklaamvara eemaldi		✓	✓	✓
Ribareklaamifilter		✓	✓	✓
Privaatsete jälgede eemaldaja		✓	✓	✓
Kaspersky VPN			✓	✓
Paroolihaldur			✓	✓
Failipurustaja			✓	✓

Salahoidla			✓	✓
Identiteet				
Identiteeti kaitsev rahakott				✓
Kaugjuurdepääsu tuvastamine				✓
Tippklassi tugiteenused				✓

Riistvara- ja tarkvaranõuded

Üldised nõuded:

- 1500 MB vaba ruumi kõvakettal
- SSE2-käsustikku toetav protsessor (v.a ARM).
- Internet (rakenduse paigalduseks ja aktiveerimiseks, Kaspersky Security Networki kasutamiseks ning andmebaaside ja rakendusmoodulite uuendamiseks)
- Microsoft Windows® Installer 4.5 või uuem
- Microsoft .NET Framework 4 või uuem
- Microsoft .NET Desktop Runtime 5.x (5.0.10 või uuem).
- [Veebikaamera juurdepääsu kaitse on tagatud ainult](#) ühilduvatele veebikaamera mudelitele

Operatsioonisüsteemi nõuded

Operatsioonisüsteem	Protsessor	Vaba operatiivmälu (RAM)	Piirangud
Microsoft Windows 11 Home (21H2, 22H2)	1 GHz või kiirem	4 GB (64-bitise operatsioonisüsteemi korral)	Windows Subsystem for Linux 2 (WSL2) ei ole toetatud.
Microsoft Windows 11 Enterprise (21H2, 22H2)			
Microsoft Windows 11 Pro (21H2, 22H2)			
Microsoft Windows 10 Home (versioonid: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)	1 GHz või kiirem	1 GB (32-bitised operatsioonisüsteemid) või 2 GB (64-bitised operatsioonisüsteemid)	
Microsoft Windows 10 Enterprise (versioonid: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			
Microsoft Windows 10 Pro (versioonid: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			
Microsoft Windows 8.1 (hoolduspakett Service Pack 0 või uuem, uuendus Windows 8.1 Update)	1 GHz või kiirem	1 GB (32-bitised operatsioonisüsteemid) või 2 GB (64-bitised operatsioonisüsteemid)	
Microsoft Windows 8.1 Pro (hoolduspakett			

Service Pack 0 või uuem, uuendus Windows 8.1 Update)			
Microsoft Windows 8.1 Enterprise (hoolduspakett Service Pack 0 või uuem, uuendus Windows 8.1 Update)			
Microsoft Windows 8 (hoolduspakett Service Pack 0 või uuem)	1 GHz või kiirem	1 GB (32-bitised operatsioonisüsteemid) või 2 GB (64-bitised operatsioonisüsteemid)	
Microsoft Windows 8 Pro (hoolduspakett Service Pack 0 või uuem)			
Microsoft Windows 8 Enterprise (hoolduspakett Service Pack 0 või uuem)			
Microsoft Windows 7 Starter (hoolduspakett Service Pack 0 või uuem)	1 GHz või kiirem	1 GB (32-bitised operatsioonisüsteemid) või 2 GB (64-bitised operatsioonisüsteemid)	
Microsoft Windows 7 Home Basic (hoolduspakett Service Pack 0 või uuem)			
Microsoft Windows 7 Home Premium (hoolduspakett Service Pack 0 või uuem)			
Microsoft Windows 7 Professional (hoolduspakett Service Pack 0 või uuem)			
Microsoft Windows 7 Ultimate (hoolduspakett Service Pack 0 või uuem)			

Ohutu sirvimise, ribareklaamifiltri ja turvaliste maksete kaitsekomponentide töö tagamiseks peab operatsioonisüsteemis töötama Base Filtering Engine.

Brauseri tugi

Laiendust Kaspersky Kaitse toetavad järgmised veebilehitsejad:

- Chromium-põhine Microsoft Edge 77.x – 104.x;
- Mozilla™ Firefox™ 52.x – 105.x;
- Mozilla™ Firefox™ ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x;
- Google Chrome™ 48.x – 105.x.

Ekraaniklaviatuuri ja krüptitud ühenduse kontrollimist toetavad järgmised veebilehitsejad:

- Chromium-põhine Microsoft Edge 77.x – 104.x;
- Mozilla Firefox 52.x – 105.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x; 102.x;
- Google Chrome 48.x – 105.x.

Kaitstud veebilehitseja režiimi toetavad järgmised veebilehitsejad:

- Microsoft Internet Explorer 11.0;
- Chromium-põhine Microsoft Edge 77.x – 104.x;
- Mozilla Firefox 52.x – 105.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x;
- Google Chrome 48.x – 105.x
- Yandexi veebilehitseja 18.3.1–22.9.1 ([piirangutega](#)).

Veebilehitsejate uuemad versioonid võivad olla toetatud, kui veebilehitseja vastavat tehnoloogiat toetab.

Kaspersky toetab Google Chrome'i ja Mozilla Firefoxi nii 32-bitistes kui ka 64-bitistes operatsioonisüsteemides.

Nõuded tahvelarvutitele

- Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10, Microsoft Windows 11
- Intel® Celeron®-i protsessor, taktsagedusega 1,66 GHz või kiirem
- 1000 MB vaba operatiivmälu (RAM)

Nõuded netbookidele

- Intel Atom™-i protsessor, 1,60 GHz või kiirem
- 1024 MB vaba operatiivmälu (RAM)
- 10,1-tolline ekraan kuvaeraldusvõimega 1024x768
- Intel GMA 950 graafikatuum või uuem

Nõuded Kaspersky Password Manageri jaoks on saadaval [selle rakenduse abifailides](#).

Ühilduvus teiste Kaspersky rakendustega

Kaspersky ühildub järgmiste Kaspersky rakendustega:

- Kaspersky Safe Kids 1.5
- Kaspersky Password Manager 10
- Kaspersky Software Updater 2.1
- Kaspersky Virus Removal Tool 2015, 2020
- Kaspersky VPN Secure Connection 4.0, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8.

Mis on uut rakenduse uusimas versioonis?

Rakenduse uusimas versioonis on järgmised uued funktsioonid ja parandused.

- Audiovoo kaitsefunktsiooni nimetatakse nüüd mikrofoni kontrolliks, leiata selle jaotise Privaatsus punktist Veebikaamera ja mikrofoni kontroll.
- Funktsiooni Seadmed minu võrgus uus nimi on Nutikodu monitor. Kasutaja poolt lisatavate seadmetüüpide loetelu on laiendatud.
- Kaspersky Premiumis
 - Kaitset Wi-Fi-võrguga ühenduse loomisel on parandatud. Rakendus tuvastab nüüd Wi-Fi-võrgu seaded, mis ei ole piisavalt turvalised.
 - Lisatud on arvutis olevate kaugjuurdepääsurakenduste tuvastamise funktsioon.
- Uus aken näitab selgitust selle kohta, kuidas automaatne uuendamine toimib.
- Parandatud on muudelt platvormidelt Kaspersky rakendusele ülemineku stsenaariumi. Link ei vii teid enam My Kasperskysse, vaid avab teisel platvormil otse akna rakenduse allalaadimiseks.
- Parandatud on viga, mille puhul WPA3 protokoll tuvastati ebaturvalisena.
- Täiustatud on arvuti taaskäivitamise vajadusega seotud teatisi.

Kuidas tellimus toimib

Kuidas tasuline tellimus toimib

Tellimus uueneb automaatselt iga perioodi lõpus, kui te seda ei tühistate. Kui tasuline periood hakkab lõppema, saadame teile meili meeldetuletusega varsti võetava tasu kohta. Järgmise perioodi eest tasumine toimub enne praeguse perioodi lõppu, et saaksite nautida püsivat kaitset küberohtude eest. Kui tellimus on edukalt uuendatud, lisatakse jooksva perioodi järelejäänud päevad uuele perioodile.

Pange tähele, et tellimuse hind võib erineda. Uuendamise hetkel võivad olla saadaval eripakkumised ja allahindlused, mis ei mõjuta teie tellimust.

Kuidas tasuta tellimus toimib

Tasuta proovitellimus aktiveerub kohe, kui tellite. Mõned päevad enne prooviperioodi lõppu saadetakse teile meeldetuletus tellimuse uuendamise kohta. Kui te prooviperioodi jooksul tellimust ei tühistate, siis uuendatakse tellimust pärast prooviperioodi lõppu automaatselt järgmiseks perioodiks.

Kui maksega on probleeme

Kui tellimust ei saa mingil põhjusel automaatselt uuendada (teie pangakaart on aegunud, blokeeritud või automaatne uuendamine on keelatud), võidakse teile anda ajapikendus, et saaksite tellimust uuendada, kui see aegub; ajapikenduse kehtivuse ajal saate rakenduse kõiki funktsioone ilma piiranguteta edasi kasutada. Kui te pole oma tellimust uuendanud, võib rakendus ajapikendusperioodi lõppemisel lülituda [piiratud funktsionaalsusega režiimi](#). Piiratud funktsionaalsusega režiimi kestus oleneb teie piirkonnast ja litsentsitingimustest. Ajapikendusperioodi aegumiskuupäeva ja piiratud funktsionaalsusega režiimi kohta leiate teavet jaotisest [Profil](#).

[Teave teenusepakujatelt ostetud tellimuste kohta](#)

Tellimuse saate hankida teenusepakujalt (nt oma internetiteenuse pakujalt). Tellimust saate peatada või jätkata, automaatselt uuendada või tühistada. Te saate hallata oma tellimust oma kontol selle teenusepakkuja veebisaidil, kes teile tellimuse müüs. Olenevalt tellimuse pakujast võivad tellimuse haldusvalikud erineda.

Tellimuse seadmes aktiveerimiseks rakendage teenusepakujalt saadud aktiveerimiskood. Mõnel juhul saab aktiveerimiskoodi automaatselt alla laadida ja rakendada.

Kui ostate teenusepakujalt tellimuse, ent teine tellimus on rakenduses juba aktiivne, kasutatakse rakendust teenusepakujalt saadud tellimusega. Oma praegust tellimust saate kuni selle aegumiseni edasi kasutada mõnes muus seadmes.

Tellimus võib olla piiranguteta (ilma aegumiskuupäevata) või piiratud kestusega (nt üheks aastaks). Piiranguteta tellimusi uuendatakse automaatselt eeldusel, et teenusepakujale on tehtud õigeaegne ettemakse. Rakenduse edasi kasutamiseks pärast piiratud tellimuse aegumist peate seda ise uuendama.

Rakenduse kasutamisel teenuseosutajalt saadud tellimusega ei saa tellimuse jätkamiseks varuaktiveerimiskoodi lisada.

Kui te ei uuendanud tellimust või kui teenusepakkuja ei saanud teie tellimust automaatselt uuendada, võidakse pärast selle aegumist teile pakkuda ajapikendusperioodi, mille jooksul saate tellimust uuendada; rakenduse kõik funktsioonid töötavad ajapikendusperioodi vältel edasi. Pärast ajapikendusperioodi lõppemist võib rakendus üle minna piiratud funktsionaalsusega režiimi. Kui teenusepakkuja ei paku ajapikendusperioodi ega piiratud funktsionaalsusega režiimi, ei saa te rakenduse funktsioone pärast tellimuse aegumist edasi kasutada.

[Teave App Store'ist, Google Playst või Huawei AppGalleryst ostetud tellimuste kohta](#)

Kui ostate tellimuse App Store'i, Google Play või Huawei AppGallery kaudu, saate tellimuse üksikasju vaadata vastavas rakendusepoes.

Tellimuse ostmine

Rakenduse tellimuse saamiseks on mitu võimalust:

[Ostke Kaspersky veebisaidilt](#)

Rakenduse tellimuse saate osta Kaspersky veebisaidilt:

[Ostke Kaspersky Basic](#)

[Ostke Kaspersky Standard](#)

[Ostke Kaspersky Plus](#)

[Ostke Kaspersky Premium](#)

Kaspersky Premium pole mõnes piirkonnas saadaval.

[Ostke rakenduse liidese abil](#)

Tellimuse ostmiseks rakenduse liidese:

1. Avage rakenduse peaaken.
2. Avage jaotis **Profil**. Kui teie seade on ühendatud teie My Kaspersky kontoga, kuvatakse siin teie meiliaadress.
3. Valiku Tellimuse teave all klõpsake nuppu **Osta kohe**.

Vaikebrauseris avaneb Kaspersky või mõne meie partneri veebisait. Järgige veebisaidil olevaid juhiseid.

[Ostmine Kaspersky partnerilt](#)

Tellimuse saate osta [Kaspersky partneri](#) poest.

Tellimuse tühistamiseks oma My Kaspersky kontol tehke järgmist.

Teil on rakenduse kasutamiseks vaja *My Kaspersky kontot*.

Olenevalt teie tellimusest võib juhtuda, et peate mõnele või kõigile rakenduse funktsioonidele juurdepääsu saamiseks seadme, millele rakendust paigaldate, ühendama oma My Kaspersky kontoga.

Oma My Kaspersky kontol saate teha järgmist.

- Vaadake teavet tellimuste ja nende kehtivusaja lõppemise kohta.
- [Seadmete kaitse kaughaldus](#).
- Kaspersky Password Manageri kasutamisel oma paroole ja muud isiklikku teavet turvaliselt salvestada ja sünkroonida.
- Laadida alla ostetud rakendusi.
- Tehnilise toega ühendust võtta.
- Tutvuda Kaspersky uute rakenduste ja eripakkumistega.

Lisateavet My Kaspersky konto kõigi funktsioonide kohta vaadake jaotisest [My Kaspersky abi](#).

Seadme ühendamine My Kaspersky kontoga

Kui ostsite tellimuse Kaspersky veebisaidilt, loodi ostuprotsessi käigus konto. Ostmisel määratud meiliaadressile saadeti parooli loomise lingiga meil.

Saate oma My Kaspersky kontole sisse logida oma meiliaadressi ja parooliga või Google'i, Facebooki või Apple'i kontoga. Kui teil juba on konto, saate oma Google'i, Facebooki või Apple'i kontoga kiirsisselogimise seadistada aknas, mida kasutatakse seadme ühendamiseks My Kaspersky kontoga. See on võimalik siis, kui kasutasite My Kaspersky konto loomisel oma Google'i, Facebooki või Apple'i konto meiliaadressi.

Facebooki ja Google'iga sisselogimine pole osades piirkondades saadaval.

Kui teil pole veel kontot, saate selle luua seadme kontoga ühendamisel. Kontole sisselogimiseks saate kasutada ka teiste Kaspersky ressursside mandaate.

Seadme ühendamiseks My Kaspersky kontoga tehke järgmist.

1. Seadme saate oma kontoga ühendada järgmiselt.
 - Ühenduse aknas rakenduse aktiveerimisel
 - Rakenduse kasutajaliidese jaotises **Profil**.
Klõpsake jaotises **Logi My Kasperskysse sisse** nuppu **Logi sisse**.
 - [My Kaspersky veebisaidil](#)
 - Rakenduse teatud funktsioonide aktiveerimisel
2. Valige konto ühendamise aknas teile kõige mugavam ühendusviis.

- **Logige sisse meiliaadressiga.** Sisestage tekstiboksi oma meiliaadress. Määratud meiliaadressile saadetakse parooliloomislingiga sõnum.

Kui seadistate oma My Kaspersky kontol kaheastmelise kinnitamise, saadetakse teie telefoni kinnituskoodi sisaldav tekstisõnum. Sisestage sisestusväljale kinnituskood ja klõpsake **Jätka**.

- **Logige sisse Google'i, Facebooki või Apple'i kontoga.**

a. Klõpsake nuppu **Sisene Google'iga, Logi sisse Facebookiga, või Sisene Apple'iga.**

See avab brauseriakna; logige selles aknas sisse oma Google'i, Facebooki või Apple'i kontole ja andke rakendusele juurdepääs teie meiliaadressile.

Kui teil pole Google'i, Facebooki või Apple'i kontot, saate selle luua ja jätkata My Kasperskysse kiirsisselogimise seadistamist.

Kui teie My Kaspersky konto jaoks on seadistatud kaheastmeline kinnitamine, seadistage My Kaspersky veebisaidil oma kontol kiirsisselogimine, seejärel minge tagasi rakendusse ja logige sisse Google'i, Facebooki või Apple'i kontoga.

Kui kasutate brauserit Microsoft Edge, vajate My Kasperskysse sisselogimise seadistamiseks Microsoft Edge'i versiooni, mis põhineb versioonil Chromium 77.x või uuemal versioonil. Ühendusvea korral valige vaikebrauseriks muu brauser, installige brauseri Microsoft Edge uusim versioon või värskendage Microsoft Windowsi operatsioonisüsteemi.

b. Minge tagasi rakendusse ja jätkake konto loomist, klõpsates nuppu **Jätka**. Järgige järgmisi ekraanil kuvatavaid juhiseid.

Teie seadmes luuakse ühendus teie My Kaspersky kontoga. Lisaks saate My Kaspersky veebisaidil oma kontole parooli seadistada.

Andmetöötlus kontole sisselogimisel

Kui logite sisse oma My Kaspersky kontole Google'i, Facebooki või Apple'iga, töödeldakse järgmisi andmeid:

- Õiguste omaniku ressursi ID
- Kinnitustaotluse jaoks loodud väärtus
- Loa tüüp
- URI, millele saadetakse autentimisteenuse pakkuja vastus

Kui logite teenusepakkuja veebisaidil kontole sisse autentimisteenuse pakkuja kaudu, töödeldakse järgmisi andmeid:

- Õiguste omaniku ressursi ID
- Teenusepakkuja infrastruktuuris autoriseerimiseks kasutatav luba
- Loa tüüp
- Autentimisteenuse pakkujatelt taotletud parameetrid
- URI, millele saadetakse autentimisteenuse pakkuja vastus

[Mõnes piirkonnas](#) palub rakendus teil lugeda veebiportaali kasutamise eesmärgil andmete töötlemist käsitlevat avaldust ja sellega nõustuda. Kui nõustute avalduse tingimustega, klõpsake **Nõustu**.

Tellimuse tühistamine

Tellimuse saate igal ajal tühistada. Tühistatud tellimust ei uuendata automaatselt ja teie seadmed on kaitstud kuni viimase tasutud perioodi lõppemiseni.

Tarbetute kulutuste vältimiseks on soovitatav tellimus tühistada enne järgmise perioodi maksekuupäeva. Pange tähele, et järgmise perioodi makse tehakse enne jooksva perioodi lõppemist, et tagada katkestusteta kaitse.

[Tellimuse tühistamine Venemaal, Valgevenes, Abhaasias, Armeenias, Aserbaidžaanis, Gruusias, Lõuna-Osseetias, Kõrgõzstanis, Mongoolias, Tadžikistanis, Türkmenistanis, Usbekistanis, Kasahstanis](#) 

Tellimuse tühistamiseks tehke järgmist.

1. Otsige postkastist meiliaadressi, mille määrasite ostu sooritamisel. Tellimuse kinnitussõnumist või tellimuse uuendamise meeldetuletuse teatest leiate lingi oma kontole või lingi oma automaatse uuendamise halduslehele.
2. Klõpsake linki.
Teid suunatakse vaikebrauseris teie isikupärastatud lehele maksepakkuja veebisaidil.
3. Saate oma tellimuse tühistada uuendamise teabega lehel.
Tellimus on tühistatud. Teie meiliaadressile saadetakse tühistamise kinnitusmeil.

[Tellimuse tühistamine teistes riikides](#) 

Tellimuse tühistamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Profil**.
3. Valiku Tellimuse teave all klõpsake nuppu **Halda kontot**. Kui te ei ühendanud oma seadet oma kontoga, klõpsake nuppu **Logi sisse**.
Avaneb My Kaspersky kontole sisselogimisaken.
4. Avage oma My Kaspersky kontol jaotis **Tellimused** ja klõpsake tellimuspaneelil.
Avaneb tellimuse üksikasjade aken.
5. Klõpsake nuppu **Tellimuse haldamine**.
Valige rippmenüüst **Tühista tellimus**. Järgige ekraanil kuvatavaid juhiseid.

Tellimus on tühistatud.

Kui tühistate oma tellimuse pärast automaatse makse tegemist järgmise perioodi eest, jääb tellimus aktiivseks kuni järgmise perioodi lõpuni. Kui soovite tühistada makse juba tasutud perioodi eest, saate taotleda raha tagastamist rahatagastuspoliitika kohaselt. Tavaliselt saate raha tagasi 30 päeva jooksul alates makse sooritamiseast. Tagasimakse tingimuste ja saadavuse kohta lisateabe saamiseks võtke ühendust tehnilise toega.

Tagasimakse taotlemisel peate esitama järgmise teabe:

- Ostukuupäev
- Teie nimi ja meiliaadress, mida kasutati ostu sooritamisel
- Tellimuse number

Pärast esitatud teabe kontrollimist kulub raha laekumiseks 5–7 tööpäeva.

Muu makseviisi määramine

Tellimuse uuendamisel kasutatakse tasude automaatsel võtmisel makseviisi, mille valisite tellimuse ostmisel. Võite määrata muu makseviisi.

[Muu makseviisi määramine Venemaal](#), [Valgevenes](#), [Abhaasias](#), [Armeenias](#), [Aserbaidžaanis](#), [Gruusias](#), [Lõuna-Osseetias](#), [Kõrgõzstanis](#), [Mongoolias](#), [Tadžikistanis](#), [Türkmenistanis](#), [Usbekistanis](#), [Kasahstanis](#) 

Muu makseviisi määramiseks tehke järgmist.

1. Otsige postkastist meiliaadressi, mille määrasite ostu sooritamisel. Tellimuse kinnitussõnumist või tellimuse uuendamise meeldetuletuse teatest leiate lingi oma kontole või lingi oma automaatse uuendamise halduslehele.
2. Klõpsake linki.
Teid suunatakse vaikebrauseris teie isikupärastatud lehele maksepakkuja veebisaidil.
3. Muutke tellimuse uuendamise teabega lehel makseviisi ja salvestage muudatused.

Muu makseviisi määramine teistes riikides

Muu makseviisi määramiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Profil**.
3. Valiku Tellimuse teave all klõpsake nuppu **Halda kontot**. Kui te ei ühendanud oma seadet oma kontoga, klõpsake nuppu **Logi sisse**.
See avab teie vaikebrauseris My Kaspersky sisselogimisakna.
4. Klõpsake lehe paremas ülanurgas meiliaadressiga linki.
5. Valige ripploendist **Konto seaded**.
6. Klõpsake vahekaarti **Makseviis**.
7. Klõpsake nuppu .
Valige rippmenüüst **Muuda**.
8. Teid suunatakse uues brauseriaknas meie ametlikul Nexway veebisaidil makseviisi muutmise lehele. Muu makseviisi määramiseks järgige ekraanil kuvatavaid juhiseid.

Seadmes tellimuse aktiveerimine

Sellest jaotisest saate teada, kuidas pärast tellimuse ostmist rakenduste kasutamist alustada. Aktiveerimiseks on vaja internetiühendust.

Kui ostsite tellimuse Kaspersky veebisaidilt

Kui ostsite tellimuse Kaspersky veebipoest, siis loodi teie My Kaspersky konto ostu sooritamise käigus. My Kaspersky kontot on vaja teie tellimuse aktiveerimiseks erinevates seadmetes ja tellimuse haldamiseks. Oma tellimuse saate aktiveerida, kui logite My Kaspersky kontole seadmest, millele rakendust paigaldate.

Tellimuse aktiveerimiseks oma seadmetes tehke järgmist.

1. Otsige postkastist meiliaadressi, mille määrasite ostu sooritamisel. Kasperskylt peaks olema kaks meili: kviitung ja juhised tellimuse aktiveerimise lõpuleviimiseks.
2. Klõpsake juhistega meilis linki **Ava My Kaspersky**, et viia konto loomine lõpule ja logida sisse.
3. Klõpsake rakenduse oma seadmesse allalaadimiseks tellimuse teabe aknas nuppu **Laadi alla**.

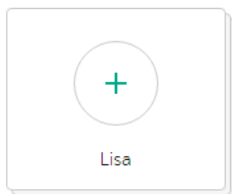
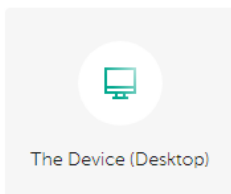
[← Kõik tellimused](#)**Kaspersky Plus**

1 aasta kaitset 10 seadmele

Tellimus: **Aktiivne**Aegumiskuupäev: **13. aug 2023****1 kogu arvust 10 seadet on kaitstud**

Laadi alla

Mõne teise seadme kaitsmine ▾

**Minu seadmed****Rakendused****Kasutajaid (1)**

Kutsu

**Lisateave**

* Tellimuse kontrollimine võib kesta kuni 24 tundi. Kuni kontrollimise lõpulejõudmiseni võib funktsionaalsus olla piiratud.

Lisa aktiveerimiskood

Salvestage kood oma kontole, et hõlpsasti rakendusi alla laadida ja seadmeid oma tellimusega linkida.

XXXXX - XXXXX - XXXXX - XXXXX

Tellimisperioodi saab alustada kohe pärast aktiveerimiskoodi lisamist! [Üksikasjad](#)

Lisa

Kas teil pole aktiveerimiskoodi? [Ostke tellimus](#)Kas te ei tea, mis on aktiveerimiskood? [Klõpsake siin.](#)

4. [Paigaldage rakendus.](#)

Kui paigaldamine on edukalt lõpule viidud, ühendatakse rakendus automaatselt teie kontoga ja aktiveeritakse teie ostetud tellimuse põhjal.

Kui tellimust uuendatakse, uuendatakse selle lõpukuupäeva automaatselt 24 tunni jooksul kõigis seadmetes, mis on selle tellimuse jaoks aktiveeritud ja mis on seotud teie My Kaspersky kontoga.

Kui ostate tellimuse Kaspersky veebipoest, algab tellimuse kehtivusaeg ostuhetkest.

Kui ostsite karbi või aktiveerimiskaardi

Kui ostsite poest karbi või aktiveerimiskaardi, vajate rakenduse aktiveerimiseks aktiveerimiskoodi. Aktiveerimiskoodi leiate karbilt, dokumentatsioonist või kaardi tagaküljelt. Aktiveerimiskood on kahekümnest numbrist ja ladina tähest koosnev kordumatu jada, mis on esitatud vormingus xxxxx-xxxxx-xxxxx-xxxxx.

Aktiveerimiskoodiga aktiveeritud tellimuse aegumist arvestatakse kuupäevast, mil aktiveerite rakenduse esimeses seadmes.

Aktiveerimiskoodi ostmisel tehke järgmist.

1. Avage [My Kaspersky veebisait](#) seadmes, mida soovite kaitsta.
2. Looge My Kaspersky konto või logige sisse olemasolevale kontole.
3. Sisestage aktiveerimiskood lehe allosas suvandi **Aktiveerimiskood on juba olemas?** all olevale sisestusväljale.

Add activation code

Save the code in your account to easily download apps and link devices to your subscription.

XXXXX - XXXXX - XXXXX - XXXXX

Your subscription term can start immediately after an activation code has been added! [Details](#)

Add

No activation code? [Purchase subscription](#)

Don't know what an activation code is? [Click here](#)

4. Klõpsake nuppu **Lisa**.

Kui aktiveerimiskoodi lisamine õnnestus, kuvatakse jaotises **Tellimused** tellimuspaneel.

5. Klõpsake tellimuspaneelil.

Subscriptions



Kaspersky Safe Kids

Subscription: **Active**

Expiration date: **Oct 01, 2022**



Kaspersky Plus

1 year protection for 10 devices

Subscription: **Active**

Expiration date: **Sep 11, 2023**



Add activation code

Save the code in your account to easily download apps and link devices to your subscription.

XXXXX - XXXXX - XXXXX - XXXXX

Your subscription term can start immediately after an activation code has been added! [Details](#)

Add

No activation code? [Purchase subscription](#)

Don't know what an activation code is? [Click here](#)

6. Klõpsake rakenduse oma seadmesse allalaadimiseks tellimuse teabe aknas nuppu **Laadi alla**.

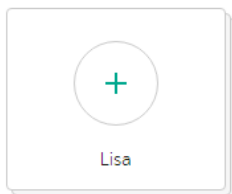
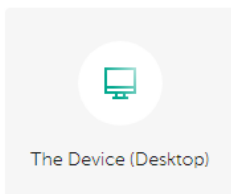
[← Kõik tellimused](#)**Kaspersky Plus**

1 aasta kaitset 10 seadmele

Tellimus: **Aktiivne**Aegumiskuupäev: **13. aug 2023****1 kogu arvust 10 seadet on kaitstud**

Laadi alla

Mõne teise seadme kaitsmine ▾

**Minu seadmed****Rakendused****Kasutajaid (1)**

Kutsu ▾

**Lisateave**

* Tellimuse kontrollimine võib kesta kuni 24 tundi. Kuni kontrollimise lõpulejõudmiseni võib funktsionaalsus olla piiratud.

Lisa aktiveerimiskood

Salvestage kood oma kontole, et hõlpsasti rakendusi alla laadida ja seadmeid oma tellimusega linkida.

XXXXX - XXXXX - XXXXX - XXXXX

Tellimisperioodi saab alustada kohe pärast aktiveerimiskoodi lisamist! [Üksikasjad](#)

Lisa

Kas teil pole aktiveerimiskoodi? [Ostke tellimus](#)Kas te ei tea, mis on aktiveerimiskood? [Klõpsake siin.](#)

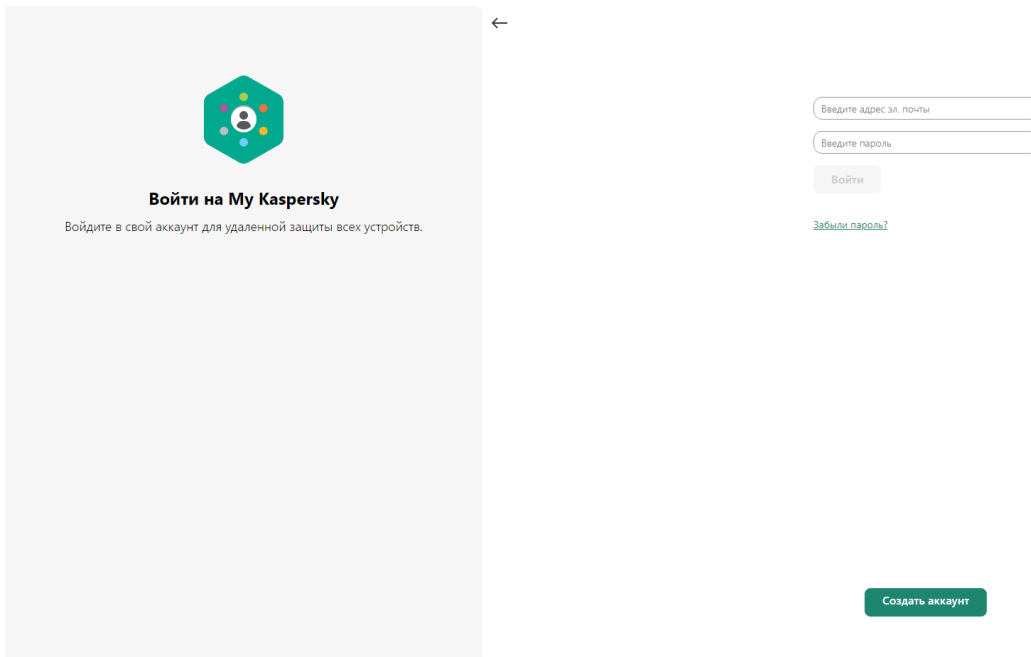
7. [Paigaldage rakendus.](#)

Kui rakendus on paigaldatud, aktiveeritakse see automaatselt teie tellimuse tingimuste kohaselt.

Kui ostsite paigalduskettaga karbi, tehke järgmist.

1. Sisestage ketas kettaseadmesse.

2. My Kaspersky konto ühendamise aknas looge konto või logige sisse olemasolevale kontole.



←

Войти на My Kaspersky
Войдите в свой аккаунт для удаленной защиты всех устройств.

Введите адрес эл. почты

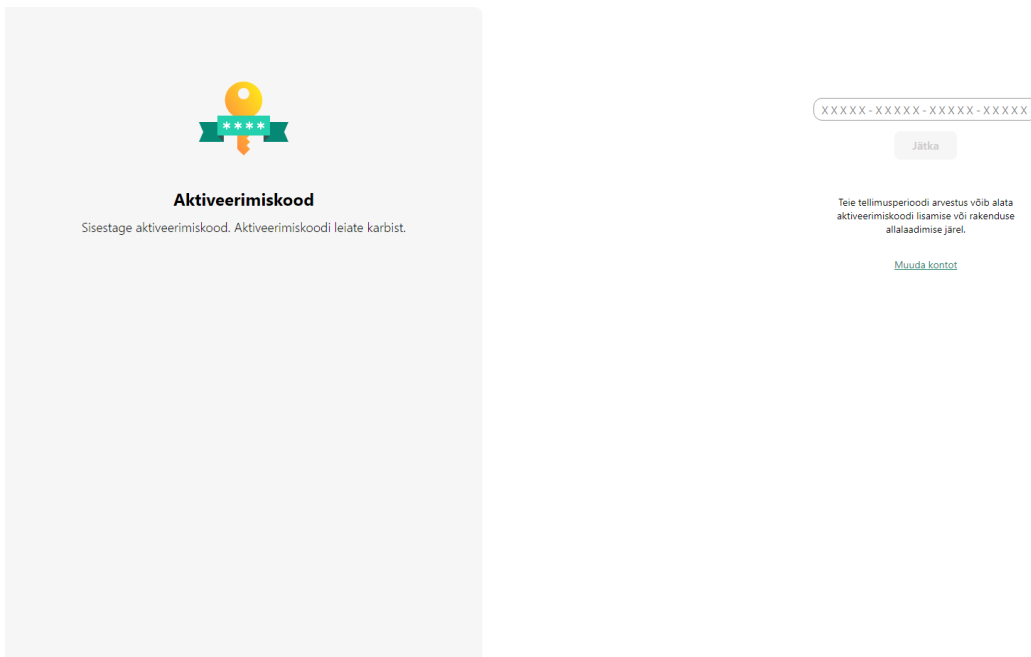
Введите пароль

Войти

[Забыли пароль?](#)

Создать аккаунт

3. Sisestage aktiveerimiskoodi aknas aktiveerimiskood tekstiboksi ja klõpsake nuppu **Jätka**.



Активировать код
Сisestage активированный код. Активированный код леиате карбист.

XXXXX-XXXXX-XXXXX-XXXXX

Jätka

Теие телимиспериоди арвестус вöиб алата активированный код исамисе вöи ракендусе алалаадимисе жает.

[Муудиа контои](#)

Активированный код салвестатаксе теие контоле жаетиссе **Теллимусед**.

4. Klõpsake nuppu **Laadi alla ja paigalda**, et laadida rakendus alla ja paigaldada seadmesse.



Kaspersky Plus

Täielik turvalisus, jõudlus ja privaatsus teie võrgumaailma täiustamiseks

Pärast installimist on see juba teie tellimusega aktiveeritud ja teie kontoga ühendatud.

Laadi alla ja installeeri

[Installeeri Kaspersky Password Manager muudesse seadmesse](#)

Installeeri kõigisse seadmesse

Skannige kaamera abil QR-koodi, et hankida Kaspersky oma nutitelefoni.

QR-koodi skannimisel või lingi klõpsamisel saadetakse ühekordne rakenduse aktiveerimise parool [järgmistele asutustele](#).

Pärast installimist on see juba teie tellimusega aktiveeritud ja teie kontoga ühendatud.



Hangi muudes seadmetes
[macOS](#) [iOS](#) [Android](#)

5. Paigaldage rakendus.

Kui rakendus on paigaldatud, aktiveeritakse see automaatselt teie tellimuse tingimuste kohaselt.

Teie aktiveerimiskood on nüüd teie [My Kaspersky kontole](#) salvestatud. Uue seadme kaitsmiseks logige kontole sisse ja laadige rakendus alla. Võite ka aktiveerimiskoodi rakenduses käsitsi sisestada.

Tellimuse aktiveerimine, kui rakendus on seadmesse juba paigaldatud

Sellest jaotisest saate teada, kuidas uuendada aegunud tellimust, lisada aktiivse tellimusega rakendusele uus aktiveerimiskood, et see uueneks automaatselt, ja minna prooviteellimusele üle tasulisele tellimusele.

Teie tellimus on aegunud

Kui teil on automaatne uuendamine aktiveeritud, uuendatakse tellimust automaatselt teiseks perioodiks ilma teie sekkumiseta. Kui teil pole automaatset uuendamist aktiveeritud, peate tellimust käsitsi uuendama.

Kui uuendate tellimust käsitsi ja olete varem rakenduses lisanud varuaktiveerimiskoodi, siis praeguse tellimuse aegumisel aktiveeritakse rakendus automaatselt varuaktiveerimiskoodiga.

Tellimuse uuendamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Profil**. Kui teie seade on ühendatud teie My Kaspersky kontoga, kuvatakse siin teie meiliaadress.
3. Valiku Tellimuse teave all klõpsake nuppu **Uuenda kohe**.

Vaikebrauseris avaneb Kaspersky eStore'i või mõne meie partneri veebisait.

Sisestage ostuprotsessi ajal oma My Kaspersky kontoga registreeritud meiliaadress. Kui teil kontot veel pole, luuakse see määratud meiliaadressiga. Pärast rakenduse ostmist ja ühendamist oma My Kaspersky kontoga aktiveeritakse tellimus seadmes automaatselt tunni aja jooksul alates uuendamisest.

Uue tellimuse saate saata seadmetesse ka oma My Kaspersky konto kaudu. Kontoga ühendatud seadmesse tellimuse saatmise kohta lisateavet vt [My Kaspersky abist](#).

Kui te pole oma tellimust uuendanud, võib rakendus lülituda [piiratud funktsionaalsusega režiimi](#).

Tellimuse uuendamine varuaktiveerimiskoodiga

Kui teil on uus aktiveerimiskood olemas, saate selle varukoodina kasutamiseks rakendusse lisada. Kui hetkel kehtiv tellimus aegub, aktiveeritakse rakendus varuaktiveerimiskoodi abil automaatselt. Sel viisil saate oma seadme jaoks tagada katkestusteta kaitse.

Vahel [ei saa](#) te varuaktiveerimiskoodi lisada.

Varuaktiveerimiskoodi ei pruugi saada lisada järgmiste piirangute tõttu.

- Kui kasutate automaatselt uuenevat tellimust, ei saa te varuaktiveerimiskoodi lisada.
- Automaatselt uueneva tellimuse aktiveerimiskoodi ei saa varuaktiveerimiskoodina lisada.
- Kui kasutate proovitellimust, ei saa te varuaktiveerimiskoodi lisada.
- Aktiveerimiskood on rakenduses juba varuaktiveerimiskoodiks määratud.
- Varukoodi ei saa lisada, kui praegune tellimus on juba aegunud.
- Tellimus pole veel teie piirkonnas saadaval.

Varuaktiveerimiskoodi lisamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Profil**. Kui teie seade on ühendatud teie My Kaspersky kontoga, kuvatakse siin teie meiliaadress.
3. Klõpsake tellimuse teabe jaotises kolme punkti ja valige **Sisestage aktiveerimiskood**.
4. Sisestage sisestusväljale aktiveerimiskood ja klõpsake nuppu **Salvesta aktiveerimiskood**.

Varuaktiveerimiskood kuvatakse aknas **Tellimuse üksikasjad**.

Kui sisestate varuaktiveerimiskoodi, mis on välja antud mitme seadme jaoks, peate tegema varukoodi rakendamise toimingud kõigis seadmetes, kus soovite tellimust automaatselt uuendada.

Kui praegune tellimus aegub või seadmest eemaldatakse, tehakse katse varukood aktiveerida ja täielikult kinnitada. Rakendus kontrollib varuaktiveerimiskoodi aegumiskuupäeva, seda, kui mitmes seadmes saab tellimust kasutada, ning tellimuse ühilduvust rakenduse paigaldatud versiooniga. On võimalik, et varuaktiveerimiskoodi aktiveerimisel tuleb luua ühendus My Kaspersky kontoga.

Kui teie lisatav varuaktiveerimiskood on selles või mõnes muus seadmes juba rakendatud, siis tellimuse varukoodiga uuendamise seisukohast loetakse aktiveerimiskuupäevaks kuupäeva, mil rakendus aktiveeriti selle koodiga esimest korda. Tellimuse uuendamiseks lisage varuaktiveerimiskood, mille aegumiskuupäev on rakenduses hetkel kasutatava tellimuse aegumiskuupäevast hilisem.

Kui rakendust ei aktiveeritud varuaktiveerimiskoodiga automaatselt, saate selle käsitsi aktiveerida, klõpsates nuppu **Proovi uuesti**. Kui hetkel kasutatav tellimus on blokeeritud, saate rakenduse aktiveerida varuaktiveerimiskoodiga, klõpsates nuppu **Aktiveeri praegu**.

Varuaktiveerimiskoodi saate saata seadmetesse ka oma My Kaspersky konto kaudu. Kontoga ühendatud seadmesse tellimuse saatmise kohta lisateavet vt [My Kaspersky abist](#).

Proovitellimuselt tasulisele tellimusele üleminek

Kui tasuta prooviperiood lõpeb, siis tellimus uuendatakse ja aktiveeritakse ilma teie sekkumiseta. Tasu tellimuse uuendamise eest võetakse teie valitud makseviisi kaudu.

Mõnes piirkonnas ei ole automaatne üleminek tasulisele tellimusele saadaval. Kui te tasuta prooviversiooni tellimisel ei sisestanud makseüksikasju hilisemaks uuendamiseks, siis peate seadmete kaitse säilitamiseks tellimuse ostma.

Proovitellimuselt tasulisele tellimusele üleminekuks tehke järgmist

1. Avage rakenduse peaaken.
2. Avage jaotis **Profil**. Kui teie seade on ühendatud teie My Kaspersky kontoga, kuvatakse siin teie meiliaadress.
3. Valiku Tellimuse teave all klõpsake nuppu **Osta kohe**.

Vaikebrauseris avaneb Kaspersky või mõne meie partneri veebisait. Sisestage ostuprotsessi ajal oma My Kaspersky kontoga registreeritud meiliaadress.

Ostetud tellimus aktiveeritakse teie seadmes automaatselt.

Rakenduse installimine või eemaldamine

Rakenduse paigaldamine

Rakendus paigaldatakse arvutisse interaktiivses režiimis, kasutades paigaldusnõustajat.

Nõustaja koosneb mitmest aknast (etapist). Nõustaja etappide arv ja järjestus olenevad piirkonnast, kus te rakenduse paigaldate. [Mõnes piirkonnas](#) palub paigaldusnõustaja nõustuda teie isiklike andmete töötlemisega seotud lisalepingutega. Nõustaja tegevuse peatamiseks sulgege mis tahes paigaldusetapis nõustaja aken.

Kui rakendust kasutatakse mitme arvuti kaitsmiseks (arvutite maksimumarvu määravad lõppkasutaja litsentsilepingu tingimused), on paigaldusprotseduur kõigis arvutites ühesugune.

Rakenduse arvutisse paigaldamiseks tehke järgmist.

- Kui kasutate installiketast, sisestage ketas kettaseadmesse ja täitke ekraanil kuvatavad juhised.
- Kui laadisite rakenduse alla internetist, käivitage see. Seejärel installitakse rakendus standardse paigaldusnõustaja abil. Sellisel juhul kuvab nõustaja mõne lokaliseerimiskeele korral mitu täiendavat paigaldusetappi.

[Rakenduse saate installida ka käsuviiba kaudu](#) .

Kaspersky rakenduse saate installida ka käsuviiba kaudu.

Teatud käske saab käivitada ainult administraatori kontol.

Käsuviiba süntaks on järgmine:

<paigalduspaketi failitee> [parameetrid]

Rakenduse paigaldamine käsuviibalt.

1. Avage käsuviip administraatorina.
2. Sisestage installifaili tee ja installimise alustamise käsk koos vajalike suvandite ja atribuutidega. Installisuvandeid ja atribuute kirjeldatakse allpool.
3. Järgige häälestusviisardi juhiseid.

Põhisuvandid

Käsu nimi	Väärtus	Näide
/s	Mitteinteraktiivne (vaikne) režiim: installimise ajal dialoogibokse ei kuvata.	saas21.exe /s
/mybirthdate=YYYY-MM-DD	Sünnikuupäev. Kui olete noorem kui 16, installimist ei käivitata. See suvand on: <ul style="list-style-type: none">• Kohustuslik mitteinteraktiivse installimise puhul• Valikuline rakenduse installimisel OEM-režiimis	saas21.exe /mybirthdate=1986-12-23
/l	Kasutatava keele valimine mitmekeelse versiooni installimisel.	saas21.exe /len-us
/t	Kaust, kuhu salvestatakse installilogi.	saas21.exe /tC:\KasperskyLab
/p<property>=<value>	Määrab installiattribuudid.	saas21.exe /pALLOWREBOOT=1 /pSKIPPRODUCTCHECK=1
/h	Kuvab spikri.	saas21.exe /h

Lisaseaded

Käsu nimi	Väärtus	Näide
/x	Toote eemaldamine.	saas21.exe /x

Kõige olulisemad installiattribuudid

Käsu nimi	Väärtus	Näide
ACTIVATIONCODE=<väärtus>	Aktiveerimiskoodi sisestamine.	
AGREETOEULA=1	Lõppkasutaja litsentsilepinguga	

	nõustumine.	
AGREETOPRIVACYPOLICY=1	Privaatsuspoliitikaga nõustumine.	
JOINKSN_ENHANCE_PROTECTION=1	Toote põhifunktsioonide parandamiseks isikuandmete saatmise nõusoleku kinnitamine.	
JOINKSN_MARKETING=1	Isikuandmete turunduseesmärkidel kasutamiseks saatmise nõusoleku kinnitamine.	
INSTALLDIR=<väärtus>	Installimiskoha määramine.	saas21.exe /p"INSTALLDIR=C:\Documents and Settings\saas21"
KLPASSWD=<väärtus>	Toote erinevate funktsioonide jaoks parooli seadistamine. Kui KLPASSWDAREA väärtust pole määratud, kasutatakse parooli vaikeulatust. <ul style="list-style-type: none"> • Rakenduse seadete muutmine • Rakenduse sulgemine 	saas21.exe /pKLPASSWD=12345678
KLPASSWDAREA=[SET EXIT UNINST]	Käsuga KLPASSWD konfigureeritud parooli ulatus: <ul style="list-style-type: none"> • SET – rakenduse seadete muutmine. • EXIT – rakendusest väljumine. • UNINST – rakenduse eemaldamine. Sellel atribuudil võib olla mitu väärtust; sel juhul tuleb väärtused eraldada semikooloniga „;“. 	
SELFPROTECTION=1	Installimise ajaks enesekaitse lubamine.	saas21.exe /pSELFPROTECTION=1
ALLOWREBOOT=1	Vajadusel taaskäivitamise lubamine	saas21.exe /pALLOWREBOOT=1
SKIPPRODUCTCHECK=1	Ära kontrollige tarkvara, mis ei ühildu Kasperskyga.	saas21.exe /pSKIPPRODUCTCHECK=1
-oembackupmode	Ära käivita rakendust pärast installimist, kui Windows on käivitatud auditirežiimis.	saas21.exe /s -oembackupmode

Seades väärtuse SKIPPRODUCTCHECK=1, võtate täieliku vastutuse Kaspersky ja muu tarkvara ühildumatuse võimalike tagajärgede eest.

SKIPPRODUCTCHECK=1 võimaldab ignoreerida ainult käsitsi eemaldatavaid rakendusi.

Liitkäsü näide, mis võimaldab arvutit installimise ajal taaskäivitada ja mitteühilduva tarkvara kontrolli vahele jätta:

```
saas21.exe /pALLOWREBOOT=1 /pSKIPPRODUCTCHECK=1
```

Paigaldusnõustaja juhendab teid järgmistes toimingutes.

1. Installimise käivitamine

Selle etapi ajal palub nõustaja rakenduse paigaldada.

Paigaldustüübist ja lokaliseerimiskeelest olenevalt võib nõustaja selle etapi käigus paluda teil lugeda teie ja Kaspersky vahel sõlmitud lõppkasutaja litsentsilepingut ja küsida, kas soovite osaleda Kaspersky Security Networkis.

[Lõppkasutaja litsentsilepingu ülevaatamine](#) 

See nõustaja etapp kuvatakse mõne lokaliseerimiskeele korral, kui installitakse internetist alla laaditud rakendust.

Selle etapi käigus palub nõustaja teil üle vaadata teie ja Kaspersky vahel sõlmitud lõppkasutaja litsentsileping.

Lugege lõppkasutaja litsentsileping põhjalikult läbi, ja kui nõustute kõigi selle tingimustega, klõpsake nuppu **Jätka** (selle nupu nimi [mõnes piirkonnas Nõustu](#)).

kaspersky

Лицензионно споразумение за Kaspersky Plus

ЛИЦЕНЗИОННО СПОРАЗУМЕНИЕ С КРАЕН ПОТРЕБИТЕЛ НА KASPERSKY („ЛИЦЕНЗИОННО СПОРАЗУМЕНИЕ“)

ВНИМАТЕЛНО ПРОЧЕТЕТЕ СЛЕДНОТО ЛИЦЕНЗИОННО СПОРАЗУМЕНИЕ, ПРЕДИ ДА ЗАПОЧНЕТЕ ДА ИЗПОЛЗВАТЕ СОФТУЕРА.

ЗА ДА СКЛЮЧИТЕ ТОВА ЛИЦЕНЗИОННО СПОРАЗУМЕНИЕ, ТРЯБВА ДА СТЕ ВЪЗРАСТЕН. АКО СТЕ ДЕТЕ, ТРЯБВА ДА ПОМОЛИТЕ ЕДИН ОТ ВАШИТЕ РОДИТЕЛИ ИЛИ ЗАКОННИЯ СИ НАСТОЙНИК ДА ПРОЧЕТЕ И ПРИЕМЕ ТОВА ЛИЦЕНЗИОННО СПОРАЗУМЕНИЕ ВМЕСТО ВАС. РОДИТЕЛ ИЛИ НОСИТЕЛ НА РОДИТЕЛСКАТА ОТГОВОРНОСТ ТРЯБВА ДА ПРИЕМЕ ТОВА ЛИЦЕНЗИОННО СПОРАЗУМЕНИЕ ВМЕСТО ВАС И ДА ПОЕМЕ ПЪЛНА ОТГОВОРНОСТ ЗА ВСИЧКИ ЗАДЪЛЖЕНИЯ, НАЛОЖЕНИ НА КРАЕН ПОТРЕБИТЕЛ СЪГЛАСНО УСЛОВИЯТА НА ТОВА ЛИЦЕНЗИОННО СПОРАЗУМЕНИЕ

Потвърждавам, че изцяло прочетох, разбирам и приемам правилата и условията на настоящото Лицензионно споразумение

Наясно съм и се съгласявам моите данни да бъдат обработвани и предавани (включително към трети държави), както е описано в Декларацията за поверителност. Потвърждавам, че съм прочел(а) и разбирам [Политика за поверителност](#)

Mõnes rakenduse versioonis saab lõppkasutaja litsentsilepingu avada, klõpsates viisardi tervituskual oleval lingil. Sel juhul on lõppkasutaja litsentsilepingu teksti sisaldavas aknas saadaval ainult **Tagasi** nupp. Klõpsates **Paigalda** nuppu, nõustute lõppkasutaja litsentsilepingu tingimustega.

kaspersky

Lõppkasutaja litsentsileping tootele Kaspersky Plus

LÕPPKASUTAJA LITSENTSILEPING

OLULINE JURIIDILINE MÄRKUS KÕIGILE KASUTAJATELE: ENNE KUI ASUTE TARKVARA KASUTAMA, LUGEGE JÄRGNEV LEPING HOOLIKALT LÄBI.

Käitades tarkvara, klõpsates installimise ajal nuppu, millega kinnitate oma nõustumist litsentsilepingu tingimustega või sisestades vastav(ad) tähemärgi(d), nõustute tingimusteta selle litsentsilepingu sätetega. Kui te selle litsentsilepingu sätetega ei nõustu, peate tarkvara installimise katkestama ja/või tarkvara kustutama.

PEALE NÕUSTUMIST KINNITAVA NUPU KLÕPSAMIST VÕI VASTAVA(TE) SÜMBOLI(TE) SISESTAMIST LITSENTSILEPINGU AKNAS ON TEIL ÕIGUS KASUTADA SEDA TARKVARA VASTAVALT KÄESOLEVA LEPINGU SÄTELE JA TINGIMUSTELE.

KUI TARKVARAGA ON KAASAS LITSENTSILEPING VÕI MÕNI SARNANE DOKUMENT, ALISTAVAD NII SUGUSES DOKUMENDIS TOODUD TARKVARA KASUTUSTINGIMUSED SELLE LÕPPKASUTAJA LITSENTSILEPINGU TINGIMUSED.

JAOTIS A. ÜLDTINGIMUSED

Seejärel jätkatakse arvutisse rakenduse paigaldamist.

Kui lõppkasutaja litsentsilepingu tingimustega ei nõustuta, siis rakendust ei paigaldata.

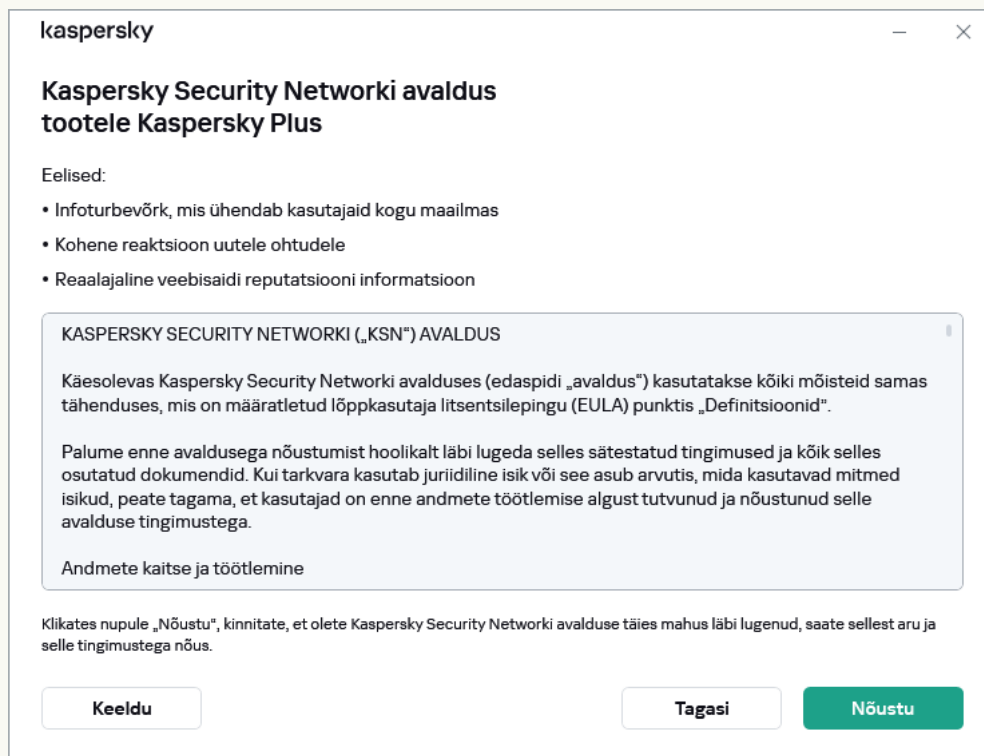
[Mõnes piirkonnas](#) tuleb teil rakenduse paigaldamise jätkamiseks nõustuda ka privaatsuspoliitika tingimustega.

[Kaspersky Security Networki avalduse läbivaatamine](#) 

Selle etapi käigus kutsub nõustaja teid osalema Kaspersky Security Networkis. Programmis osalemine hõlmab ettevõttele AO Kaspersky Lab teabe saatmist teie arvutis tuvastatud ohtude, käitatavate rakenduste ja allalaaditud allkirjastatud rakenduste ning teie operatsioonisüsteemi kohta. Teilt saadud isiklike andmeid ei koguta, töödelda ega salvestata.

Lugege Kaspersky Security Networki avaldus läbi ja tehke järgmist.

- Kui nõustute kõigi selle tingimustega, klõpsake nuppu **Nõustu**.
- Kui te ei soovi Kaspersky Security Networkis osaleda, klõpsake nuppu **Keeldu**.



Mõnes rakenduse versioonis tuleb Kaspersky Security Networki avaldusega nõustumiseks märkida ruut **Soovin osaleda teenuses Kaspersky Security Network** `WELCOME_CHECK_PRIVACY_POLICY_PART1 = Kuva` viisardi tervituskval. Seda avaldust saate lugeda, klõpsates linki **Kaspersky Security Network**. Pärast lepingu lugemist klõpsake installimise jätkamiseks nuppu **Tagasi**. Kui ruut **Soovin osaleda teenuses Kaspersky Security Network** `WELCOME_CHECK_PRIVACY_POLICY_PART1 = Kuva` on märgitud, nõustute Kaspersky Security Networki avalduse tingimustega, klõpsates nuppu **Paigalda**.

Kaspersky Security Networki avaldus tootele Kaspersky Plus

Eelised:

- Infoturbevõrk, mis ühendab kasutajaid kogu maailmas
- Kohene reaktsioon uutele ohtudele
- Reaalajaline veebisaidi reputatsiooni informatsioon

KASPERSKY SECURITY NETWORKI („KSN“) AVALDUS

A. SISSEJUHATUS

Lugege see dokument põhjalikult läbi. Käesolev dokument sisaldab olulist teavet, mida te enne meie teenuste või tarkvara kasutamast teadma peaksite. Oleme jätnud endale õiguse muuta käesolevat avaldust mis tahes ajal, avaldades muudatused antud lehel.

AO Kaspersky Lab (edaspidi Kaspersky) on koostanud käesoleva avalduse, et teavitada ja avalikustada oma tarkvara andmete kogumise ja levitamise tavaid.

Kaspersky on võtnud endale eesmärgiks pakkuda kõigile oma klientidele parimat teenust ja eriti arvestada teie kahtlusi andmetöötluse osas.

Tagasi

Pärast Kaspersky Security Networkis osalemisega nõustumist või sellest keeldumist jätkatakse rakenduse paigaldamist.

[Mõnes rakenduse versioonis](#) sisaldab Kaspersky Security Networki avaldus teavet isiklike andmete töötlemise kohta.

2. Rakenduse paigaldamine

Rakenduse paigaldamine võib veidi aega võtta. Oodake, kuni see on lõpuni viidud. Pärast paigaldamise lõpuleviimist jätkab paigaldusnõustaja automaatselt järgmist etappi.

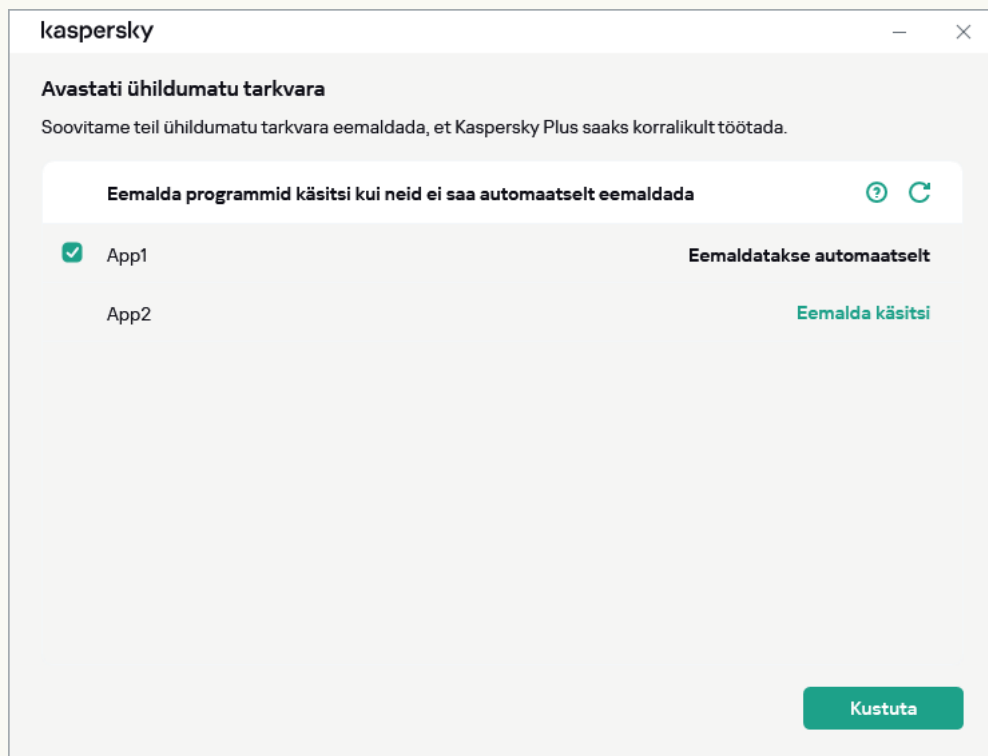
[Kontrollid rakenduse paigaldamisel](#) 

Rakendus teeb installimise ajal mitu kontrolli. Need kontrollid võivad tuvastada järgmisi probleeme.

- *Operatsioonisüsteemi mittevastamine tarkvaranõuetele.* Paigaldamise ajal kontrollib nõustaja järgmiste tingimuste täitmist.
 - operatsioonisüsteem ja hoolduspakett vastavad tarkvaranõuetele;
 - kõik nõutavad rakendused on saadaval;
 - installimiseks on piisavalt vaba kettaruumi;
 - rakendust installival kasutajal on administraatoriõigused.

Kui mõni ülaltoodud nõuetest ei ole täidetud, kuvatakse asjakohane teade.

- *Arvutis ühildumatute rakenduste leidumine.* Kui tuvastatakse ühildumatuid rakendusi, kuvatakse need ekraanil loendina ja teil palutakse need eemaldada. Rakendused, mida ei saa automaatselt eemaldada, tuleb käsitsi eemaldada, klõpsates nuppu **Eemalda käsitsi**.



Ühildumatute rakenduste eemaldamisel peate operatsioonisüsteemi taaskäivitama, misjärel jätkub Kaspersky installimine automaatselt.

[Kaspersky Password Manageri paigaldamine koos Kaspersky Plusi või Kaspersky Premiumiga](#)

Enne installimise lõpuleviimist palub Kaspersky teil installida ka [paroolide kaitsmiseks ette nähtud Kaspersky Password Manageri](#). Kaspersky Password Manageri installimine võib jätkuda ka pärast Kaspersky installimise lõpuleviimist ning Kaspersky Password Manageri installimise lõpuleviimisel ei kuvata eraldi teadet.

Plaanid Kaspersky Basic ja Kaspersky Standard ei sisalda Kaspersky Password Manageri. Kui soovite parooliga kaitseks kasutada Kaspersky Password Manageri, saate selle alla laadida ja paigaldada eraldi rakendusena või lülituda Kaspersky Plusile.

3. Installimise lõpuleviimine

Selles etapis teavitab nõustaja teid rakenduse paigaldamise lõpuleviimisest.

Kõik vajalikud rakendusekomponendid käivitatakse pärast paigaldamise lõppu automaatselt.

Mõnel juhul tuleb teil paigaldamise lõpuleviimiseks operatsioonisüsteem taaskäivitada.

Interneti ohutu sirvimise tagamiseks paigaldatakse koos rakendusega veebilehitsejate lisandmoodulid.

Kui käitate audio ja video salvestus- või taasesitusrakendusi pärast Kaspersky installimist esimest korda, võib audio ja video taasesitusel või salvestamisel esineda katkestusi. See on vajalik selleks, et lülitada sisse funktsioonid, mis kontrollivad rakenduste juurdepääsu helisalvestusseadmetele. Audio-riistvara kontrolliv süsteemiteenus taaskäivitub, kui Kaspersky esimest korda käivitatakse.

Kaspersky Plus või Kaspersky Premium paigaldatakse koos Kaspersky VPN Secure Connectioniga, mis on mõeldud turvalise ühenduse loomiseks virtuaalse privaatsõrgu (VPN) kaudu. Kaspersky VPN Secure Connectioni saab eemaldada Kaspersky rakendusest eraldi. Kui VPN-i kasutamine on teie riigis keelatud, siis Kaspersky VPN Secure Connectionit ei paigaldata.

Kui laadisite rakenduse alla oma My Kaspersky kontolt, aktiveerub rakendus pärast installimist automaatselt koos tellimusega teie kontolt.

Paigaldamine teiste Kaspersky rakenduste peale

Selle rakenduse võib paigaldada järgnevate Kaspersky rakenduste peale, ilma neid eelnevalt eemaldamata:

- Kaspersky Free
- Kaspersky Anti-Virus
- Kaspersky Internet Security
- Kaspersky Total Security
- Kaspersky Security Cloud

Uue rakenduse paigaldamisel eemaldatakse varem paigaldatud rakendused Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Security Cloud, Kaspersky Total Security. Eemaldatud rakenduse litsentsi saab kasutada uue Kaspersky rakenduse jaoks, välja arvatud Kaspersky Total Security litsents. Eemaldatud rakenduste seaded säilitatakse.

Uue rakenduse paigaldamisel eemaldatakse varem paigaldatud rakendus Kaspersky Free. Kaspersky Free seadeid ei salvestata.

Kui lähete Kaspersky Total Securitylt üle Kaspersky Basicule või Kaspersky Standardile, säilitatakse failide varukoopiaid, kuid neid ei kuvata nendes rakendustes. Saate lisada failide varukoopiaid käsitsi. Kui lähete Kaspersky Total Securitylt üle Kaspersky Plusile, säilitatakse failide koopiaid ja need kuvatakse automaatselt.

Brauserilaiend Kaspersky Kaitse

Selleks, et Kaspersky toetaks brausereid täielikult, tuleb brauseritesse installida ja sisse lülitada laiend Kaspersky Kaitse. Laiend Kaspersky Kaitse sisestab kaitstud brauseris avatud veebilehele ja liiklusesse skripti. Selle skripti abil suhtleb rakendus veebilehega ja edastab andmeid pankadele, mille veebisait kaitseb turvaliste maksete komponent. Rakendus kaitseb skripti kaudu edastatud andmeid digiallkirja abil. Rakendus saab skripti manustada ilma laiendit Kaspersky Kaitse kasutamata.

Rakendus allkirjastab skripti poolt edastatud andmed installitud viirusekaitseandmebaaside ja Kaspersky Security Networkile esitatud päringute abil. Rakendus saadab Kaspersky Security Networkile päringuid hoolimata sellest, kas olete Kaspersky Security Networki avalduse tingimustega nõustunud või mitte.


Laiendiga Kaspersky Kaitse saate brauseriga töötades teha järgmist.

[Privaatse sirvimise haldus.](#)

[Ribareklaamifiltri haldus.](#)

[Arvatavast andmepüügist teada anda.](#) 


Arvatavast andmepüügisaidist teatamiseks tehke nii.

1. Veenduge, et olete lehel, mida peate andmepüügileheks.
2. Klõpsake brauseri tööriistaribal nuppu  **Kaspersky Kaitse**.
3. Valige laiendi menüüst **Teavita arvatavast andmepüügist**.
4. Kontrollige, et avanevas aknas kuvataks selle veebisaidi veebiaadressi, mida kahtlustate andmepüügis.
5. Klõpsake **Teavita**.

Teie aruanne saadetakse Kaspersky Security Networkile.

[Teatamine veebisaidi probleemist](#) 

Veebisaidi probleemist teatamiseks tehke nii.

1. Veenduge, et olete lehel, mille problemaatilisusest soovite teada anda.
2. Klõpsake brauseri tööriistaribal nuppu  **Kaspersky Kaitse**.
3. Valige laiendi menüüst **Teatage meile veebisaidi probleemist**.
4. Kontrollige, et avanevas aknas kuvataks selle veebisaidi veebiaadressi.
5. Kirjeldage tekstiboksis probleemi.
6. Klõpsake **Teavita**.

Sõnum on edastatud.

[Ekraaniklaviatuuri avamine](#)

Kaspersky Kaitse laienduse paigaldamine Chromiumi-põhises Microsoft Edge'is, Mozilla Firefoxis ja Google Chrome'is

Brauseritesse Google Chrome ja Mozilla Firefox installitakse laiend Kaspersky Kaitse automaatselt. Kaspersky palub teil laiendi aktiveerida. Ka Chromiumi-põhisesse brauserisse Microsoft Edge installitakse laiend Kaspersky Kaitse automaatselt, kuid rakendus ei palu teil laiendit aktiveerida. Teil tuleb laiend ise aktiveerida.

Yandexi veebilehitseja tugi

Yandexi veebilehitseja kasutamise korral töötavad järgmised rakendusekomponendid.

- Kaitstud veebilehitseja
- URL-i nõustaja
- Ohutu sirvimine
- Andmepüügivastane kaitse

Privaatse sirvimise ja ribareklaamifiltri komponendid töötavad, kuid neid ei saa Yandexi veebilehitsejas seadistada.

Internet Exploreri tugi

Alates Kaspersky rakenduse versioonist 4 ei toeta Kaspersky Kaitse laiendus enam Internet Exploreri veebilehitsejat. Kui soovite Internet Exploreris laiendi Kaspersky Kaitse kasutamist jätkata, saate võtta uuesti kasutusele rakenduse vanema versiooni.

Rakenduse eemaldamine

Pärast rakenduse eemaldamist on teie arvuti ja isiklikud andmed kaitseta.

Rakendus eemaldatakse paigaldusnõustaja abil.

Rakenduse eemaldamine operatsioonisüsteemis Windows 7

Nõustaja käivitamiseks arvutis, mille operatsioonisüsteem on Microsoft Windows 7 või vanem versioon,

Valige menüüs **Start Kõik rakendused** → **Kaspersky** → **Eemalda Kaspersky**.

Rakenduse eemaldamine operatsioonisüsteemis Windows 8

Viisardi käivitamine arvutis, mille operatsioonisüsteem on Microsoft Windows 8 või uuem väljalase:

1. Leidke installitud rakendus ühel järgmistest meetoditest:

- Operatsioonisüsteemis Windows 8 klõpsake nuppu **Alusta** ja valige kiirkäivituskuvalt Kaspersky rakendus.
- Windows 10 ja uuemates versioonides klõpsake nuppu **Alusta** ja leidke rakendus loendist või kasutage otsinguriba.

2. Tehke Kaspersky rakenduse otseteeikoonil paremklõps.

3. Valige kontekstimenüüst **Desinstalli**.

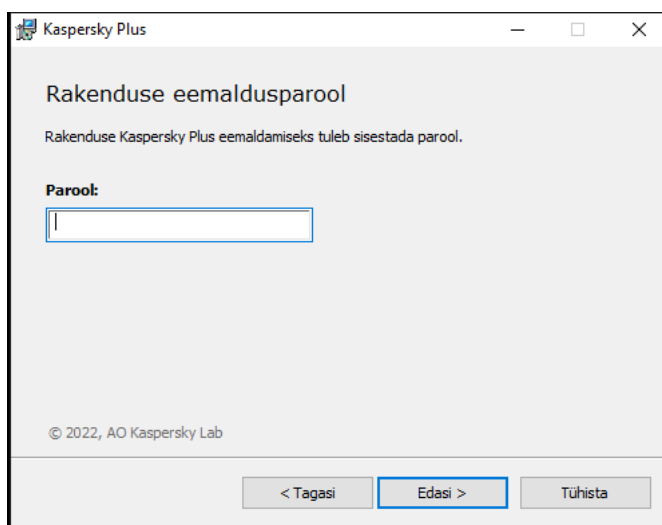
4. Avanenud aknas valige loendist Kaspersky.

5. Klõpsake loendi ülaservas nuppu **Eemalda/ Redigeeri**.

Käivitub rakenduse häälestusviisard.

Eemaldamine hõlmab järgmisi toiminguid.

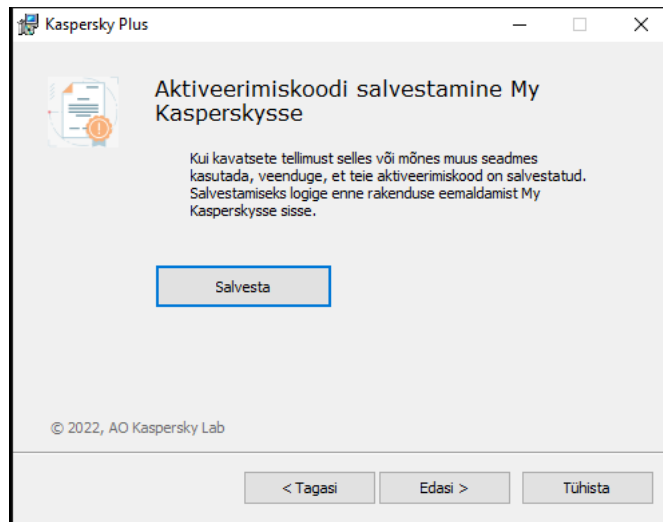
1. Rakenduse eemaldamiseks tuleb teil sisestada rakenduse seadetele juurdepääsemiseks ette nähtud parool. Kui te ei saa mingil põhjusel parooli sisestada, siis rakenduse eemaldamine keelatakse. Pärast parooli sisestamist klõpsake nuppu **Kinnita**.



See etapp on saadaval ainult siis, kui rakenduse eemaldamise jaoks on määratud parool.

2. Tellimuse salvestamine teie My Kaspersky kontole.

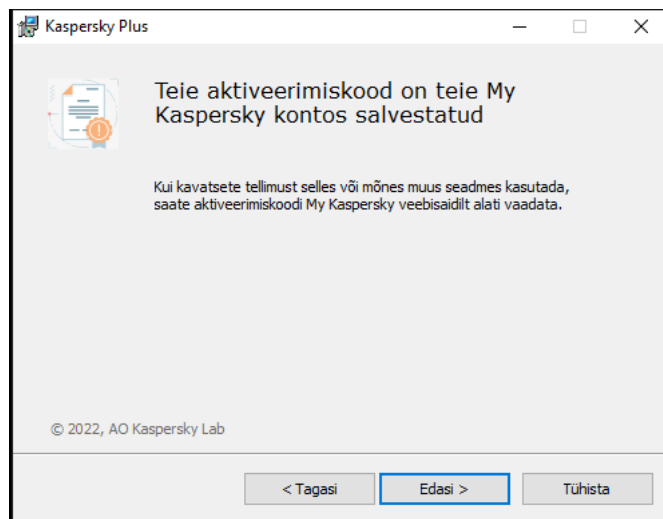
Selles etapis saate määrata, kas soovite tellimuse oma My Kaspersky kontole salvestada, et seda tulevikus kasutada.



a. Kui soovite tellimust salvestada, klõpsake nuppu **Salvesta**.

b. Klõpsake **Edasi >**.

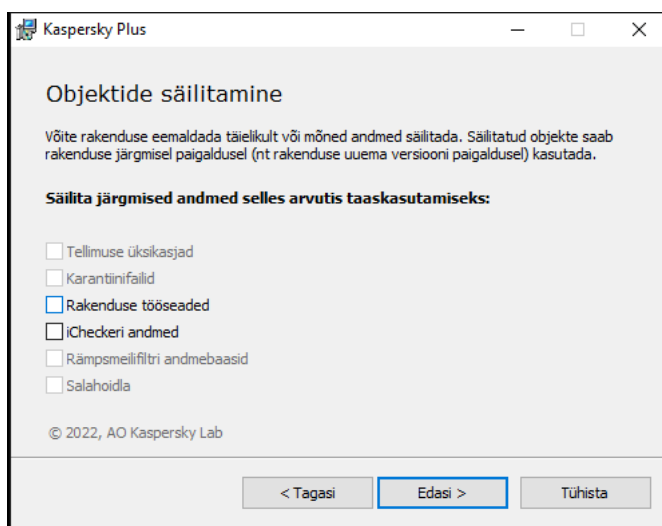
Kuvatakse aken salvestatud tellimusega.



a. Klõpsake **Edasi >**.

3. Andmete salvestamine edasiseks kasutamiseks

Selles etapis saate määrata, millised rakenduse kasutatavad andmed soovite rakenduse järgmiseks paigalduskorraks alles hoida (näiteks rakenduse uuema versiooni paigaldamiseks).



Saate salvestada järgmised andmed.

- **Tellimuse üksikasjad** on andmekogum, mis kõrvaldab vajaduse aktiveerida rakendus tulevase paigaldamise käigus, kuna võimaldab teil seda kasutada praeguse tellimuse alusel, välja arvatud juhul, kui tellimus aegub enne paigaldamise alustamist.
- **Karantiinifailid** on failid, mille rakendus on kontrollinud ja teisaldanud karantiini.

Pärast arvutist rakenduse eemaldamist pole karantiini pandud failid enam saadaval. Nende failidega toimingute tegemiseks peab olema installitud Kaspersky rakendus.

- **Rakenduse tööseaded** on rakenduse seadistamisel valitud rakenduseseadete väärtused.

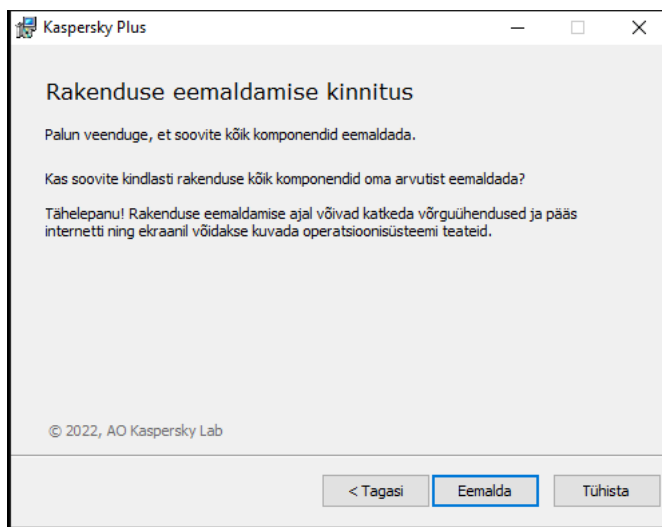
Kaitseseadeid saate eksportida ka käsuviibalt järgmise käsu abil: `avp.com EXPORT <faili_nimi>`.

- **iCheckeri andmed** on failid, mis sisaldavad teavet objektide kohta, mida on [iCheckeri tehnoloogia](#) abil juba kontrollitud.
- **Rämpsmailifiltri andmebaasid** on andmebaasid, mis sisaldavad kasutaja lisatud rämpsmeilisõnumite näidiseid.
- **Salahoidla** sisaldab salahoidla funktsiooni abil salvestatud faile.

Rakenduse desinstallimise jätkamiseks klõpsake nuppu **Edasi >**.

4. Eemaldamise kinnitamine

Kuna rakenduse eemaldamine ohustab teie arvuti ja isiklike andmete turvalisust, palutakse teil rakenduse eemaldamise kavatsus kinnitada. Selleks klõpsake nuppu **Eemalda**.



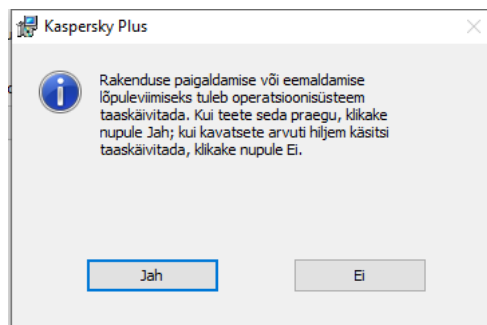
5. Eemaldamise lõpuleviimine

Selles etapis eemaldab paigaldusnõustaja rakenduse arvutist. Oodake, kuni eemaldamine on lõpule viidud.

Mõnes piirkonnas ei pruugi see funktsioon saadaaval olla.

Rakenduse eemaldamise ajal tuleb operatsioonisüsteem taaskäivitada. Viivitamatu taaskäivitamise tühistamise korral lükatakse eemaldamistoimingu lõpuleviimine edasi operatsioonisüsteemi taaskäivitamiseni või arvuti väljalülitamise ja järgmise käivituskorran.

6. Arvuti taaskäivitamiseks klõpsake nuppu **Jah**.



Rakenduse uuendamine

Rakendust uuendatakse automaatselt, kui olete uuenduste seadete aknas (**automaatselt** → **Turvalisus** → **Viirusetõrjeandmebaaside uuendamine**) valinud uuendusrežiimi **Andmebaaside uuendamise graafik**.

Rakendust uuendatakse automaatselt, kui [paigaldate rakenduse uue versiooni](#) olemasoleva asemele.

Rohkemate seadmete kaitsmine

Saadaval ainult plaanides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Saate tellimusega kaitsta kõiki oma seadmeid, mis kasutavad operatsioonisüsteemi Windows, Android, iOS või macOS. Täpne seadmete arv, millega saate tellimust kasutada, oli ostu sooritamisel kirjas tellimuse atribuutides.

Saate alati kontrollida, mitut seadet te juba kaitsete ja kui palju veel saate kaitsta oma rakenduse **Profil** jaotises ja oma [Minu Kaspersky kontol](#)². Sealt leiate ka hõlpsasti kasutatavad tööriistad kaitse jagamiseks teiste seadmetega.

Nende tööriistade abil kaitse jagamiseks ei ole aktiveerimiskoodi vaja, tellimus kantakse üle teie konto kaudu. Kui te ei ole oma My Kaspersky kontole vastava seadme kaudu kunagi sisse loginud, palume teil seda protsessi käigus teha. Pärast installimist aktiveeritakse rakendused teie kontolt tellimuse abil automaatselt.

Rakenduse kaitse jagamiseks toimige järgmiselt:

1. Avage rakenduse peaaaken.
2. Avage jaotis **Profil**.
3. Klõpsake nuppu **+**. Mõnes tellimuses on nupul **Kaitse seadet** tekst.
4. Tehke **Kaitske rohkem seadmeid** aknas üks järgmistest valikutest:

- **Skannige QR-kood**

Suunake **QR-kood** vahekaardil oma telefoni kaamera QR-koodile.

See avab teie mobiilseadmes rakenduse allalaadimislehed Google Play poe, App Store'i või Huawei AppGallery poodides. Kui olete rakenduse alla laadinud ja paigaldanud, loob rakendus automaatselt ühenduse My Kasperskyga ja hakkab teie seadet kaitsma.

Android-seadmes QR-koodi kasutamisega nõustute esitama Google Playle ühekordse parooli, et saaksite rakenduse oma nutitelefonis aktiveerida.

- **Saada link e-posti teel**

- a. Mine jaotisesse **Meili teel**.
- b. Klõpsake linki.
See avab teie vaimbrauseris My Kaspersky sisselogimisakna.
- c. Sisestage aknas **Saada meili teel** tekstiväljale meiliaadress ja klõpsake nuppu **Saada**.
- d. Laadige rakendus alla, järgides e-postis olevat linki.
Pärast allalaadimist ja installimist loob rakendus automaatselt ühenduse teie My Kaspersky kontoga.

Mõne tellimuslepingu korral võidakse kuvada ainult üldist teavet kaitstavate seadmete koguarvu kohta.

Lisateavet seadme kaitse kaughaldamise, tellimusest kasutaja eemaldamise või tellimusest seadme eemaldamise kohta leiate jaotisest [My Kaspersky abi](#)².

Rakenduse põhifunktsioonid

Sellest jaotisest leiab teavet rakenduse põhiseadistuse kohta, sealhulgas teadete ja kasutajaliidese konfigureerimise ning võimalike turbeprobleemide lahendamise kohta.

Arvutikaitse seisundi hindamine ja turvaprobbleemide lahendamine

Arvutikaitsega seotud probleeme kujutab rakenduse peakna ülaservas kuvatav tähis. Roheline näitab, et teie arvuti on kaitstud. Kollane tähistab turvaprobbleeme ja punane näitab, et arvuti turvalisus on tõsisel ohus. Soovitame probleemid ja turvaohud viivitamatult parandada.

Akna **Teatiste keskus** avamiseks saate rakenduse peaknas klõpsata nuppu **Üksikasjad**. See aken sisaldab üksikasjalikku teavet arvuti kaitse seisundi kohta ning soovitusi probleemide ja ohtude lahendamiseks võimalike toimingute kohta.

Kaitsega seotud probleemid on rühmitatud kategooriate kaupa. Iga probleemi korral kuvatakse loend toimingutest, mille saate probleemi lahendamiseks teha.

Jaotises **Olek** kuvatakse teave arvutikaitse oleku ja tellimuse oleku kohta. Lahendamist nõudvate probleemide tuvastamise korral kuvatakse teate kõrval nupp **Paranda**; selle nupu klõpsamisel saate turbeprobleemid lahendada.

Jaotises **Soovitused** on loetletud toimingud, mis tuleks teha rakenduse töö optimeerimiseks ja tõhusamaks kasutamiseks.

Jaotises **Uudised** kuvatakse [küberturbeuudiseid](#).

Nupu **Kuva N eiratud teadet** klõpsamisel kuvatakse teatiseid, millele on rakendatud toiming **Ignoreeri**. Eiratud teated ei mõjuta rakenduse põhiaknas kuvatava kaitsetähise värvi.

Arvuti turbeprobleemide lahendamine

Arvuti turbeprobleemide lahendamiseks tehke järgmist.

1. Avage rakenduse peaken.
2. Klõpsake rakenduse põhiakna ülaosas linki **Üksikasjad**, et avada aken **Teatiste keskus**.
3. Avage jaotis **Olek**. Selles jaotises kuvatakse teie arvuti turbeprobleemid.
 - Valige loendist probleem ja klõpsake soovitud toimingunuppu, nt **Paranda**.
 - Kui te ei soovi seda probleemi kohe lahendada, valige ripploendist **Ignoreeri**. Ignoreeritud teatiste loendit saate hiljem vaadata, klõpsates nuppu **Kuva N eiratud teatist**.
4. Avage jaotis **Soovitused**. Selles jaotises kuvatakse soovitused, mis pole kohustuslikud, kuid aitavad teil rakenduse kasutust optimeerida ja arvutit paremini kaitsta.
 - a. Valige loendist soovitus.
 - b. Klõpsake soovitatud toimingu kõrval asjakohast nuppu. Näiteks võite soovituse **Lülita sisse** kõrval klõpsata nuppu **Kas soovite segavatest hüpikreklaamidest lahti saada?**

5. Avage jaotis **Uudised**. Sellest jaotisest leiate [küberturbega seotud uudiseid](#). Järgmise uudisepostituse lugemiseks või eelmisele uudisele naasmiseks kasutage navigeerimisnuppe.

Turvauudised

Sellest jaotisest leiate teavet Kaspersky turvauudiste kohta.

Teave turvauudiste kohta

Iga päev toimub maailmas üha rohkem massilisi paroolivargusi, andmebaasihäkkimisi ja e-panganduspettusi. Kaspersky turvauudised annavad selliste kuritegude kohta värsket teavet ja aitavad teil vältida olukordi, kus võite langeda häkkerite ohvriks. Tagamaks, et saadud turvauudised oleksid teie jaoks asjakohased, analüüsib rakendus teavet teie külastatud ressursside ja kasutatavate rakenduste kohta. Seda teavet kasutatakse ainult teie jaoks oluliste või huvipakkuvate uudiste valimiseks.

Turvauudised kuvatakse teadete keskuses koos teiste Kaspersky uudistega. Turvauudiste teated kuvatakse tegumiriba teavitusalal. Teateaknad sisaldavad uudise pealkirja ja lühisoovitust uudises kirjeldatud probleemi lahendamise kohta.

Raskusastme põhjal on uudised liigitatud järgmistesse tüüpidesse.

- *Tähtsad uudised* – uudised sündmustest, mis võivad ohustada teie turvalisust (näiteks uudised Facebooki paroolide massilise varguse kohta). Tähtsate uudiste aknad on kollased.
- *Üldised uudised* – teavitamiseks mõeldud uudised (näiteks uudised üha sagedamini esinevatest juhtumitest, kus Trooja programmi pahavara on põhjustanud e-panganduses andmeturbemurde). Üldiste uudiste aknad on rohelised.


Kui ekraanil kuvatakse teade turvauudise kohta, saate uudise täisteksti avamiseks klõpsata hüpikaknas nuppu **Üksikasjad** või hüpikakna sulgeda. Uudiste täisteksti saate igal ajal avada, kui valite teadete keskuse uudiste loendist soovitud uudise.

Kui te ei soovi kindlas seadmes turvauudiseid saada, [saate keelata uudiste kuvamise](#). Kui te ei soovi uudiseid mitte üheski seadmes, [saate My Kasperskys keelata uudiste vastuvõtmise](#).

Turvauudiseid ei kuvata esimesel töötunnil pärast rakenduse paigaldamist.

Turvauudiste lubamine või keelamine

Turvauudiste lubamiseks või keelamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Liidese seaded**.

Avatakse aken **Liidese seaded**.

4. Tehke jaotises **Reklaammaterjalid** ühte järgmistest.

- Kui soovite saada turvauudiseid, märkige ruut **Võta Kasperskyst vastu teavitusteateid ja reklaame**.
- Kui te ei soovi turvauudiseid saada, eemaldage ruudust **Võta Kasperskyst vastu teavitusteateid ja reklaame** märged.

My Kasperskys turvauudiste saamise lubamine või keelamine

My Kasperskys turvauudiste saamise lubamiseks või keelamiseks tehke järgmist.

1. Avage My Kaspersky avaleht.

2. Klõpsake nuppu **Logi sisse** ning sisestage konto loomisel määratud meiliaadress ja parool.

3. Klõpsake nuppu .

See avab teadete kuvamise akna.

4. Teadete sätete akna avamiseks klõpsake linki **Seaded**.

5. Tehke üks järgmistest toimingutest.

- Kui soovite turvauudiste vastuvõtmise lubada, märkige ruut **Turvauudised**.
- Kui soovite turvauudiste vastuvõtmise keelata, eemaldage ruudust **Turvauudised** märged.

Rakenduse tegevuste logi ja üksikasjalik aruanne

Peaaknas on lühiülevaade kõikidest tegevustest, mida rakendus töö käigus teeb. See teave aitab teil täpselt mõista, kuidas rakendus teie seadet ja andmeid kaitseb.

Ajaskaala vaatamiseks toimige järgmiselt.

1. Avage rakenduse peaaken.

Vaadake jaotises **Avaleht Ajaskaala** alt rakenduse tegevuste lühiajalugu.

2. Rakenduse tegevuste ajaloo vaatamiseks klõpsake nuppu **Kuva kõik**.

Avaneb aken üksikasjaliku kirjeldusega rakenduse tegevuste kohta ja sündmuste toimumise aja kohta.

3. Rakenduse üksikasjaliku aruande vaatamiseks klõpsake nuppu **Kuva aruanded**.

See viib teid aknasse **Aruanded**.

Üksikasjalik aruanne avaneb ka siis, kui klõpsate jaotises **Turvalisus Aruanded**. Aknas **Aruanded** kuvatakse andmed tabelina. Aruannete hõlpsamaks vaatamiseks saate kasutada mitmesugused filtreerimisvalikud.

Rakenduse kasutajaliidese seadistamine

See jaotis sisaldab teavet rakenduse liidese seadmise kohta.

Rakenduse teadete seadistamine

Tegumiriba teavitusalas kuvatavad teated teavitavad teid rakenduse sündmustest, mis vajavad teie sekkumist. Sündmuse kriitilisusest olenevalt võite saada järgmist tüüpi teateid.

- *Kriitilised teated* teavitavad teid sündmustest, millel on arvutiturvalisuse seisukohast kriitiline tähtsus, näiteks operatsioonisüsteemist pahatahtliku objekti või ohtliku tegevuse avastamisest. Kriitiliste teadete ja hüpiksõnumite aknad on punased.
- *Olulised teated* teavitavad teid arvutiturvalisuse seisukohast potentsiaalselt olulistest sündmustest, näiteks operatsioonisüsteemist arvatavalt nakatunud objekti või kahtlase tegevuse avastamisest. Oluliste teadete ja hüpiksõnumite aknad on kollased.
- *Teabeteated* teavitavad teid sündmustest, millel pole arvutiturvalisuse seisukohast kriitilist tähtsust. Teabeteadete ja hüpiksõnumite aknad on rohelised.


Kui ekraanil kuvatakse teade, tuleb teil teha üks teates pakutavatest valikutest. Optimaalne valik on see, mida Kaspersky eksperdid soovivad vaikevalikuna.

Teade võib automaatselt sulguda arvuti taaskäivitamisel, Kaspersky rakenduse sulgemisel või Windows 8 ühendatud ooterežiimis. Sissetungide vältimise teated suletakse automaatselt pärast 500 sekundi möödumist. Rakenduse käivitamise kohta kuvatavad teated suletakse automaatselt pärast 1 tunni möödumist. Teate automaatse sulgumise korral teeb Kaspersky rakendus soovitatud vaiketoimingut.

Rakenduse teadete seadmise kohta teabe saamiseks klõpsake allolevaid linke.

[Teadete edastamise seadistamine](#) 

Teatereeglite loomiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Liidese seaded**.
4. Teadete seadete akna avamiseks klõpsake plokis **Teatised** linki **Teadete seaded**.
5. Valige vasakul kuvatud loendist komponent.
Akna paremas servas kuvatakse loend sündmustest, mis võivad aset leida selle komponendi töötamise ajal.
6. Valige loendist sündmus ja märkige järgmiste seast soovitud ruudud.
 - **Salvesta kohalikku aruandesse**. Sündmuse toimumise korral kirjutatakse teave selle sündmuse kohta aruandesse, mida talletatakse kohalikus arvutis.
 - **Teavita ekraanil**. Sündmuse toimumise korral kuvatakse tegumiriba teavitusalas rakenduseikooni kohal hüpikteade.


Vasakus allnurgas kuvatava ripploendi abil saate määrata, millised teated soovite kohalikku aruandesse salvestada.

- **Vaikimisi**. Selle valiku korral salvestab loodud aruanne Kaspersky ekspertide valitud sündmused.
- **Käsitsi**. See valik tehakse automaatselt, kui seadistate sündmuste aruandesse salvestamise funktsiooni käsitsi.
- **Kriitiline**. Selle valiku korral salvestatakse genereeritud aruandesse **Kriitilised sündmused** (sealhulgas *rakenduse rikkesündmused* komponentide **Süsteemi audit** ja **Sissetungitõrje** kohta).
- **Oluline**. Selle valiku korral salvestatakse genereeritud aruandesse **Kriitilised sündmused** (sealhulgas *rakenduse rikkesündmused* komponentide **Süsteemi audit** ja **Sissetungitõrje** kohta) ning **Hoiatused**.
- **Informatiivne**. Selle valiku korral salvestab loodud aruanne kõik sündmused.


Teavitused kõigi sündmusega **Rakendus töötab ja töötleb andmeid vastavalt asjaomastele õigusaktidele ja kasutab sobivat infrastruktuuri** seotud muudatuste kohta kuvatakse alati tegumiriba ekraanil. Märkeruudu tühjendamine ei muuda sätet.

[Kaspersky uudiseid ja eripakkumisi sisaldavate teadete edastamise seadistamine](#) 

Kui soovite olla kursis viimaste küberturbeuudistega ja saada Kasperskylt eripakkumisi, tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Avage jaotis **Liidese seaded**.
4. Kui soovite saada teateid arvuti turvalisuse uudiste kohta märkige plokis **Teata uudistest** ruut **Võta Kasperskyst vastu teavitusteateid ja reklaame**.
5. Tehke jaotises **Reklaammaterjalid** ühte järgmistest.
 - Kui soovite saada teatise arvuti turvauudiste kohta, märkige ruut **Võta Kasperskyst vastu teavitusteateid ja reklaame**.
 - Märkige ruut **Näita teavet veebisaitide eripakkumiste kohta**, kui soovite Kaspersky veebisaitide külastamisel saada parimaid pakkumisi.
 - Kui soovite pärast tellimuse aegumist saada Kasperskylt teateid turbeuudiste kohta, märkige ruut **Võta vastu informatiivseid sõnumeid ja reklaame pärast kehtiva tellimuse aegumist**.

Teavitushelide lubamine


1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Liidese seaded**.
4. Märkige plokis **Teated** ruut **Luba heliteated**.
Vaikehelisignaali vahetamiseks seakiunatuse vastu tippige aknasse **Info** tähed **IDKFA**.

Heliteateid ei esitata operatsioonisüsteemis Microsoft Windows 10.

Kuidas konfigureerida teavitusi, kui rakendust kasutab laps

Kui teie arvutisse on installitud Kaspersky Safe Kids, saate Kaspersky teated ajaks, kui arvutit kasutab laps, sisse või välja lülitada.

Teavituste konfigureerimiseks, kui rakendust kasutab laps, tehke järgmist.


1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Avage jaotis **Liidese seaded**.
4. Valige suvand:
 - Kaspersky teadete väljalülitamiseks ajaks, kui rakendust kasutab laps, tühjendage märkeruut **Kuva teateid laste kontodel**.
 - Kaspersky teadete sisselülitamiseks ajaks, kui rakendust kasutab laps, märkige ruut **Kuva teateid laste kontodel**.

Üksikasjad [Kaspersky rakenduse konfigureerimise kohta, kui arvutit kasutab laps](#).

Rakenduse kujundusteema muutmine

Rakenduse kujundusteema muutmise võimalus pole kõigis piirkondades saadaval.

Rakenduse kujundusteema muutmiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Liidese seaded**.
4. Tehke plokis **Kujundusteema** üks järgmistest valikutest:
 - **Sama nagu operatsioonisüsteemil**. Kasutatakse praegust operatsioonisüsteemi kujundusteemat.
 - **Hele**. Kasutatakse heledat rakenduse kujundusteemat.
 - **Tume**. Kasutatakse tumedat rakenduse kujundusteemat.
 - **Kasuta kohandatud kujundusteemat**, kui soovite kasutada kohandatud kujundusteemat. Klõpsake nuppu **Vali** ja sisestage kohandatud kujundusteema faile sisaldava ZIP-arhiivi või kausta tee.


Kujundusteema rakendatakse pärast rakenduse taaskäivitamist.

Rakenduseikooni muutmine

See jaotis sisaldab teavet, kuidas muuta rakenduseikooni töölaual ja teavitusalas.

[Rakenduseikooni muutmine](#)


Rakenduseikooni muutmiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Liidese seaded**.
4. Tehke plokis **Rakenduse ikoon** üks järgmistest valikutest:
 - **Standardikoon**. Selle valiku korral kuvatakse töölaual ja teavitusalas rakenduse standardikoon.
 - **Midori Kuma**. Selle valiku korral kuvatakse töölaual ja teavitusalas ikoon, mis kujutab Midori Kuma nime kandva karumaskoti pilti.

Kui soovite siiski kasutada traditsioonilist K-tähega rakenduseikooni, tippige aknasse **Info IDDQD**. Muudatuste rakendamiseks peate arvuti taaskäivitama.

[Ikooni muutmine teavitusalas vastavalt kaitse seisundile](#)

Teavitusalal Kaspersky rakenduseikooni muutmiseks vastavalt rakenduse olekule tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Liides**.
4. Valige plokis **Näita rakenduste seisundit teavitusalal** seisund ja märkige ruut.


Kui rakendus lülitub valitud seisundile vastavasse olekusse, muutub teavitusalas rakenduseikoon.

Juurdepääsu rakenduse haldusfunktsioonidele kaitsmine parooliga

Ühte arvutit võivad ühiselt kasutada mitu kasutajat, kellel on erinev kogemuste pagas ja arvutikasutusoskus. Eri kasutajate piiramatult juurdepääs rakendusele ja selle seadetele võib vähendada arvuti turvalisust.

Rakendusele juurdepääsu piiramiseks saate kontole KLAdmin määrata administraatori parooli. Sellel kasutajal on rakenduse seadete haldamiseks ja muutmiseks ning teistele kasutajatele rakenduse juurdepääsuõiguste andmiseks piiramatud õigused. Pärast kasutaja KLAdmin parooli loomist saate määrata rakenduse juurdepääsuõigused eri kasutajatele või kasutajagruppidele.

KLAdmin -i administraatoriparooli loomiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Liidese seaded**.
4. Seadke **Parooliga kaitse** asendisse **Sees**.
5. Avanenud aknas täitke väljad **Kasutajanimi** (soovitav on KLAdmin), **Sisestage parool** ja **Kinnitage parool**.
Tugeva parooli loomiseks järgige järgmisi nõuandeid.
 - Parool peab sisaldama vähemalt kaheksat ja mitte rohkem kui 128 tähemärki.
 - Parool sisaldab vähemalt ühte numbrit.
 - Parool sisaldab nii väiketähti kui ka suurtähti.
 - Parool peab sisaldama vähemalt ühte erimärki (näiteks: ! @ # \$ % ^ & *).
6. Klõpsake nuppu **Salvesta**.

Unustatud parooli ei saa taastada. Kui olete parooli unustanud, võtke rakenduse seadetele juurdepääsu taastamiseks ühendust tehnilise toega.

Kasutaja KLAdmin saab määrata õigused järgmistele kasutajatele ja kasutajagruppidele.

- Kasutajagrupp **Kõik**. Sellesse gruppi kuuluvad kõik operatsioonisüsteemi kasutajad. Kui annate sellele grupile konkreetse toimingute tegemiseks loa, on grupi kasutajatel alati lubatud seda toimingut teha isegi juhul, kui kasutajagruppi **Kõik** kuuluval konkreetset kasutajal või kasutajagrupil pole toimingute tegemiseks eraldi luba. Vaikimisi ei ole grupi **Kõik** liikmetel lubatud teha mitte ühtki toimingut.
- <süsteemikasutaja>. Vaikimisi pole valitud kasutajal lubatud teha mitte ühtki toimingut. See tähendab, et kui proovite teha keelatud toimingut, palutakse teil sisestada konto KLAdmin parool.

[Kasutaja või kasutajagrupi lisamine](#) 

1. Klõpsake jaotise **Liidese seaded** plokis **Näita rakenduste seisundit teavitusalal** nuppu **Lisa**.
Avatakse aken **Lisa õigusi kasutajale või rühmale**.
2. Operatsioonisüsteemi kasutaja või kasutajagrupi valimise akna avamiseks klõpsake linki **Vali kasutaja või rühm**.
3. Määrake objektinime sisestusväljal kasutaja või kasutajagrupi nimi (näiteks **Administraator**).
4. Klõpsake **OK**.
5. Akna **Lisa õigusi kasutajale või rühmale** plokis **Õigused** märkige ruudud nende toimingute kõrval, mille soovite konkreetsele kasutajale või kasutajagrupile lubada.

Kasutaja või kasutajagrupi õiguste muutmine ?

Valige jaotise **Liidese seaded** plokis **Näita rakenduste seisundit teavitusalal** loendist kasutaja või kasutajagrupp ja klõpsake nuppu **Muuda**.

Üksikule kasutajale või kasutajagrupile toimingute lubamine ?

1. Avage grupi **Kõik** aken **Lisa õigusi kasutajale või rühmale** ja eemaldage märged toimingute lubamise ruudust, kui see on märgitud.
2. Avage valitud kasutaja aken **Lisa õigusi kasutajale või rühmale** ja märkige toimingute lubamise ruudud.

Üksikule kasutajale või kasutajagrupile toimingute keelamine ?

1. Avage grupi **Kõik** aken **Lisa õigusi kasutajale või rühmale** ja eemaldage märged toimingute lubamise ruudust, kui see on märgitud.
2. Avage valitud kasutaja aken **Lisa õigusi kasutajale või rühmale** ja eemaldage märged toimingute lubamise ruudust.


Kui proovite teha akna **Lisa õigusi kasutajale või rühmale** loendis sisalduvat mis tahes toimingut, küsib rakendus parooli. Sisestage parooliaknas praeguse kasutajakonto kasutajanimi ja parool. Toiming tehakse, kui määratud kontol on toimingute tegemiseks luba. Parooliaknas saate määrata ajavahemiku, mille jooksul ei pea kasutaja parooli uuesti sisestama.

Parooliaknas saate sisestuskeelt vahetada klahvikombinatsiooniga **ALT + tõstuklahv**. Muude otseteede korral sisestuskeelt ei vahetata – ka siis mitte, kui see otsetee on konfigureeritud operatsioonisüsteemis.

Rakenduse vaikeseadete taastamine

Saate igal ajal taastada Kaspersky ekspertide soovitatud rakenduse seaded. Seadete taastamise korral seatakse kõigile kaitsekomponentidele turbetase **Optimaalne**.

Rakenduse vaikeseadete taastamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Halda seadeid**.
4. Seadete taastamise nõustaja käivitamiseks klõpsake linki **Taasta**.
5. Klõpsake **Edasi**.
Nõustaja aken näitab rakenduse seadete tagasi Kaspersky ekspertide seadistatud vaikeseadeteks taastamise edenemist.
6. Pärast rakenduse vaikeseadete taastamise lõpuleviimist klõpsake nuppu **Valmis**.

Rakenduse seadete rakendamine teises arvutis

Kui olete Kaspersky endale meelepärasel moel häälestanud, saate samu seadeid rakendada ka mõnes teises arvutis. Selle tulemusel häälestatakse Kaspersky mõlemas arvutis täiesti ühtemoodi.


Kaspersky rakenduse seaded salvestatakse konfiguratsioonifaili, mille saate teisaldada ühest arvutist teise.

Kaspersky rakenduse seaded teisaldatakse ühest arvutist teise kolmes etapis.

1. Salvestage Kaspersky rakenduse seaded konfiguratsioonifaili.
2. Teisaldage konfiguratsioonifail teise arvutisse (näiteks meili teel või irdkettal).
3. Importige seaded konfiguratsioonifailist teise arvutisse installitud Kaspersky rakendusse.

[Seadete eksportimine](#) 

Kaspersky seadete eksportimiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige aknas **Seaded** jaotis **Halda seadeid**.
4. Valige **Ekspordi**.
5. Avaneb aken **Salvesta**.
6. Sisestage konfiguratsioonifaili nimi ja klõpsake nuppu **Salvesta**.


Rakenduse seaded on nüüd salvestatud konfiguratsioonifaili.

Kaspersky rakenduse seadeid saate eksportida ka käsuviibalt järgmise käsu abil: `avp . com EXPORT <faili_nimi>`.

Kaspersky rakenduse seadete eksportimisel salvestatakse komponenti Turvalised maksed lisatud veebisaidiaadressid ainult praeguse kasutaja jaoks. Seadete importimisel teise arvutisse veebisaitide aadresse ei salvestata.

Seadete importimine

Seadete importimiseks teise arvutisse installitud Kaspersky rakendusse tehke järgmist.

1. Avage teises arvutis Kaspersky peaaken.
2. Klõpsake akna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige aknas **Seaded** jaotis **Halda seadeid**.
4. Valige **Impordi**.
Avaneb aken **Ava**.
5. Määrake konfiguratsioonifail ja klõpsake nuppu **Ava**.

Seaded imporditakse teise arvutisse installitud Kaspersky rakendusse.

Kaitse peatamine tähendab kõigi kaitsekomponentide mõneks ajaks ajutiselt väljalülitamist.

Kui kaitse on peatatud või Kaspersky rakendus ei tööta, jälgitakse teie arvutis töötavate rakenduste tegevust. Teave rakendustegevuse seire tulemuste kohta salvestatakse operatsioonisüsteemi. Kui Kaspersky rakendus taaskäivitatakse või kaitse taastatakse, kasutab rakendus seda teavet teie arvuti kaitsmiseks pahatahtlike toimingute eest, mis võivad olla tehtud ajal, kui kaitse oli peatatud või kui Kaspersky rakendus ei töötanud. Teave rakendustegevuse seire tulemuste kohta salvestatakse määramata ajaks. See teave kustutatakse, kui Kaspersky rakendus eemaldatakse teie arvutist.

Arvutikaitse peatamiseks tehke järgmist.

1. Valige tegumiriba teavitusalal kuvatava Kaspersky ikooni kontekstimenüüst käsk **Peata kaitse**.

Avatakse aken **Kaitse peatamine**.

2. Valige aknas **Kaitse peatamine** ajavahemik, mille möödumise järel kaitse taastatakse.

- **Peata**: – kaitse lülitatakse sisse pärast ripploendist valitud ajavahemiku möödumist.
- **Peata, kuni rakendus taaskäivitub** – kaitse lülitatakse sisse pärast rakenduse uuesti käivitamist või operatsioonisüsteemi taaskäivitamist (kui rakendus käivitub süsteemi käivitamise korral automaatselt).
- **Peata** – kaitset jätkatakse siis, kui teie otsustate seda jätkata.

3. Klõpsake nuppu **Peata kaitse** ja kinnitage avanenud aknas oma valik.

[Arvutikaitse taastamine](#)

Arvutikaitse taastamiseks tehke järgmist.

Valige tegumiriba teavitusalal kuvatava Kaspersky ikooni kontekstimenüüst **Taasta kaitse**.

Kaspersky rakenduse hindamine

Saate meie rakendust hinnata ja saata oma hinde Kasperskyle.

Mõni aeg pärast paigaldamist pakub rakendus teile võimalust selle töö hindamiseks.

Rakenduse hindamiseks tehke järgmist.

1. Aknas **Me hindame teie arvamust** tehke üht järgmistest.

- Kui olete Kaspersky hindamiseks valmis, hinnake rakendust 10-pallisel skaalal.
- Kui te ei soovi rakendust hinnata, klõpsake hindamisakna sulgemiseks nuppu **x**.

2. Klõpsake nuppu **Saada**.

3. Akna sulgemiseks klõpsake nuppu **Sule**.

Milliseid andmeid rakenduse hindamisel edastatakse

Lisaks hinnangule töötleb Kaspersky järgmist teavet, mis on vajalik küsitluse analüüsimiseks.

- Kaspersky rakenduse nimi ja versioon
- Operatsioonisüsteemi versioon
- Kaspersky rakenduse aktiveerimispiirkond ja kasutajaliidese keel
- Kaspersky rakenduse kasutusperiood

Turvalisus

Tänapäeva häkkerid muutuvad teie seadmetesse sissemurdmises järjest targemaks. Uus lunavara-, andmepüügi- ja muud tüüpi pahavara nõuab uusi küberturbelahendusi, et oleksite kasvavatest ohtudest sammu võrra ees. Lõime uue Kaspersky rakenduse selleks, et aidata teil tänapäevaste ohtudega sammu pidada. Uurige, mida saate teha, et end turvaliselt tunda.

Arvuti kontrollimine

Kontrolli käigus otsib rakendus nakatunud faile ja pahavara. Kontrolle on mitut eri tüüpi, mis erinevad otsingu kestuse ja ulatuse poolest.

- Täiskontroll. Kontrollib kõiki arvutialasid. Selle kontrolli lõpuleviimiseks kulub palju aega.
- Kiirkontroll. Kontrollib nii operatsioonisüsteemi käivitamisel laaditud objekte kui ka süsteemimälu ja algladimisfaile. Selle kontrolli lõpuleviimiseks ei kulu kuigi palju aega.
- Valikuline kontroll. Kontrollib valitud faili või kausta.
- Irdkettakontroll. Kontrollib irdkettaid, näiteks arvutiga ühendatud kõvakettaid ja USB-mäluseadmeid.
- Kiire failide kontroll. See valik käivitab failikontrolli kontekstimenüüst.
- Taustal toimuv kontroll. Süsteemimälu, süsteemisektsiooni, algladimissektorite ja käivitusobjektide kontroll ning rootkit'ide otsing.
- Rakenduse haavatavuste kontroll. Arvutist otsitakse rakendustest haavatavusi, mida pahavara saab teie süsteemi nakatamiseks ära kasutada.

Pärast rakenduse installimist soovitame teil teha arvuti täiskontrolli.

Kiirkontrolli käivitamine

Kiirkontrolli käigus kontrollib rakendus vaikumisi järgmisi objekte.

- Operatsioonisüsteemi käivitamisel laaditud objektid
- Süsteemi mälu
- Ketta algladimissektorid

Kiirkontrolli käivitamiseks tehke järgmist.

1. Avage rakenduse peaaaken ja tehke seal järgmist.

- Minge jaotisse **Avaleht** ja klõpsake nuppu **Kiirkontroll**.
- Avage jaotis **Turvalisus**.

1. Klõpsake jaotises **Kontroll** nuppu **Valige kontroll**.
2. Avatakse aken **Kontroll**.
3. Valige aknas **Kontroll** jaotis **Kiirkontroll**.
4. Klõpsake jaotises **Kiirkontroll** nuppu **Käivita kontroll**.

Rakendus käivitab arvuti kiirkontrolli.

Täiskontrolli käivitamine

Täiskontrolli käigus kontrollib rakendus vaikumisi järgmisi objekte.

- Süsteemi mälu
- Operatsioonisüsteemi käivitamisel laaditud objektid
- Süsteemi varuhoidla
- Kõvakettad ja irdkettad

Soovitame teha täiskontrolli kohe pärast rakenduse arvutisse installimist.

Täiskontrolli käivitamiseks tehke järgmist.

1. Avage rakenduse peaaken ja minge jaotisse **Turvalisus**.
2. Klõpsake jaotises **Kontroll** nuppu **Valige kontroll**.
Avatakse aken **Kontroll**.
3. Valige aknas **Kontroll** jaotis **Täiskontroll**.
4. Valige nupu **Käivita kontroll** kõrval asuvast ripploendist toiming, mis tuleks teha pärast kontrollimise lõpetamist.
5. Klõpsake **Käivita kontroll**.

Rakendus käivitab arvuti täiskontrolli.

Kohandatud kontrolli käivitamine

Valikulise kontrolliga saate kontrollida, kas failis, kaustas või kettal on viiruseid ja muid ohte.

Kohandatud kontrolli käivitamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Turvalisus**.

3. Klõpsake jaotises **Kontroll** nuppu **Valige kontroll**.

Avatakse aken **Kontroll**.

4. Valige aknas **Kontroll** jaotis **Valikuline kontroll**.

5. Klõpsake nuppu **Vali** ja määrake avanenud faili- või kaustavaliku aknas soovitud objekt.

6. Klõpsake **Käivita kontroll**.

Irdkettakontrolli käivitamine

Arvutiga ühendatud irdkettad võivad sisaldada viirusi või muid ohtlikke rakendusi. Arvuti nakatumise ennetamiseks kontrollib Kaspersky rakendus irdkettaid. Irdkettakontrolli saate seadistada arvutiga irdketta ühendamise korral käivituma käsitsi või automaatselt. Vaikimisi on lubatud irdketaste automaatne kontrollimine.

Irdkettakontrolli käsitsi käivitamiseks tehke järgmist.

1. Avage rakenduse peaaaken.

2. Avage jaotis **Turvalisus**.

3. Klõpsake jaotises **Kontroll** nuppu **Valige kontroll**.

Avatakse aken **Kontroll**.

4. Valige aknas **Kontroll** jaotis **Irdkettakontroll**.

5. Valige ripploendist välisseadme kettatähis ja klõpsake nuppu **Käivita kontroll**.

Rakendus alustab ühendatud seadme kontrollimist.

Faili või kausta kontekstimenüükontrolli käivitamine

Faili või kausta kontekstimenüükontrolli käivitamiseks tehke järgmist.

1. Paremkõpsake faili või kausta, mida tuleb kontrollida.

2. Valige avanenud kontekstimenüüs **Kontrolli, kas on viiruseid**.

Rakendus alustab valitud faili või kausta kontrollimist.

Microsoft Windows 11 arvutis peate rakenduse käskude nägemiseks objekti kontekstimenüüd laiendama.

Taustal toimuva kontrolli sisselülitamine või väljalülitamine

Taustal toimuv kontroll on automaatne kontrollimisrežiim, milles ei kuvata teateid. See kontroll nõuab vähem arvutiressursse kui muud tüüpi kontrollid (näiteks täiskontroll). Selles režiimis kontrollib rakendus süsteemimälu, süsteemimahte, algladimis sektoreid ja käivitusobjekte ning otsib rootkit'e.

Taustkontroll käivitatakse järgmistel juhtudel.


- Pärast andmebaaside ja rakendusmoodulite uuendamist
- 30 minutit pärast rakenduse käivitamist
- Iga kuue tunni tagant.
- Kui arvuti jääb jõudeolekusse viieks või enamaks minutiks (pärast ekraanisäästja käivitumist).

Taustkontroll katkestatakse, kui täidetud on üks järgmistest tingimustest.

- Arvuti muutub uuesti aktiivseks
- Arvuti (sülearvuti) lülitub akurežiimile.


Kui taustal toimuvat kontrolli pole tehtud rohkem kui kümme päeva, siis kontrolli ei peatata. Taustkontrolli käigus ei kontrolli rakendus faile, mille sisu asub OneDrive'i pilvsalvestusruumis.

Taustkontrolli lubamiseks või keelamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Turvalisus**.
3. Klõpsake jaotises **Kontroll** nuppu **Valige kontroll**.
Avatakse aken **Kontroll**.
4. Klõpsake ikooni  jaotises **Kontroll toimub taustal**.
Avatakse aken **Taustal tehtava kontrolli seaded**.
5. Seadke aknas **Taustal tehtava kontrolli seaded** lüliti asendisse **Sees** või **Väljas**.

Kontrollimise ajakava loomine

Kontrollimise ajakava loomiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Turvalisus**.
3. Klõpsake jaotises **Kontroll** nuppu **Valige kontroll**.
Avatakse aken **Kontroll**.
4. Valige aknas **Kontroll** kontrolli tüüp ja klõpsake ikooni .
5. Avanenud aknas klõpsake akna **Kontrollimise ajakava** avamiseks linki **Kontrollimise ajakava**.

6. Valige akna **Kontrollimise ajakava** loendis **Käivita kontroll** ajavahemik, näiteks **iga päev**, ja määrake kontrolli algusaeg.

Kontrollimise ajakava ei saa luua kontekstimenüüst käivitatava kontrolli ega taustal toimuva kontrolli jaoks.

Arvutisse paigaldatud rakenduste haavatavuste otsimine

Teie arvutisse paigaldatud rakendustel võib olla haavatavusi, mida pahavara saab ära kasutada. Arvuti kontrollimine aitab need haavatavused üles leida ja ennetada arvuti nakatumist.


Rakenduse haavatavuste kontrolli käivitamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Turvalisus**.
3. Klõpsake jaotises **Kontroll** nuppu **Valige kontroll**.
Avatakse aken **Kontroll**.
4. Valige aknas **Kontroll** jaotis **Rakenduse haavatavuste kontroll**.
5. Klõpsake **Käivita kontroll**.

Rakendus käivitab arvuti rakenduste haavatavuste kontrolli.

Kindla faili, kausta või ohutüübi kontrollimisest välja jätmine

Kindla faili, kausta või ohutüübi kontrollimisest välja jätmiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige **Turvaseaded** → **Ohud ja erandid**.
4. Akna **Halda erandeid** avamiseks klõpsake linki **Erandid**.
5. Klõpsake **Lisa**.
6. Erandi lisamiseks on järgmised võimalused.
 - Klõpsake nuppu **Sirvi** ja valige kaust või fail, mille soovite kontrollimisest välja jätta. Klõpsake **Vali**.
 - Sisestage faili või kausta täisnimi või mask väljale **Fail või kaust**.
 - Sisestage väljale **Objekt** ohutüübi täisnimi või mask vastavalt tuvastatud objekti Kaspersky liigitusele.

- Kui täidate mõlemad väljad (**Fail või kaust** ja **Objekt**), ei kontrollita määratud faili või kausta määratud ohutüübi suhtes.
 - Kui soovite faile kontrollimisest välja jätta räsi põhjal, sisestage räsi väljale **Faili räsi**.
7. Tühjendage nende kaitsekomponentide märkeruudud, millele välistamisreeglit ei rakendata. Soovi korral võite lisada kommentaari.
8. Valige reegli jaoks olek **Aktiivne** ja klõpsake nuppu **Lisa**.

Määratud objektid jäetakse kontrollimisest välja.

[Lisateave akna „Ohud ja erandid“ seadete kohta](#)

OneDrive'i pilvhoidlas failide kontrollimine

Versioonis Windows 10 RS3 või uuemas versioonis ei kontrolli rakendus pilvhoidlas olevaid faile. Kui rakendus tuvastab kontrollimise ajal sellised failid, kuvatakse teade, mis kinnitab, et pilvhoidlas olevaid faile ei kontrollitud.

OneDrive'i pilvhoidlas olevaid faile ei kontrolli järgmised komponendid.

- Täiskontroll
- Valikuline kontroll
- Kiirkontroll
- Taustal toimuv kontroll.

Rakenduse tööaruanne sisaldab kontrollimisel vahele jäetud OneDrive'i pilvhoidla failide loendit.

OneDrive'i pilvhoidlast kohalikku arvutisse alla laaditud faile kontrollivad reaajas töötavad kaitsekomponendid. Kui faili kontrollimine lükati edasi ja fail laaditakse enne kontrolli algust OneDrive'i pilvhoidlasse tagasi üles, võidakse see fail kontrolli ajal vahele jätta.

Rakenduste ja skriptide käitamisel laadivad sissetungitõrje ja süsteemiseire komponendid rakendused kontrollimiseks OneDrive'i pilvhoidlast kohalikku arvutisse alla.

Veendumaks, et OneDrive'i failid kuvatakse Exploreris, lülitage sisse funktsioon [OneDrive'i klientrakendus nõudetailid](#). Kui teil on internetiühendus, saate neid kasutada samamoodi nagu kõiki muid arvutis olevaid faile.

Viirusekaitse andmebaaside ja rakendusemoodulite uuendamine

See jaotis sisaldab teavet andmebaasi ja rakendusemooduli uuenduste kohta.

Andmebaaside ja rakendusemoodulite uuendamisest

Rakenduse installipakett sisaldab andmebaase ja rakendusemooduleid. Neid andmebaase kasutatakse järgmiselt.

- Rakendus tuvastab enamiku ohtudest Kaspersky Security Networki abil, mille kasutamiseks on vajalik internetiühendus.
- Rakendus tuvastab reklaamvara, automaatvalijad ja muu legitiimse tarkvara, mida sissetungijad võivad kasutada teie arvuti ja isiklike andmete kahjustamiseks.

Täieliku kaitse tagamiseks soovime viirusekaitse andmebaase ja rakendusemooduleid uuendada kohe pärast rakenduse paigaldamist.

Andmebaase ja rakendusemooduleid uuendatakse etappide kaupa.

1. Rakendus käivitab andmebaaside ja rakendusemoodulite uuenduse määratud seadete kohaselt: automaatselt, ajakava järgi või nõudmisel. Rakendus võtab ühendust uuendusallikaga, millesse on talletatud viirusekaitse andmebaasi ja rakendusemooduli uuenduspakett.
2. Rakendus võrdleb olemasolevaid andmebaase uuendusallikas saadaolevate andmebaasidega. Kui andmebaasid on erinevad, laadib rakendus andmebaaside puuduvad osad alla.

Seejärel kasutab rakendus arvutist viiruste ja muude ohtude otsimiseks uuendatud andmebaase ja rakendusemooduleid.

Uuendusallikad

Saate kasutada järgmisi uuendusallikaid.

- Kaspersky uuendusserverid
- HTTP- või FTP-server
- Võrgukaust

Erikaalutlused viirusekaitse andmebaaside ja rakendusemoodulite uuendamisel

Viirusekaitse andmebaaside ja rakendusemoodulite uuendustel on järgmised piirangud ja erijooned.

- Viirusekaitse andmebaasid loetakse aegunuks ühe päeva pärast ja väga aegunuks seitsme päeva pärast.
- Kaspersky serveritest uuenduspaketi allalaadimiseks on vaja internetiühendust.
- Viirusekaitse andmebaaside ja rakendusemoodulite uuendused ei ole saadaval järgmistel juhtudel.
 - Tellimus on aegunud ja ajapikendus või piiratud funktsionaalsuse režiim pole saadaval.
 - Kasutatakse mahupõhist mobiilset internetiühendust. See piirang kehtib arvutites, mille operatsioonisüsteem on Microsoft Windows 8 või uuem väljalase, kui sisse on lülitatud automaatsed uuendused või ajastatud uuendused ning mahupõhise mobiilandmesideühenduse jaoks on seatud liikluspiirang. Kui soovite, et rakendus uuendaks sellisel juhul viirusekaitse andmebaase ja rakendusemooduleid, eemaldage jaotises **Seaded** → **Turvaseaded** → **Täpsemad seaded** → **Võrgu seaded** märge ruudust **Piira liiklust mahupõhistel ühendustel**.
 - Rakendust kasutatakse teenusepakkuja kaudu ostetud tellimuse alusel ja te olete teenusepakkuja veebisaidil oma tellimuse lõpetanud.

Uuenduspaketi paigaldamine

Uuenduspaketi (paiga) saamisel installib rakendus selle automaatselt. Uuenduspaketi paigaldamise lõpuleviimiseks peate arvuti taaskäivitama. Kuni arvuti taaskäivitamiseni on rakenduse ikoon teavitusalas punane ja rakenduse aknas **Teatiste keskus** kuvatakse meeldetuletust arvuti taaskäivitamise kohta.

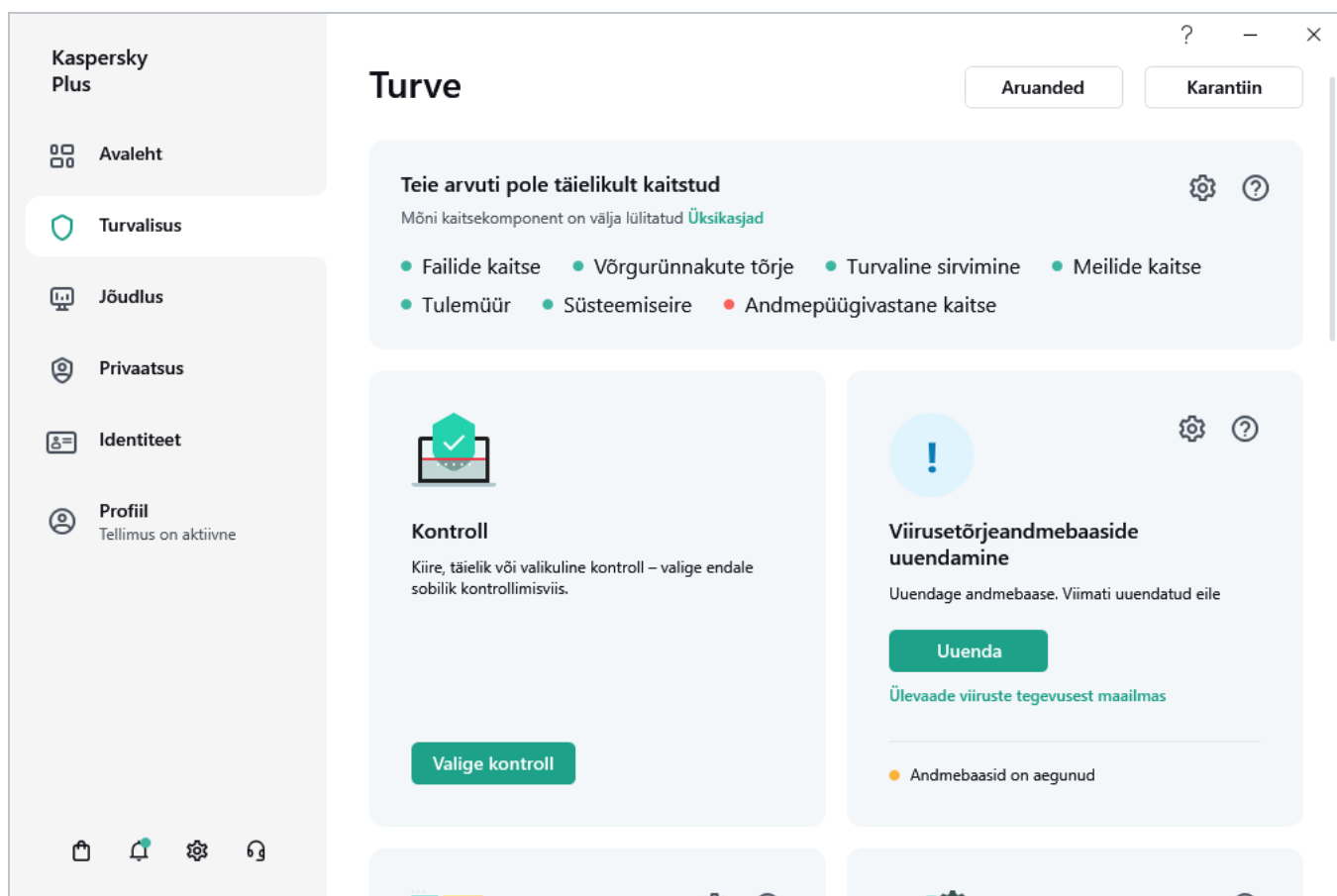
Andmebaaside ja rakendusemoodulite uuenduse käivitamine

Vaikimisi värskendatakse andmebaase ja rakendusemooduleid automaatselt. Te ei pea midagi tegema. Kui automaatsed värskendused on välja lülitatud, saate rakenduste andmebaase ja mooduleid värskendada käsitsi.

Andmebaaside ja rakendusemoodulite uuenduse käivitamiseks tehke nii.

1. Avage rakenduse peaken.
2. Avage jaotis **Turvalisus**.
3. Klõpsake jaotises **Viirusetõrjeandmebaaside uuendamine** nuppu **Uuenda**.

Viirusetõrjeandmebaaside värskendamine



Sissetungitõrje

Kaspersky rakendus aitab vähendada tundmatute rakenduste kasutamisega seotud riske (näiteks viiruste ja muu pahavaraga nakatumise riski).

Kaspersky rakendus sisaldab komponente ja tööriistu, mis võimaldavad kontrollida rakenduse reputatsiooni ja tegevust teie arvutis.

Sissetungitõrje kohta

Saadaval ainult plaanides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Sissetungitõrje komponent ei lase rakendustel teha toiminguid, mis võivad olla operatsioonile ohtlikud, ning kontrollib juurdepääsu operatsioonisüsteemi ressurssidele (sh kaugarvutites asuvatele failiresurssidele) ja teie isiklikele andmetele.

Sissetungitõrje jälgib operatsioonisüsteemis arvutisse paigaldatud rakenduste tehtavaid toiminguid ja reguleerib neid reeglite alusel. Need reeglid piiravad rakenduste kahtlast tegevust, sealhulgas rakenduste juurdepääsu kaitstud ressurssidele, näiteks failidele ja kaustadele, registrivõtmetele ja võrguaadressidele.

64-bitistes operatsioonisüsteemides ei saa seadistada rakenduste õigusi teha järgmisi toiminguid.

- Otsejuurdepääs füüsilisele mälule
- Printeridraiveri haldamine
- Teenuse loomine
- Teenuse lugemine
- Teenuse muutmine
- Teenuse ümberseadistamine
- Teenuse haldamine
- Teenuse käivitamine
- Teenuse eemaldamine
- Juurdepääs veebilehitseja siseandmetele
- Juurdepääs operatsioonisüsteemi kriitilistele objektidele
- Juurdepääs paroolihoidlale
- Silumisõiguste seadmine
- Operatsioonisüsteemi programmiliideste kasutamine
- Operatsioonisüsteemi programmiliideste kasutamine (DNS)
- Muude rakenduste programmiliideste kasutamine
- Süsteemimoodulite muutmine (KnownDlls)
- Draiverite käivitamine

64-bitises Microsoft Windows 8 ja Microsoft Windows 10 operatsioonisüsteemis ei saa seadistada rakenduste õigusi teha järgmisi toiminguid.

- Windowsi teadete saatmine teistele protsessidele
- Kahtlased toimingud
- Klaviatuurinuhkide paigaldamine
- Sissetulevate voosündmuste kinnipüüdmine
- Ekraanipiltide tegemine

Rakenduste võrgutegevust kontrollib tulemüüri komponent.

Arvutis rakenduse esmakordsel käivitamisel kontrollib sissetungitõrje rakenduse ohutust ja määrab selle gruppi (usaldusväärsed, ebausaldusväärsed, tugevad piirangud või nõrgad piirangud). Grupp määrab reeglid, mida Kaspersky rakenduse tegevuse kontrollimiseks kasutab.

Kaspersky rakendus määrab rakendused usaldusgruppidesse (Usaldusväärsed, Ebausaldusväärsed, Tugevad piirangud või Nõrgad piirangud) ainult juhul, kui Sissetungitõrje ja/või Tulemüür on sisse lülitatud. Kui mõlemad komponendid on välja lülitatud, siis rakendusi usaldusgruppidesse määrav funktsioon ei tööta.


Rakenduste kontrolli reegleid saate muuta käsitsi.

Rakenduste jaoks loodud reeglid pärandatakse edasi tütarrakendustele. Näiteks juhul, kui keelate cmd.exe jaoks kogu võrgutegevuse, keelatakse see ka notepad.exe korral, kui see käivitatakse cmd.exe kaudu. Rakendus ei päri reegleid, kui see pole selle rakenduse tütarrakendus, mille kaudu see käivitatakse.

Sissetungitõrje seadete muutmine

Saadaval ainult plaanides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Sissetungitõrje seadete muutmiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Turvaseaded**.
4. Valige komponent **Sissetungitõrje**.
5. Klõpsake aknas **Sissetungitõrje seaded** linki **Rakenduste haldus**, et avada aken **Rakenduste haldus**.
6. Akna **Rakenduste reeglid** avamiseks valige loendist soovitud rakendus ja topeltklõpsake selle nime.
7. Operatsioonisüsteemi ressurssidele juurdepääsemise reeglite rakendusesti seadistamiseks tehke järgmist.
 - a. Valige vahekaardil **Failid ja süsteemiregister** asjakohane ressursikategooria.
 - b. Menüü avamiseks klõpsake veerus ressursi jaoks saadaoleva toiminguga ikooni (**Loe**, **Kirjuta**, **Kustuta** või **Loo**). Valige menüüs asjakohane üksus (**Päranda**, **Luba**, **Küsi kasutajalt** või **Keela**).

8. Et seadistada rakenduse õiguseid teha operatsioonisüsteemis mitmesuguseid toiminguid, tehke järgmist.
- Valige vahekaardil **Õigused** asjakohane õiguste kategooria.
 - Menüü avamiseks klõpsake veerus **Toiming** ikooni ja valige asjakohane üksus (**Päranda, Luba, Küsi kasutajalt** või **Keela**).
9. Et seadistada rakenduse õiguseid teha võrgus mitmesuguseid toiminguid, tehke järgmist.
- Klõpsake vahekaardil **Võrgureeglid** nuppu **Lisa**.
Avatakse aken **Võrgureegel**.
 - Avanenud aknas määrake vajalikud reegliseaded ja klõpsake käsku **Salvesta**.
 - Määrake uue reegli prioriteet. Selleks valige reegel ja nihutage seda loendis üles või alla.
10. Kindlate rakendustoimingute kontrollimisest väljaarvamiseks märkige vahekaardil **Erandid** ruudud nende toimingute kõrval, mille soovite jätta kontrollimata.
11. Klõpsake **Salvesta**.
- Kõigile Sissetungitõrje reeglite jaoks loodud eranditele pääseb juurde Kaspersky rakenduse seadete akna jaotises **Ohud ja erandid**.
- Sissetungitõrje jälgib ja piirab rakenduse toiminguid kooskõlas määratud seadetega.

Rakenduse reputatsiooni kontrollimine

Kaspersky võimaldab kontrollida rakenduste reputatsiooni kogu maailmast pärinevate kasutajate abil. Rakenduse reputatsioon koosneb järgmistest kriteeriumidest.

- Tarnija nimi
- Teave [digiallkirja](#) kohta (kui rakendus on digiallkirjastatud)
- Teave grupi kohta, millesse on rakenduse määranud sissetungitõrje või kõige suurem arv Kaspersky Security Networki kasutajaid.
- Rakendust kasutavate Kaspersky Security Networki kasutajate arv (saadaval, kui rakendus on lisatud Kaspersky Security Networki andmebaasi gruppi „Usaldusväärsed“).
- Aeg, millest alates on rakendus Kaspersky Security Networkis teada.
- Riigid, kus rakendus on kõige laialdasema levikuga.

Rakenduse reputatsiooni saate kontrollida pärast Kaspersky Security Networkis osalemisega nõustumist.

Rakenduse reputatsiooni teadasaamiseks tehke järgmist.

Avage rakenduse käivitusfaili kontekstimenüü ja valige **Kontrolli reputatsiooni KSNis**.

See avab akna teabega rakenduse reputatsiooni kohta Kaspersky Security Networkis.

Nõrkade seadete kontroll

Sellest jaotisest leiab teavet nõrkade operatsioonisüsteemi seadete kohta ning kuidas operatsioonisüsteemi nõrku seadeid otsida ja parandada.

Teave operatsioonisüsteemi nõrkade seadete kohta

Kui töötate arvutiga, võivad operatsioonisüsteemi seaded muutuda teie või käivitavate rakenduste toimingute tulemusena. Operatsioonisüsteemi seadete muutmine võib ohustada teie arvuti turvalisust. Näiteks kui brauseris on lubatud praeguse kasutajanime ja parooliga automaatne sisselogimine, võib kolmanda osapoole veebisait teie parooli pealt kuulata.

Operatsioonisüsteemi nõrgad seaded saab jagada kahte tüüpi:

- *Kriitilised seaded.* Sellised seaded on võrdsustatud operatsioonisüsteemi haavatavustega.
- *Soovitavad seaded.* Operatsioonisüsteemi turvalisuse parandamiseks on soovitatav neid seadeid muuta.

Vaikimisi skannib rakendus operatsioonisüsteemi nõrku seadeid vähemalt kord päevas. Kui tuvastatakse operatsioonisüsteemis nõrgad seaded, palub rakendus teil need operatsioonisüsteemi turvalisuse taastamiseks parandada. Nõrga seade üksikasjade vaatamiseks klõpsake rakenduse aknas vastava seade kõrval olevat linki.

Kui klõpsate teavitusaknas oleval lingil, avaneb aken **Nõrkade seadete kontroll**, kus kuvatakse operatsioonisüsteemis tuvastatud nõrgad seaded. Teave nõrkade sätete kohta kuvatakse ka teatiste keskuses. Teatiste keskusest saab jätkata nõrkade seadete vaatamist ja parandamist.

Aknas **Nõrkade seadete kontroll** saab teha järgmisi toiminguid.

- Operatsioonisüsteemi nõrkade seadete parandamine.
- Ignoreeri: jätab operatsioonisüsteemi nõrgad seaded muutmata.
- Tühista: operatsioonisüsteemi varem määratud nõrkade seadete taastamine algsesse olekusse.

Rakendus tuvastab arvuti operatsioonisüsteemi kõigi kasutajakontode nõrgad seaded. Arvuti teiste kasutajakontode nõrku seadeid saab parandada ainult siis, kui olete operatsioonisüsteemi sisse loginud administraatorikontoga.

Kui te pole arvuti administraator, saab nõrku seadeid ignoreerida ainult oma kasutajakonto puhul. Kõigi kasutajakontode nõrku seadeid saab ignoreerida ainult arvuti administraator.

Kasutaja saab [käsitsi käivitada](#) või [keelata nõrkade seadete kontrolli](#).

Kasutaja saab kaughallata oma arvuti kaitset ja saata rakendusest My Kaspersky nõrkade seadete parandamise käsu.

Kuidas leida ja parandada operatsioonisüsteemi nõrku seadeid

Operatsioonisüsteemi nõrkade sätete leidmiseks ja parandamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Valige jaotis **Turvalisus**.
3. Jaotises **Turvalisus** valige **Nõrkade seadete kontroll**.
4. Klõpsake **Kontroll**.

Käsk käivitab nõrkade seadete kontrolli. Kui kontrollimine on lõppenud, näete kontrolli tulemusi jaotises **Nõrkade seadete kontroll**.

5. **Nõrkade seadete kontroll** akna avamiseks klõpsake **Kuva**.
6. Valige aknas **Nõrkade seadete kontroll** nõrga seade puhul rakendatav toiming.


- Nõrk seade tuvastatud. Tehke üks järgmistest toimingutest.
 - Kõigi nõrkade seadete parandamiseks klõpsake nuppu **Paranda kõik**.
 - Üha nõrga seade parandamiseks klõpsake nuppu **Paranda**.
 - Kui avatud rakendused segavad nõrga seade parandamist, klõpsake nuppu **Kuva**, et vaadata segavate rakenduste loendit.

Seade parandamist takistava rakenduse sulgemiseks tehke ühte järgmistest.

 - Klõpsake häiriva rakenduse nimest paremal asuvat nuppu **X**, et sulgeda see tavapäraselt. Kui rakendus tuvastab salvestamata muudatusi, palub see teil need salvestada.
 - Et sulgeda kõik segavad rakendused ilma andmeid salvestamata, klõpsake nuppu **Sundsule**.
 - Nõrga seadistuse muutmata jätmiseks valige nupu **Paranda** kõrval asuvast ripploendist käsk **Ignoreeri**.
 - Kaspersky tehnilise toe veebisaidilt nõrga seade kohta teabe vaatamiseks valige nupu **Paranda** kõrval asuvast ripploendist käsk **Loe lisaks**.
- Varasemalt parandatud nõrgad seaded.
 - Et taastada määratud seade algolekusse, klõpsake nuppu **Võta tagasi** nuppu.
 - Kaspersky tehnilise toe veebisaidilt nõrga seade kohta teabe vaatamiseks valige nupu **Võta tagasi** kõrval asuvast ripploendist käsk **Loe lisaks**.
- Ignoreeritud seaded. Muutmata jäetud nõrkade seadete loendi avamiseks klõpsake linki **Näita kõiki teate N eiratud seadet** kõrval ja seejärel nuppu **Paranda**.

Kuidas lubada nõrkade seadete kontrollimist

Nõrkade seadete kontroll keelamiseks toimige järgnevalt.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Avage jaotis **Jõudlusseaded**.
4. Klõpsake **Arvutiressursside kasutus**.
5. Tühjendage märkeruut **Otsi operatsioonisüsteemi nõrku seadeid**.

Rakendus ei otsi operatsioonisüsteemi nõrku seadeid ega näita nende kohta hoiatusi.

Võrguseire

Saadaval ainult plaanides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Võrguseire komponent võimaldab teil reaalajas vaadata arvuti võrgutegevuste andmeid, võrgutegevust blokeerida või luua arvutisse installitud rakenduste jaoks võrgu- ja paketiireegleid.

Võrguseire seadete avamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Turvalisus**.
3. Klõpsake jaotises **Võrguseire** nuppu **Kuva**.

Avatakse aken **Võrguseire**.

Jaotises **Võrgutegevus** kuvatakse kõik praegu aktiivsed võrguühendused. Kuvatakse nii sissetulevad kui ka väljaminevad ühendused. Lingi **Blokeeri kogu võrgutegevus** kaudu saate kõik võrguühendused blokeerida.

Jaotises **Avatud pordid** on loetletud kõik avatud võrgupordid. Selles jaotises saate ka rakenduste jaoks võrgu- ja paketiireegleid luua.

Jaotises **Võrguliiklus** kuvatakse teie arvuti ja teiste samas võrgus asuvate arvutite vahelise sissetuleva ja väljamineva võrguliikluse maht.

Jaotises **Blokeeritud arvutid** on ära toodud selliste kaugarvutite IP-aadresside loend, millega seoses on võrgurünnakute tõrje komponent tuvastanud võrgurünnete katseid ja mille võrguliiklus on blokeeritud.

Nutikodu monitor

See jaotis sisaldab teavet selle kohta, kuidas saada Kaspersky rakendusest teada, millised seadmed on ühendatud teie kaabliga Etherneti võrku ja Wi-Fi-võrku.

Komponent Nutikodu monitor

Saadaval ainult plaanides *Kaspersky Plus* ja *Kaspersky Premium*.

Häkkerid võivad teie parooli püüda või teie koduvõrku häkkida, et teie Internetti ära kasutada või teie andmeid varastada. Kaspersky rakendus kaitseb teie kaabliga Etherneti võrke ja Wi-Fi-võrke volitamata ühenduste eest.

Kui kinnitate, et teie koduvõrk on õigesti tuvastatud, hakkame jälgima sellesse võrku ühendatud seadmeid ja ka mõningaid haavatavusi, nagu Wi-Fi-võrgu parooli tugevust ning ruuteri krüpteerimist. Kui avastame võrgus haavatavusi või uue seadme, mida te ei ole tuntud seadmeks määranud, siis hoiatame teid selle eest ja anname soovitusi, et saaksite võtta meetmeid oma koduvõrgu ja seda kasutavate seadmete kaitsmiseks.

Teated koduvõrgu haavatavuste kohta on saadaval ainult Kaspersky Premiumis. Teated uute seadmete kohta, mis teie koduvõrguga ühenduvad, on saadaval pakettides *Kaspersky Plus* ja *Kaspersky Premium*.

Kui mõni seade loob ühenduse teie võrguga, kuvab Kaspersky rakendus vastava teate ja küsib, kas soovite vaadata selle võrguga ühendatud seadmeid:


- Kui nõustute, [näitab Kaspersky rakendus selle võrguga ühendatud seadmete nimekirja](#) ja teavitab teid, kui võrguga loob ühenduse uus seade.
- Kui keeldute, [ei teavita Kaspersky rakendus teid](#), kui ühendus selle võrguga uuesti luuakse, ega näita ühendatud seadmete nimekirja.

Võite [Nutikodu monitori välja lülitada](#). Kui lülitate komponendi välja, lõpetab Kaspersky rakendus teie võrguga ühenduste loomistest teavitamise.

Wi-Fi-võrkudega ühenduse loomiseks saadaolevate muude turbemeetodite kohta leiate teavet [tehnilise toe veebisaidilt](#).

Nutikodu monitori sisse- ja väljalülitamine

Nutikodu monitori sisse- või väljalülitamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake akna allservas nuppu .
Avatakse aken **Seaded**.
3. Valige jaotis **Turvaseaded**.
4. Valige tule müüri komponent.
5. Tehke üks järgmistest toimingutest.
 - Nutikodu monitori sisselülitamiseks märkige ruut **Kuva minu võrkudega ühendatud seadmed**.
 - Nutikodu monitori väljalülitamiseks tühjendage märkeruut **Kuva minu võrkudega ühendatud seadmed**.

Minu võrgus olevate seadmete vaatamine

Kaspersky rakendus näitab teie Wi-Fi-võrku või kaabliga Etherneti võrku ühendatud seadmete kohta järgmist teavet.

- Seadme nimi
- Seadme tootja
- Seadme tüüp (nt arvuti, mobiilseade, ruuter, mängukonsool või videokaamera)
- Seadmesse paigaldatud operatsioonisüsteem
- MAC-aadress (seadme kordumatu võrgu ID)
- Seadme IP-aadress
- Aeg, millal lahtiühendatud seadmed viimati võrgus tuvastati
- Teie seadmesse installitud Kaspersky rakendused

[Teie võrku ühendatud seadmete kuvamiseks tehke järgmist.](#) 

1. Avage rakenduse peaaaken.

2. Tehke üks järgmistest toimingutest.

- Avage **Turvalisus** ja klõpsake jaotises **Nutikodu monitor** nuppu **Kuva**.
- Klõpsake rakenduse peaaknas jaotises **Nutikodu monitor** nuppu **Kuva**.
- Klõpsake peaakna alumises osas kuvatud linki <**võrgu nimi**>.

Avaneb aken **Nutikodu monitor**, mis näitab võrku, millega teie arvuti on ühendatud.

3. Kui soovite edastada teabe selle võrguga ühendatud seadmete kohta oma mobiilseadmetesse, märkige ruut **Näita minu mobiilseadmetes teavet seadmete kohta selles võrgus**.

4. Võrguga ühendatud seadmete nägemiseks klõpsake nuppu **Jah, näita seadmeid**.

Aknas **Nutikodu monitor** on järgmine teave.

- Seadmed, mis on praegu teie võrku ühendatud.
- Seadmed, mis olid mõnda aega tagasi teie võrku ühendatud.
- Seadme olek võrgus:
 - ühendatud seadmed rohelised;
 - lahti ühendatud seadmed on hallid;
 - uued seadmed on tähistatud sõnaga **uus**.

[Seadme nime muutmiseks tehke järgmist.](#)

1. Valige aknas **Nutikodu monitor** seadmete loendist sobiv seade.

Avaneb aken selle seadme kohta teabe kuvamiseks.

2. Sisestage väljale **Seadme nimi** uue seadme nimi.

[Seadme tüübi muutmine](#)

1. Valige aknas **Nutikodu monitor** seadmete loendist sobiv seade.

Avaneb aken selle seadme kohta teabe kuvamiseks.

2. Klõpsake väljal **Seadme tüüp** nuppu **Valige tüüp**, et avada aken **Seadme tüüp**.

3. Valige selles aknas seadme kategooria ja tüüp, näiteks **Koduseadmed** → **Külmik**.

4. Klõpsake **Salvesta**.

Seadmele võrgujuurdepääsu keelamine


Seadmele võrgujuurdepääsu keelamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Tehke üks järgmistest toimingutest.
 - Avage **Turvalisus** ja klõpsake jaotises **Nutikodu monitor** nuppu **Kuva**.
 - Klõpsake rakenduse peaaknas jaotises **Nutikodu monitor** nuppu **Kuva**.
 - Klõpsake peaakna alumises osas kuvatud linki **<võrgu nimi>**.
3. Aknas **Nutikodu monitor** valige seade, mille ühenduse soovite katkestada.
See avab akna selle seadme teabega, mis sisaldab ka teavet seadme MAC-aadressi kohta.
4. Kirjutage üles seadme MAC-aadress
5. Blokeerige seadme MAC-aadress oma brauseri seadetes. Külastage vastava müüja veebisaiti, et vaadata oma ruuteri kasutusjuhendit.

Kui MAC-aadress on blokeeritud, ei saa seade teie võrguga ühendust luua.

Loendist ühendusteta võrgu kustutamine

Loendist ühendusteta võrgu kustutamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Tehke üks järgmistest toimingutest.
 - Avage **Turvalisus** ja klõpsake jaotises **Nutikodu monitor** nuppu **Kuva**.
 - Klõpsake rakenduse peaaknas jaotises **Nutikodu monitor** nuppu **Kuva**.
3. Klõpsake peaakna alumises osas kuvatud linki **<võrgu nimi>**.
See viib teid aknasse **Nutikodu monitor**.
4. Klõpsake loendi laiendamiseks sellest paremal olevat noolt ja klõpsake nuppu  võrgu kõrval, mille soovite eemaldada.

Võrk kustutatakse loendist.

Märguannete keelamine, kui seadmed ühenduvad minu võrguga

Märguannete keelamiseks, kui seadmed ühenduvad võrguga, tehke järgmist.

1. Avage rakenduse peaaaken.

2. Tehke üks järgmistest toimingutest.

- Avage **Turvalisus** ja klõpsake jaotises **Nutikodu monitor** nuppu **Kuva**.
- Klõpsake rakenduse peaknas jaotises **Nutikodu monitor** nuppu **Kuva**.
- Klõpsake peakna alumises osas kuvatud linki **<võrgu nimi>**.

3. Aknas **Nutikodu monitor** klõpsake võrgu kõrval nuppu ******* ja valige **Lülita teated välja**.

Kaspersky rakendus ei näita teile enam teateid, kui mõni seade loob selle võrguga ühenduse.

Valitud võrguga seotud teated saate välja lülitada ka siis, kui Kaspersky rakendus näitab teadet, et mingi seade ühendus selle võrguga. Selleks klõpsake teateaknas lingil **Lülita teated selle võrgu puhul välja**.

Nutikodu monitori kohta tagasiside saatmine

*Kaspersky*le komponendi *Nutikodu monitor* toimimise kohta tagasiside saatmiseks tehke järgmist.

1. Avage rakenduse peaaaken.

2. Tehke üks järgmistest toimingutest.

- Avage **Turvalisus** ja klõpsake jaotises **Nutikodu monitor** nuppu **Kuva**.
- Klõpsake rakenduse peaknas jaotises **Nutikodu monitor** nuppu **Kuva**.
- Klõpsake peakna alumises osas kuvatud linki **<võrgu nimi>**.

3. Aknas **Nutikodu monitor** klõpsake nuppu ******* ja valige **Saada tagasisidet**.

Avatakse aken **Aidake meil tarkvara paremaks muuta! Andke meile tagasisidet**.

4. Hinnake komponenti 5-pallisel skaalal, valides 1–5 täрни.

5. Kui andsite komponendile 3–5 täрни:

a. Kui soovite lisada tagasisidele kommentaari, sisestage see väljale **Üksikasjad**.

b. Märkige ruut **Nõustun tarkvara paremaks muutmiseks jagama oma isiklike andmeid (arvuti unikaalne ID) ning nõustun dokumendiga Privaatsuspoliitika**.

6. Kui andsite komponendile 1–2 täрни:

a. Kui soovite Kasperskyt komponendiga Nutikodu monitor seotud probleemist teavitada, valige ripploendist **Teema** lähima tähendusega teema.

Saate valida loendist ühe järgmistest valikutest.

- **Tüütu kasutada**. Valige see üksus, kui komponendi Nutikodu monitor kasutamisel tekib ebamugavusi.
- **Rakendusel võtab võrgust seadmete otsimine kaua aega**. Valige see üksus, kui komponent Nutikodu monitor töötab liiga aeglaselt.

- **Rakendus tuvastab võrgus asuvaid seadmeid valesti.** Valige see üksus, kui rakendus määrab Wi-Fi- või Etherneti võrku ühendatud seadmete nimed ja/või tüübid valesti.
- **Uute seadmete kohta võrgus on liiga palju teateid.** Valige see üksus, kui rakendus kuvab teile Wi-Fi- või Etherneti võrgus olevate uute seadmete kohta liiga palju teateid.
- **Madalam arvuti jõudlus.** Valige see üksus, kui komponendi Nutikodu monitor kasutamine halvendab teie arvuti jõudlust.
- **Komponenti ei saa konfigurereida.** Valige see üksus, kui komponendi Nutikodu monitor konfigureerimisel tekib probleeme.
- **Muu.** Valige see üksus, kui teised üksused ei sobi teie probleemi kirjeldamiseks.

b. Kui soovite lisada tagasisidele kommentaari, sisestage see väljale **Üksikasjad**.

c. Märkige ruut **Nõustun tarkvara paremaks muutmiseks jagama oma isiklike andmeid (arvuti unikaalne ID) ning nõustun dokumendiga Privaatsuspoliitika**.

7. Klõpsake **Saada**.

Nende andmete saatmise korral saab ja töötleb Kaspersky järgmist teavet.

- Teie tagasiside, mis sisaldab komponentide jõudluse hinnangut, probleemi teemat ja kommentaare.
- Operatsioonisüsteemi teave ja versioon.
- Teave paigaldatud rakenduse ja selle versiooni kohta.

Kaspersky saab ja töötleb seda teavet krüpteeritud kujul, et analüüsida vigu ja parandada komponendi Nutikodu monitor jõudlust. Kaspersky ei nõua teilt tagasiside saatmisel isikuandmete esitamist ega kogu selliseid andmeid. Üksikasjalikumat teavet isikuandmete töötlemise kohta leiate [Kaspersky privaatsuspoliitikast](#).

Kaspersky-eelne viiruse-eemaldus

See jaotis sisaldab teavet operatsioonisüsteemi taastamise kohta pärast selle nakatumist pahavaraga.

Operatsioonisüsteemi taastamine pärast nakatumist

Kui kahtlustate, et arvuti operatsioonisüsteem on pahavara tegevuse või süsteemirikke tõttu rikutud või muudetud, kasutage *Microsoft Windowsi veaotsingu nõustajat*, mis puhastab süsteemi kõigist pahatahtlike objektide jälgedest. Kaspersky soovib nõustaja käivitada pärast arvutist nakkuse eemaldamist, et kõrvaldada kindlasti kõik nakkuste põhjustatud ohud ja kahjustused.

Nõustaja kontrollib, kas süsteemis on muudatusi, mis võivad hõlmata juurdepääsu blokeeritud võrgule, teadaolevate vormingute failinimelaiendite muutmist, juhtpaneeli blokeerimist jne. Eri liiki kahjustuste põhjused erinevad. Need põhjused võivad hõlmata pahavara tegevust, vale süsteemiseadistust, süsteemirikkeid või süsteemi optimeerimiseks kasutatud rakenduste rikkeid.

Pärast ülevaatuselõppu analüüsib nõustaja teavet, et hinnata, kas süsteemis on viivitamatut sekkumist vajavaid kahjustusi. Ülevaatusel põhjal koostab viisard loendi toimingutest, mis tuleb teha kahju kõrvaldamiseks. Nõustaja rühmitab need toimingud kategooriate järgi vastavalt tuvastatud probleemide raskusastmele.

Operatsioonisüsteemi veaotsing Microsoft Windowsi veaotsingu nõustaja abil

Microsoft Windowsi veaotsingu nõustaja käivitamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Valige **Turvalisus** → **Microsoft Windowsi veaotsing**.
3. Klõpsake **Otsi kahju**.

Avaneb Microsoft Windowsi veaotsingu nõustaja aken.

Nõustaja koosneb mitmest lehest (etapist), mille sirvimiseks saate klõpsata nuppe **Tagasi** ja **Edasi**. Pärast lõpetamist nõustaja sulgemiseks klõpsake nuppu **Valmis**. Mis tahes etapis nõustaja peatamiseks klõpsake nuppu **Tühista**.

Nõustaja etappe on üksikasjalikumalt kirjeldatud allpool.

Operatsioonisüsteemi taastamise käivitamine

a. Valige üks kahest nõustaja töörežiimist.

- **Otsi kahjustusi, mida on põhjustanud pahavara tegevus.** Nõustaja otsib probleeme ja võimalikke kahjustusi.
- **Pööra muudatused tagasi.** Nõustaja pöörab tagasi varem tuvastatud probleemidele ja kahjustustele rakendatud parandused.

b. Klõpsake **Edasi**.

Probleemide otsing

Kui tegite valiku **Otsi kahjustusi, mida on põhjustanud pahavara tegevus**, otsib nõustaja probleeme ja võimalikke kahjustusi, mis tuleks parandada. Kui otsing on lõpule jõudnud, jätkab nõustaja automaatselt järgmist etappi.

Kahjustuste parandustoimingute valimine

Kõik eelmises etapis leitud kahjustused rühmitatakse vastavalt sellele, millist ohtu need endast kujutavad. Iga kahjugrupi korral soovib Kaspersky kahjustuste parandamiseks ette nähtud toimingukomplekti.

Gruppe on kolm.

- *Tungivalt soovitatavad toimingud* kõrvaldavad probleemid, mis kujutavad endast tõsist turvaohtu. Soovitame teil parandada kõik sellesse gruppi kuuluvad kahjustused.
- *Soovitatavad toimingud* püüavad parandada kahjustused, mis võivad kujutada ohtu. Soovitame teil parandada ka sellesse gruppi kuuluvad kahjustused.
- *Lisatoimingud* parandavad operatsioonisüsteemi kahjustused, mis pole praegu ohtlikud, kuid võivad tulevikus ohustada arvuti turvalisust.

Gruppi kuuluvate kahjustuste kuvamiseks laiendage valitud grupi loend.

Kui soovite, et nõustaja parandaks kindlat tüüpi kahjustused, märkige kahjustuse kirjelduse kõrval kuvatav ruut. Vaikimisi parandab viisard kahjustused, mis kuuluvad soovitatavate ja tungivalt soovitatavate toimingute gruppi. Kui te ei soovi kindlat tüüpi kahjustusi parandada, eemaldage selle kõrval kuvatavast ruudust märged.

On tungivalt soovitatav jätta vaikimisi märgitud ruutudest märked eemaldamata, kuna see jätkaks teie arvuti ohtude suhtes haavatavaks.

Kui olete nõustaja toimingukomplekti määranud, klõpsake nuppu **Edasi**.

Kahjustuste parandamine

Nõustaja teeb eelmises etapis valitud toimingud. Kahju parandamine võib aega võtta. Pärast kahjustuste parandamist jätkab nõustaja automaatselt järgmist etappi.

Nõustaja lõpuleviimine

Nõustajast väljumiseks klõpsake nuppu **Valmis**.

Operatsioonisüsteemi avariitaaste

Kaspersky päästeketas on ette nähtud operatsioonisüsteemi avariitaasteks. Kaspersky päästekettaga saate kontrollida ja parandada nakatunud arvutit, millest ei saa nakkust eemaldada muude meetoditega (näiteks viirusetõrjerakendustega).

Kaspersky päästeketta kohta leiate üksikasjalikumad teavet [tehnilise toe veebisaidilt](#).

Kustutatud või desinfitseeritud faili taastamine

Kustutatud või desinfitseeritud failide varukoopiad paigutatakse teie arvutis erikausta, mille nimi on *Karantiin*. Failide varukoopiad salvestatakse erivormingus, mis pole teie arvutile ohtlik. Karantiinis hoitava varukoopia põhjal saate kustutatud või parandatud faili taastada.

Soovitame kustutatud või parandatud failide taastamist vältida, kuna need võivad ohustada teie arvutit!

Rakendus ei eemalda nakkusi Windows Store'i rakendustest. Kui kontrollitulemused näitavad, et selline rakendus on ohtlik, kustutatakse see teie arvutist. Kui Windows Store'i rakendus kustutatakse, ei loo Kaspersky rakendus sellest varukoopiat. Selliste objektide taastamiseks peate kasutama operatsioonisüsteemi taastetööriistu (üksikasjaliku teabe saamiseks lugege arvutisse paigaldatud operatsioonisüsteemi dokumentatsiooni) või uuendama rakendusi Windows Store'i kaudu.

Kustutatud või desinfitseeritud faili taastamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Turvalisus**.
3. Klõpsake Kaspersky rakenduseaknas ülal paremal kuvatavat nuppu **Karantiin**.
Avatakse aken **Karantiin**.
4. Valige avanenud aknas **Karantiin** loendist vajalik fail ja klõpsake nuppu **Taasta**.

Meili kaitsmine


Selles jaotises on teave selle kohta, kuidas kaitsta teie meili rämpsmeilide, viiruste ja muude ohtude vastu.

Meilide kaitse seadistamine

Kaspersky rakendus võimaldab otsida Meilide kaitse abil meilisõnumitest ohtlikke objekte. Meilide kaitse käivitub operatsioonisüsteemi käivitamise ajal ja töötab pidevalt arvuti muutmälus (RAM), kontrollides kõiki meilisõnumeid, mis saadetakse või saabuvad POP3-, SMTP-, IMAP- ja NNTP-protokollide kaudu, samuti POP3-, SMTP- ja IMAP-protokollide krüptitud ühenduste (SSL) kaudu.

Vaikimisi kontrollib meilide kaitse nii sissetulevaid kui ka väljaminevaid meilisõnumeid. Vajaduse korral saate sisse lülitada ainult sissetulevate meilisõnumite kontrollimise.

Meilide kaitse seadistamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Turvaseaded**.
4. Valige jaotises **Turvaseaded** meilide kaitse komponent.
See viib teid aknasse **Meilide kaitse seaded**.
5. Veenduge, et akna ülal servas kuvatav lüliti, mis lülitab meilide kaitse sisse/välja, oleks sisse lülitatud.
6. Valige turvatase.
 - **Optimaalne.** Selle turvaseme seadmise korral kontrollib meilide kaitse sissetulevaid ja väljaminevaid sõnumeid ning manustatud arhiive ning teeb heuristilise analüüsi, mille üksikasjalikkuse tase on **Keskmine kontroll**.
 - **Madal.** Selle turvaseme valimise korral kontrollib meilide kaitse ainult sissetulevaid sõnumeid ilma manustatud arhiive kontrollimata.
 - **Äärmuslik.** Selle turvaseme seadmise korral kontrollib meilide kaitse sissetulevaid ja väljaminevaid sõnumeid ning manustatud arhiive ning teeb heuristilise analüüsi, mille üksikasjalikkuse tase on **Põhjalik kontroll**.
7. Valige jaotises **Toiming ohu avastamisel** toiming, mille soovite, et meilide kaitse teeks nakatunud objekti avastamise korral (nt parandamine).

Kui meilisõnumist ei tuvastata ühtegi ohtu või kui kõik nakatunud objektid on edukalt parandatud, tehakse sõnum kättesaadavaks. Kui komponent ei saa nakatunud objekti parandada, siis nimetab Meilide kaitse sõnumiobjekti ümber või kustutab selle ja lisab sõnumi teemareale teate, et Kaspersky rakendus on sõnumit töödeldud. Enne objekti kustutamist loob Kaspersky rakendus sellest varukoopia ja teisaldab selle [karantiini](#).

Kui täiendate rakenduse uuemaks versiooniks, siis kasutaja seadistatud meilide kaitse seadeid ei salvestata. Uus rakenduseversioon kasutab meilide kaitse vaikeseadeid.

Kui Kaspersky rakendus tuvastab kontrolli käigus sõnumitekstis arhiivi parooli, kasutatakse parooli arhiivi sisust pahavara otsimiseks. Parooli ei salvestata. Enne kontrollimist pakitakse arhiiv lahti. Kui arhiivi lahtipakkimisel ilmneb rakendusekrahh, saate lahtipakitud failid käsitsi kustutada järgmisest asukohast: %systemroot%\temp. Failidel on eesliide „PR“.

Soovimatute meilide (rämpsmeili) blokeerimine

Kui teile saadetakse suures koguses soovimatuid sõnumeid (rämpsmeile), soovitame lülitada sisse rämpsmeilifiltri komponendi ja määrata sellele turbetaseme **Optimaalne**.

Rämpsmeilifiltri sisselülitamiseks ja optimaalse turbetaseme määramiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Privaatsusseaded**.
4. Valige rämpsmeilifiltri komponent.
Aknas kuvatakse rämpsmeilifiltri seaded.
5. Lülitage rämpsmeilifilter lüliti abil sisse.
6. Veenduge, et jaotises **Turvalisuse tase** oleks määratud turbetase **Optimaalne**.

Rämpsmeilifiltrile rakenduvad järgmised piirangud.

- Kasutatavast protokollist olenemata saab rämpsmeilifiltri komponent analüüsida ainult meiliserverist täielikult alla laaditud sõnumeid.
- Rämpsmeilifiltri komponent ei kontrolli MAPI-protokolli abil edastatud meilisõnumeid.

Rämpsmeilifiltri komponent lülitatakse välja, kui täiendate rakenduse uuemaks versiooniks. Komponenti saate sisse lülitada käsitsi.

[Mõnes rakenduse versioonis](#) tuleb teil rämpsmeilifiltri komponendi sisselülitamiseks nõustuda rämpsmeilifiltri jaoks andmete töötlemise avalduse tingimustega.

Osalemine Kaspersky Security Networkis

Kaspersky rakendus tõhustab teie arvuti kaitset pilvekaitse abil. Pilvekaitse rakendatakse Kaspersky Security Networki infrastruktuuri abil, mis kasutab kogu maailmas kasutajatelt saadud andmeid.

Kaspersky Security Network (KSN) on Kaspersky pilvepõhine teabebaas, mis sisaldab teavet rakenduste ja veebisaitide reputatsiooni kohta. Kaspersky Security Networki andmete kasutamine tagab Kaspersky rakenduse kiirema reageerimise uutele ohtudele, parandab mõne kaitsekomponendi jõudlust ja vähendab valehäirete tõenäosust.

Kasutajate osalemine Kaspersky Security Networkis võimaldab Kasperskyl kiiresti saada teavet uute ohtutüüpide ja -allikate kohta, töötada välja nende neutraliseerimiseks ette nähtud lahendusi ja vähendada valehäirete arvu. Kaspersky Security Networkis osalemine võimaldab teil pääseda juurde rakenduste ja veebisaitide reputatsioonistatistikale.


Kui osalete Kaspersky Security Networkis, saadate Kasperskyle automaatselt [teavet oma operatsioonisüsteemi häälestuse ning Kaspersky rakenduste protsesside algus- ja lõpuaegade kohta](#).

Kaspersky Security Networkis osalemise lubamine ja keelamine

Osalemine Kaspersky Security Networkis on vabatahtlik. Kaspersky Security Networki (KSN) kasutamise saate sisse või välja lülitada Kaspersky rakenduse installimise käigus ja/või igal ajal pärast rakenduse installimist.

Kaspersky Security Networkis osalemise lubamiseks ja keelamiseks tehke järgmist.

1. Avage rakenduse peaaaken.

2. Klõpsake põhiakna allservas nuppu .

Avatakse aken **Seaded**.

3. Valige **Turvaseaded** → **Kaspersky Security Network**.

Avaneb aken **Kaspersky Security Network**, milles kuvatakse Kaspersky Security Networki üksikasjad ja Kaspersky Security Networkis osalemise seaded.

4. Kaspersky Security Networkis osalemine lülitage sisse või välja akna ülaservas kuvatava lüliti abil.

- Kui soovite Kaspersky Security Networkis osaleda, seadke lüliti asendisse **Sees**.
Avaneb Kaspersky Security Networki avalduse tekstiakn. Kui nõustute avalduse tingimustega, klõpsake **Olen nõus**.
- Kui te ei soovi Kaspersky Security Networkis osaleda, seadke lüliti asendisse **Väljas**.

[Mõnes Kaspersky rakenduse versioonis](#) on aknas **Kaspersky Security Network** Kaspersky Security Networki teabe asemel **Kaspersky Security Networki avaldus**.

Kaspersky Security Networki avaldusega nõustumiseks tehke järgmist.

1. Klõpsake jaotises **Kaspersky Security Networki avaldus** nuppu **Nõustu**.

Avaneb Kaspersky Security Networki avaldus. See avaldus võimaldab Kaspersky ekspertidel teie kaitse parandamiseks saada kiiresti teavet teie arvutis tuvastatud ohtude kohta, käitatavate rakenduste ja allalaaditavate allkirjastatud rakenduste kohta, samuti teavet operatsioonisüsteemi kohta.

2. Kui nõustute avalduse tingimustega, klõpsake nuppu **Nõustu**.

Kaspersky Security Networki avaldusest keeldumiseks

klõpsake jaotises **Kaspersky Security Networki avaldus** nuppu **Keeldu**.

Kaspersky Security Networki ühenduse kontrollimine

Võite kaotada ühenduse Kaspersky Security Networkiga järgmistel põhjustel.

- Te ei osale Kaspersky Security Networkis.

- Teie arvutil puudub internetiühendus.
- Praegune võtmeseisund ei võimalda Kaspersky Security Networkiga ühendust luua. Näiteks ei pruugi ühendus KSN-iga olla saadaval järgmistel põhjustel.
 - Rakendus pole aktiveeritud.
 - Litsents või tellimus on aegunud.
 - Tuvastatud on litsentsivõtme probleeme (näiteks võti on lisatud keelunimekirja).

Võtme praegune seisund kuvatakse jaotises My Kaspersky.

Kaspersky Security Networki ühenduse kontrollimiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Valige **Turvaseaded** → **Kaspersky Security Network**.

Aknas **Kaspersky Security Network** kuvatakse Kaspersky Security Networkiga loodud ühenduse olek.

Kaitse riistvara virtualiseerimise abil

Sellest jaotisest saate teada, kuidas saate arvutit kaitsta riistvara virtualiseerimise abil.

Teave riistvara virtualiseerimist kasutava kaitse kohta

Kui Kaspersky rakendus on installitud 64-bitisesse operatsioonisüsteemi Microsoft Windows 8, Microsoft Windows 8.1 või Microsoft Windows 10, kasutab see [hüperviisori](#) tehnoloogiat lisakaitseks keeruka pahavara vastu, mis võib teie isiklikud andmed lõikepuhvri või andmepüügi kaudu kinni püüda.

Vaikimisi on riistvara virtualiseerimist kasutav kaitse sisse lülitatud. Kui kaitse on käsitsi välja lülitatud, saate [selle rakenduse seadete aknas käsitsi sisse lülitada](#).


Arvutites, kus töötab 64-bitine Microsoft Windows 8, Microsoft Windows 8.1 või Microsoft Windows 10, on Kaspersky riistvara virtualiseerimist (hüperviisorit) kasutaval kaitisel järgmised piirangud.

- See funktsioon pole saadaval, kui arvutis töötab mõni muu tootja hüperviisor (nt ettevõtte VMware™ virtualiseerimistarkvara kasutatav hüperviisor). Pärast kolmanda osapoole hüperviisori sulgemist on ekraanipiltidevastane kaitse taas saadaval.
- See funktsioon pole saadaval, kui teie arvuti protsessor (CPU) ei toeta riistvara virtualiseerimise tehnoloogiat. Täpsemat teavet selle kohta, kas teie protsessor toetab riistvara virtualiseerimist, leiate arvutiga tarnitud dokumentidest või protsessoritootja veebisaidilt.
- See funktsioon pole saadaval, kui kaitstud veebilehitseja käivitamisel töötab kolmanda osapoole hüperviisor (näiteks VMware'i hüperviisor).
- See funktsioon pole saadaval, kui riistvara virtualiseerimine on teie arvutis välja lülitatud. Arvutis riistvaralise virtualiseerimise sisselülitamise kohta leiate täpsemat teavet arvuti tehnilistest dokumentidest või protsessoritootja veebisaidilt.

- See funktsioon pole saadaval, kui Microsoft Windows 10 operatsioonisüsteemis on sisse lülitatud Device Guard.
- See funktsioon pole saadaval, kui Microsoft Windows 10 operatsioonisüsteemis on sisse lülitatud virtualiseerimispõhine kaitse (VBS).

Riistvara virtualiseerimist kasutava kaitse sisselülitamine

Riistvara virtualiseerimist kasutava kaitse sisselülitamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige **Turvaseaded** → **Privaatsusseaded** → **Andmesisestuskaitse**.
4. Märkige ruut **Kasuta riistvara virtualiseerimist, kui see on saadaval**. See märkeruut kuvatakse, kui rakendus on paigaldatud 64-bitisesse Windows 8, Windows 8.1 ja Windows 10 operatsioonisüsteemi.
5. Kui soovite riistvara virtualiseerimise sisse lülitada operatsioonisüsteemi käivitamisel, märkige ruut **Kasuta riistvara virtualiseerimise täpsemaid funktsioone**.

Kui riistvara virtualiseerimine lülitatakse teie arvutis välja, lülitatakse välja ka riistvara virtualiseerimist kasutav kaitse.

Kaitse Antimalware Scan Interface'i (AMSI) abil

Sellest jaotisest saate teada, et kolmanda osapoole rakendused, näiteks Microsoft Office, võivad saata Kaspersky rakendusele skripte, et kontrollida neid liidese Antimalware Scan Interface (AMSI) abil, samuti saate siit teada, kuidas AMSI kaitse Kaspersky rakenduses välja lülitada.

Teave Antimalware Scan Interface'i (AMSI) kaitse kohta

Antimalware Scan Interface (AMSI) võimaldab AMSI-ga ühilduval kolmanda osapoole rakendusel saata objekte (näiteks PowerShell skripte) lisakontrolliks Kaspersky rakendusse ja võtta vastu nende objektide kontrollimise tulemused. Sellised kolmanda osapoole rakendused võivad olla näiteks Microsoft Office'i rakendused. AMSI-liidese kohta leiate lisateavet [Microsofti dokumentatsioonist](#).

Antimalware Scan Interface võimaldab ainult tuvastada ohu ja teatada tuvastatud ohust kolmanda osapoole rakendust. Pärast ohuteate saamist takistab kolmanda osapoole rakendus kahjulikud toimingud (näiteks lülitub välja).

Kaspersky rakendus võib kolmanda osapoole rakenduse taotluse tagasi lükata näiteks juhul, kui rakendus ületab kindlas ajavahemikus lubatud taotluste maksimumarvu. Sellisel juhul kuvab Kaspersky rakendus tagasilükatud taotluse kohta teate. Kui saate sellise teate, ei pea te mitte midagi tegema.

Kaitse pahavaravastase skannimise liidesega on saadaval operatsioonisüsteemides Windows 10 Home/Pro/Education / Enterprise ja Windows 11 Home/Pro/Enterprise.


Antimalware Scan Interface'i kaitse lubamine

Antimalware Scan Interface'i kaitse lubamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige **Turvaseaded** → **AMSI kaitse**.
4. Märkige jaotises **Skriptikontroll** ruut **Kontrolli skripte liidesega Antimalware Scan Interface (AMSI)**.

Antimalware Scan Interface'i kontrollist skripti väljajätmine

Antimalware Scan Interface'i kontrollist skripti väljajätmiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige **Turvaseaded** → **AMSI kaitse**.
4. Märkige jaotises **Skriptikontroll** ruut **Kontrolli skripte liidesega Antimalware Scan Interface (AMSI)**.
5. Akna **Erandid** avamiseks klõpsake linki **Halda erandeid**.
6. Klõpsake aknas **Erandid** nuppu **Lisa**.
Avaneb aken **Uue erandi lisamine**.
7. Määrake väljal **Fail või kaust** skripti sisaldav kaust.
8. Määrake väljal **Objekt** skripti nimi.

Maski abil saate eranditesse lisada ka mitu sama tüüpi faili.

9. Märkige jaotises **Kaitsekomponendid** ruut komponendi failide kaitse komponendi kõrval.
10. Valige olek **Aktiivne**.

Määratud objekti ei kontrollita Antimalware Scan Interface'i abil.

Arvutikaitse kaughaldus

Kui teie arvutisse on installitud Kaspersky ja see on My Kasperskyga ühendatud, saate selle arvuti kaitset kaugteel hallata.

Arvutikaitse kaughaldamiseks logige sisse oma My Kaspersky kontole ja avage jaotis **Seadmed**.

Jaotises **Seadmed** saate teha järgmist.

- Arvuti turvaprobleemide loendi vaatamine ja probleemide kaugteel parandamine
- Arvutist viiruste ja muude ohtude otsimine
- Uuenda andmebaasid ja rakendusemoodulid
- Kaspersky komponentide häälestamine

Kui arvuti kontroll käivitatakse My Kaspersky kaudu, töötleb Kaspersky tuvastatud objekte automaatselt, ilma teie sekkumiseta. Viiruse või muu ohu tuvastamise korral proovib Kaspersky rakendus nakkuse eemaldada ilma arvutit taaskäivitamata. Kui nakkust ei saa eemaldada ilma arvutit taaskäivitamata, kuvatakse My Kasperskys arvuti turvaprobleemide loendis teade, et arvuti tuleb nakkuse eemaldamiseks taaskäivitada.

Kui My Kasperskys tuvastatud objektide loend sisaldab üle 10 üksuse, siis üksused rühmitatakse. Sel juhul saab tuvastatud objekte My Kaspersky kaudu töödelda ainult ühiselt, ilma et igat objekti saaks eraldi uurida. Sellisel juhul soovitame objektide eraldi uurimiseks kasutada arvutisse paigaldatud rakenduse kasutajaliidest.

Arvutikaitse kaughalduse kasutamine

Arvutikaitse kaughalduse kasutamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Profil**.
3. Klõpsake jaotises **Logi My Kasperskysse sisse** nuppu **Logi sisse**.
4. Tehke avanenud aknas üks järgmistest toimingutest.
 - Kui teil on konto, sisestage oma meiliaadress ja parool ning looge ühendus My Kasperskyga.
 - Kui teil pole kontot, sisestage tekstiväljale oma meiliaadress ja klõpsake nuppu **Loo**. Määratud meiliaadressile saadetakse parooliloomisingiga sõnum.

Pärast ühenduse loomist kuvatakse jaotises **Profil** teave teie ühenduse kohta kontoga. Nüüdsest saate oma My Kaspersky kontolt hallata selle arvuti kaitset kaugteel.

Lisateavet seadmete kaitse kaughaldamise kohta leiate jaotisest [My Kaspersky abi](#).

Jõudlus

Seadme aeglaseks muutumise või hangumisega puutuvad kokku paljud kasutajad. Mõnikord keelduvad rakendused avanemast või brauser ei reageeri otsustaval hetkel. Põhjusi, miks see võib juhtuda, on mitu. Tagage oma seadme stabiilne töö paljudeks aastateks.

Kiirkäivitus

Kas teie arvuti käivitamine võtab liiga kaua aega? Tavaliselt juhtub see siis, kui operatsioonisüsteemi käivitumisel käivitatakse palju rakendusi. Anname teile teada, millised rakendused teie arvutit käivitamisel aeglustavad, ja aitame teil nende rakenduste automaatkäivituse keelata.

Arvuti käivitamise kiirendamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Jõudlus**.
3. Klõpsake nuppu **Kuva rakendused** jaotises **Kiire käivitus**.

Avaneb aken **Arvuti käivitumise kiirendamine** arvuti käivitamisel käivituvate rakenduste loendiga.

Veerg **Mõju käivitumisele** näitab teavet iga rakenduse mõju kohta arvuti käivitumisele. See teave võetakse operatsioonisüsteemist ja sõltub sellest, kui palju arvutiressursse rakendus kasutab (protsessori koormus ja muutmälu).

4. Valige loendist rakendus ja seadke lüliti **Automaatkäivitus** asendisse **Väljas**.

Rakendust ei käivitata enam operatsioonisüsteemi käivitumisel.

Arvuti kiirendamine

Aja jooksul koguneb operatsioonisüsteemidesse palju digitaalset prügi, mis halvendab teie arvuti jõudlust. Jõudlust halvendavad ka erinevad failid, mida ei kasutata, ja Windowsi registriprobleemid. Kaspersky rakendus hoiatab teid, kui nende andmete hulk muutub liiga suureks, ja teile antakse võimalus otsustada, millised andmed kustutada.

Operatsioonisüsteemi puhastamiseks tehke järgmist.


1. Avage rakenduse peaaaken.
2. Avage jaotis **Jõudlus**.
3. Jaotises **Arvuti kiirendaja** klõpsake nuppu **Otsi** (või **Kuva**, kui otsing on juba tehtud).

Kaspersky teeb otsingu ja koostab järgmise sisuga aruande.

- **Kasutamata süsteemifailid.** Klõpsake nuppu **Kuva** et vaadata üksikasjalikku aruannet operatsioonisüsteemi kasutamata failide kohta. Klõpsake nende failide kustutamiseks nuppu **Tühjenda**.
- **Windowsi registriprobleemid.** Klõpsake nuppu **Kuva**, et vaadata üksikasjalikku aruannet Windowsi registriprobleemide kohta, mille saate kustutada ilma operatsioonisüsteemi kahjustamata. Tuvastatud probleemide parandamiseks klõpsake nuppu **Paranda**.

Kasutamata failide eemaldamine ja tuvastatud probleemide parandamine muudab teie arvuti kiiremaks.

Arvuti töö kiirendamise viiside automaatotsingu väljalülitamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Jõudlus**.
3. Klõpsake jaotises **Arvuti kiirendaja** nuppu .
4. Tühjendage märkeruut **Arvuti töö kiirendamise viiside automaatotsing**.

Rakenduseuuendaja

Sellest jaotisest leiate teavet selle kohta, kuidas värskendada installitud rakendusi Kaspersky rakenduse abil.

Saadaval ainult plaanides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Teave rakenduseuuendaja kohta

Kui te pole pikka aega arvutis rakendusi uuendanud, võivad rakendused olla haavatavad. Sissetungijad saavad haavatavusi ära kasutada teie arvuti või andmete kahjustamiseks.

Paigaldatud rakenduste uuendamine parandab teie arvuti turvalisust. Kaspersky rakenduse abil saate otsida installitud rakenduste värskendusi ning uusimad värskendused alla laadida ja installida.

Kaspersky rakendus jagab rakenduste värskendused kahte tüüpi:

- *Oluline* – uuendused, mis parandavad paigaldatud rakenduste haavatavusi ja teie arvuti turvalisust.
- *Soovitatav* – uuendused, mis täiustavad funktsioone ja/või teevad paigaldatud rakendustesse muudatusi.

Kaspersky rakendus otsib regulaarselt värskendusi. Kui Kaspersky rakendus leiab teie arvutisse installitud rakendusele uue värskenduse, näitab Kaspersky rakendus teavitusalal hüpikteadet. Teave saadaolevate uuenduste saadavuse, arvu ja tüübi kohta kuvatakse teadete keskuses. Teadete keskuse kaudu saate kuvada, alla laadida ja [paigaldada saadaolevad uuendused](#).

Samuti saate [käsitsi käivitada rakenduste uuenduste otsingu](#).

Kaspersky rakendus laadib alla ja installib kõik teadaolevate rakenduste värskendused vaikimisi, kui need ei nõua nõustumist uute lõppkasutaja litsentsilepingutega.

Windows 8 ja hilisemates versioonides peatab Kaspersky rakendus rakenduste värskenduste automaatse allalaadimise, kui kasutatakse mahupõhist internetiühendust. Uuenduste allalaadimist jätkatakse pärast piiramatut ühenduse taastamist. Kui käivitasite värskenduse käsitsi, laadib Kaspersky rakendus värskenduse alla hoolimata sellest, kas kasutate piiratud ühendust või mitte.

Teatud rakenduste uuendamiseks võib vaja minna arvuti administraatoriõigusi.

Rakendused, mida te ei soovi värskendada või mille jaoks te ei soovi installida üksikuid värskendusi, lisab Kaspersky rakendus erandite loendisse. Saate [erandite loendit vaadata ja muuta](#).

Enne esimese rakenduste värskenduste otsingu käivitamist võib Kaspersky rakendus nõuda andmebaaside ja rakendusemoodulite uuendamist.

Rakenduste uuenduste otsimine


Rakenduste uuenduste otsingu käivitamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Jõudlus**.
3. Klõpsake jaotises **Rakenduseuuendaja** nuppu **Otsi uuendusi**.

See käivitab rakenduste uuenduste otsingu.

Rakenduseuuendaja seadete muutmise

Rakenduseuuendaja seadete muutmiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Jõudlusseaded**.
4. Klõpsake **Rakenduseuuendaja**.
Avatakse aken **Rakenduseuuendaja seaded**.
5. Kui te ei soovi, et Kaspersky rakendus laadiks alla ja installiks automaatselt sellised rakenduste värskendused, mis ei nõua nõustumist uue lõppkasutaja litsentsilepinguga, tühjendage märkeruut **Laadib uuendused automaatselt alla ja paigaldab, kui sellega ei kaasne litsentsilepinguga nõustumist**.

Vaikimisi on see ruut märgitud.

6. Valige jaotises **Rakenduseuuenduste otsimine**, millised rakendusevärskendused Kaspersky rakendus alla laadib ja installib.
 - Valige **Olulised uuendused, mis parandavad arvuti turvalisust**, kui soovite, et Kaspersky rakendus installiks ainult olulised värskendused, mis kõrvaldavad tarkvara haavatavusi ja suurendavad teie arvuti turvalisust.
 - Valige **Kõik tuntud rakenduste uuendused**, kui soovite, et Kaspersky rakendus installiks kõik tarkvaravärskendused.

Uuenduste otsingu režiimi seadistamine

Uuenduste otsingu režiimi seadistamiseks installitud rakenduste jaoks tehke järgmist.

1. Avage rakenduse peaaaken.

2. Klõpsake põhiakna allservas nuppu .

Avatakse aken **Seaded**.

3. Valige jaotis **Jõudlusseaded**.

4. Klõpsake **Rakenduseuuendaja**.

Avatakse aken **Rakenduseuuendaja seaded**.

5. Märkige plokis **Uuendus** ruut **Luba rakenduseuuenduste otsing**.

6. Akna **Häälesta uuenduste otsingurežiim** avamiseks klõpsake linki **Uuenduste otsingu režiim**.

7. Tehke ripploendis **Otsi uuendusi** üks järgmistest valikutest.

- **automaatselt**. Selle valiku korral otsib Kaspersky rakendus vähemalt üks kord 24 tunni jooksul rakendusevärskendusi vastavalt rakendusesisestele seadetele.
- **iga päev / iga nädal / Iga kuu**. Kui teete ühe nendest valikutest, otsib Kaspersky rakendus värskendusi teie määratud ajakava põhjal minutilise täpsusega. Kui teha üks neist valikutest, on saadaval loend **Lükka käitamine pärast rakenduse käivitust edasi N minutit**.

8. Märkige ruut **Kui arvuti on välja lülitatud, otsi uuendusi järgmisel päeval**, et käivitada ajastatud otsingu vahelejätmise korral otsing siis, kui arvuti sisse lülitatakse. Kui ruut pole märgitud, käivitab rakendus uuenduste otsingu ainult ajastatud ajal, kui arvuti on sisse lülitatud.

9. Seadete salvestamiseks klõpsake nuppu **Salvesta**.

Rakenduseuuenduste loendi vaatamine

Kaspersky rakendus otsib arvutisse installitud rakenduste värskendusi regulaarselt. Teavet rakenduste jaoks saadaolevate uuenduste arvu ja tüüpide kohta saab vaadata teadete keskusest.

Rakenduste uuenduste otsingu põhjal genereeritud loendi kuvamiseks tehke järgmist.

1. Avage rakenduse peaaken.

2. Klõpsake akna ülaserivas nuppu **Üksikasjad**.

Avatakse aken **Teatiste keskus**.

3. Klõpsake jaotises **Olek** saadaolevate rakenduseuuenduste teate real nuppu **Näita**.

Avatakse aken **Rakenduseuuendaja**, mis sisaldab saadaolevate rakenduseuuenduste loendit.

4. Kõigi loendis kuvatud rakenduste uuendamiseks klõpsake nuppu **Uuenda kõik** (pole kõigis piirkondades saadaval).


5. Kindlate rakenduste valikuliseks uuendamiseks tehke üks järgmistest toimingutest.

- Klõpsake uuendatava rakenduse real nuppu **Uuenda**.


Enne rakenduse uuendamist on soovitatav lugeda lõppkasutaja litsentsilepingut. Lõppkasutaja litsentsilepingud on saadaval ripploendis **Litsentsilepingud**. Vaikimisi ühtib lõppkasutaja litsentsilepingu keel rakenduse kasutajaliidese keelega. Kui lõppkasutaja litsentsileping ei ole saadaval rakenduse kasutajaliidese keeles, siis esitatakse lõppkasutaja litsentsilepingu tekst Kaspersky rakenduse liidese keeles. Kõigil muudel juhtudel esitatakse lõppkasutaja litsentsilepingu tekst inglise keeles või esimeses saadaolevas keeles, kui ingliskeelne tekst pole saadaval.

- Menüü avamiseks klõpsake nuppu  ja valige **Ära seda rakendust uuenda**, kui soovite, et Kaspersky rakendus lõpetaks teie teavitamise valitud rakendusele saadaolevatest värskendustest.

Valitud rakendus teisaldetakse [erandite loendisse](#). Kaspersky rakendus lõpetab selle rakenduse jaoks välja antud uute värskenduste kohta teadete kuvamise.

- Menüü avamiseks klõpsake nuppu  ja valige **Jäta see uuendus vahele**, kui soovite, et Kaspersky rakendus lõpetaks teie teavitamise valitud värskendusest.

Valitud uuendus teisaldetakse erandite loendisse. Kaspersky rakendus kuvab teate, kui selle rakenduse jaoks antakse välja uus värskendus.

- Menüü avamiseks klõpsake nuppu  ja valige **Ava tootja veebisait**, kui soovite valitud rakenduse uuenduse käsitsi alla laadida ja paigaldada.

Tarkvaratootja veebisait avatakse operatsioonisüsteemi vaikeveebilehitsejas. Veebisaidil saab uuenduse kuvada ja käsitsi alla laadida.

Akna liides, rakenduste värskendusprogramm ja lõppkasutaja litsentsilepingute kuvamine võivad olenevalt Kaspersky rakenduse lokaliseerimiskeelest erineda.

Uuenduse või rakenduse eemaldamine erandite loendist

[Rakenduste uuenduste loendi vaatamisel](#) saate jätta vahele teated üksikute uuenduste kohta või jätta vahele teated kindla rakenduse kõigi uuenduste kohta. Kaspersky rakendus lisab need värskendused ja rakendused erandite loendisse.

Erandite loendist uuenduse või rakenduse eemaldamiseks tehke järgmist.

1. Avage rakenduse peaaaken.

2. Klõpsake põhiakna allservas nuppu .

Avatakse aken **Seaded**.

3. Valige jaotis **Jõudluseaded**.

4. Klõpsake **Rakenduseuuendaja**.

Avatakse aken **Rakenduseuuendaja seaded**.

5. Akna **Erandid** avamiseks klõpsake linki **Erandid**.

Loend **Erandid** sisaldab rakendusi ja uuendusi, mille korral olete märkinud, et ühtegi uuendust pole vaja, samuti rakenduste üksikuid uuendusi, mida te ei paigaldanud.

6. Valige loendist uuendus või rakendus ja klõpsake nuppu **Kustuta**.

Järgmise värskenduste otsingu ajal teavitab Kaspersky rakendus teid erandite loendist eemaldatud rakendustele saadaolevatest värskendustest.

Duplikaadid

Teie arvuti võib salvestada identsete failinimede ja identse sisuga faile. Need duplikaatfailid kasutavad liiga palju mälu, võtavad kõvakettal ruumi ja muudavad arvuti aeglasemaks. Duplikaatfailide funktsiooni abil saate otsida duplikaatfaile ja kustutada lisakoopiad.

Duplikaatfailide eemaldamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Jõudlus**.
3. Valige jaotise **Duplikaadid** ripploendist otsinguala.
4. Klõpsake **Otsi**.
5. Valige otsingutulemuste aknas failid ja klõpsake nuppu **Kustuta**.

Duplikaatfailid eemaldatakse teie arvutist, kuid algandmed säilitatakse.

Suured failid

Proovite oma arvutisse andmeid salvestada, kuid avastate äkki, et kõvaketas on peaaegu täis. Kas see tuleb tuttav ette? Sel juhul aitame teil otsida üles ja kustutada suured failid, mida te enam ei vaja.

Arvutis suurte failide leidmiseks ja nende eemaldamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Jõudlus**.
3. Määrake ripploendis **Failid, mille maht on suurem kui** jaotises **Suured failid** otsitavate failide suurus, näiteks **> 1 GB**.
4. Valige otsingu jaoks konkreetne kaust või jätkke vaikeväärtus **Kasutaja kaustad** muutmata.
5. Klõpsake **Otsi**.

Otsing viiakse läbi ja avaneb aken **Suured failid**. See kuvab leitud suurte failide loendi. Saate faile sortida failitüübi järgi. Selleks valige failikategooria, näiteks **Pildid**.

6. Tehke järgmised toimingud.
 - Kui soovite kõik failid eemaldada, märkige ruut **Vali kõik** ja klõpsake nuppu **Kustuta**.
 - Muul juhul märkige ruudud vastavate failide kõrval ja klõpsake nuppu **Kustuta**.

Valitud failid eemaldatakse teie arvutist.

Kasutamata rakendused

Arvuti jõudlust mõjutavad erinevad tegurid ja paigaldatud rakenduste arv on üks neist. Mida rohkem rakendusi olete paigaldanud, seda aeglasemalt teie arvuti töötab. Selle põhjuseks on asjaolu, et mõned rakendused, sealhulgas teie teadmata paigaldatud rakendused, võivad käivituda automaatselt, kasutades protsessori ressursse ja RAM-i ning sooritades tarbetuid ja mõnikord isegi pahatahtlikke toiminguid.

Kaspersky rakendus aitab teil need rakendused leida ja eemaldada.

Selliste rakenduste eemaldamiseks, mida te ei kasuta, tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Jõudlus**.
3. Klõpsake nuppu **Otsi** jaotises **Kasutamata rakendused**.

Pärast otsingu lõpetamist kuvab Kaspersky rakendus kasutamata rakenduste loendi. Selles loendis saate valida konkreetsed rakendused, mida eemaldada.

4. Rakenduse eemaldamiseks klõpsake eemaldatava rakenduse kõrval olevat nuppu **Eemalda**.

Rakendus eemaldatakse teie arvutist.

Kõvaketta seisundi jälgimisfunktsioon

Sellest jaotisest leiate teavet selle kohta, kuidas kontrollida arvuti kõvaketta või ühendatud välise kõvaketta seisundit Kaspersky rakenduse abil.

Teave kõvaketta seisundi jälgimisfunktsiooni kohta

Saadaval ainult plaanides Kaspersky Plus ja Kaspersky Premium.

Kui teie kõvaketas saab ootamatult kahjustada, võib see põhjustada kõvakettale salvestatud andmete kaotsimineku. Kaspersky rakendus võimaldab jälgida kõvaketaste seisundit S.M.A.R.T.-funktsiooni abil. (Enesekontrolli analüüsi ja aruandluse tehnoloogia). See tehnoloogia põhineb kõvaketta peamiste jõudlusnäitajate pideval jälgimisel. Kaspersky rakendust kasutades saate kiiresti teada, kui kõvaketta seisund halveneb, ja kopeerida andmed kahjustatud ketastelt teistele andmekandjatele.


Kui kõvaketta seisundi jälgimisfunktsioon on [sisse lülitatud](#), jälgib Kaspersky rakendus pidevalt teie kõvaketaste seisundit ja teavitab teid, kui nende seisund halveneb. Saate [vaadata nii sisemiste kui ka väliste kõvaketaste seisundit](#). Teated kõvaketta seisundi halvenemise kohta kuvatakse tegumiriba teavitusalal. Üksikasjalikud aruanded kõvaketta jälgimise tulemuste kohta kuvatakse jaotises **Aruanded**.

Kui kõvaketta seisund halveneb ja andmete salvestamine sellele pole enam turvaline, pakub Kaspersky rakendus andmekao vältimiseks välja [andmete kopeerimise kõvakettalt muule andmekandjale](#). Võite kopeerida andmed kahjustatud kõvakettalt mis tahes töökorras andmekandjale, mis on parasjagu saadaval.

Võite [kõvaketta seisundi jälgimisfunktsiooni keelata](#). Pärast kõvaketta seisundi jälgimisfunktsiooni väljalülitamist ei teavita Kaspersky rakendus teid enam teie kõvaketaste seisundimuutustest ega paku teile võimalust andmete kopeerimiseks kahjustatud kõvakettastelt teistele andmekandjatele.

Kõvaketta seisundi jälgimisfunktsiooni sisse- või väljalülitamine

Kõvaketta seisukorra jälgimisfunktsiooni sisse- või väljalülitamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige **Jõudlusseaded** → **Arvutiressursside kasutus**.
4. Tehke üks järgmistest toimingutest.
 - Kõvaketta seisundi jälgimisfunktsioon sisselülitamiseks märkige ruut **Teosta kõvaketta seisukorra kontroll**.
 - Kõvaketta seisundi jälgimisfunktsioon väljalülitamiseks tühjendage märkeruut **Teosta kõvaketta seisukorra kontroll**.

Kõvaketta seisundi kontrollimine

Kaspersky rakendus jälgib pidevalt nii teie arvuti sisemiste kui ka väliste kõvaketaste seisundit. Jälgimine töötab taustal. Kui kõvaketta seisund halveneb ja andmete salvestamine kettale pole enam turvaline, annab rakendus sellest teile teada ja pakub välja andmete kopeerimise muule andmekandjale.

Aknas **Kõvaketta seisundi jälgimisfunktsioon** kuvatakse kõvaketta kohta järgmine teave.

- Ketta seisukord.
- Ketta temperatuur.

Kõvaketas võib olla ühes järgmistest olekutest.

- *Hea* – uuele kõvakettale vastav olek.
- *Keskmine* – kõvakettaga on ilmnenud väikesed probleemid.
- *Halb* – kõvaketta olek on kriitiline, võimalik on andmekadu.

Kõvaketta temperatuurivahemik võib olla üks järgmistest.

- *Hea* – kõvaketas ei ole ülekuumenemas.
- *Keskmine* – kõvaketta temperatuur on veidi tõusnud.
- *Halb* – kõvaketas on ülekuumenemas.

Diagramm **Ketta seisukorra ajalugu** näitab teavet ketta seisukorra muutuse kohta määratud aja jooksul. Maksimaalne kuvatav aeg on 1 aasta.

Kaspersky rakendus näitab teie kõvaketaste kohta ka järgmist statistikat.

- *Sisselülitatud oleku tunnid kokku* – kõvaketta kogu tööaeg tundides.
- *Toitetsükli arv kokku* – kõvaketta sisselülituste koguarv.

Ketta <ketta nimi> **S.M.A.R.T.-atribuutide** aruanne näitab teavet kõvaketta S.M.A.R.T.-parameetrite väärtuste kohta, mis on sorditud raskusastme järgi. Parameetrite komplekt võib olenevalt kõvaketta tootjast ja mudelist erineda.

Arvuti kõvaketaste praeguse seisundi kontrollimiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Jõudlus**.
3. Jaotises **Kandke hoolt oma kõvaketta ja andmete eest** tehke järgmist.
 - Kui soovite graafikut vaadata, klõpsake nuppu **Ajalugu**.
 - Kui soovite aruannet vaadata, klõpsake nuppu **Üksikasjad**.

See viib teid aknasse, kus saate vaadata kõvaketta seisundi üksikasju.

Andmete kopeerimine kahjustatud kõvakettalt

Kui ühe või enama kõvaketta seisund halveneb ja andmete salvestamine neile pole enam turvaline, annab Kaspersky rakendus sellest teile teada ning pakub andmekao vältimiseks välja andmete kopeerimise neilt kõvaketastelt muule andmekandjale.

Andmete kopeerimiseks kahjustatud kõvakettalt töökorras kõvakettale tehke järgmist.

1. Tehke üks järgmistest toimingutest.
 - Kui saate teate, et kõvaketta seisund halvenes, klõpsake teavitusaknas nuppu **Üksikasjad**.
Avaneb aken **Kõvaketta seisundi jälgimisfunktsioon**.
 - Klõpsake nuppu **Kopeeri andmed** aknas **Kõvaketta seisundi jälgimisfunktsioon**.
2. Klõpsake avanenud aknas **Andmete kopeerimine** nuppu **Käivita varundamine**.
Avatakse aken **Vali hoidla**.
3. Aknas **Vali hoidla** valige kahjustatud kettalt andmete kopeerimiseks töökorras kõvaketas.
4. Klõpsake **Edasi**.
Avatakse aken **Valige kopeeritavad failid ja kaustad**.
5. Tehke üks järgmistest toimingutest.
 - Pukseerige failid Windows Explorerist akna **Valige kopeeritavad failid ja kaustad** esiletõstetud alale.
 - Klõpsake lingil **valige need loendist**.
Avanevas Exploreri aknas saate valida failid ja kaustad, mida kopeerida töökorras kõvakettale.
6. Pärast kõigi kopeeritavate failide ja kaustade loendisse lisamist klõpsake nuppu **Edasi**.

Avatakse aken **Kausta loomine andmete kopeerimiseks**.

7. Tehke üks järgmistest toimingutest.

- Klõpsake nuppu **Edasi**, et luua valitud töökorras kõvakettal uus kaust ning kopeerida kahjustatud kettalt failid ja kaustad sinna.
- Klõpsake nuppu **Muuda**, et valida töökorras kõvakettal olemasolev kaust ning kopeerida failid ja kaustad kahjustatud kõvakettalt sinna.

8. Tehke üks järgmistest toimingutest.

- Kui valitud töökorras kõvakettal on valitud failide ja kaustade kopeerimiseks piisavalt kettaruumi, klõpsake kopeerimise alustamiseks nuppu **Edasi**.
- Kui valitud heal kõvakettal pole valitud failide ja kaustade kopeerimiseks piisavalt kettaruumi, klõpsake nuppu **Tagasi**, et valida muu töökorras kõvaketas ja proovida uuesti.

9. Kui kopeerimine on lõppenud, tehke üht järgmistest.

- Kahjustatud kõvakettalt kopeeritud faile sisaldava kausta avamiseks klõpsake nuppu **Ava kaust**.
- Akna sulgemiseks klõpsake nuppu **Valmis**.

Andmete kopeerimiseks kahjustatud kõvakettalt Dropboxi veebihoidlasse tehke järgmist.

1. Tehke üks järgmistest toimingutest.

- Kui saate teate, et kõvaketta seisund halvenes, klõpsake teavitusaknas nuppu **Üksikasjad**.
Avaneb aken **Kõvaketta seisundi jälgimisfunktsioon**.
- Klõpsake nuppu **Kopeeri andmed** aknas **Kõvaketta seisundi jälgimisfunktsioon**.

2. Klõpsake avanenud aknas **Andmete kopeerimine** nuppu **Käivita varundamine**.

Avatakse aken **Vali hoidla**.

3. Aknas **Vali hoidla** valige oma Dropboxi veebihoidla.

Saate teha ka ühe järgmistest toimingutest.

- Kui hoidla ei ole aktiivne, klõpsake nuppu **Aktiveeri**.
- Hoidka väljalülitamiseks klõpsake linki **Eemalda hoidla**.

4. Klõpsake **Edasi**.

Avatakse aken **Andmete kopeerimine**.

5. Tehke üks järgmistest toimingutest.

- Pukseerige failid Windows Explorerist akna **Andmete kopeerimine** esiletõstetud alale.
- Klõpsake lingil **valige need loendist**.
Avanevas Exploreri aknas saate valida failid ja kaustad, mida kopeerida Dropboxi veebihoidlasse.

6. Pärast kõigi kopeeritavate failide ja kaustade loendisse lisamist klõpsake nuppu **Käivita varundamine**.

Algab andmete kopeerimine.

7. Kui kopeerimine on lõppenud, tehke üht järgmistest.

- Kui andmete varundamine on edukalt lõpetatud, klõpsake akna sulgemiseks nuppu **Valmis**.
- Kui rakendus andis teada, et varundamine ebaõnnestus, vabastage veebihoidlas ruumi ja proovige uuesti.

[OneDrive'i pilvhoidlasse salvestatud andmete kopeerimisele](#) kehtivad piirangud.

Kõvaketta seisundi jälgimisfunktsiooni piirangud

Mõnikord ei saa Kaspersky rakendus kõvaketta olekut järgmiste piirangute tõttu kindlaks teha.

- Kõvaketas ei toeta S.M.A.R.T-tehnoloogiat.
- S.M.A.R.T.-funktsioon on kõvakettal välja lülitatud.
- Kaspersky rakendus ei toeta järgmist.
 - Ühendatud kõvaketta tüüp
 - Kõvaketta USB-kontrolleri tüüp
- Kõvaketas on välja lülitatud.
- Kõvaketas kuulub virtuaalarvutile (näiteks VMWare). Selliste kõvaketaste seisunditeavet kas ei kuvata üldse või kuvatakse valesti.

Varundamine ja taastamine

Sellest jaotisest leiate teavet andmete varundamise kohta.

Teave varundamise ja taastamise kohta

Saadaval ainult plaanides Kaspersky Plus ja Kaspersky Premium.

Varundamise ja taastamise funktsioon kaitseb andmeid kaotsimineku eest, kui arvuti läheb rikki või varastatakse või kui andmed kogemata kustutatakse või häkkerid need rikuvad.

Andmete varundamiseks [looge](#) ja [käivitage](#) varundustegum. Tegumi saab käivitada automaatselt ajakava järgi või käsitsi. Samuti saate rakendusest vaadata teavet lõpule viidud varundustegumite kohta.

Andmete varukoopiaid on soovitatav salvestada irdketastele või veebihoidlasse.

Kaspersky rakendus ei saa luua kettast täielikku koopiat, kui kettal on aktiivne Microsoft Windowsi operatsioonisüsteem.

Kaspersky rakendus võimaldab varukoopiate loomiseks kasutada järgmisi hoidlatüüpe.

- Kohalik ketas
- Irdketas (nt väline kõvaketas)
- Võrguketas
- [Veebihoidla](#).

Kasutaja juurdepääsuõigustel põhinevate tegumite loomine

Varundustegumid luuakse kohalikus arvutis failide suhtes kehtivate kasutaja juurdepääsuõiguste põhjal.

Kui teil pole arvutis kohaliku administraatori õigusi, pääsete juurde ainult enda loodud tegumitele. Kui teil on arvutis kohaliku administraatori õigused, kuvatakse teile kõik varundustegumid, kuid te ei saa teiste kasutajate loodud tegumeid muuta.

Varundustegumid, mis on loodud varem ilma kasutajaõigusi arvesse võtmata, on saadaval kõigile arvuti kasutajatele. Kuid kui sellist tegumit muudetakse, siis käitatakse tegumit seda muutnud kasutaja õiguste põhjal.

Kasutaja juurdepääsuõigustel põhinevate tegumite taastamine

Kui teil pole arvutis kohaliku administraatori õigusi, saate andmeid taastada ainult enda loodud varundustegumitest ja ainult kaustades, millele teil on õigus juurde pääseda. Kui teil on arvutis kohaliku administraatori õigused, saate andmeid taastada kõigist varundustegumitest ja mis tahes kaustas.

Kausta kopeeritud failide kogumaht võib ületada kausta mahtu, kui see sisaldab muude kaustade linke (näiteks kausta „Dokumendid“ kopeerimise korral kopeeritakse ka kaustad „Minu muusika“, „Minu pildid“ ja „Minu videod“, kui kaust „Dokumendid“ sisaldab nende kaustade linke).

Teave OneDrive'is varundamise ja taastamise kohta

Failide varundamisel arvutis olevasse OneDrive'i kausta käitub Kaspersky rakendus erinevalt olenevalt sellest, kas pilvefail on OneDrive'i kausta alla laaditud.

- Kui fail on pilves ja teie arvuti OneDrive'i kaustas, teeb Kaspersky rakendus sellest failist varukoopia.
- Kui faili pole pilves, kuid see on teie arvuti OneDrive'i kaustas, teeb Kaspersky sellest failist varukoopia.
- Kui fail kuvatakse OneDrive'i kaustas, kuid seda talletatakse ainult pilves, mitte teie arvutis, teeb Kaspersky rakendus sellest failist varukoopia.

Varundustegumi loomine

Varundustegumi loomiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Valige jaotis **Jõudlus**.
3. Klõpsake jaotises **Varundamine ja taastamine** nuppu **Vali failid**.

Käivitub varundustegumi loomise nõustaja.

Nõustaja koosneb mitmest lehest (etapist), mille sirvimiseks saate klõpsata nuppe **Tagasi** ja **Edasi**. Pärast lõpetamist nõustaja sulgemiseks klõpsake nuppu **Valmis**. Mis tahes etapis nõustaja peatamiseks klõpsake nuppu **Tühista**.

Nõustaja etappe on üksikasjalikumalt kirjeldatud allpool.

1. etapp. Failide valimine

Nõustaja selles etapis valige varundatavate failide tüüp või määrake varundatavad kaustad.

- Kiirseadistamiseks valige üks eelmääratud failitüüpidest (kaustade „Minu dokumendid“ ja „Töölaud“ failid, fotod ja pildid, filmid ja videod, muusikafailid). Kui kinnitate selle valiku, suunab nõustaja teid 4. etappi „Varuhoidla valimine“.

Kaspersky rakendus ei loo kaustades „Töölaud“ ja „Minu dokumendid“ olevatest failidest varukoopiaid, kui need kaustad asuvad võrgukettal.

- Varundatavate kaustade käsitsi määramiseks valige **Loo varukoopiaid failidest, mis on määratud kaustades**.

2. etapp. Varundatavate kaustade valimine

Kui tegite nõustaja eelmises etapis valiku **Loo varukoopiaid failidest, mis on määratud kaustades**, klõpsake nuppu **Lisa kaust** ja valige avanenud aknas **Varundatava kausta valimine** kaust või lohistage soovitud kaust rakendusaknasse.

Kui soovite määrata valitud kaustadest varundatavad failikategooriad, märkige ruut **Piira varundamist failitüüpide järgi**.

3. etapp. Varundatavate failitüüpide valimine

Kui märkisite nõustaja eelmises etapis ruudu **Piira varundamist failitüüpide järgi**, märkige nõustaja selles etapis varundatavate failitüüpide vastas kuvatavad ruudud.

4. etapp. Varuhoidla valimine

Selles etapis valige varuhoidla.

- **Veebihoidla.** Tehke see valik, kui soovite varukoopiaid talletada Dropboxi veebihoidlas. [Veebihoidla tuleb aktiveerida](#) enne, kui seda saab kasutada. Kui varundate andmed veebihoidlasse, ei loo Kaspersky rakendus varukoopiaid andmetüüpidest, mille kasutamist piiravad Dropboxi kasutusreeglid.
- **Kohalik ketas.** Kui soovite varukoopiaid salvestada kohalikule kettale, valige loendist asjakohane kohalik ketas.
- **Võrguketas.** Kui soovite varukoopiaid salvestada võrgukettale, valige loendist asjakohane võrguketas.
- **Irdketas.** Kui soovite varukoopiaid salvestada irdkettale, valige loendist asjakohane irdketas.

Andmekaitse tagamiseks soovitame kasutada veebihoidlat või luua varukoopiaid irdketastel.

[Võrguhoidla lisamine](#) ?

Võrguhoidla lisamiseks tehke järgmist.

1. Klõpsake linki **Lisa võrguhoidla**, et avada aken **Lisa võrguhoidla**, ja valige võrguhoidla.
2. Sisestage võrguhoidlaga ühenduse loomiseks nõutavad andmed.
3. Klõpsake nuppu **OK**.

[Irdketta lisamine hoidlana](#) ?

Irdketta lisamiseks varukoopiate hoidlana tehke järgmist.

1. Akna **Ühendu olemasoleva hoidlaga** avamiseks klõpsake linki **Hoidlaga ühendamine**.
2. Valige jaotis **Irdketas**.
3. Klõpsake nuppu **Sirvi** ja määrake avanenud aknas irdketas, kuhu soovite salvestada failide varukoopiaid.

Märkige ruut **Kasuta hoiustamise täpsemaid seadeid**, kui soovite seadistada failihoidla seadeid, näiteks säilitatavate varukoopiaaversioonide arvu ja varukoopiate säilitamise kestust.

5. etapp. Varundamise ajakava loomine

Nõustaja selles etapis tehke üks järgmistest toimingutest.

- Kui soovite varundustegumi käivitada automaatselt, määrake varundustegumi ajakava.
 - a. Valige ripploendist **Käivita varundamine** ajavahemik, mille järel tegumit käivitatakse (näiteks **iga päev**), ja sisestage väljale **Algusega** tegumi käivitamise kellaeg.
 - b. Sisestage jaotisesse **Konto** oma Windowsi konto kasutajanimi ja parool selles arvutis. Teie Windowsi konto andmeid on vaja varundamisel failidele juurdepääsemiseks.

c. Kui soovite varundamise käivitada võimalikult kiiresti pärast arvuti sisselülitamist, märkige ruut **Kui arvuti on määratud ajal välja lülitatud, käivita ajastatud varundus arvuti käivitamisel**. Oletagem näiteks, et varundamine on ajastatud igaks nädalavahetuseks. Kui arvuti oli nädalavahetusel välja lülitatud, tehakse varundamine pärast tööpäeval arvuti sisselülitamist. Kui ruut on märkimata, tehakse varundamine ajakava järgi, ilma et varundamist proovitakse pärast nurjunud katset uuesti.

- Kui soovite tegumi käivitada käsitsi, tehke loendis **Käivita varundamine** valik **käsitsi**.

Varundustegumitega töötamisel pidage meeles järgmist.

- Kui loote ajastatud varundustegumi, tuleb teil sisestada oma konto andmed selles arvutis.
- Kui loote nõudmisel käivitatava varundustegumi, tuleb teil sisestada oma konto andmed selles arvutis.
- Kui muudate nõudmisel käivitatava tegumi ajastatud tegumiks, tuleb teil sisestada oma konto andmed selles arvutis.

6. etapp. Varukoopiate kaitsmiseks parooli seadmine

Varukoopiatele juurdepääsu parooliga kaitsmiseks märkige ruut **Luba parooliga kaitse** ning täitke väljad **Varukoopiatele juurdepääsu parool** ja **Kinnitage parool**.

Parool on nõutav selleks, et kaitsta varuhoidlat volitamata juurdepääsu eest.

Rakendus küsib teilt parooli järgmistel juhtudel.

- Kui loote kohalikul kettal või irdkettal (nt mäluseadmel) varuhoidla esimest korda. Kohalikul kettal või samal irdkettal edasiste varundustegumite loomise korral ei palu rakendus teil enam parooli sisestada. Kasutatakse eelnevalt sisestatud parooli.

Kui kopeerite kohaliku varukoopiate hoidla irdkettale ja ühendate selle irdketta teise arvutiga, küsib rakendus teilt sellest hoidlast andmete kopeerimiseks või taastamiseks parooli.

- Kui ühendate irdketta arvutiga. Rakendus kontrollib irdketast ja küsib teilt parooli, kui tuvastab irdkettalt varukoopiate hoidla.

7. etapp. Failiversioonide hoidla seaded

See etapp on saadaval, kui 4. etapis „Varuhoidla valimine“ on märgitud ruut **Kasuta hoiustamise täpsemaid seadeid**.

Määrake failihoidla seaded.

- Märkige ruut **Piira faili varukoopiate versioonide arvu** ja sisestage väljale **Varukoopiate versioonid**, mida säilitada varukoopiate arv, mida soovite igast failist säilitada.
- Märkige ruut **Piira varukoopiate versioonide hoiustamise perioodi** ja sisestage väljale **Säilita varasemaid varukoopiate versioone kuni päevade arv**, mille jooksul iga failiversiooni varukoopiat tuleb säilitada.

8. etapp. Varundustegumi nime sisestamine

Selles etapis tehke järgmist.

- Sisestage varundustegumi nimi.
- Pärast nõustaja lõpuleviimist varundamise automaatkäivitamiseks märkige ruut **Käivita varundamine pärast häälestamise lõppemist**.

9. etapp. Nõustaja lõpuleviimine

Selles aknas kuvatakse varuhoidla seadistamise edenemine. Seadistusprotsess võib pisut aega võtta.

Kui seadistamine on lõpule viidud, klõpsake nuppu **Valmis**.

Varundustegum on loodud. Teie loodud tegum kuvatakse aknas **Varundamine ja taastamine**.

Varundustegumi käivitamine

Varundustegumi käivitamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Valige jaotis **Jõudlus**.
3. Klõpsake jaotises **Varundamine ja taastamine** nuppu **Kuva varukoopiad**.
4. Valige avanenud aknas **Varundamine ja taastamine** soovitud varundustegum ja klõpsake nuppu **Käivita**.

Varundustegum käivitatakse.

Varukoopiast andmete taastamine

Varukoopiast andmete taastamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Valige jaotis **Jõudlus**.
3. Klõpsake jaotises **Varundamine ja taastamine** nuppu **Kuva varukoopiad**.

Avatakse aken **Varundamine ja taastamine**.

- Klõpsake asjakohase varundustegumi vastas kuvatavat nuppu **Failide taastamine**.
- Akna avamiseks klõpsake nuppu **Halda hoidlaid** ja klõpsake asjakohase varuhoidla vastas kuvatavat nuppu **Failide taastamine**.

4. Kui varukoopia loomisel on määratud parool, sisestage aknas **Hoidlasse sisenemiseks sisestage parool** see parool.

5. Valige ripploendist **Varundamise kuupäev ja kellaaeg** varukoopia loomise kuupäev ja kellaaeg.

6. Tehke üks järgmistest toimingutest.

- Kui soovite taastada kõik andmed, märkige ruut **Kõik andmed**.
- Kui soovite taastada ainult kindlad kaustad, märkige asjakohaste kaustade kõrval kuvatavad ruudud.
- Kui soovite taastada ainult kindlad failid, märkige veerus **Nimi** asjakohaste failide kõrval kuvatavad ruudud.

7. Ainult kindlat tüüpi failide taastamiseks valige ripploendist **Faili tüüp** soovitud failitüübid.

8. Klõpsake **Taasta valitud failid**.

Avatakse aken **Failide taastamine varukoopiatest**.

9. Valige üks kahest võimalusest.

- **Algne kaust**. Selle valiku korral taastab rakendus andmed alguses kaustas.
- **Määratud kaust**. Selle valiku korral taastab rakendus andmed määratud kaustas. Et valida kaust, kus soovite andmed taastada, klõpsake nuppu **Sirvi**.

10. Valige ripploendis **Kui failinimed on vastuolus** toiming, mille rakendus peab tegema, kui taastatava faili nimi langeb kokku sihtkaustas juba sisalduva faili nimega.

- **küsi** – kui failinimed langevad kokku, palub rakendus teil valida ühe järgmistest võimalustest: asendada fail varukoopiaga, salvestada mõlemad failid või jätta fail taastamata.
- **asenda fail varukoopiaga** – Kaspersky rakendus kustutab olemasoleva faili ja asendab selle varukoopiast taastatud failiga.
- **salvesta mõlemad failid** – Kaspersky rakendus jätab olemasoleva faili muutmata ja salvestab varukoopiast taastatud faili samasse kausta uue nimega.
- **ära seda faili taasta** – Kaspersky rakendus jätab olemasoleva faili muutmata ja ei taasta varukoopiast samanimelist faili.

11. Klõpsake **Taasta**.

Taastamiseks valitud failid taastatakse varukoopiast ja salvestatakse määratud kausta.

Andmete taastamine FTP-hoidlast

Kaspersky rakendus ei toeta FTP kaudu varundamist ja taastamist. FTP-hoidla kaudu mõnes muus Kaspersky rakenduses loodud varukoopiate taastamiseks järgige alltoodud juhiseid.

FTP-hoidlast varukoopiate taastamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Valige jaotis **Jõudlus**.

3. Klõpsake jaotises **Varundamine ja taastamine** nuppu **Kuva varukoopiad**.
Avatakse aken **Varundamine ja taastamine**.
4. Akna **Halda hoidlaid** avamiseks klõpsake linki **Hoidlad**.
5. Avage Windows Exploreris FTP-hoidla kaust.
6. Kopeerige andmed (sh fail `storage.xml`) kohalikule kettale (näiteks `C:\<kausta nimi>`).
7. Klõpsake aknas **Hoidlad** FTP-hoidla kõrval nuppu **Hoidla kustutamine**.
8. Klõpsake kustutamise kinnitusaknas nuppu **Kustuta**.
Hoidla on nüüd kustutatud.
9. Klõpsake aknas **Hoidlad** nuppu **Ühendu olemasoleva hoidlaga**.
10. Valige aknas **Hoidlaga ühendamine** jaotis **Kohalik ketas** ja klõpsake nuppu **Sirvi** ning määrake FTP-hoidlast kohalikule kettale kopeeritud varukoopiaid sisaldava kausta tee.
11. Klõpsake aknas **Hoidlad** ühendatud hoidla kõrval nuppu **Failide taastamine**.
12. Tehke [tavapärased taastetoimingud](#).

Kaspersky taastevahendi abil varukoopiast andmete taastamine

Kaspersky taastevahend võimaldab teil hallata varuhoidla andmeid arvutis, kus Kaspersky rakendus on rikunud või eemaldatud. Vaikimisi asub vahend pärast rakenduse paigaldamist rakenduse seadistuskaustas paiknevas Kaspersky taastevahendi kaustas. Vahendi kasutamiseks arvutis, kus Kaspersky rakendus on paigaldamata või rikunud, kopeerige vahend irdkettale.

Kaspersky taastevahendi käivitamiseks vajate kohaliku administraatori õigusi.

[Taastevahendi käivitamine](#)

Taastevahendi käivitamiseks tehke järgmist.

1. Avage irdketas, kuhu olete vahendi kopeerinud.
2. Käivitage Kaspersky taastevahendi kaustas fail `kasperskylab.pure.restoretool`.

Avaneb taastevahendi peaken. Aknas kuvatakse rakenduses seadistatud vaikehoidla. Saate määrata mõne muu hoidla tee.

[Taastevahendi abil hoidla avamine](#)

Taastevahendi abil hoidla avamiseks tehke järgmist.

1. Käivitage taastevahend.

Vahend tuvastab varuhoidla tee automaatselt, kui see on loodud kohalikul C: kettal.

2. Kui varuhoidla asub teisel kettal, klõpsake taastevahendi peaaknas nuppu **Määra hoidla**.

3. Avanenud aknas klõpsake nuppu **Sirvi** ja määrake varuhoidla tee.

4. Klõpsake nuppu **Vali hoidla**.

[Varukoopiast andmete taastamine](#) 

Varukoopest andmete taastamiseks tehke järgmist.

1. Käivitage taastevahend.
2. Tehke taastevahendi peaknas järgmised toimingud.
 - a. Valige ripploendist **Varundustegum** tegum, mille tulemusel on loodud teie soovitud varukoopest.
 - b. Valige ripploendist **Varundamise kuupäev ja kellaaeg** kuupäev ja kellaaeg, millal on loodud asjakohased varukoopest.
3. Valige taastatavad failid. Selleks märkige loendis asjakohaste kaustade kõrval ruudud.
Kaustapuu ja faililoendi vaheldumisi aktiveerimiseks klõpsake välja **Otsing** kõrval kuvatavat nuppu.
4. Klõpsake **Taasta valitud failid**.
Avatakse aken **Taastatavatele failidele asukoha valimine**.
5. Avanenud aknas valige taastavate failide salvestamiseks soovitud asukoht.
 - **Algne kaust**. Andmete taastamiseks alguses kaustas tehke see valik.
 - **Määratud kaust**. Tehke see valik, kui soovite andmete taastamise kausta ise valida. Andmete taastamise kausta valimiseks klõpsake nuppu **Sirvi**.
6. Valige ripploendis **Kui failinimed on vastuolus** toiming, mille rakendus peab tegema, kui taastatava faili sihtkaust sisaldab juba samanimelist faili.
 - **küsi** – kui failinimed langevad kokku, palub rakendus teil valida ühe järgmistest võimalustest: asendada fail varukoopest, salvestada mõlemad failid või jätta fail taastamata.
 - **asenda fail varukoopestiga** – Kaspersky rakendus kustutab olemasoleva faili ja asendab selle varukoopest taastatud failiga.
 - **salvesta mõlemad failid** – Kaspersky rakendus jätab olemasoleva faili muutmata ja salvestab varukoopest taastatud faili samasse kausta uue nimega.
 - **ära seda faili taasta** – Kaspersky rakendus jätab olemasoleva faili muutmata ja ei taasta varukoopest samanimelist faili.
7. Klõpsake **Taasta**.
Avatakse aken **Failide taastamine**. Aknas kuvatakse varukoopest failide taastamise edenemine.
Taastamise saate peatada nupu **Peata** abil.
Valitud failide vajalikud varukoopest taastatakse.

Teave veebihoidla kohta

Kaspersky rakendus võimaldab teil Dropboxi teenuse kaudu salvestada oma andmete varukoopest kaugserveris talletatavasse veebihoidlasse.

Veebihoidla kasutamiseks tehke järgmist.

- Veenduge, et arvutil oleks internetiühendus.
- Looge konto veebipõhise andmehoidlateenuse pakkuja veebisaidil.
- Aktiveerige veebihoidla.

Saate kasutada sama Dropboxi kontot, et varundada ühte veebihoidlasse andmed eri seadmetest, millesse on installitud Kaspersky.

Veebihoidla mahu määrab veebihoidlateenuste pakkuja, s.t Dropboxi veebiteenus. Veebiteenuse kasutustingimuste kohta leiate üksikasjalikumad teavet [Dropboxi veebisaidilt](#).

Failide Dropboxi kopeerimisel ei erista Kaspersky rakendus faili ja/või failitee nimes suur- ja väiketähti. Seega, kui proovite luua varukoopiaid failidest, mille nimed ja/või teed erinevad ainult suurtähestuse poolest, loob Kaspersky rakendus ainult ühe varukoopia, kuna Dropboxis tekib konflikt.

Veebihoidla aktiveerimine

Veebihoidla aktiveerimiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Valige jaotis **Jõudlus**.
3. Klõpsake jaotises **Varundamine ja taastamine** nuppu **Vali failid**.
Käivitus [varundustegumi loomise nõustaja](#).
4. Valige andmetüübi valimise aknas varundatav andmetüüp või määrake soovitud failid käsitsi.
5. Tehke hoidla valimise aknas valik **Veebihoidla** ja klõpsake nuppu **Aktiveeri**.

Veebihoidla loomiseks on vaja internetiühendust.

Avaneb Dropboxi kontosse sisselogimise dialoogiboks.

6. Tehke avanenud aknas üks järgmistest toimingutest.
 - Kui te pole registreerunud Dropboxi kasutajaks, viige registreerumine lõpule.
 - Kui olete registreerunud Dropboxi kasutaja, logige sisse oma Dropboxi kontosse.
7. Veebihoidla aktiveerimise lõpuleviimiseks kinnitage, et Kaspersky rakendusel on andmete varundamiseks ja taastamiseks lubatud kasutada teie Dropboxi kontot. Kaspersky rakendus teisaldab salvestatud andmete varukoopiaid eraldi kausta, mis luuakse Dropboxi rakenduste talletuskaustas.
Pärast veebihoidla aktiveerimise lõpuleviimist avaneb hoidla valimise aken. See sisaldab valimiseks saadaolevate veebihoidlate loendit. Aktiveeritud veebihoidla korral kuvab rakendus kasutatud ruumi ja andmete talletamiseks saadaoleva vaba ruumi hulka.

Failide Dropboxi kopeerimisel ei erista Kaspersky rakendus faili ja/või failitee nimes suur- ja väiketähti. Seega, kui proovite luua varukoopiaid failidest, mille nimed ja/või teed erinevad ainult suurtähestuse poolest, loob Kaspersky rakendus ainult ühe varukoopia, kuna Dropboxis tekib konflikt.

Praegune tegevus

Kui olete märganud, et teie arvuti kipub hanguma või töötab tavapärasest aeglasemalt, võite avada akna **Rakenduste tegevus**, kus on ära toodud praegu töötavate rakenduste ja aktiivsete protsesside loend, ning sulgeda rakendused, mis tarbivad liiga palju ressursse.

Praeguse tegevuse vaatamiseks ja/või rakenduse sulgemiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Jõudlus**.
3. Klõpsake jaotises **Praegune tegevus** nuppu **Kuva tegevus**.
Sellega avatakse akna **Rakenduste tegevus** vahekaart **Käivitatud**.
4. Valige rakenduste loendist rakendus, mis tarbib kõige suuremal hulgal protsessoriressursse (veerg **Protsessor**) ja/või muutmälu (veerg **Mälu**), ning klõpsake nuppu **Katkesta protsess**.

Rakendus suletakse.

Režiim „Mitte segada“

Režiimis „Mitte segada“ ei kuva Kaspersky rakendus teie arvuti turbesündmuste kohta hüpikteateid, kui töötate, õpite, osalete videokõnes või vaatate filmi. Režiim „Mitte segada“ lülitatakse sisse ja välja automaatselt. Te ei pea ise rakenduse seadeid muutma.

Pärast režiimist „Mitte segada“ väljumist kasutab rakendus tegumiriba teavitusalat, et kuvada teade mis tahes sündmuse kohta, mis toimus teie hõivatuse ajal. Kui sündmusi oli mitu, klõpsake nuppu **Vaade**, et minna lehele **Teatiste keskus** ja vaadata kõiki sündmusi.

Samuti saate **Teatiste keskus** jaotise **Olek** vahekaardil **Teatisted** vaadata kõiki viimase kolme päeva jooksul toimunud sündmusi.

Lisateavet teadete kuvamise kohta leiate abi jaotisest Teave teadete kohta.

Mängurežiim


Kui Kaspersky rakendus töötab täisekraanrežiimis koos mõne muu rakendusega (eriti arvutimängudega), võib esineda järgmisi probleeme.

- Rakenduse või mängu jõudlus väheneb süsteemiressursside puudumise tõttu;

- Kaspersky rakenduse teateaknad häirivad kasutajat mängimise ajal.

Vältimaks Kaspersky rakenduse seadete käsitsi muutmist iga kord, kui lülitate sisse täisekraanrežiimi, saate kasutada mängurežiimi. Kui kasutate mängurežiimi ja mängite või töötate rakendustega täisekraanrežiimis, ei käivita Kaspersky rakendus kontrollimis- ja uuendamistegumeid ega kuva teateid.

Mängurežiimi sisselülitamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige **Jõudlusseaded** → **Arvutiressursside kasutus**.
4. Märkige ruut **Mängurežiim**.

Samuti saate märkida ruudu **Režiim Ära sega**. Selles režiimis ei näe te teateid, kui töötate aktiivselt mõne rakendusega, samuti ei alustata kontrolli ja uuendamise tegumeid.

Akusäästja

Kui akusäästja režiim on aktiveeritud, lükkab Kaspersky rakendus ajastatud kontrollimis- ja uuendamistegumid edasi. Vajaduse korral saate kontrolli ja uuendamise tegumid käivitada käsitsi.


Akusäästja režiimi saate sisse või välja lülitada ka aknas [Arvutiressursside kasutus](#), märkides või tühjendades märkeruudu **Akusäästja**.

Operatsioonisüsteemi koormuse optimeerimine

Kui käivitate arvutikontrolli Kaspersky rakenduse abil, võib see kasutada märkimisväärsel hulgal süsteemiressursse. Süsteemi koormuse optimeerimiseks saate häälestada Kaspersky rakenduse käitama kontrollimistegumeid (süsteemimälu, süsteemisektsiooni ja käivitusobjektide jaoks) ning uuendada andmebaase ajal, kui arvuti on lukustatud või ekraanisäästja aktiveeritud. See lisaseade võimaldab teil parandada arvuti turvalisust, ilma et peaksite selle kasutamise ajal jõudluse arvel kompromisse tegema.

Kui arvuti töötab akutoitel, siis ei täida Kaspersky rakendus arvuti jõudeolekus tegumeid, et pikendada aku kasutusaega.

Operatsioonisüsteemi koormuse optimeerimiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige **Jõudlusseaded** → **Arvutiressursside kasutus**.
4. Märkige ruut **Kui protsessor ja kettasüsteemid on suure koormuse all, lükka arvuti kontrollimistoimingud edasi**.

Privaatsus

Tänapäeval leiavad aset tohutud andmelekked, turundajad jälgivad iga teie sammu võrgus – digitaalne must nimekiri on pea lõputu. Teie privaatsuse kaitsmine on muutumas ülioluliseks. Siit saate teada, kuidas Kaspersky rakendus teie privaatsust võrgus kaitseb, et saaksite oma digitaalset jalajälge hallata ja kontrollida.

Kaspersky VPN

Saadaval ainult plaanides Kaspersky Plus ja Kaspersky Premium.

VPN-ühendus luuakse Kaspersky VPN Secure Connectioni abil, mida pakutakse tellimusplaani Kaspersky Plus osana. Kaspersky VPN Secure Connectioni saate käivitada menüüst **Start** (operatsioonisüsteemis Microsoft Windows 7 ja varasemates versioonides), avakuvalt (operatsioonisüsteemis Microsoft Windows 8 ja hilisemates versioonides) või Kaspersky rakenduse aknast.

Kaspersky VPN Secure Connectioni käivitamiseks Kaspersky rakenduse aknast tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Privaatsus**.
3. Klõpsake jaotises **Kaspersky VPN** nuppu **Ava**.

See avab Kaspersky VPN Secure Connectioni peakna.

Lisateavet Kaspersky VPN Secure Connectioni toimimise kohta leiate [selle rakenduse abifailidest](#).

Andmelekkedekontroll

Selles jaotises selgitatakse, kuidas kontrollida, kas teie kasutajakonto andmed on avalikult kättesaadavad.

Teave andmelekkedekontrolli kohta

Pakettide Kaspersky Basic ja Kaspersky Standard andmelekkedekontroll võimaldab teil ainult My Kaspersky kontot käsitsi kontrollida. Teie My Kaspersky konto ja teiste kontode automaatne kontroll on saadaval ainult pakettides Kaspersky Plus ja Kaspersky Premium.

Enamik kasutajaid loob töö, ostlemise ja suhtlemise eesmärgil kontosid erinevatel veebisaitidel. Alati on olemas oht, et ründajad võivad veebilehte häkkida ja pääseda ligi kasutajate andmetele. Kui kasutate sama meiliaadressi ja parooli erinevate saitide puhul, on tõenäolisem, et teie andmed lekivad.

Kaspersky rakendusega saate [kontrollida](#), kas mõnelt teie kasutajakontolt on andmeid lekkinud. Kui kontrollimisel selgub, et teie andmed võivad olla avalikult kättesaadavad, teavitab rakendus teid sellest ja kuvab nimekirja saitidest, kust andmed võisid lekkida, võimaliku lekke kuupäeva ja avalikult kättesaadavate andmete kategooria.

Kaspersky rakendus kontrollib ka seda, kas teie kontodelt on lekkinud andmeid pimevõrku. Kui leke leitakse, hoiatab rakendus teid selle eest.

Kaspersky ei too kasutajakontode kontrollimisel andmeid lihttekstina ning kasutab neid ilma salvestamata ainult määratud kontrolli jaoks. Lekke tuvastamisel ei saa Kaspersky rakendus juurdepääsu teie kasutajaandmetele, vaid annab ainult teavet andmekategooriate kohta, mis võivad olla avalikult kättesaadavad.

Kaspersky rakendus võib teid teavitada järgmiste andmekategooriate võimalikust lekkest.

- **Isiklikud andmed:** näiteks passiandmed, biomeetrilised andmed, andmed vanuse kohta.
- **Pangaandmed:** näiteks krediitkaartide ja pangakontode numbrid, teave krediitkaartidel ja pangakontodel olevate vahendite kohta.
- **Tegevusajalugu:** näiteks autentimistõendid, paroolide ajalugu.

Vaikimisi proovib Kaspersky rakendus kontrollida teie kasutajakontosid vastavatel veebisaitidel autoriseerimise ajal. Autoriseerimisel krüpteeritakse teie veebisaidile sisselogimiseks kasutatav meiliaadress ja edastatakse KSNi pilve. Kui kontrolli käigus selgub, et teie andmed võivad olla avalikult kättesaadavad, saadetakse teile vastav teade. [Andmelekkekontrolli](#) saab välja lülitada.

Automaatseks kontrollimiseks saab lisada kuni 50 kontot. Kontode loendeid Kaspersky rakenduses ei sünkroonita seadmete vahel. Lisatud kontosid kontrollitakse kord päevas.

Kontode lisamine automaatseks kontrollimiseks mõeldud loendisse ei pruugi saada olla teie piirkonnas.

Kaspersky rakendus kontrollib perioodiliselt teie My Kaspersky kontoga lingitud meiliaadressi. Esimene selline kontroll tehakse 48 tundi pärast Kaspersky installimist. Täiendav kontroll tehakse iga 24 tunni järel.

My Kaspersky konto andmelekkekontroll ei tööta, kui Kaspersky rakendus pole ühendatud My Kasperskyga või kui rakendusse pole sisestatud My Kaspersky konto parooli.

Andmelekkekontrolli lubamine või keelamine

Kontokontrolli lubamiseks või keelamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Valige jaotis **Privaatsus**.
3. Klõpsake jaotises **Andmelekkekontroll** nuppu **Otsi lekkeid**.
Avatakse aken **Andmelekkekontroll**.
4. Andmelekkekontrolli komponendi lubamiseks või keelamiseks kasutage lülitit.

Kuidas kontrollida, kas teie andmed võivad muutuda avalikult kättesaadavaks

Et kontrollida, kas teie andmed võivad muutuda avalikult kättesaadavaks, tehke järgmist.

1. Avage rakenduse peaaaken.
2. Valige jaotis **Privaatsus**.
3. Klõpsake jaotises **Andmelekkekontroll** nuppu **Otsi lekkeid**.

Avatakse aken **Andmelekkekontroll**.

4. Tippige sisestusväljale oma meiliaadress ja klõpsake nuppu **Kontrolli**.

Kaspersky rakendus alustab antud aadressi kontrollimist. Kui kontrollimisel selgub, et teie andmed võivad olla avalikult kättesaadavad, teavitab rakendus teid sellest ja kuvab nimekirja saitidest, kust andmed võisid lekkida, võimaliku lekke kuupäeva ja avalikult kättesaadavate andmete kategooria. Andmekategooria lingile klõpsamisel kuvatakse soovitusel, kuidas minimeerida nende andmete võimaliku lekke tagajärgi.

Kaspersky rakendus võimaldab teil kontrollida võimalikke andmelekkeid mitte ainult enda, vaid ka näiteks teie sõprade ja pereliikmete kasutajakontodelt.

Kuidas luua automaatseks kontrollimiseks kontode loendit

Automaatseks kontrollimiseks kontode loendi loomiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Valige jaotis **Privaatsus**.
3. Klõpsake jaotises **Andmelekkekontroll** nuppu **Otsi lekkeid**.
Avatakse aken **Andmelekkekontroll**.
4. Väljal **Kontrollige rohkem kontosid** määrake selle konto meiliaadress, mille soovite automaatse kontrollimise loendisse lisada, ja klõpsake nuppu **Kontrolli**.
Teie lisatud konto kuvatakse loendis **Kontod**.

Kontode lisamine automaatseks kontrollimiseks mõeldud loendisse ei pruugi saadaval olla teie piirkonnas.

Privaatne sirvimine

Sellest jaotisest leiab teavet selle kohta, kuidas saab Kaspersky rakendus teid kaitsta teie veebitegevuse jälgimise eest.

Teave privaatsel sirvimisel

Saadaval ainult plaanides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Mõned veebisaidid kasutavad teie Interneti-tegevuste kohta teabe kogumiseks jälgimisteenuseid. Seejärel analüüsitakse seda teavet ja kasutatakse teile reklaamide näitamiseks.

Privaatsel sirvimisel komponent on loodud takistama teie veebitegevuse kohta teabe kogumist.

Avastamise režiimis tuvastab privaatse sirvimise komponent andmete kogumise katsed, loeb need kokku ja kirjutab selle teabe [aruandesse](#). Vaikimisi on sisse lülitatud avastamise režiim ja andmete kogumine on [lubatud kõikidel veebisaitidel](#).

Blokeerimise režiimis tuvastab ja blokeerib privaatse sirvimise komponent andmete kogumise katsed ning kirjutab teabe nende katsete kohta [aruandesse](#). Selles režiimis on andmete kogumine blokeeritud [kõigil veebisaitidel](#), välja arvatud järgmistel:

- [eranditesse lisatud](#) veebisaidid;
- Kaspersky ja meie partnerite veebisaidid;
- veebisaidid, mis Kaspersky andmetel ei pruugi jälgimisteenuste blokeerimise korral olla kasutatavad.

Blokeeritud andmete kogumise katsete loendur näitab kogu saidi blokeeringute koguarvu, mis oleneb sellest, mitu saidilehte on veebilehitsejas avatud. Kui veebilehitsejas on avatud üks leht, võetakse arvesse ainult sellel saidilehel blokeeritud andmete kogumise katseid. Kui veebilehitsejas on avatud sama saidi mitu lehte, võetakse arvesse saidi kõikil veebilehitsejas avatud lehtedel blokeeritud andmete kogumise katseid.

Komponenti Privaatne sirvimine saate hallata Kaspersky rakenduse kasutajaliidese kaudu või [brauseris](#) laiendi Kaspersky Kaitse abil.


Privaatsel sirvimisel on järgmised piirangud.

- Rakendus ei blokeeri kategooriasse „Suhtlusvõrgud“ kuuluva jälgimise teenuse andmekogumist, kui viibite asjakohase suhtlusvõrgu veebisaidil.
- Kui veebilehte, kust andmekogumiskatse pärineb, ei ole võimalik kindlaks teha, ei blokeeri Kaspersky rakendus seda andmekogumiskatset ega kuva selle kohta teavet.
- Kui veebilehe, kust andmekogumiskatse pärineb, saab küll kindlaks teha, kuid seda ei ole võimalik vastendada ühegi brauseris hetkel avatud veebilehega, teeb Kaspersky rakendus Privaatse sirvimise seadetes määratud toimingut (blokeerib või lubab andmete kogumise). Rakendus kuvab andmekogumiskatse teavet aruannetes, kuid ei lisa seda teavet veebilehitsejas kuvatavasse privaatse sirvimise statistikasse.

Komponent on vaikimisi välja lülitatud.

Andmete kogumise blokeerimine

Andmete kogumise blokeerimiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Privaatsus**.
3. Valige komponent **Privaatne sirvimine** ja klõpsake ikooni .
Avatakse aken **Privaatse sirvimise seaded**.
4. Kui komponent on välja lülitatud, siis selle sisselülitamiseks seadke akna ülaservas kuvatav lüliti asendisse **Sees**.
5. Valige **Blokeeri andmete kogumine**.
Kaspersky rakendus blokeerib andmekogumiskatsed kõikil veebisaitidel, välja arvatud [erandid](#).

6. Kui soovite andmete kogumise blokeerida või lubada jälgimisteenuste kategooria põhjal, tehke järgmist.

a. Akna **Kategooriad ja erandid** avamiseks klõpsake linki **Kategooriad ja erandid**.

b. Vaikimisi on andmete kogumine blokeeritud kõigi jälgimisteenusekategooriate ja kõigi suhtlusvõrkude jaoks. Eemaldage märged ruutudest, mis on kuvatud nende jälgimisteenusekategooriate ja suhtlusvõrkude vastas, mille jaoks soovite andmete kogumise lubada.

Kõigil veebisaitidel andmete kogumise lubamine

Kõigil veebisaitidel andmete kogumise lubamiseks tehke järgmist.

1. Avage rakenduse peaaken.

2. Avage jaotis **Privaatsus**.

3. Valige komponent **Privaatne sirvimine** ja klõpsake ikooni .

Avatakse aken **Privaatse sirvimise seaded**.

4. Kui komponent on välja lülitatud, siis selle sisselülitamiseks seadke akna ülaservas kuvatav lüliti asendisse **Sees**.

5. Valige **Kogu vaid statistikat**.

Kaspersky rakendus tuvastab ja loendab teie veebitegevuse jälgimise katseid neid blokeerimata. Komponenti töötulemusi saate vaadata [aruandest](#).

Andmete kogumise lubamine erandina

Saate kindlatel veebisaitidel oma tegevuse jälgimise lubada erandina.

Erandina andmete kogumise lubamiseks tehke järgmist.

1. Avage rakenduse peaaken.

2. Avage jaotis **Privaatsus**.

3. Valige komponent **Privaatne sirvimine** ja klõpsake ikooni .

Avatakse aken **Privaatse sirvimise seaded**.

4. Kui komponent on välja lülitatud, siis selle sisselülitamiseks seadke akna ülaservas kuvatav lüliti asendisse **Sees**.

5. Valige **Blokeeri andmete kogumine**.

Kaspersky rakendus blokeerib andmekogumiskatsed kõigil veebisaitidel, välja arvatud erandid.

6. Vaikimisi on kasutusel erand, mis lubab andmete kogumise Kaspersky ja meie partnerite veebisaitidel. Kui soovite nendel veebisaitidel andmete kogumise blokeerida, eemaldage ruudust **Luba andmete kogumine Kaspersky ja tema partnerite veebisaitidel** mäрге.

7. Vaikimisi on kasutusel erand, mis lubab andmete kogumise veebisaitidel, mis Kaspersky andmetel ei pruugi andmete kogumise blokeerimise korral olla kasutatavad. Kui soovite nendel veebisaitidel andmete kogumise blokeerida, eemaldage ruudust **Luba andmete kogumine ühildumatutel veebisaitidel** mäрге.

Ühilduvusprobleemide lahendamise korral uuendab Kaspersky ühildumatute veebisaitide loendit.

8. Kui soovite erandeid täpsustada, tehke järgmist.

a. Akna **Kategooriad ja erandid** avamiseks klõpsake linki **Kategooriad ja erandid**.

b. Akna **Erandid** avamiseks klõpsake linki **Privaatse sirvimise erandid**.

c. Klõpsake **Lisa**.

d. Sisestage avanenud aknas selle veebisaidi aadress, kus soovite tegevuse jälgimise lubada, ja klõpsake nuppu **OK**.

Määratud veebisait lisatakse erandite loendisse.

Samuti saate valitud veebisaidil andmete kogumise lubada, kui see on avatud [veebilehitsejas](#).

Andmete internetist kogumise katsete aruande vaatamine

Teie andmete internetist kogumise katsete aruande vaatamiseks tehke järgmist.

1. Avage rakenduse peaaaken.

2. Avage jaotis **Privaatsus**.

3. Valige komponent **Privaatne sirvimine** ja klõpsake ikooni .

Avatakse aken **Privaatse sirvimise seaded**.

Kui komponent on välja lülitatud, siis selle sisselülitamiseks seadke akna ülaservas kuvatav lüliti asendisse **Sees**.

Aknas kuvatakse koondaruanne teabega teie andmete internetist kogumiseks tehtud katsete kohta.

Andmekogumiskatsete aruannet saate vaadata ka [brauserist](#) või rakenduse tööaruandest.

Veebilehitsejas privaatsuse sirvimise komponendi haldamine

Privaatsuse sirvimise komponenti saate hallata otse veebilehitsejas.

- Komponenti sisselülitamine, kui see on välja lülitatud
- Andmete kogumise (tuvastatud) katsete kohta statistika vaatamine
- Akna „Privaatsuse sirvimise seaded“ avamine
- Andmete kogumise blokeerimine või lubamine

Veebilehitsejas privaatsuse sirvimise komponendi haldamiseks tehke järgmist.

Klõpsake veebilehitseja tööriistaribal nuppu  **Kaspersky Kaitse**.

Avanenud menüüs kuvatakse teave komponendi töö ja komponendi juhtelementide kohta.

Paroolihaldur

See jaotis sisaldab teavet paroolide kaitsmise kohta.

Paroolide kontrollimine ja turvaline säilitamine

Saadaval ainult plaanides Kaspersky Plus ja Kaspersky Premium.

Kui olete aktiivne internetikasutaja, peate tavaliselt kasutama palju erinevaid paroole, näiteks pankade veebisaite külastades ning sotsiaalvõrgustikke ja meiliteenuseid kasutades. Suurt hulka paroole on ebamugav kasutada, sest peate meeles pidama, millist parooli konkreetsel veebisaidil kasutate. Seetõttu valivad kasutajad sageli lihtsa lahenduse ja kasutavad erinevatel veebisaitidel ühte lihtsat parooli. See pole aga turvaline lahendus. Lihtsa parooli, mida kasutatakse mitmel veebisaidil, võivad hakerid kergesti murda või kinni püüda. Kui see juhtub pangasaidi parooliga, võite oma raha kaotada.

Kontrollige parooli tugevust

Kaspersky rakendus [kontrollib teie poolt internetis loodud paroolide turvalisust](#). Kui paroolid ei ole piisavalt turvalised, aitab Kaspersky teil luua tugevad paroolid ja hoida neid turvalises kohas.

Kaitse sama parooli kasutamise vastu

Kui sisestate parooli veebisaidile, kus parooli turvalisus on eriti oluline (näiteks suhtlusvõrgus), palub Kaspersky rakendus [lubada kaitse sama parooli kasutamise vastu](#).

Kui kaitse sama parooli kasutamise vastu on sisse lülitatud, siis kontrollib Kaspersky rakendus, kas olete järgmistesse kategooriatesse kuuluvatele veebisaitidele sisestatavaid paroole varem kasutanud.

- pankade ja maksesüsteemide veebisaidid;
- suhtlusvõrgud;
- meiliteenused.

Kui sisestatavat parooli on nende kategooriate veebisaitidel juba kasutatud, teavitab Kaspersky rakendus teid sellest ja pakub uue parooli loomist. Võite [valida veebisaitide kategooriad](#), mille korral tuleks jälgida samade paroolide kasutamist.

Paroolide ja dokumentide turvaline talletamine

Kaspersky Password Manager on mõeldud teie paroolide ja dokumentide turvaliseks hoidmiseks. See kasutab teie isiklike andmete (paroolid, isikuandmed, finants- ja meditsiiniline teave) turvaliseks talletamiseks spetsiaalset krüpteeritud hoidlat.

Kaspersky Password Manageri saate alla laadida Kaspersky rakenduse aknast.

[Kaspersky Password Manageri allalaadimine ja paigaldamine](#) 

Paroolide kaitsmise jaoks Kaspersky Password Manageri allalaadimiseks ja paigaldamiseks

1. Avage rakenduse peaaken.
2. Avage jaotis **Privaatsus**.
3. Klõpsake jaotises **Parooliturve** nuppu **Allalaadimine**.

Kaspersky Password Manageri installipakett laaditakse teie arvutisse alla. Kaspersky Password Manageri installimiseks täitke oma arvutisse rakenduste installimise tavajuhised.

[Kaspersky Password Manageri käivitamine Kaspersky rakenduse aknas](#)

Kui Kaspersky Password Manager on juba installitud, tehke selle käivitamiseks järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Privaatsus**.
3. Klõpsake jaotises **Parooliturve** nuppu **Käivitus**.

Avaneb Kaspersky Password Manageri aken.

Kaspersky Password Manageri kasutusjuhendi leiate [Kaspersky Password Manageri abi](#) veebisaidilt.

Paroolide turvalisuse kontrollimine

Saadaval ainult pakettis Kaspersky Premium.

Teie internetikontod on suures ohus, kui neil on korduvad või nõrgad paroolid (näiteks qwerty või 12345) või kui paroolid põhinevad andmetel, mida on lihtne ära arvata või enda valdusse saada (näiteks teie sugulaste nimed või sünnikuupäevad).

Kaspersky rakendus aitab teil kiiresti kontrollida, kui keerulised on teie paroolid ja kas sama parooli kasutatakse rohkem kui ühel kontol.

Parooli turvalisuse kontrollimiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Valige jaotis **Privaatsus**.
3. Tehke **Parooliturve** all üks järgmistest toimingutest.
 - Kui Kaspersky Paroolihaldur ei ole veel installitud, klõpsake nuppu **Allalaadimine**. Nupu nimi võib olla **Alusta** või **Ava**, kui Kaspersky Paroolihaldur ei ole häälestatud, on aegunud või ühendatud My Kaspersky kontoga, mis ei vasta kontole, millega on ühendatud Kaspersky rakendus.

See käivitab Kaspersky Paroolihalduri installimise. Järgige nõustaja juhiseid.

- Kui kontrolli ei ole veel tehtud, klõpsake nuppu **Kontrolli**,
- Kui kontroll on juba tehtud, klõpsake nuppu **Üksikasjad**.

Kontrolli tulemused kuvatakse jaotises **Parooliturve** ohutuskategooriate kaupa.

Lisateavet paroolikontrollide kohta leiate jaotisest [Kaspersky Password Manageri abi](#).

Paroolide turvalisuse konfigureerimine

Paroolide turvaseadete muutmiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotise **Privaatsusseaded** alamjaotis **Andmesisestuskaitse**.
4. Märkige ruut **Näita nõuandeid tugeva parooli loomiseks**, kui soovite, et Kaspersky rakendus kontrolliks teie poolt veebisaitidel loodud paroolide tugevust ja annaks soovitusi tugevate paroolide loomiseks.
Kui teil on paigaldatud Kaspersky Password Manager, soovib teade teile tugevat parooli. Kui Kaspersky Password Manageri pole paigaldatud, soovime see alla laadida ja paigaldada, et saaksite alati luua tugevad paroolid.
5. Märkige ruut **Hoiata sama parooli kasutamise eest veebisaitidel**, kui soovite, et Kaspersky rakendus kontrolliks, kas olete pankade, suhtlusvõrkude või meiliteenuste veebisaitidele sisestatavaid või loodavaid paroole varem kasutanud.
6. Kui soovite valida veebisaitide kategooriaid, mille korral tuleb kontrollida identsete paroolide kasutamist, klõpsake linki **Valige veebisaitide kategooriad**, et avada aken **Veebisaitide kategooriad**.
7. Märkige järgmiste kategooriate ruudud:
 - **Internetipangad ja maksesüsteemid**. Kui loote või sisestate internetis parooli, kontrollib Kaspersky rakendus, kas olete seda parooli pankade või maksesüsteemide veebisaitidel juba kasutanud.
 - **Sotsiaalvõrgustikud**. Kui loote või sisestate internetis parooli, kontrollib Kaspersky rakendus, kas olete seda parooli suhtlusvõrkudes juba kasutanud.
 - **Suhtlusvõrgud**. Kui loote või sisestate internetis parooli, kontrollib Kaspersky rakendus, kas olete seda parooli meiliteenustes juba kasutanud.

Turvalised maksed

Sellest jaotisest leiate veebipõhiste finantstehingute ja ostude Kaspersky rakenduse abil kaitsmise juhendi.

Teave finantstehingute ja veebiostude kaitsmise kohta

Selleks, et kaitsta pankade ja maksesüsteemide veebisaitidele sisestatavaid konfidentsiaalseid andmeid (nt pangakaardinumbrid, e-panganduse paroolid) ning vältida veebimaksete tegemisel raha varastamist, palub Kaspersky rakendus avada sellised veebisaidid Kaitstud veebilehitsejas.

Kaitstud veebilehitseja on veebilehitseja erirežiim, mis on loodud teie andmete kaitsmiseks panga või maksesüsteemi veebisaitide kasutamisel. Kaitstud veebilehitseja käivitatakse eraldatud keskkonnas, et muud rakendused ei saaks lisada kaitstud veebilehitseja protsessi oma koodi. Kaspersky rakendus loob Mozilla Firefox'i ja Google Chrome'i brauseritele eriprofiilid, et kolmanda osapoole lisandmoodulid ei saaks Kaitstud veebilehitsejat mõjutada. Rakendus ei mõjuta teie andmeid, mille veebilehitsejad võivad salvestada neile loodud profiilidesse.

Kui kasutate Chromiumi-põhist Microsoft Edge'i, Google Chrome'i, Mozilla Firefox'i või Internet Explorerit, avatakse kaitstud veebilehitseja uues aknas.

Rakendus kasutab kaitstud veebilehitseja mitme funktsiooni pakkumiseks [laiendust Kaspersky Kaitse](#).

Veebilehitsejad, mis ei täida [tarkvaranõuded](#), ei saa kaitstud veebilehitseja režiimis töötada. Selliste veebilehitsejate asemel käivitatakse kaitstud veebilehitseja režiimis kas Chromiumi-põhine Microsoft Edge või mõni muu rakenduse seadetes konfigureeritud veebilehitseja.

Kaitstud veebilehitsejat ei saa käivitada järgmistel tingimustel:

- Märkeruut **Lülita Enesekaitse sisse** on akna **Arvutiressursside kasutus** jaotises **Jõudlusseaded** tühjendatud.
- Javascript on veebilehitsejas keelatud.

Kaitstud veebilehitseja kasutamine Yandexi veebilehitsejas

Kaspersky rakendus aitab teie finantstehinguid Yandexi brauseris kaitsta mõningate piirangutega. Kaitstud veebilehitseja käivitamiseks lisab rakendus veebilehele (ja liiklusse) eriskripti. Laiendus Kaspersky Kaitse pole saadaval. Privaatse sirvimise ja ribareklaamifiltri komponendid töötavad, kuid neid ei saa Yandexi veebilehitsejas seadistada.

Kaitstud veebilehitseja võimalused

Kaitstud veebilehitseja režiimis kaitseb rakendus järgmist tüüpi ohtude eest.

- Ebausaldusväärsed moodulid. Rakendus kontrollib ebausaldusväärseid mooduleid iga kord, kui külastate panga või maksesüsteemi veebisaiti.
- Rootkit'id. Rakendus otsib kaitstud veebilehitseja käivitamisel rootkit'e.
- Panga või maksesüsteemi veebisaitide kehtetud serdid. Rakendus kontrollib serte, kui külastate panga või maksesüsteemi veebisaiti. Kontroll tehakse ründe ohvriks langenud sertide andmebaasi põhjal.

Kaitstud veebilehitseja olek

Kui avate veebisaidi kaitstud veebilehitsejas, kuvatakse veebilehitseja akna servades raam. Raami värv tähistab kaitse olekut.

Veebilehitseja akna raam võib kuvada järgmisi värvitähiseid.

- Roheline raam. Tähendab, et kõik kontrollid on edukalt tehtud. Võite jätkata kaitstud veebilehitseja kasutamist.
- Kollane raam. Tähendab, et kontrollide käigus on leitud turvaprobleeme, mis tuleb lahendada. Rakendus suudab tuvastada järgmised ohud ja turvaprobleemid.
 - Ebausaldusväärne moodul. Nõutav on arvuti kontrollimine ja nakkuse eemaldamine.
 - Rootkit. Nõutav on arvuti kontrollimine ja nakkuse eemaldamine.
 - Panga või maksesüsteemi veebisaidi kehtetu sert.

Kui te ei kõrvalda tuvastatud ohte, pole tagatud panga või maksesüsteemi veebisaidi ühendusseansi turvalisus. Kaitstud veebilehitseja käivitamine ja kasutamine vähendatud kaitsega registreeritakse Windowsi sündmuselogis.

Teave ekraanipiltidevastase kaitse kohta

Teie andmete kaitsmiseks kaitstud veebisaitide sirvimise ajal ei lase Kaspersky rakendus nuhkvaral teha volitamata kuvatõmmiseid. Ekraanipiltidevastane kaitse on vaikimisi lubatud. Ekraanipiltidevastane kaitse töötab isegi siis, kui [riistvara virtualiseerimine](#) on keelatud.

Teave löikepuhvri andmete kaitse kohta


Kaspersky rakendus blokeerib veebimaksete tegemisel rakenduste volitamata juurdepääsu löikepuhvriks, takistades sedasi kurjategijate andmevargusi. Blokeering on aktiivne ainult juhul, kui ebausaldusväärne rakendus proovib saada volitamata juurdepääsu teie löikepuhvriks. Kui kopeerite andmed rakenduse aknast käsitsi teise rakenduse aknasse (näiteks Notepadist tekstiredaktori aknasse), on juurdepääs löikepuhvriks lubatud.

Löikepuhvri kaitse ei tööta, kui arvutis on keelatud [riistvara virtualiseerimine](#).

Kui Kaitstud veebilehitseja käivitatakse operatsioonisüsteemis Microsoft Windows 10, blokeerib Kaspersky rakendus platvormi Universal Windows rakenduste suhtlemise löikepuhvriga.

Turvaliste maksete seadete muutmine

Turvaliste maksete seadistamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Privaatsusseaded**.
4. Klõpsake **Turvalised maksed**.

Aknas kuvatakse turvaliste maksete komponendi seaded.

5. Turvaliste maksete sisselülitamiseks klõpsake akna ülaservas kuvatavat lülitit.
6. Valige jaotises **Pankade ja maksesüsteemide esmasel külastamisel toimi järgmiselt** toiming, mille rakendus peab tegema, kui avate veebilehitsejas panga või maksesüsteemi veebisaidi esmakordselt.
 - Valige **Käivita Kaitstud veebilehitseja**, kui soovite, et rakendus avaks veebisaidi kaitstud veebilehitsejas.
 - Valige **Küsi kasutajalt**, kui soovite, et rakendus küsiks teilt veebisaidi külastamise korral, kas soovite veebisaidi kaitstud veebilehitsejas avada või mitte.
 - Valige **Ära käivita Kaitstud veebilehitsejat**, kui soovite, et rakendus ei avaks veebisaiti kaitstud veebilehitsejas.
7. Avage jaotises **Lisaks ripploend Veebisaitide avamiseks Turvaliste maksete aknast kasuta järgmist** ja valige veebilehitseja, mille rakendus käivitab kaitstud veebilehitseja režiimis, kui külastate panga või maksesüsteemi veebisaiti turvaliste maksete aknast.

Saate valida ühe arvutisse paigaldatud veebilehitsejatest või kasutada operatsioonisüsteemi vaikeveebilehitsejat.

Kindla veebisaidi jaoks turvaliste maksete seadistamine

Kindla veebisaidi jaoks turvaliste maksete seadistamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Privaatsus**.
3. Valige jaotis **Turvalised maksed** ja klõpsake nuppu **Kuva veebisaidid**.

Avatakse aken **Turvalised maksed**.
4. Veebisaiditeabe sisestusväljade avamiseks klõpsake linki **Lisa veebisait Turvalistesse maksetesse**.
5. Sisestage väljale **Sisestage veebiaadress (URL) Turvalistesse maksetesse lisamiseks** selle veebisaidi veebiaadress, mille soovite avada kaitstud veebilehitsejas.

Veebisaidi aadressile peab eelnema HTTPS-protokolli eesliide (näiteks <https://example.com>), mida kaitstud veebilehitseja vaikinisi kasutab.

6. Valige toiming, mille kaitstud veebilehitseja peab tegema veebisaidi avamise korral.
 - Kui soovite avada veebisaidi kaitstud veebilehitsejas igal külastuskorral, valige **Käivita Kaitstud veebilehitseja**.
 - Kui soovite, et veebisaidi avamise korral küsiks Kaspersky rakendus teilt, mida teha, valige **Küsi kasutajalt**.
 - Kui soovite turvalised maksed veebisaidil välja lülitada, valige **Ära käivita Kaitstud veebilehitsejat**.
7. Välja **Lisa kirjeldus** avamiseks klõpsake linki **Kirjeldus** ja sisestage veebisaidi nimi või kirjeldus.
8. Klõpsake **Lisa**.

Turvaliste maksete kohta tagasiside saatmine

Saate saata Kasperskyle tagasisidet turvaliste maksete komponendi toimimise kohta või teatada komponendi probleemist.

[Tagasiside saatmine](#)

Turvaliste maksete komponendi toimimise kohta tagasiside saatmiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Turvalisus**.
3. Valige jaotis **Turvalised maksed** ja klõpsake nuppu **Kuva veebisaidid**.
Avatakse aken **Turvalised maksed**.
4. Turvaliste maksete komponendi jõudluse kohta tagasiside andmiseks ette nähtud akna avamiseks klõpsake linki **Saada tagasisidet**.
5. Hinnake turvaliste maksete komponenti 5-pallisel skaalal, valides 1–5 täрни.
6. Kui soovite lisada tagasisidele kommentaari, sisestage kommentaari tekst väljale **Üksikasjad**.
7. Klõpsake **Saada**.

[Probleemist teatamine](#)

Kaitstud veebilehitseja probleemist teatamiseks tehke järgmist.

1. Klõpsake kaitstud veebilehitseja allservas kuvatud hüpikaknas linki **Teata probleemist**.

Avanenud aken võimaldab teil teatada turvaliste maksete komponendi probleemist.

2. Valige ripploendist **Probleem** üksus, mis kirjeldab probleemi kõige täpsemalt.

- **Ma ei kasuta seda.** Valige see üksus, kui te ei kasuta turvaliste maksete komponenti või olete otsustanud turvaliste maksete komponendi kasutamisest loobuda.
- **Veebisait avaneb aeglaselt.** Valige see üksus, kui veebisaidi avamine võtab kauem aega kui tavaveebilehitsejas.
- **Kaitstud veebilehitseja käivitub, kui seda vaja pole.** Valige see üksus, kui kaitstud veebilehitsejas avanevad veebisaidid, mis ei nõua turvaliste maksete komponendi kasutamist.
- **Veebisaidi autoriseerimine ebaõnnestub.** Valige see üksus, kui kaitstud veebilehitsejas avatud veebisaidi autoriseerimiskatsetel ilmneb tõrkeid.
- **Veebisait kuvatakse valesti või see ei avane.** Valige see üksus, kui veebisait ei avata kaitstud veebilehitsejas või kui neid kuvatakse tõrgete või moonutustega.
- **Vead veebisaidi sertifikaadi kinnitamisel.** Valige see üksus, kui veebisaidi sertide valideerimisel kuvatakse tõrketeateid.
- **Ekraanipildi tegemine pole kaitstud veebilehitseja töötamise ajal võimalik.** Valige see üksus, kui kaitstud veebilehitsejas ei looda ekraanipilte.
- **Vead klaviatuurilt või lõikelaualt andmete sisestamisel.** Valige see üksus, kui kaitstud veebilehitsejas andmete sisestamisel ilmnevad tõrked.
- **Kaitstud veebilehitsejas avatud veebilehte ei saa printida.** Valige see üksus, kui te ei saa printida veebisaidi avatud lehte.
- **Kuvatakse hoiatus, mis ütleb, et olulised operatsioonisüsteemi uuendused on paigaldamata.** Valige see üksus, kui kaitstud veebilehitseja käitamise ajal kuvatakse teade „Kriitilised süsteemi uuendused ei ole paigaldatud“.
- **Kaitstud veebilehitsejana töötab teine veebilehitseja.** Valige see üksus, kui kaitstud veebilehitseja avatakse muus veebilehitsejas kui selles, kus te selle käivitate.
- **Vead töötamisel.** Valige see üksus, kui kaitstud veebilehitseja on kumanud tõrke.
- **Muu.** Valige see üksus, kui teised üksused ei sobi teie probleemi kirjeldamiseks.

3. Kaspersky probleemi kohta lisateabe saamiseks sisestage selle kirjeldus tekstiväljale **Üksikasjad**.

4. Klõpsake nuppu **Saada**.

Kui Kaspersky rakendus ei saa teie tagasisidet saata (näiteks internetiühendus puudub), salvestatakse see tagasiside teie arvutisse. Tagasisidet talletatakse avalikult 30 päeva.

Turvaliste maksete komponendi toimimise kohta saate tagasisidet saata kuni 10 korda päevas.

Tagasiside saate saata ka pärast seda, kui turvaliste maksete komponent on keelatud. Pärast komponendi keelamist saate tagasisidet saata kord kuus.

Veebikaamera ja mikrofoni kontroll

See jaotis sisaldab teavet selle kohta, kuidas vältida teie veebikaamera kaudu jälgimist ja teie mikrofoni pealtkuulamist.

Saadaval ainult plaanides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Teave rakenduse veebikaamerale ja mikrofoni juurdepääsu kohta

Sissetungijad võivad teid teie veebikaamera kaudu jälgida või teid teie mikrofoni juurdepääsu saamisel pealt kuulata. Kaspersky rakendus kaitseb teie veebikaamerat ja mikrofoni volitamata juurdepääsu eest, kui komponent „Veebikaamera ja mikrofoni kontroll“ on sisse lülitatud. Komponendi seadetes saate kas kõigi rakenduste juurdepääsu veebikaamerale ja mikrofoni blokeerida või valida, et teid teavitataks iga kord, kui mõni rakendus proovib saada juurdepääsu teie veebikaamerale või mikrofoni.

Kui komponent on sisse lülitatud, kuid juurdepääs teie veebikaamerale ja mikrofoni pole täielikult blokeeritud, siis antakse või keelatakse juurdepääs selle usaldusgrupi alusel, millesse vastav rakendus kuulub. Juurdepääs blokeeritakse rakendustele, mis kuuluvad gruppi „Tugevad piirangud“ või „Ebausaldusväärsed“.

Sissetungide vältimise seadete aknas saate gruppi „Tugevad piirangud“ või „Ebausaldusväärsed“ kuuluvate rakenduste juurdepääsu [veebikaamerale](#) või [mikrofoni](#) lubada. Kui veebikaamerale või mikrofoni püüab juurde pääseda rakendus grupist Nõrgad piirangud, siis blokeerib Kaspersky rakendus juurdepääsu ja, kui olete komponendi seadetes valinud teadete saamise, teavitab teid.

Teatise ripploendist saate rakenduse juurdepääsu veebikaamerale või mikrofoni blokeerida või [avada juurdepääsuseaded](#). Teatist ei kuvata, kui mõni rakendus töötab teie arvutis täisekraanrežiimis.

Teatise ripploendist saate valida, kas teatised peita või avada teatiste kuvamisseaded.

[Kuidas Kaspersky veebikaamerat haldab](#) 

Vaikimisi lubab Kaspersky rakendus veebikaamerale juurde pääseda teie luba vajavatel rakendustel, kui rakenduse graafilist kasutajaliidest alles laaditakse, suletakse või see ei reageeri ja te ei saa juurdepääsu käsitsi lubada.

Veebikaamerajuurdepääsu kaitsefunktsioonil on järgmised omadused ja piirangud.

- Kaspersky rakendus kontrollib veebikaamera andmetest tuletatud videoid ja fotosid.
- Kaspersky rakendus kontrollib helisignaali, kui see sisaldub veebikaamerast pärinevas videoos.
- Kaspersky rakendus kontrollib ainult USB või IEEE1394 kaudu ühendatud veebikaameraid, mida kuvatakse Windowsi seadmehalduris pildindusseadmetena.

Ühilduvate veebikaamerate loendi kuvamiseks klõpsake seda [linki](#).

Veebikaamerale volimata juurdepääsu vastase kaitse aktiveerimiseks peab sissetungitõrje komponent olema sisse lülitatud.

Veebikaamera kaitsel on [piirangud, kui rakendus on paigaldatud operatsioonisüsteemi Microsoft Windows 10 aastapäevavärskendusse \(RedStone 1\)](#).

[Kuidas Kaspersky mikrofoni haldab](#)


Mikrofoni kaitsel on järgmised eriomadused.

- Et see funktsioon saaks töötada, peab sissetungitõrje komponent olema sisse lülitatud.
- Pärast rakenduse jaoks helisalvestusseadmetele juurdepääsu seadete muutmist (näiteks kui aknas „Sissetungitõrje seaded“ on rakendusel keelatud juurdepääs audiovoole) tuleb rakendus taaskäivitada enne, kui selle jaoks peatatakse audiovoo vastuvõtt.
- Kaspersky rakendus kaitseb juurdepääsu ainult sisseehitatud mikrofonidele ja välistele mikrofonidele. Teisi heli voogedastusseadmeid ei toetata.
- Kaspersky rakendus lubab rakendusel audiovoogu vastu võtta ja ei kuva ühtegi teadet, kui rakendus alustas audiovoo vastuvõtmist enne Kaspersky rakenduse käivitamist või kui määrasite rakenduse gruppi Ebausaldusväärsed või Tugevad piirangud alles pärast seda, kui rakendus alustas audiovoo vastuvõtmist.

Kaspersky rakendus ei taga DSLR-kaamerate, videokaamerate ja seikluskaamerate audiovoo kaitset.

Rakenduse veebikaamerale või mikrofonile juurdepääsu seadete muutmine

Rakenduste veebikaamerale või mikrofonile juurdepääsu seadeid saate muuta nii.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.

3. Valige jaotises **Privaatsusseaded** komponent **Veebikaamera ja mikrofoni kontroll**.

4. Valige **Veebikaamera seaded** all üks järgmistest toimingutest.

- **Blokeeri kõikide rakenduste juurdepääs veebikaamerale.** Juurdepääs veebikaamerale on kõigi teie arvutisse installitud rakenduste jaoks blokeeritud.
- **Teavita, kui rakendus kasutab veebikaamerat.** Vaikimisi juurdepääsu omavate rakenduste juurdepääs veebikaamerale on lubatud. Kuvatakse teatis, et konkreetne rakendus kasutab veebikaamerat.

5. Valige **Mikrofoni seaded** all üks järgmistest toimingutest.

- **Blokeeri kõikide rakenduste juurdepääs mikrofonile.** Juurdepääs mikrofonile on kõigi teie arvutisse installitud rakenduste jaoks blokeeritud.
- **Teavita, kui rakendus kasutab mikrofoni.** Vaikimisi juurdepääsu omavate rakenduste juurdepääs mikrofonile on lubatud. Kuvatakse teatis, et konkreetne rakendus kasutab mikrofoni.

Veebikaamerale juurdepääsu lubamine või blokeerimine üksiku rakenduse jaoks

Rakenduse jaoks veebikaamerale juurdepääsu lubamiseks või blokeerimiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Turvalisus**.
3. Valige komponent **Sissetungitõrje**.
4. Akna **Rakenduste haldus** avamiseks klõpsake linki **Rakenduste haldus**.
5. Valige loendist rakendus, millel soovite lubada helisalvestusseadmetele juurde pääseda. Akna **Rakenduste reeglid** avamiseks topeltklõpsake rakendust.
6. Avage aknas **Rakenduste reeglid** vahekaart **Õigused**.
7. Valige õiguste kategooriate loendis **Operatsioonisüsteemi muutmine** → **Kahtlased muudatused operatsioonisüsteemis**.
8. Valige **Juurdepääs veebikaamerale**.
9. Valige veerus **Toiming Luba** või **Keela**.
10. Klõpsake **Salvesta**.

Kui valite **Blokeeri kõikide rakenduste juurdepääs veebikaamerale**, blokeeritakse rakenduste juurdepääs veebikaamerale sõltumata usaldusgrupist ja käsitsi antud lubadest.

Mikrofonile juurdepääsu lubamine või blokeerimine üksiku rakenduse jaoks

Rakenduse jaoks mikrofonile juurdepääsu lubamiseks või blokeerimiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Turvalisus**.
3. Valige komponent **Sissetungitõrje**.
4. Akna **Rakenduste haldus** avamiseks klõpsake linki **Rakenduste haldus**.
5. Valige loendist rakendus, mille juurdepääsu mikrofonile soovite lubada, ja tehke sellel topeltklõps, et avada aken **Rakenduste reeglid**.
6. Avage aknas **Rakenduste reeglid** vahekaart **Õigused**.
7. Valige õiguste kategooriate loendis **Operatsioonisüsteemi muutmine** → **Kahtlased muudatused operatsioonisüsteemis** → **Juurdepääs helisalvestusseadmetele**.
8. Valige veerus **Toiming Luba** või **Keela**.
9. Rakendustel audiovoole juurdepääsemise lubamise või keelamise sündmuste kohta teadete saamiseks klõpsake veerus **Toiming** ikooni ja valige **Logi sündmusi**.
10. Klõpsake **Salvesta**.

Kui valite **Blokeeri juurdepääs kõikide rakenduste jaoks**, blokeeritakse rakenduste juurdepääs mikrofonile, sõltumata usaldusgrupist ja käsitsi antud lubadest.

Nuhkvara tuvastamine

Kurjategijad võivad muidu igati legitiimseid rakendusi kasutada teie isiklike andmete varastamiseks ja teie järel nuhkimiseks. Enamik neid rakendusi on kasulikud ja paljudele inimestele abiks. Nende rakenduste hulgas on näiteks IRC kliendid, automaatsed numbrivalijad, allalaadimishaldurid, süsteemitegevuse monitorid, paroolihaldusutiliidid, FTP, HTTP või Telneti serverid.

Kui aga kurjategijad peaksid teie arvutis neile rakendustele juurde pääsema või need salaja teie arvutisse installima, saavad nad mõnda funktsiooni kasutada teie isiklike andmete varastamiseks või muude ebaseaduslike tegevuste jaoks.

Allpool leiate eri tüüpi nuhkvarast ülevaate.

Tüüp	Nimi	Kirjeldus
Client-IRC	IRC kliendid	Inimesed installivad neid rakendusi omavahel IRC-jututubades vestlemiseks. Kurjategijad saavad neid rakendusi kasutada pahavara ehk ründevara levitamiseks.
Dialer	Automaatsed numbrivalijad	Saab modemi kaudu salaja telefoniühendusi luua.
Downloader	Allalaadimishaldurid	Saab veebilehtedelt salaja faile alla laadida.
Monitor	Rakenduste seire	Lubab tegevuse jälgimist arvutis, kuhu selline rakendus on installitud (näiteks saab jälgida, millised rakendused töötavad ja kuidas need

		teistes arvutites asuvate rakendustega andmeid vahetavad).
PSWTool	Paroolitaaste tööriistad	Võimaldavad kasutajatel ununenud parooli vaadata ja taastada. Kurjategijad installivad sellised rakendused salaja inimeste arvutisse samal otstarbel.
RemoteAdmin	Kaughalduse tööriistad	Süsteemiadministraatorid kasutavad selliseid tööriistu laialdaselt kaugarvutitele juurdepääsuks, et neid jälgida ja juhtida. Kurjategijad installivad sellised rakendused inimeste arvutisse salaja samal eesmärgil, et kaugarvutites nuhkida ja neid juhtida. Õiguspärased kaughaldustööriistad erinevad tagaustest (kaugjuhtimist võimaldavatest trooja programmidest). Tagauksed suudavad süsteemi sisse imbuda ja end ise sinna installida, kasutaja loata; legitiimsed rakendused sellisel viisil käituda ei saa.
Server-FTP	FTP-serverid	Töötavad FTP-serveritena. Kurjategijad saavad neid teie arvutisse installida selleks, et avada FTP-protokolli kaudu kaugjuurdepääs teie arvutile.
Server-Proxy	Puhverserverid	Töötavad puhverserveritena. Kurjategijad installivad neid arvutitesse rämpsposti saatmiseks.
Server-Telnet	Telneti serverid	Töötavad Telneti serveritena. Kurjategijad installivad neid teie arvutisse selleks, et avada Telneti protokolli kaudu kaugjuurdepääs teie arvutile.
Server-Web	Veebiserverid	Töötavad veebiserveritena. Kurjategijad saavad neid teie arvutisse installida selleks, et avada HTTP-protokolli kaudu kaugjuurdepääs teie arvutile.
RiskTool	Kohalikud tööriistad	Need tööriistad annavad kasutajatele arvutite haldamiseks lisavõimalusi (nt failide või aktiivsete rakenduseakende peitmiseks või aktiivsete protsesside sulgemiseks).
NetTool	Võrgutööriistad	Need tööriistad annavad arvutikasutajatele lisavõimalused teiste samas võrgus töötavate arvutitega suhtlemiseks (kaugarvutite taaskäivitamiseks, avatud portide leidmiseks, neisse arvutitesse installitud rakenduste käivitamiseks).
Client-P2P	P2P-võrgukliendid	Need tööriistad võimaldavad inimestel kasutada P2P-võrke (võrdõigusvõrke). Kurjategijad saavad neid kasutada pahavara levitamiseks.
Client-SMTP	SMTP kliendid	Saavad salaja meilisõnumeid saata. Kurjategijad installivad neid arvutitesse rämpsposti saatmiseks.
WebToolbar	Veebitööriistaribad	Lisavad teiste rakenduste kasutajaliidesesse otsimootorite tööriistaribad.
FraudTool	Kelmusvara	Jäljendab teisi rakendusi. Näiteks on olemas viirusetõrjet jäljendav kelmusvara, mis kuvab arvutis teateid pahavara leidmise kohta, ent tegelikult ei leia, puhasta ega paranda sellised rakendused midagi.

Kui lülitate nuhkvaratõrje sisse, hoiatame teid katsetest pääseda juurde teie asukohaandmetele, sõnumitele ja muudele isiklikele andmetele.

Aknas [Ohtude ja erandite seaded](#) saate sisse lülitada ka nuhkvarakaitse, märkides ruudu **Avasta muud tarkvara, mida sissetungijad võivad kasutada arvuti või isiklike andmete kahjustamiseks**.

Ribareklaamifilter

Sellest jaotisest leiate teavet selle kohta, kuidas saab Kaspersky teid internetis ribareklaamide eest kaitsta.

Teave ribareklaamifiltri kohta

Saadaval ainult plaanides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Ribareklaamifiltri komponent on loodud pakkuma veebi sirvimise ajal kaitset ribareklaamide eest. Ribareklaamifilter blokeerib teie külastatud veebisaitidel ja mõne rakenduse liideses kuvatud ribareklaamid. Ribareklaamifilter blokeerib ribareklaamid Kaspersky rakenduse andmebaasidele manustatud teadaolevate ribareklaamide loendi alusel. Ribareklaamide blokeerimist saate hallata Kaspersky rakenduse liidese kaudu või otse brauseris.

Vaikimisi on ribareklaamid lubatud loendis **Kaspersky veebisaidid** sisalduvatel veebisaitidel. Selle loendi on koostanud Kaspersky eksperdid ja see sisaldab Kaspersky veebisaitide ja meie partnerite veebisaitide, mis hostivad Kaspersky reklaame. Seda loendit saate vaadata või keelata selle kasutamise, kui peate vajalikuks blokeerida ribareklaamid Kaspersky ja selle partnerite veebisaitidel.

Blokeeritud ribareklaamide loendur näitab kogu saidil blokeeritud ribareklaamide koguarvu, mis oleneb sellest, mitu saidilehte on veebilehitsejas avatud. Kui veebilehitsejas on avatud üks leht, võetakse arvesse ainult sellel saidilehel blokeeritud sisu. Kui veebilehitsejas on avatud sama saidi mitu lehte, võetakse arvesse saidi kõigil veebilehitsejas avatud lehtedel blokeeritud ribareklaamid.

Ribareklaamifiltri töö kohta leiate teavet aruannetest.

Ribareklaamifiltrile rakenduvad järgmised piirangud.


- Mõned saidid tuvastavad, et nende lehtedel olevad reklaamid on blokeeritud ja ei näita sisu enne, kui kasutaja reklaamiblokeerija välja lülitab. Sellise saidi sisu vaatamiseks peate [selle aadressi välistuste hulka lisama](#).
- Kui ribareklaami veebilehte ei ole võimalik kindlaks teha, ei blokeeri Kaspersky rakendus seda ribareklaami ega kuva selle kohta teavet.
- Kui ribareklaami veebilehte saab kindlaks teha, kuid seda ei saa vastendada ühegi veebibrauseris avatud veebilehega, siis Kaspersky rakendus kas blokeerib ribareklaami või lubab seda kuvada olenevalt kindlaks tehtud teabest. Rakendus kuvab selle ribareklaami teavet aruannetes, kuid ei lisa seda teavet veebilehitsejas kuvatavasse ribareklaamifiltri statistikasse.
- Veebilehitsejas kuvatav ribareklaamifiltri statistika võib sisaldada ribareklaame, mis blokeeriti veebilehtede eelmisel laadimiskorral, sealhulgas varem blokeeritud ja uuesti laaditud ribareklaame.
- Veebilehitsejas kuvatav ribareklaamifiltri statistika ei sisalda ribareklaame, mis blokeeriti lehe dünaamilises sisus pärast veebisaidi laadimist.

Ribareklaamifiltri komponendi sisselülitamine

Ribareklaamifiltri komponent on vaikimisi välja lülitatud. Selle saate sisse lülitada Kaspersky rakenduse kasutajaliidese kaudu või brauseris laiendi Kaspersky Kaitse abil.


[Ribareklaamifiltri sisselülitamine Kaspersky rakenduse kasutajaliidese kaudu](#) 

Ribareklaamifiltri sisselülitamiseks Kaspersky rakenduse kasutajaliidese kaudu tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Privaatsusseaded**.
4. Valige komponent Ribareklaamifilter.
Avatakse aken **Ribareklaamifiltri seaded**.
5. Komponenti sisselülitamiseks klõpsake akna ülal servas kuvatavat lülitit.

[Ribareklaamifiltri sisselülitamine veebilehitsejas](#)

Ribareklaamifiltri sisselülitamiseks veebilehitsejas tehke järgmist.

1. Klõpsake veebilehitseja tööriistaribal nuppu  **Kaspersky Kaitse**.
2. Klõpsake jaotise **Ribareklaamifilter** rippmenüüs nuppu **Lülita sisse**.

Pärast ribareklaamifiltri sisse- või väljalülitamist tuleb teil muudatuste jõustamiseks veebileht veebilehitsejas uuesti laadida.

Ribareklaamide blokeerimine


Ribareklaamifilter blokeerib veebisaitide ribareklaamid Kaspersky rakenduse andmebaasidele manustatud teadaolevate ribareklaamide loendi alusel. Kui ribareklaam kuvatakse veebisaidil isegi siis, kui ribareklaamifilter töötab, võib see tähendada, et ribareklaami pole teadaolevate ribareklaamide loendis. Saate selle ribareklaami kuvamise blokeerida käsitsi.

Ribareklaami blokeerimiseks peate selle lisama blokeeritud ribareklaamide loendisse. Seda saate teha otse veebisaidil või Kaspersky rakenduses.

Kui ribareklaam on veebisaidil, mis on nende veebisaitide loendis, millel on [ribareklaamid lubatud](#), ei saa te selle ribareklaami kuvamist blokeerida.

[Veebilehel ribareklaami blokeerimine](#)


Veebilehel ribareklaami blokeerimiseks tehke järgmist.

1. Veenduge, et veebilehitsejas oleks paigaldatud ja lubatud [Kaspersky Kaitse laiendus](#).
2. Kui ribareklaamifilter on keelatud, lubage see.
 - a. Klõpsake veebilehitseja tööriistaribal nuppu  **Kaspersky Kaitse**.
 - b. Klõpsake jaotise **Ribareklaamifilter** rippmenüüs nuppu **Lülita sisse**.
3. Viige hiirekursor blokeeritava ribareklaami kohale ja paremklõpsake.
4. Valige avanenud kontekstimenüüs **Lisa Ribareklaamifiltri andmebaasi**.
Avaneb aken **Blokeeritud ribareklaami lisamine**.
5. Klõpsake aknas **Blokeeritud ribareklaami lisamine** nuppu **Lisa**.
Ribareklaami URL lisatakse blokeeritud ribareklaamide loendisse.
6. Ribareklaami kuvamise peatamiseks värskendage veebilehitsejas veebilehte.

Ribareklaami ei kuvata järgmisel korral, kui külastate seda veebilehte.

[Ribareklaami blokeerimine Kaspersky rakenduses](#) 

Ribareklaami blokeerimiseks Kaspersky rakenduses tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Privaatsusseaded**.
4. Valige komponent Ribareklaamifilter.
Avatakse aken **Ribareklaamifiltri seaded**.
5. Komponendi Ribareklaamifilter sisselülitamiseks klõpsake akna ülaservas kuvataval lülitil.
6. Klõpsake aknas **Ribareklaamifiltri seaded** linki **Blokeeritud ribareklaamid**, et avada aken **Blokeeritud ribareklaamid**.
7. Klõpsake aknas **Blokeeritud ribareklaamid** nuppu **Lisa**.
8. Avanenud aknas sisestage väljale **Veebiaadressi mask (URL)** ribareklaami aadress või aadressimask.
9. Määrake ribareklaami olekuks **Aktiivne**.
10. Klõpsake **OK**.

Kaspersky rakendus blokeerib määratud ribareklaami.

Ribareklaamide lubamine

Saate lubada nii üksiku ribareklaami kui ka kõik teie määratud veebisaidi ribareklaamid.

[Üksiku ribareklaami lubamine](#) 

Üksiku ribareklaami lubamiseks tehke järgmist.


1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Privaatsusseaded**.
4. Valige komponent Ribareklaamifilter.
Avatakse aken **Ribareklaamifiltri seaded**.
5. Komponendi Ribareklaamifilter sisselülitamiseks klõpsake akna ülaservas kuvataval lülitil.
6. Klõpsake aknas **Ribareklaamifiltri seaded** linki **Lubatud ribareklaamidega veebilehed**, et avada aken **Lubatud ribareklaamidega veebilehed**.
7. Klõpsake aknas **Lubatud ribareklaamidega veebilehed** nuppu **Lisa**.
8. Avanenud aknas sisestage väljale **Veebileht** ribareklaami aadress või aadressimask.
9. Valige olek **Aktiivne**.
10. Klõpsake **OK**.

Rakendus ei blokeeri määratud ribareklaami.

Kui ribareklaam on lisatud lubatud ribareklaamide loendisse, kuid ribareklaam kuulub reklaamiplokki, mille omaduste tõttu blokeerib ribareklaamifilter selle veebisaidil, blokeeritakse ribareklaam koos reklaamiplokiga.

[Veebisaidil kõigi ribareklaamide lubamine](#) 


Veebisaidil kõigi ribareklaamide lubamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Privaatsusseaded**.
4. Valige komponent Ribareklaamifilter.
Avatakse aken **Ribareklaamifiltri seaded**.
5. Komponendi Ribareklaamifilter sisselülitamiseks klõpsake akna ülaservas kuvataval lülitil.
6. Klõpsake aknas **Ribareklaamifiltri seaded** linki **Lubatud ribareklaamidega veebilehed**, et avada aken **Lubatud ribareklaamidega veebilehed**.
7. Klõpsake aknas **Lubatud ribareklaamidega veebilehed** nuppu **Lisa**.
8. Avanenud aknas sisestage väljale **Veebileht URL**, näiteks `example.com`.
9. Valige olek **Aktiivne**.
10. Klõpsake **OK**.

Veebisait lisatakse lubatud ribareklaamidega veebisaitide loendisse. Kaspersky ei blokeeri selle loendi veebisaitide ribareklaame isegi juhul, kui ribareklaam on [lisatud blokeeritud ribareklaamide loendisse](#).

Ribareklaamifiltri filtrite seadistamine

Ribareklaamifiltri filtrite seadistamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Privaatsusseaded**.
4. Valige komponent Ribareklaamifilter.
Avatakse aken **Ribareklaamifiltri seaded**.
5. Komponendi Ribareklaamifilter sisselülitamiseks klõpsake akna ülaservas kuvataval lülitil.
6. Akna **Filtrite loend** avamiseks klõpsake linki **Filtrite loend**.
7. Seadistage aknas **Filtrite loend** filtrid vastavalt vajadusele.

- **Soovitav.** Sellesse gruppi kuuluvad teie piirkonnale vastav üldfilter ja keelefilter. Need filtrid on vaikimisi lubatud.
- **Temaatiline.** See grupp sisaldab kahte filtrit.
 - **Suhtlusvõrgud.** Lubage see filter, kui soovite blokeerida suhtlusvõrkude veebisaitidel üksusi, nagu nupud „Meeldib“ ja „Jaga“.
 - **Häirivad üksused.** Lubage see filter, kui soovite blokeerida hüpikaknad, aknad ja muud elemendid, mis ei kuulu konkreetsele veebisaidile.
- **Keele-spetsiifiline.** Selles filtrigrupis saate valida keele. Rakendus blokeerib määratud keeles veebisaitidel ribareklaamid.

Ribareklaamifiltri haldamine veebilehitsejas

Kaspersky Kaitse laienduse abil saate hallata ribareklaamifiltri komponenti otse veebilehitsejas.

Kaspersky Kaitse laiendus võimaldab teil teha järgmisi toiminguid.

- Komponenti lubamine ja keelamine
- Blokeeritud ribareklaamide statistika vaatamine
- Ribareklaamifiltri komponendi seadete akna avamine
- Teabe vaatamine selle kohta, kas veebilehitsejas avatud veebisaidil on ribareklaamid blokeeritud või mitte, ja veebisaidil ribareklaamide kuvamise haldamine

[Ribareklaamifiltri haldamine Kaspersky Kaitse laienduse kaudu](#)

Kaspersky Kaitse laienduse kaudu ribareklaamifiltri komponendi haldamiseks tehke järgmist.

Klõpsake veebilehitseja tööriistaribal nuppu  **Kaspersky Kaitse**.

Avanenud menüüs kuvatakse teave komponendi töö ja komponendi juhtelementide kohta.

Soovimatute rakenduste installimise blokeerija

Vahel installite mõne soovitud programmi ja avastate alles hiljem, et sellega koos installiti ka mitu muud rakendust, mida te ei soovinud. Kas see tuleb tuttav ette? Need soovimatud rakendused installitakse teie teadmata ja võivad teid pommitada reklaamidega või isegi ära vahetada teie vaikebrauseri.

Kui soovite selle probleemi igaveseks unustada, lülitage sisse **Soovimatute rakenduste paigaldamise blokeerija** jaotises **Privaatsus**. Soovimatute rakenduste installimise blokeerija tühjendab automaatselt kõigi installimiseks soovitatud täiendavate rakenduste märkeruudud, et teid säästa nende käsitsi tühjendamise vaevast.

Samuti saate soovimatute rakenduste installimise blokeerija sisse lülitada [rakendushalduri](#) seadete aknas.


Selleks märkige ruut **Tühjenda rakenduste paigaldamisel automaatselt lisatarkvara paigaldamise märkeruudud. Hoiata lisatarkvara paigaldamise katsete korral.**

Soovimatute rakenduste installimise blokeerija ei pruugi toetada kõiki paigaldatavaid rakendusi. Kui paigaldatavat rakendust ei toetata, on soovimatute rakenduste paigaldamist võimatu blokeerida. Meie eksperdid täiendavad toetatud paigaldavate rakenduste loendit pidevalt.

Rakendushalduri seadete muutmise

Saadaval ainult plaanides *Kaspersky Standard*, *Kaspersky Plus* ja *Kaspersky Premium*.

Rakendushalduri seadete muutmiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Valige jaotis **Privaatsus**.
3. Klõpsake jaotises **Soovimatute rakenduste paigaldamise blokeerija** nuppu .
See viib teid aknasse **Rakendushalduri seaded**.
4. Märkige seaderühmas **Soovimatute rakenduste paigaldamise blokeerija** ruut **Tühjenda rakenduste paigaldamisel automaatselt lisatarkvara paigaldamise märkeruudud. Hoiata lisatarkvara paigaldamise katsete korral**, et blokeerida uute rakenduste installimise ajal täiendava tarkvara installimine. Kui uue rakenduse installimise ajal takistatakse mõni soovimatu toiming, teavitab Kaspersky rakendus teid sellest.
Kui ruudust **Tühjenda rakenduste paigaldamisel automaatselt lisatarkvara paigaldamise märkeruudud. Hoiata lisatarkvara paigaldamise katsete korral** eemaldati märged pärast rakenduse installimise alustamist, jätkab soovimatute rakenduste installimise blokeerija töötamist kuni poolelioleva installimise lõpuni. Paigaldamiseks pakutavate lisarakenduste vastas kuvatavatest ruutudest eemaldatakse märged ja lisarakendusi ei paigaldata. Funktsioon lülitatakse välja järgmisel paigalduskorral. Lisarakendused paigaldatakse koos põhirakendusega.
5. Märkige ruut **Ära kuva paigaldusetappe, mis sisaldavad reklaame ja pakkumisi lisaprogrammide paigaldamiseks**, et blokeerida arvutisse uue tarkvara paigaldamise ajal reklaame sisaldavate paigaldusetappide kuvamine. Selliste installisetappide eemaldamise korral teavitab Kaspersky rakendus teid sellest.

Reklaamprogrammide eemaldaja

Kas näete sageli palju tüütuid reklaame? Kaspersky rakendus saab teie arvutist kustutada teie brauserites ja töölaua reklaame kuvavad rakendused. Lisaks reklaamprogrammidele eemaldame ka kõik automaatsed helistamisprogrammid ja kahtlased pakkimiskirjed, mis võivad sisaldada viiruseid või muid ohte. Lülitage **Reklaamvaraeemaldi** sisse ja tüütud reklaamid on minevik!

Reklaamvara eemaldamiseks toimige järgmiselt.

1. Avage rakenduse peaaken.
2. Avage jaotis **Privaatsus**.
3. Lülitage sisse **Reklaamvaraeemaldi** funktsioon.

Salahoidla

Selles jaotises kirjeldatakse, kuidas kaitsta andmeid salahoidlate abil.

Teave salahoidla kohta

Saadaval ainult plaanides Kaspersky Plus ja Kaspersky Premium.

Salahoidlad on ette nähtud teie konfidentsiaalsete andmete kaitsmiseks volitamata juurdepääsu eest. *Salahoidla* on teie arvutisse talletatud andmete hoidla, mille saate lukustada või lukust avada ainult teile teadaoleva parooliga. Lukustatud salahoidlasse talletatud failide muutmiseks peate sisestama parooli. Kui olete sisestanud vale parooli 10 korda järjest, blokeeritakse juurdepääs salahoidlale üheks tunniks.

Parooli kaotamise või unustamise korral ei saa te oma andmeid taastada.

Salahoidlate loomiseks kasutab Kaspersky rakendus andmekrüptimisalgoritmi AES XTS, mille efektiivne võtmepikkus on 56 bitti.

Kui teie arvutis on kasutusel FAT32 failisüsteem, saate luua kuni 4 GB mahuga salahoidlaid.

Failide teisaldamine salahoidlasse

Failide teisaldamiseks salahoidlasse tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Privaatsus**.
3. Tehke jaotises **Salahoidla** ühte järgmistest.

[Kui teil pole veel salahoidlat](#) 

1. Klõpsake **Loo hoidla**.
2. Klõpsake aknas **Salahoidla** nuppu **Lisa** ja valige failid Windows Exploreris või pukseerige failid Kaspersky rakenduse aknasse.
Valitud failid kuvatakse aknas **Salahoidla**.
3. Klõpsake **Jätka**.
4. Sisestage salahoidla nimi ja määrake selle asukoht või kasutage nende seadete vaikeväärtusi.
5. Sisestage salahoidla maht.
6. Salahoidlale kiirjuurdepääsu võimaldamiseks märkige ruut **Loo töölauaial salahoidla otsetee**.
7. Klõpsake **Jätka**.
8. Täitke väljad **Salahoidlale juurdepääsu parool** ja **Kinnitage parool** ning klõpsake nuppu **Jätka**.
9. Valige, mida teha failide väljaspool salahoidlat asuvate algeksemplaridega.
 - Failide väljaspool salahoidlat asuvate algeksemplaride kustutamiseks klõpsake nuppu **Kustuta**.
 - Failide väljaspool salahoidlat asuvate algeksemplaride säilitamiseks klõpsake nuppu **Jäta vahele**.
10. Klõpsake **Valmis**.
Vastloodud salahoidla kuvatakse salahoidlate loendis.
11. Salahoidla lukustamiseks klõpsake nuppu **Lukusta**.
Lukustatud salahoidla andmed on kättesaadavad ainult pärast parooli sisestamist.

[Kui teil on salahoidla juba olemas](#)

1. Akna **Mul juba on salahoidla** avamiseks klõpsake linki **Salahoidla**.
2. Valige oma salakaust aknas **Salahoidla** ja klõpsake nuppu **Ava lukust**.
3. Sisestage parool ja klõpsake nuppu **Ava Windows Exploreris**.
Salahoidla avatakse Windows Exploreris.
4. Teisaldage failid salahoidlasse.
5. Sulgege Windows Exploreri aken.
6. Klõpsake Kaspersky rakenduse kasutajaliidese aknas **Salahoidla** nuppu **Lukusta**.

Kui lisada salahoidlasse sama nime, kuid eri täheregistriga failid, ei pruugi üks neist failidest salahoidla avamiskatsel saada val olla. Andmete kaotamiseks vältimiseks soovime sellised failid lisada eri salahoidlatesse või panna failidele kordumatud nimed.

Juurdepääs salahoidlas talletatavatele failidele

Salahoidlas talletatavatele failidele juurdepääsuks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Privaatsus**.
3. Klõpsake jaotises **Salahoidla** nuppu **Mul juba on salahoidla**.
Avatakse aken **Salahoidla**.
4. Klõpsake salahoidla nime kõrval nuppu **Ava lukust**.
5. Sisestage parool ja klõpsake nuppu **Ava Windows Exploreris**.

Salahoidlasse talletatud failid kuvatakse Exploreri aknas. Faile saate vajaduse korral redigeerida või lisada uusi faile ja salahoidla siis jälle sulgeda.

Ümbernimetatud salahoidla avamise katse võib põhjustada tõrke. Selle vältimiseks soovime avada salahoidla, mille soovite ümber nimetada, pakkida selles olevad andmed lahti ning luua nende andmetega uus salahoidla, millele panete soovitud nime.

Mõnikord võib teistes Kaspersky rakendustes loodud salahoidlate avamisel olla vajalik salahoidlate teisendamine vanast vormingust uude vormingusse. Kui proovite Kaspersky rakenduse kasutajaliidesel salahoidlat avada, soovib Kaspersky rakendus vajaduse korral teisendamist.

Salahoidla teisendamine uude vormingusse võib hoidla mahust olenevalt võtta kaua aega.

Kui Kaspersky rakenduse eemaldamisel on aknas **Säilita järgmised andmed selles arvutis taaskasutamiseks** märkeruut **Rakenduse tööseaded** tühi ja märkeruut **Salahoidla** märgitud, siis peate Kaspersky rakenduse praeguse või tulevase versiooni järgmisel installimisel salahoidlad käsitsi lisama, klõpsates linki **Mul juba on salahoidla** aknas **Salahoidla**.

Failipurustaja

Saadaval ainult plaanides Kaspersky Plus ja Kaspersky Premium.

Isiklike andmete lisakaitse tagamiseks saab kustutatud teavet kaitsta nii, et hakerid ei saaks seda loata taastada.

Kaspersky rakendus sisaldab andmete jäädavalt kustutamise tööriista, mis muudab andmete taastamise tavaliste tarkvaratööriistadega võimatuks.

Kaspersky rakendus võimaldab kustutada andmed järgmistelt andmekandjatelt nii, et neid ei saa taastada.

- Kohalikud kettad. Kustutamine on võimalik, kui teil on andmete kirjutamiseks ja kustutamiseks vajalikud õigused.
- Irdkettad või muud seadmed, mis loetakse irdkandjateks (näiteks disketid, mälukaartid, USB-mäluseadmed või mobiiltelefonid). Andmed saab mälukaardilt kustutada, kui selle ülekirjutamisvastane mehaaniline kaitse on välja lülitatud.

Kustutada saate andmed, millele teil oma isiklikul kontrol juurdepääs. Enne andmete kustutamist veenduge, et töötavad rakendused ei kasutaks neid.

Andmete jäädavaks kustutamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Avage jaotis **Privaatsus**.
3. Klõpsake jaotises **Failipurustaja** nuppu **Vali failid**.
Avatakse aken **Failipurustaja**.
4. Klõpsake nuppu **Sirvi** ja valige avanenud aknas **Kustutatavate failide kustutamine** jäädavalt kustutatav kaust või fail.

Süsteemifailide ja -kaustade kustutamine võib põhjustada operatsioonisüsteemirikkeid.

5. Valige ripploendist **Andmete kustutamise meetod** nõutav andmekustutusalgoritm.

SSD-st ja USB-seadmetest andmete kustutamiseks on soovitatav rakendada **Kiire kustutamine (soovitatav)** või **GOST R 50739-95, Venemaa**. Muud kustutusmeetodid võivad SSD-d või USB-seadet kahjustada.

- **Kiire kustutamine (soovitatav)**. Kustutustoiming koosneb kahest andmete ülekirjutustsüklist: nullide ja pseudojuhuarvude kirjutamisest. Selle algoritmi põhieelis on selle jõudlus. Kiire kustutamine takistab andmete taastamist tavaliste taastetööriistade abil.
- **GOST R 50739-95, Venemaa**. Algoritm teostab ühe pseudojuhuarvudega ülekirjutamise tsükli ja kaitseb andmeid tavatööriistadega taastamise eest. See algoritm vastab Venemaa riikliku tehnilise komisjoni liigituse kohaselt kaitseklassile 2 (6-st).
- **Bruce Schneier Algorithm**. Protsess koosneb seitsmest ülekirjutustsüklist. Meetod erineb Saksa VSITR-ist ülekirjutusjärjestuse poolest. Seda täiustatud andmekustutusemeetodit peetakse üheks kõige usaldusväärsemaks.
- **VSITR Standard, Saksamaa**. Teostatakse seitse ülekirjutustsükli. Algoritmi peetakse usaldusväärseks, kuid selle teostamine võtab palju aega.
- **NAVSO P-5239-26 (MFM) Standard, USA** ja **NAVSO P-5239-26 (RLL) Standard, USA**. Kasutatakse kolme ülekirjutustsükli. Standardid erinevad teineteisest teabe ülekirjutusejärjestuse poolest.
- **DoD 5250.22-M standard, USA**. Algoritm teostab kolm ülekirjutustsükli. Seda standardit kasutab Ameerika Ühendriikide kaitseministeerium.

6. Klõpsake **Kustuta**.

7. Klõpsake avanenud kustutamise kinnitusaknas nuppu **Kustuta**.

Kolmanda osapoole rakenduste kasutatavaid faile ei saa kustutada.

Privaatsete jälgede eemaldaja

Saadaval ainult plaanides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Operatsioonisüsteemis registreeritakse kasutaja arvutis tehtud toimingud. Salvestatakse järgmine teave.

- Kasutajate sisestatud otsingupäringute ja külastatud veebisaitide üksikasjad
- Teave käivitatud rakenduste ning avatud ja salvestatud failide kohta
- Microsoft Windowsi sündmuselogi kirjed
- Muu teave kasutaja tegevuse kohta

Varasemate kasutajatoimingute kohta salvestatud teabes sisalduvatele konfidentsiaalsetele andmetele võivad juurdepääsu saada sissetungijad ja kõrvalised isikud.

Rakendus sisaldab privaatsete jälgede eemaldamise nõustajat, mis eemaldab operatsioonisüsteemist kasutajategevuse jäljed.

Privaatsete jälgede eemaldamise nõustaja käivitamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Privaatsus**.
3. Klõpsake jaotises **Privaatsete jälgede eemaldaja** nuppu **Otsi tegevusi**.

Nõustaja koosneb mitmest lehest (etapist), mille sirvimiseks saate klõpsata nuppe **Tagasi** ja **Edasi**. Pärast lõpetamist nõustaja sulgemiseks klõpsake nuppu **Valmis**. Mis tahes etapis nõustaja peatamiseks klõpsake nuppu **Tühista**.

Nõustaja etappe on üksikasjalikumalt kirjeldatud allpool.

Nõustaja käivitamine

a. Valige üks kahest nõustaja töörežiimist.

- **Otsi jälgi kasutaja tegevusest**. Nõustaja otsib arvutist teie tegevuse jälgi.
- **Pööra muudatused tagasi**. Nõustaja pöörab tagasi privaatsete jälgede eemaldamise nõustaja varem tehtud muudatused. See valik on saadaval, kui nõustaja on tegevusjärgi varem eemaldanud.

b. Nõustaja käivitamiseks klõpsake nuppu **Edasi**.

Tegevusjälgede otsing

Kui tegite valiku **Otsi jälgi kasutaja tegevusest**, otsib nõustaja teie arvutist tegevusjärgi. Otsing võib aega võtta. Kui otsing on lõpule jõudnud, jätkab nõustaja automaatselt järgmist etappi.

Privaatsete jälgede eemaldaja toimingute valimine

Kui otsing on lõpule jõudnud, teavitab nõustaja teid tuvastatud [tegevusjälgedest](#) ja küsib, millised toimingud soovite nende eemaldamiseks teha.

Gruppi kaasatud toimingute kuvamiseks laiendage valitud grupi loend.

Kui soovite, et nõustaja teeks teatud toimingud, märkige toimingu kõrval vastav ruut. Vaikimisi teeb nõustaja kõik soovitatavad ja tungivalt soovitatavad toimingud. Kui te ei soovi kindlat toimingut teha, eemaldage selle kõrval kuvatavast ruudust märged.

On tungivalt soovitatav jätta vaikimisi märgitud ruutudest märked eemaldamata, kuna see jätab teie arvuti ohtude suhtes haavatavaks.

Kui olete nõustaja toimingukomplekti määranud, klõpsake nuppu **Edasi**.

Privaatsete jälgede eemaldaja

Nõustaja teeb eelmises etapis valitud toimingud. Tegevusjälgede eemaldamine võib pisut aega võtta. Teatud tegevusjälgede eemaldamiseks tuleb arvuti taaskäivitada; kui see on vajalik, annab nõustaja sellest teile teada.

Kui eemaldamine lõpule jõudnud, jätkab nõustaja automaatselt järgmist etappi.

Nõustaja lõpuleviimine

Nõustajast väljumiseks klõpsake nuppu **Valmis**.

Internetis isiklike andmete kaitsmine

Selles jaotises on teave teie interneti sirvimise turvalisemaks muutmise ja andmete varguse eest kaitsmise kohta.

Teave internetis isiklike andmete kaitsmise kohta

Kaspersky rakendus aitab teie isiklike andmeid varguse eest kaitsta.

- Paroolid, kasutajanimed ja muud registreerimisandmed
- Kontonumbrid ja pangakaardinumbrid

Kaspersky rakendus sisaldab komponente ja tööriistu, mis võimaldavad teil kaitsta isiklike andmeid kurjategijate eest, kes kasutavad selliseid meetodeid nagu [andmepüük](#) ja klaviatuuri abil sisestatud andmete kinnipüüdmine.

Andmepüügi eest kaitseb andmepüügivastane kaitse, mida rakendatakse ohutu sirvimise ja rämpsmeilifiltri komponentides. Põhjaliku andmepüügivastase kaitse tagamiseks lülitage need komponendid sisse.

Klaviatuuri abil sisestatud andmete kinnipüüdmise eest kaitsevad ekraaniklaviatuur ja klaviatuurikaitse.

Privaatsete jälgede eemaldamise nõustaja eemaldab arvutist kõik andmed kasutaja tegevuse kohta.

Turvalised maksed ja Kaspersky VPN kaitsevad andmeid internetis pangateenuste kasutamisel ja veebipoodides ostlemisel.

Teave ekraaniklaviatuuri kohta

Interneti kasutamise ajal peate sageli sisestama oma isiklikud andmed või kasutajanime ja parooli. Seda juhtub näiteks veebisaitidel, veebipoodides ja internetipangas konto registreerimise käigus.

On oht, et isiklikud andmed võib kinni püüda riistvaraklaviatuuri andmepüüdur ehk klaviatuurinuhk, mis on klahvivajutusi salvestav programm. Ekraaniklaviatuuri tööriist takistab klaviatuuri abil sisestatud andmete kinnipüüdmist.

Paljud nuhkvaraks liigitatud programmid saavad jäädvustada ekraanipilte, mis edastatakse seejärel automaatselt sissetungijale edasiseks analüüsiks, et varastada kasutaja isiklikke andmeid. Ekraaniklaviatuur kaitseb sisestatud isiklikke andmeid ekraanipiltide kaudu kinnipüüdmise eest.

Ekraaniklaviatuuril on järgmised funktsioonid.

- Saate klõpsata ekraaniklaviatuuri nuppe hiirega.
- Erinevalt riistvaraklaviatuuridest ei saa ekraaniklaviatuuril korraga vajutada mitut klahvi. Sellepärast tuleb klahvikombinatsiooni (näiteks **ALT+F4**) sisestamiseks esmalt klõpsata esimest klahvi (näiteks **ALT**), siis teist klahvi (näiteks **F4**) ja seejärel uuesti esimest klahvi. Klahvi teine klõps toimib samamoodi nagu riistvaraklaviatuuril klahvi vabastamine.
- Ekraaniklaviatuuri keelt saab muuta sama otsetee abil, mis on operatsioonisüsteemi seadetes määratud riistvaraklaviatuuri jaoks. Selleks paremklõpsake teist klahvi (näiteks juhul, kui operatsioonisüsteemi seadetes on klaviatuuri keele muutmiseks seadistatud otsetee **VASAKPOOLNE ALT+SHIFT**, vasakklõpsake klahvi **VASAKPOOLNE ALT** ja seejärel paremklõpsake klahvi **SHIFT**).

Ekraaniklaviatuuri abil sisestatud andmete kaitse tagamiseks taaskäivitage arvuti pärast Kaspersky rakenduse installimist.

Ekraaniklaviatuuri kasutamisel on järgmised piirangud.

- Ekraaniklaviatuur takistab isiklike andmete kinnipüüdmist ainult Chromiumi-põhise Microsoft Edge'i, Mozilla Firefox'i või Google Chrome'i veebilehitsejas kasutamise korral. Teistes veebilehitsejates ei kaitse ekraaniklaviatuur sisestatud isiklikke andmeid kinnipüüdmise eest.
- Ekraaniklaviatuur ei saa teie isiklike andmeid kaitsta, kui andmete sisestamist nõudev veebisait on häkitud, sest sel juhul hangivad sissetungijad teabe otse veebisaidilt.
- Ekraaniklaviatuur ei takista ekraanipilte, mis tehakse klahviga **Print Screen** ja muude operatsioonisüsteemi seadetes määratud klahvikombinatsioonide abil.
- Kaspersky rakendus ei kaitse operatsioonisüsteemis Microsoft Windows 8 ja 8.1 (ainult 64-bitises) volitamata kuvatõmmiste eest, kui ekraaniklaviatuuri aken on avatud, kuid Kaitstud veebilehitseja protsess on käivitamata.

Ekraaniklaviatuuri avamine

Ekraaniklaviatuuri saate avada järgmistel viisidel.

- Chromiumi-põhise Microsoft Edge'i, Mozilla Firefox'i või Google Chrome'i tööriistaribal
- Veebisaitide sisestusväljadel kuvatava ekraaniklaviatuuri kiirkäivitusikooni abil


Veebisaitide sisestusväljadel kiirkäivitusikooni kuvamise saate [seadistada](#).

Ekraaniklaviatuuri kasutamise korral lülitab Kaspersky rakendus veebisaitide sisestusväljade automaattäitmise funktsiooni välja.

- Klaviatuuril klahvikombinatsiooni vajutamise teel

[Ekraaniklaviatuuri käivitamine veebilehitseja aknas](#)

Chromiumi-põhise Microsoft Edge'i, Mozilla Firefoxi või Google Chrome'i veebilehitseja tööriistariba kaudu ekraaniklaviatuuri avamiseks tehke järgmist.

1. Klõpsake veebilehitseja tööriistaribal nuppu  **Kaspersky Kaitse**.
2. Valige avanenud menüüs üksus **Ekraaniklaviatuur**.

[Ekraaniklaviatuuri käivitamine riistvaraklaviatuuri abil](#)


Riistvaraklaviatuuri abil ekraaniklaviatuuri avamiseks tehke järgmist.

Vajutage klahvikombinatsiooni **CTRL+ALT+SHIFT+P**.

See klahvikombinatsioon ei kuva ekraaniklaviatuuri, kui sama klahvikombinatsiooni kasutab juba mõni muu rakendus, näiteks Microsoft Word.

Ekraaniklaviatuuri ikooni kuvamise seadistamine

Veebisaitide sisestusväljadel ekraaniklaviatuuri kiirkäivitusikooni kuvamise seadistamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Privaatsusseaded**.
4. Klõpsake aknas **Privaatsusseaded** nuppu **Andmesisestuskaitse**.
Aknas kuvatakse andmesisestuskaitse seaded.
5. Märkige plokis **Ekraaniklaviatuur** ruut **Ava ekraaniklaviatuur, vajutades klahvikombinatsiooni CTRL+ALT+SHIFT+P**.
6. Kui soovite, et ekraaniklaviatuuri kiirkäivitusikoon oleks kuvatud kõigi veebisaitide sisestusväljadel, märkige ruut **Näita andmesisestusväljadel kiirkäivitusikooni**.
7. Kui soovite, et ekraaniklaviatuuri kiirkäivitusikoon oleks kuvatud ainult kindlatesse kategooriasse kuuluvate veebisaitide avamise korral, märkige ruudud nende veebisaidikategooriate kõrval, mille sisestusväljadel tuleb

ekraaniklaviatuuri kiirkäivitusikoon kuvada.

Mis tahes valitud kategooriasse kuuluva veebisaidi avamise korral kuvatakse ekraaniklaviatuuri kiirkäivitusikoon.

8. Kui soovite kindlal veebisaidil ekraaniklaviatuuri kiirkäivitusikooni kuvamise sisse või välja lülitada, tehke järgmist.

a. Akna **Ekraaniklaviatuur** avamiseks klõpsake plokis **Halda erandeid** linki **Ekraaniklaviatuuri erandid**.

b. Klõpsake akna allservas nuppu **Lisa**.

c. Avaneb ekraaniklaviatuuri erandi lisamise aken.

d. Sisestage väljale **Veebiaadressi mask** soovitud veebisaidi veebiaadress.

e. Määrake jaotises **Ulatus**, kus soovite ekraaniklaviatuuri kiirkäivitusikooni kuvada (või mitte kuvada): määratud lehel või veebisaidi kõigil lehtedel.

f. Määrake jaotises **Ekraaniklaviatuuri ikoon**, kas soovite ekraaniklaviatuuri kiirkäivitusikooni kuvada või mitte.

g. Klõpsake **OK**.

Määratud veebisait kuvatakse akna **Ekraaniklaviatuuri erandid** loendis.

Määratud veebisaidi avamise korral kuvatakse sisestusväljadel ekraaniklaviatuuri kiirkäivitusikoon vastavalt määratud seadetele.

Teave arvuti klaviatuuri abil sisestatud andmete kaitse kohta

Kaitstes arvutiklaviatuuri abil sisestatud andmeid, saate ennetada klaviatuuri abil veebisaitidele sisestatud andmete kinnipüüdmist. Klaviatuuri abil sisestatud andmete kaitse sisselülitamiseks tuleb veebilehitsejas [aktiveerida Kaspersky Kaitse laiendus](#). Arvutiklaviatuuri abil sisestatud andmete kaitse saate seadistada mitmesugustel veebisaitidel. Pärast klaviatuurikaitse seadistamist kuvatakse selle välja kõrval, millele kursor on seatud, hüpikteade klaviatuurikaitse sisselülitamise kohta. Vaikimisi on klaviatuurikaitse sisse lülitatud kõigi veebisaidikategooriate jaoks, välja arvatud internetisuhtlus.

Andmesisestuskaitse piirangud

Andmesisestuskaitse on Kaspersky rakenduses järgmised piirangud.

- Klaviatuurikaitse ei tööta rakenduseliivakastides käitatavates veebilehitsejates.
- Klaviatuurikaitse ei saa kaitsta teie isiklike andmeid, kui selliste andmete sisestamist nõudev veebisait on häkitud, sest sel juhul saavad sissetungijad teabe kätte otse veebisaidilt. Klaviatuurikaitse töötab ainult järgmistes veebilehitsejates: Chromiumil põhinev Microsoft Edge, Mozilla Firefox, Mozilla Firefox ESR ja Google Chrome, kui Kaspersky kaitse laiendus on installitud ja sisse lülitatud.
- Kaitse töötab ainult järgmistele tingimustele vastavatel lehtedel.
 - Leht on klaviatuurikaitset nõudvate URL-aadresside loendis või lehtede kategoorias.
 - Leht on avatud kaitstud veebilehitsejas.
 - Leht ei ole URL-i erandite loendis.

- Lehel on paroolisestusväli; rakenduse seadetes peaks märkeruut **Parooli sisestamise väljad kõigil veebisaitidel** olema märgitud.
- Kontrollimaks, kas see ruut on märgitud, valige jaotises **Privaatsusseaded** esmalt **Andmesisestuskaitse** ja seejärel **Klaviatuurikaitse**.
- Kaitse töötab ainult järgmistele tingimustele vastavatel väljadel.
 - Sisestusväli on üherealine ja vastab HTML-sildile <input>.
 - Sisestusväli ei ole peidetud: tüübiatribuudi väärtus pole „hidden“ ja CSS-i laadilehel pole välja kuvamise väärtuseks määratud „none“.
 - Sisestusvälja tüüp ei ole edastamisnupp, raadionupp, märkeruut, käsunupp ega pilt.
 - Sisestusväli ei tohi olla kirjutuskaitstud (readOnly).
 - Sisestusväli peaks olema sisestamiseks valmis (saama endale fookuse).
 - Kui väljal on maksimumpikkuse atribuut (maxlength), peaks sisestatavate märkide arvu alampiir olema suurem kui kolm.
- Kaitse ei tööta järgmistes olukordades.
 - Andmete sisestamiseks kasutatakse IME-tehnoloogiat.
 - Sisestusväli pole paroolisestusväli.


Kui olete Kaspersky rakenduse installinud, ent ei ole veel arvutit pärast seda veel taaskäivitanud, ei püüa rakendus kinni esimest kasutaja sisestatud märki (ükskõik millises rakenduses).

Kui teil tekib probleeme, [saatke päring](#) koos probleemi üksikasjaliku kirjeldusega My Kaspersky kaudu Kaspersky tehnilise toe meeskonnale.

My Kasperskyga töötamise juhised leiate jaotisest [Abi](#).

Arvuti klaviatuuri abil sisestatud andmete kaitse seadistamine

Arvuti klaviatuuri abil sisestatud andmete kaitse seadistamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Avage jaotis **Privaatsusseaded**.
4. Klõpsake **Andmesisestuskaitse**.
Avatakse aken **Andmesisestuskaitse seaded**.
5. Märkige akna allserva jaotises **Klaviatuurikaitse** ruut **Lülita Klaviatuurikaitse sisse**.
6. Märkige nende veebisaidikategooriate ruudud, millel soovite kaitsta klaviatuuri abil sisestatud andmeid.

7. Kui soovite lubada või keelata klaviatuuri abil sisestatud andmete kaitse kindlal veebisaidil, tehke järgmist.

- a. Akna **Ekraaniklaviatuuri erandid** avamiseks klõpsake linki **Halda erandeid**.
- b. Klõpsake aknas nuppu **Lisa**.
- c. Avaneb klaviatuurikaitse erandi lisamise aken.
- d. Sisestage avanenud aknas väljale **Veebiaadressi mask** veebisaidi aadress.
- e. Valige veebisaidi jaoks üks andmesisestuskaitse valikutest (**Rakenda määratud lehele** või **Rakenda tervele veebisaidile**).
- f. Valige toiming, mis tuleb andmesisestuskaitsele sellel veebisaidil teha (**Kaitse** või **Ära kaitse**).
- g. Klõpsake **OK**.

Määratud veebisait kuvatakse akna **Ekraaniklaviatuuri erandid** loendis. Selle veebisaidi avamise korral on andmesisestuskaitse aktiivne ja töötab vastavalt seadetele.


Veebisaidi ohutuse kontrollimine

Kaspersky rakendus võimaldab kontrollida veebisaidi turvalisust enne, kui klõpsate selle avamiseks linki. Veebisait kontrollitakse *URL-i nõustaja* komponendiga.

URL-i nõustaja komponent kontrollib linke Chromiumi-põhises Microsoft Edge'is, Google Chrome'is või Mozilla Firefoxis avatud veebilehel. Kaspersky rakendus kuvab kontrollitud lingi kõrval ühte järgmistest ikoonidest.

 – kui lingitud veebileht on Kaspersky andmetel turvaline

 – kui teave lingitud veebilehe ohutuse kohta puudub


 – kui Kaspersky andmetel saavad hakerid teie arvutit või andmeid kahjustada, kasutades veebilehte, millele link viib

 – kui Kaspersky andmetel võib veebileht, millele link viib, olla nakatunud või häkitud

 – kui lingitud veebileht on Kaspersky andmetel ohtlik
Lingi kohta üksikasju sisaldava hüpikakna kuvamiseks viige hiirekursor vastavale ikoonile.

Vaikimisi kontrollib Kaspersky rakendus linke ainult otsingutulemites. URL-i kontrolli saate sisse lülitada igal veebisaidil.

Veebisaitidel URL-i kontrollimise konfigureerimiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Turvaseaded**.

4. Klõpsake **Turvaline sirvimine**.

Avatakse aken **Turvalise sirvimise seaded**.

5. Lingi **Täpsemad seaded** klõpsamisel avanevad Turvalise sirvimise täpsemad seaded.

6. Märkige plokis **URL-i nõustaja** ruut **Kontrolli URL-e**.

7. Kui soovite, et Kaspersky rakendus kontrolliks kõigi veebisaitide sisu, valige **Kõigil veebisaitidel peale määratute**.

8. Vajaduse korral määrake aknas **Erandid** usaldatud veebisaidid. Selle akna avamiseks klõpsake linki **Halda erandeid**. Kaspersky rakendus ei kontrolli kindlaksmääratud veebilehtede sisu.

9. Kui soovite, et Kaspersky rakendus kontrolliks ainult kindlate veebilehtede sisu, tehke järgmist.

a. Valige **Ainult määratud veebisaitidel**.

b. Akna **Konfigureeri kontrollitavad veebisaidid** avamiseks klõpsake linki **Kontrollitud veebisaidid**.

c. Klõpsake **Lisa**.

d. Sisestage selle veebilehe aadress, mille sisu soovite kontrollida.

e. Valige veebilehe kontrollimisolek (kui see on *Aktiivne*, kontrollib Kaspersky rakendus veebilehe sisu).

f. Klõpsake **OK**.

Määratud veebileht kuvatakse akna **Kontrollitud veebisaidid** loendis. Kaspersky rakendus kontrollib sellel veebilehel olevaid URL-aadresse.

10. URL-i kontrollimise täpsemate seadete muutmiseks klõpsake akna **Turvalise sirvimise täpsemad seaded** jaotises **URL-i nõustaja** linki **Konfigureeri URL-i nõustaja**, et avada aken **Kontrollitavad URL-id**.

11. Kui soovite, et Kaspersky rakendus teavitaks teid linkide ohutusest kõigil veebilehtedel, tehke jaotises **Kontrollitavad URL-id** valik **Kõik URL-id**.

12. Kui soovite, et Kaspersky rakendus kuvaks teabe selle kohta, kas link kuulub teatud veebisaidisisu-kategooriasse (näiteks *Ebasündsused, roppused*), tehke järgmist.

a. Märkige ruut **Näita informatsiooni veebisaitide sisu kategooriate kohta**.

b. Märkige ruudud nende veebisaidisisu kategooriate kõrval, mille kohta tuleb kommentaarides kuvada teave.

Kaspersky rakendus kontrollib kindlaksmääratud veebilehtedel linke ja kuvab teavet linkide kategooriate kohta vastavalt valitud seadetele.

Krüptitud ühenduste seadete muutmine

Krüptitud ühendused luuakse SSL- ja TLS-protokollide kaudu. Vaikimisi kontrollib Kaspersky rakendus selliseid ühendusi siis, kui kaitsekomponendid (nt Meilide kaitse, Rämpsemailfilter, Turvalised maksed, URL-i nõustaja, Privaatne sirvimine, Turvaline sirvimine ja Ribareklaamifilter) seda taotleavad.

Krüptitud ühenduste seadete muutmiseks tehke järgmist.

1. Avage rakenduse peaaken.

2. Klõpsake põhiakna allservas nuppu .

Avatakse aken **Seaded**.

3. Avage jaotis **Turvaseaded**.

4. Klõpsake jaotises **Täpsemad seaded** nuppu **Võrgu seaded**.

5. Minge aknas **Võrgu seaded** jaotisse **Krüpteeritud ühenduste kontroll**.

6. Valige toiming, mis tuleb teha, kui loote veebisaitidega krüptitud ühenduse.

- **Ära kontrolli krüpteeritud ühendusi.** Kaspersky rakendus ei kontrolli krüptitud ühendusi.
- **Kontrolli krüpteeritud ühendusi, kui seda nõuab kaitsekomponent.** Kaspersky rakendus kontrollib krüptitud ühendusi ainult URL-i nõustaja nõudmisel. Vaikimisi on valitud see toiming.
- **Kontrolli alati krüpteeritud ühendusi.** Kaspersky rakendus kontrollib krüptitud ühendusi alati.

Kui klõpsate linki **Kuva sertifikaadid**, avaneb aken populaarsete veebisaitide kasutatavate usaldusväärsete sertifikaatide loendiga. Sertifikaadid lisatakse sellesse loendisse, kui klõpsate veebisaidi külastamisel Kaspersky hoiatuses nuppu **Lisa usaldusväärsete sertifikaatide hulka ja jätk**. Pärast sertifikaadi loendisse lisamist loetakse veebisait usaldusväärseks. Sertifikaate saate lisada või eemaldada aknas **Usaldusväärsed juursertifikaadid**, kasutades nuppe **Lisa** ja **Kustuta**.

Kui teie arvutis on mitu kasutajakontot ja üks kasutajatest aktsepteerib uue sertifikaadi, lisatakse see sertifikaat ka kõigi teiste kasutajate usaldusväärsete sertifikaatide loendisse.

7. Valige toiming, mis tuleb teha, kui krüptitud ühenduste kontrollimisel ilmneb tõrkeid.

- **Ignoreeri.** Selle toimingu valimise korral katkestab Kaspersky rakendus ühenduse veebisaidiga, mille kontrollitõrge ilmnes.
- **Küsi.** Kui veebisaidiga loodud krüptitud ühenduse kontrollimisel ilmneb tõrge, kuvab Kaspersky rakendus teate, kust saate valida soovitud toimingu.
 - **Ignoreeri.** Kaspersky rakendus katkestab ühenduse veebisaidiga, millel kontrollitõrge ilmnes.
 - **Lisa domeen eranditesse.** Kaspersky rakendus lisab veebisaidi aadressi usaldusväärsete aadresside loendisse. Kaspersky rakendus ei kontrolli usaldusväärsete aadresside loendisse lisatud veebisaitide krüptitud ühendusi. Nende veebisaitide vaatamiseks klõpsake linki **Usaldusväärsed aadressid**.

Vaikimisi on tehtud see valik.

- **Lisa domeen eranditesse.** Kaspersky rakendus lisab veebisaidi usaldusväärsete aadresside loendisse. Kaspersky rakendus ei kontrolli usaldusväärsete aadresside loendisse lisatud veebisaitide krüptitud ühendusi. Need veebisaidid kuvatakse aknas **Usaldusväärsed aadressid**, mille avamiseks saab klõpsata linki **Usaldusväärsed aadressid**.

8. Klõpsake linki **Usaldusväärsed aadressid**, et avada aken **Usaldusväärsed aadressid**, ja tehke järgmised toimingud.

- a. Krüptitud ühenduste kontrolli erandite loendisse veebisaidi lisamiseks klõpsake nuppu **Lisa**.
- b. Sisestage väljale **Domeeninimi** veebisaidi domeeninimi.
- c. Klõpsake **Lisa**.

Kaspersky rakendus ei kontrolli selle veebisaidiga loodud krüptitud ühendusi. Võtke arvesse, et kui lisate veebisaidi usaldusväärsete aadresside loendisse, võib see veebisaidil piirata kaitsekomponentide (nt Turvalised maksed, URL-i nõustaja, Privaatne sirvimine, Ohutu sirvimine ja Ribareklaamifilter) kontrollifunktsioone.

Teave Wi-Fi-võrkudega turvalise ühenduse loomise kohta

Saadaval ainult plaanides Kaspersky Plus ja Kaspersky Premium.

Avalikud Wi-Fi-võrgud võivad olla alakaitstud, näiteks kui Wi-Fi-võrk kasutab haavatavat krüptimisprotokolli või nõrka parooli. Internetiostude tegemisel ebaturvalistes Wi-Fi-võrkudes edastatakse teie paroolid ja muud konfidentsiaalsed andmed krüptimata tekstina. Håkkerid saavad teie konfidentsiaalseid andmeid, näiteks teie pangakaardi numbrit, kinni pda ja saada juurdepåsu teie rahale.

Oma turvalisuse tagamiseks ebaturvaliste Wi-Fi-võrkude kasutamisel saate VPN-i lubada spetsiaalse eriserveri kaudu, mis asub teie mratud piirkonnas. Veebisaidi liiklus suunatakse esmalt eriserverisse ja alles seejrel saadetakse krptitud turvalise henduse kaudu teie seadmesse.

Kaspersky VPN-i komponendi kasutamiseks peate [kivitama Kaspersky VPN-i](#). Kaspersky VPN Secure Connection on installitud koos Kaspersky rakendusega pakettis Kaspersky Plus.

Kaspersky VPN-i komponent pakub jrgmisi eeliseid.

- Maksessteemide ja broneerimissaitide turvaline kasutamine. Veebimaksete tegemisel, hotellitubade broneerimisel vi autode rimisel ei saa hkkerid veebisaidil teie pangakaardi numbrit kinni pda.
- Teie salajase teabe kaitsmine. Keegi ei saa teie arvuti IP-aadressi ega teie asukohta kindlaks teha.
- Teie privaatsuse kaitse. Keegi ei saa suhtlusvrkudes teie erakirjavahetust kinni pda ja lugeda.

VPN-hendust saab kasutada ka muud tpi vrguhenduste jaoks, niteks kohaliku internetihenduse vi USB-modemi henduse jaoks.

Vaikimisi ei palu Kaspersky VPN Secure Connection teil VPN-i lubada, kui veebisaidiga henduse loomiseks kasutatakse HTTPS-protokolli.

Kui muudate pankade, maksessteemide, broneerimise, suhtlusvrkude, vestluste vi meiliteenuste veebisaitide klastamisel oma piirkonda vi linna, vivad aktiveeruda pettusevastased ssteemid (ssteemid, mis on ette nhtud veebis tehtavate rahatehingute analsimiseks pettuse mrkide suhtes).


VPN-henduse kasutamist vivad reguleerida kohalikud õigusaktid. Te vite VPN-hendust kasutada ainult ettenhtud otstarbel ja kohalikke õigusakte rikkumata.

Wi-Fi-vrkude haavatavuste kohta teadete seadistamine

Kui Kaspersky VPN Secure Connection ei ole teie arvutisse installitud, kuvab Kaspersky rakendus teate Wi-Fi-vrguga hendumise ja teie parooli ebaturvalise edastamise kohta internetis. Saate lubada vi blokeerida henduse ja paroolide edastamise teavituskna.

Pärast Kaspersky VPN Secure Connectioni paigaldamist muutuvad Wi-Fi-võrkudega ühenduse loomisel ja paroolide krüptimata kujul edastamise teadete kuvamise seaded mitteaktiivseteks. Wi-Fi-võrgu ühenduste teavituste seadeid saate konfigureerida jaotises [Kaspersky VPN Secure Connection](#).

Wi-Fi-võrkude haavatavuste kohta kuvatavate teadete seadistamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotis **Turvaseaded**.
4. Valige komponent **Tulemüür**.
Aknas kuvatakse tulemüüri komponendi seaded.
5. Märkige ruut **Teata haavatavustest Wi-Fi-võrkudes**, kui soovite haavatavate Wi-Fi-võrkudega ühenduse loomise korral saada teateid. Kui te teateid ei soovi, eemaldage ruudust märg. Sellele märkeruudule pääseb juurde juhul, kui arvutisse ei ole paigaldatud Kaspersky VPN Secure Connectionit.
6. Klõpsake linki **Vali kategooriad** ja valige Wi-Fi-võrgu haavatavuste kategooriad. Kui proovite luua ühenduse asjakohase haavatavusega Wi-Fi-võrguga, teavitab Kaspersky rakendus teid sellest.
7. Ruudu **Teata haavatavustest Wi-Fi-võrkudes** märkimise korral saate teadete kuvamise täpsemaid seadeid muuta.
 - Märkige ruut **Blokeeri paroolide ebaturvaline edastus internetis ja kuva hoiatus**, kui soovite internetis väljade **Parool** täitmisel paroolide krüptimata tekstivormingus edastamise blokeerida.
 - Kui klõpsate linki **Lülita sisse**, taastatakse paroolide krüptimata kujul edastamise teadete kuvamise seadete vaikeväärtused. Kui olete krüptimata kujul paroolide edastamise kohta teadete kuvamise varem blokeerinud, jätkatakse nüüd nende teadete kuvamist.

Kaitstud Wi-Fi-võrkudega ühenduse loomise korral kuvab rakendus teate, mis küsib, kas usaldate uut võrku. Saate teha ühe järgmistest valikutest.

- **Ei, keela väline juurdepääs arvutile.** Kõik selle võrgu välised ühendused peale teie seadmest algatatud ühenduste blokeeritakse. Internetti saate edasi kasutada. Samuti saate külastada kõiki veebisaitide. Teised selles võrgus asuvad kasutajad ei saa teie arvutis leiduvate ressurssidega ühendust (nt ei pääse nad juurde teie ketaste sisule, sh ühiskaustadele).
- **Piira, kuid võimalda jagatud juurdepääs.** Internetti saate edasi kasutada. Samuti saate külastada kõiki veebisaitide. Teised selles võrgus asuvad kasutajad ei saa juurdepääsu teie arvutis leiduvatele ressurssidele, välja arvatud neile, mis on antud ühiskasutusse (nt ühiskaustad).
- **Jah, luba kogu võrgutegevus.** Lubatakse kõik ühendused selles võrgus. Internetti saate edasi kasutada. Samuti saate külastada kõiki veebisaitide. Teised selles võrgus asuvad kasutajad saavad teie arvutiga ühenduse luua ilma piiranguteta (nt pääsevad nad juurde teie ketaste sisule).

Identiteet

Kaspersky Premium sisaldab tööriistu teie digitaalse identiteedi kaitsmiseks ja spetsiaalset kanalit tehnilise toega ühenduse võtmiseks.

Identiteeti kaitsev rahakott

Kui hoiate arvutis olulisi dokumente, näiteks fotoga isikutunnistuste koopiaid, valitsuse dokumente, lepinguid jms, soovitame lisada need dokumendid turvalisse rahakotti. Identiteeti kaitsev rahakott on krüpteeritud fail, millele juurdepääsuks on vaja sisestada põhiparool. See tagab teie isikuandmete turvalisuse, takistades kolmandate isikute juurdepääsu dokumentidele.

Põhiparoolist

Põhiparool on parool, mida Kaspersky rakendus kasutab teie rahakotis hoitavate andmete krüpteerimiseks. Soovitame kasutada põhiparooli, mis on vähemalt kaheksa märgi pikkune ja sisaldab nii suurtähti, väiketähti, numbreid kui ka erimärke.

Turvalisuse huvides ei salvesta Kaspersky rakendus põhiparooli teie seadmetesse ega saada seda pilvsalvestusruumi. Soovitame põhiparooli kas meelde jätta või üles kirjutada ja hoida seda turvalises kohas, sest unustatud parooli ei ole võimalik taastada.

Teave krüpteerimise kohta

Kaspersky rakendus krüpteerib andmed sümmeetrilise krüpteerimisalgoritmi abil, mis põhineb täiustatud krüpteerimisstandardil (AES). Võti arvutatakse teie põhiparoolist paroolipõhise võtmetuletusfunktsiooni 2 (PBKDF2) põhjal. AES-algoritmi kasutatakse laialdaselt kogu maailmas salajaste andmete kaitsmiseks. See algoritm nõuab minimaalselt muutmälu, nii et teie andmed saab krüpteerida ja dekrüpteerida mõne sekundiga.

[Dokumendi lisamine rahakotti](#) 

1. Avage rakenduse peaaaken.

2. Avage jaotis **Identiteet**.

3. Jaotises **Identiteeti kaitsev rahakott** tehke järgmist.

- Kui rahakotti ei ole veel ühendatud, klõpsake nuppu **Allalaadimine**, et laadida alla rakendus Kaspersky Password Manager, kui see pole veel installitud. Nupu nimi võib olla **Käivitus** või **Ava**, kui Kaspersky Password Manager ei ole häälestatud, on aegunud või ühendatud My Kaspersky kontoga, mis ei vasta kontole, millega on ühendatud Kaspersky rakendus.

a. Kaspersky Password Manageri allalaadimiseks ja installimiseks järgige Paigaldusnõustaja juhiseid.

b. Kaspersky rakendus soovib rahakoti luua ja ühendada. Järgige nõustaja juhiseid. Rahakoti ühendamisel palutakse teil luua ka põhiparool.

- Kui olete rahakoti juba ühendanud, klõpsake nuppu **Lisa dokument**.


1. Klõpsake jaotises **Dokumendid** nuppu **Lisa dokument**.

2. Valige rippmenüüst:

- **Otsi faile**. Avaneb Exploreri aken. Sisestage väljale **Faili nimi** tee failini ja klõpsake nuppu **Ava**. Valige dokumendile kategooria (kiireks leidmiseks tulevikus) ja klõpsake nuppu **Lisa**.
- **Otsi automaatselt**. Rakendus otsib JPEG-, PNG-, BMP- ja PDF-faile, mis sisaldavad teksti. Leitud faile analüüsitakse ja liigitatakse need valitsuse väljastatud isikutunnistuste või pangakaartide alla. Valige dokumendid ja klõpsake nuppu **Lõpeta**.

Valitud dokumendid lisatakse rahakotti JPEG- või PDF-failidena.

[Dokumendi eraldamine rahakotist](#) 

1. Avage rakenduse peaaken.
2. Avage jaotis **Identiteet**.
3. Klõpsake jaotises **Identiteeti kaitsev rahakott** nuppu **Lisa dokument**.
4. Sisestage oma põhiparool.
5. Valige üks dokument või hoidke all klahvi Shift ja valige neil klõpsates mitu dokumenti.
6. Dokumentide allalaadimiseks on järgmised võimalused.
 - Tehke dokumendi kontekstimenüü avamiseks paremklõps ja valige **Laadi alla**.
 - Klõpsake nuppu  ja valige avanenud menüüst **Laadi alla**.
7. Valige aknas **Salvesta kausta** koht, kuhu soovite dokumendi salvestada.
8. Vajaduse korral saate dokumendi nime muuta.
9. Klõpsake nuppu **Salvesta**.

Dokument salvestatakse teie seadmesse. Allalaaditud failid on samas vormingus kui vastavad rahakotis olevad dokumendid (JPEG või PDF).

Kaugjuurdepääsu tuvastamine

Kaugjuurdepääsurakendused on seaduslik tarkvara, mille abil saab luua kaugarvutiga võrgu kaudu ühenduse. Kaugjuurdepääsurakenduste hulka kuuluvad TeamViewer, LogMeIn Pro ja Remotely Anywhere. Häkkerid võivad selliseid rakendusi kasutada selleks, et saada teie arvuti üle kontrolli, installida pahavara, esineda teiena või luurata teie järel.

Me kontrollime, kas teie arvutisse on installitud kaugjuurdepääsurakendusi, ja aitame need eemaldada, et keegi ei saaks teie seadme üle kontrolli.

Kaugjuurdepääsurakenduste leidmiseks oma arvutist tehke järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Identiteet**.
3. Klõpsake jaotises **Kaugjuurdepääsu tuvastamine** nuppu **Kuva**.
4. Avaneb aken **Kaugjuurdepääsu tuvastamine**, kus näete, millised kaugjuurdepääsurakendused teie arvutist leiti. Selles aknas saate teha järgmist.
 - Kaugjuurdepääsurakenduse lühikirjelduse nägemiseks klõpsake rakenduse kõrval olevat nuppu **Üksikasjad**.
 - Kui soovite rakenduse eemaldada, valige rakenduse kõrval olevast ripploendist **Eemalda**. See viib teid aknasse **Programmid ja funktsioonid**, kus saate vastava rakenduse eemaldada.

- Kui te ei soovi rakendust hetkel eemaldada, valige rakenduse kõrval olevast ripploendist **Ignoreeri**. Rakendus lisatakse gruppi **Peidetud** ja te saate hiljem selle juurde tagasi pöörduda.

Kaugjuurdepääsurakenduste otsing ei tööta, kui komponent Sissetungitõrje on välja lülitatud.

Tippklassi tugiteenused

Kaspersky Premiumi tugiteenused telefoni teel pole mõnes piirkonnas saadaval. Premium-tugiteenuseid saab kasutada ainult tasulise tellimuse olemasolul.

Premium-tugi pakub täiendavat kaitset ja mugavust, nagu eelisjuurdepääs, ekspertpaigaldusteenused, viiruste otsimine ja eemaldamine ning arvuti seisundi kontroll.

Ekspertpaigaldusteenused

Kui teie arvutis tekib installimisel probleem, võite meile helistada ja Kaspersky ekspert teeb kaugjuurdepääsu teel järgmist:

- käivitab kaugühenduse kaudu installimise;
- kontrollib, et installimine kulgeks vigadeta;
- annab ülevaate rakenduse seadetest ja funktsioonidest;
- vastab kõigile teie küsimustele rakenduse ja installimisprotsessi kohta;
- kohandab rakenduse seaded teie vajadustele vastavaks;
- kinnitab, et rakendus on installitud, õigesti häälestatud ja töötab korrektselt.

Prioriteetne tugiliin

Eelisjuurdepääs Premium-toe agendile telefoni või vestluse teel. Nende klientide telefonikõned võetakse esimesena ette (liiguvad järjekorra etteotsa). Pakutav vestluseprogramm sisaldab kaugabi võimalusi.

IT kaugabi

Ühe klõpsuga juurdepääs vestlusele Premium-toe agendiga, mis sisaldab piiramatut kaugabi. Istuge ja lõõgastuge, kuni me kõik korda teeme!

Viiruste otsimine ja eemaldamine ekspertide poolt

Viiruste ja nuhkvara professionaalne eemaldamine mis tahes Windowsi seadmest, kuhu on installitud Kaspersky rakendus.

Arvuti seisundi kontrollimise teenused

Seisundikontrolli käigus teevad meie eksperdid mitmepunktilise ülevaatus, et teie seade oleks kõrgeimal kaitse- ja jõudlustasemel.

Kaspersky Premiumi tugiteenuste kasutamiseks helistage selle riigi telefoninumbri, kus te Kaspersky Premiumi tellimuse ostsite.

Ühildumatute rakenduste eemaldamine

Kaspersky rakendus kontrollib regulaarselt, kas teie arvutis on [ühildumatuid rakendusi](#). Sellised rakendused lisatakse ühildumatute rakenduste loendisse. Saate loendi läbi vaadata ja otsustada, mida ühildumatute rakendustega teha.

Soovitatav on ühildumatud rakendused arvutist kustutada. Vastasel juhul ei saa Kaspersky rakendus teie arvutit täielikult kaitsta.

Allpool on mõned põhjused, mille tõttu kolmanda osapoole rakendus ei pruugi Kaspersky rakendusega ühilduda.

- Failide kaitse ja rakenduse konflikt.
- Tule müüri ja rakenduse konflikt.
- Rämpseilifiltri ja rakenduse konflikt.
- Rakendus häirib võrguliikluse kaitset.
- Salahoidla ja rakenduse konflikt.
- Kaspersky Password Manageri ja rakenduse konflikt.

[Ühildumatute rakenduste eemaldamine](#)

Ühildumatute rakenduste eemaldamiseks:

1. Avage rakenduse peaaken.
2. Klõpsake akna ülaserivas nuppu **Üksikasjad**.
Avatakse aken **Teatiste keskus**.
3. Klõpsake jaotises **Soovitused** tuvastatud ühildumatute rakenduste teate real nuppu **Näita**.
Avaneb aken **Leiti ühildumatu tarkvara**, mis sisaldab tuvastatud ühildumatute rakenduste loendit.
4. Märkige ruudud nende ühildumatute rakenduste nimede kõrval, mille soovite eemaldada, ja klõpsake nuppu **Eemalda**. Eemaldamine toimub nende rakenduste pakutavate eemaldamistööriistade abil. Eemaldamise käigus võidakse rakenduse eemaldamisega seotud seadete eemaldamise või muutmise kohta küsida teie nõusolekut.
5. Kui arvutis on ikka veel ühildumatuid rakendusi, mida ei saa automaatselt eemaldada, kuvatakse aken selliste rakenduste loendiga. Ühildumatute rakenduste käsitsi eemaldamiseks klõpsake nuppu **Eemalda käsitsi**. See avab operatsioonisüsteemi tavaakna, mis sisaldab paigaldatud rakenduste loendit. Eemaldage ühildumatud rakendused operatsioonisüsteemi juhiste järgi.
6. Pärast ühildumatute rakenduste eemaldamist taaskäivitage arvuti.

Rakenduse kasutamine käsuviiba abil

Kaspersky rakendusega saate töötada käsurea kaudu.

Käsuviiba süntaks on järgmine:

```
avp.com <käsk> [seaded]
```

Käsuviibasüntaksi spikri kuvamiseks sisestage järgmine käsk:

```
avp.com [ /? | HELP ]
```

Selle käsuga saate tuua täieliku loendi käskudest, mis on Kaspersky rakenduse käsurea kaudu haldamiseks saadaval.

Kindla käsu süntaksi spikri kuvamiseks saate sisestada ühe järgmistest käskudest:

```
avp.com <käsk> /?  
avp.com HELP <käsk>
```

Käsuviibal saate rakendusele viidata kas rakenduse paigalduskausta järgi või üksuse avp.com täieliku tee abil.

Rakenduse sündmuste logimise (jäljefailide loomise) saate käsuviiba abil sisse või välja lülitada, kui olete varem rakenduse seadete aknas Kaspersky rakenduse haldamisele juurdepääsu kaitsmiseks [määranud parooli](#).

Kui te pole rakenduse seadete aknas parooli seadnud, ei saa te käsuviiba abil parooli luua ja sündmuste logimist sisse lülitada.

Teatud käske saab käivitada ainult administraatori kontol.

Tehnilise toega ühenduse võtmine

Selles jaotises kirjeldatakse tehnilise toe saamise viise ja tingimusi.

Tehnilise toe saamine

Kui te ei leia probleemile lahendust rakenduse dokumentatsioonist või [mõnest muust rakenduse kohta käivast teabeallikast](#), soovime pöörduda tehnilise toe poole. Külstage [tehnilise toe veebisaiti](#) ja võtke ühendust meie asjatundjatega, kes oskavad vastata teie küsimustele rakenduse installimise ja kasutamise kohta.

Enne tehnilise toega ühenduse võtmist lugege läbi [toe eeskiri](#).

Tehnilist tuge osutatakse ainult kasutajatele, kes on ostnud rakenduse kasutustellimuse. Tasuta versioonide kasutajatele pole tehniline tugi saadaval.

Tehnilise toe jaoks teabe kogumine

Kui olete tehnilise toe spetsialistidele teatanud probleemist, võivad nad paluda teil luua ja tehnilisele toele saate aruande, mis sisaldab teavet teie operatsioonisüsteemi kohta. Samuti võivad tehnilise toe spetsialistid paluda teil luua jäljefaili. Jäljefail võimaldab etapiviisiliselt jälgida rakenduse käskude täitmisprotsessi ja määrata kindlaks rakenduse tööetapi, kus tõrge ilmneb.

Rakenduse tööga seotud probleemide korral parema toe osutamiseks võivad tehnilise toe spetsialistid silumise eesmärgil paluda teil diagnostika ajal ajutiselt muuta rakenduse seadeid. Selleks võib teil olla vaja teha järgmised toimingud.

- Laiendatud diagnostikateabe kogumine
- Rakenduse üksikkomponentide seadistamiseks tavakasutajaliidese kaudu juurdepääsetamatute eriseadete muutmine
- Hoidla ümberseadistamine ja kogutud diagnostikateabe saatmine
- Võrguliikluse kinnipüüdmise seadistamine ja võrguliikluse salvestamine faili

Tehnilise toe spetsialistid annavad teile nende toimingute tegemiseks kogu vajaliku teabe (etapiviisilised juhendid, muudetavad seaded, skriptid, käsurea lisafunktsioonid, silumismoodulid, eriutiliidid jne) ja teavitavad teid silumise eesmärgil kogutavatest andmetest. Pärast laiendatud diagnostikateabe kogumist salvestatakse see kasutaja arvutisse. Kogutud andmeid ei saadeta automaatselt Kasperskyle.

Eelnimetatud toimingud on soovitatav teha ainult tehnilise toe spetsialisti järelevalve all pärast sellekohaste juhiste saamist. Ise rakenduse seadete muutmine viisil, mida pole kirjeldatud abimaterjalides või mida ei ole soovitanud tehnilise toe spetsialistida, võib põhjustada operatsioonisüsteemi aeglustumist ja krahhe, vähendada teie arvuti kaitsetaset ning kahjustada töödeldava teabe kättesaadavust ja terviklust.

Teave teenuse andmefailide sisu ja talletamise kohta

Jälje- ja tömmisefaile talletatakse arvutis krüptimata kujul seitse päeva pärast andmete logimise väljalülitamist. Pärast seitsme päeva möödumist kustutatakse jäljefailid ja tömmisefailid jäädavalt.

Jäljefaile talletatakse kaustas ProgramData\Kaspersky Lab.

Jäljefailide nimevorming on järgmine: KAV<versiooni number_kuupäevXX.XX_kellaaegXX.XX_pidXXX.><jäljefaili tüüp>.log.


Jäljefailid võivad sisaldada konfidentsiaalseid andmeid. Jäljefaili sisu vaatamiseks avage see tekstiredaktoris (näiteks Notepad).

Jõudluse jäljefaile saab vaadata Windowsi jõudlusanalüsaatori utiliidi abil. Selle utiliidi saate alla laadida Microsofti veebisaidilt.

Jälgimise sisselülitamine

Seadistage jäljejälitus ainult Kaspersky tehnilise toe eksperdilt vastavate juhiste saamise korral.

Rakenduste ja jõudluse jälgimise lubamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake akna allservas nuppu .
Avatakse aken **Kasutajatugi**.
3. Akna **Kasutajatoe tööriistad** avamiseks klõpsake linki **Kasutajatoe tööriistad**.
4. Lubage ja seadistage rakenduste ja jõudluse jäljejälitus Kaspersky tehnilise toe eksperdi juhiste järgi.
5. Muudatuste salvestamiseks klõpsake nuppu **Salvesta**.

Piirangud ja hoiatused

Kaspersky rakendusel on mõningaid mittekriitilisi tegevuspiiranguid.

Teatud komponentide tööga ja failide automaatse töötlemisega seotud piirangud

Nakatunud faile ja pahatahtlikke linke töödeldakse automaatselt kooskõlas Kaspersky spetsialistide loodud reeglitega. Neid reegleid ei saa käsitsi muuta. Reegleid võidakse uuendada pärast andmebaaside ja rakendusemoodulite uuendust. Samuti uuendatakse automaatselt tulemüüri, veebikaamera kaitse, rakendushalduri ja sissetungitõrje reegleid.

Kui seadmekontroll käivitatakse My Kasperskyst, töödeldakse faile automaatselt rakenduses määratud reeglite alusel. Seadmes tuvastatud faile saab My Kaspersky taotluse alusel automaatselt töödelda ilma teie kinnitusetä.

Kaspersky Security Networkiga loodud ühenduse piirangud

Töö ajal võib rakendus esitada teabepäringuid Kaspersky Security Networki. Kui Kaspersky Security Networkist andmete hankimine nurjub, teeb rakendus otsused kohalike viirusekaitse andmebaaside põhjal.

Süsteemiseire funktsioonide piirangud

Krüptorite (kasutaja faile krüpteeriva pahavara) vastasel kaitsel on järgmised piirangud.

- Selle funktsiooni käitamiseks kasutatakse süsteemikausta Temp (Ajutised failid). Kui kausta Temp sisaldaval süsteemidraivil pole ajutiste failide loomiseks piisavalt kettaruumi, siis krüptorivastast kaitset ei pakuta. Sellisel juhul ei kuvata rakenduses teadet, et faile pole varundatud (kaitset ei pakuta).
- Ajutised failid kustutatakse automaatselt, kui sulgete Kaspersky rakenduse või lülitate komponendi Süsteemiseire välja.
- Kaspersky rakenduse avariisulgemise korral ei kustutata ajutisi faile automaatselt. Ajutiste failide kustutamiseks tühjendage kaust Temp käsitsi. Selleks avage aken **Käivita** ja tippige väljale **Ava** väärtus %TEMP%. Klõpsake nuppu **OK**.
- Krüptorivastast kaitset pakutakse failidele, mis asuvad NTFS-vormingus andmedraividel.
- Taastatavate failide arv ei tohi krüptimisprotsessi kohta ületada 50 tk.
- Failide muudatuste kogumaht ei tohi ületada 100 MB. Seda limiiti ületavate muudatustega faile ei saa taastada.
- Võrguliidese kaudu algatatud failimuudatusi ei jälgita.
- EFS-iga krüptitud faile ei toetata.
- Krüptorivastase kaitse sisselülitamiseks tuleb pärast Kaspersky rakenduse installimist arvuti taaskäivitada.

Krüpteeritud ühenduste kontrolli piirangud

Kontrollimisalgoritmide rakendamise tehniliste piirangute tõttu ei toeta krüpteeritud ühenduste kontroll TLS 1.0 protokoll ja uuemate versioonide (eriti NPN-i ja ALPN-i) teatud laiendusi. Nende protokollide kaudu loodud ühendused võivad olla piiratud. SPDY-protokoll toetavad veebilehitsejad kasutavad SPDY asemel TLS-protokoll kaudu HTTP-d isegi juhul, kui server, millega ühendus luuakse, toetab SPDY-d. See ei mõjuta ühenduse turvataset. Kui server toetab ainult SPDY-protokoll ja ühendust ei saa luua HTTPS-protokoll kaudu, ei jälgi rakendus loodud ühendust.

Rakendus ei töötle HTTP/2-protokoll laienduste kaudu edastatud liiklust.

Kaspersky ei luba andmeid vahetada QUIC-protokoll kaudu. Brauserid kasutavad standardset transpordiprotokoll (TLS või SSL) hoolimata sellest, kas veebilehitsejas on QUIC-protokoll tugi sisse lülitatud või mitte.

Kaspersky jälgib ainult neid krüptitud ühendusi, mida on võimeline dekrüpteerima. Rakendus ei jälgi erandite loendis lisatud ühendusi (link **Veebisaidid** aknas **Võrgu seaded**).

Järgmised komponendid dekrüpteerivad ja kontrollivad krüptitud liiklust automaatselt.

- Ohutu sirvimine
- Turvalised maksed
- URL-i nõustaja.

Kaspersky rakendus dekrüpteerib brauseri Google Chrome kasutamisel krüptitud liikluse, kui selles brauseris on laiend Kaspersky Kaitse välja lülitatud.

Kaspersky rakendus ei jälgi liiklust, kui brauser laadib veebilehe või selle elemendid interneti asemel kohalikust vahemälust.

Klientrakendusega The Bat krüptitud ühenduste kontrollimise piirangud

Kuna meiliklient The Bat kasutab oma sertifikaadisalve, loeb Kaspersky rakendus selle meilikiendi ja serveri vahel HTTPS-ühenduse loomiseks kasutatud sertifikaadi ebausaldusväärseks. Selle vältimiseks seadistage meiliklient The Bat töötama kohaliku Windowsi sertifikaadisalvega.

Krüptitud ühenduste kontrollimiserandite piirangud

Kui krüptitud ühenduste kontrollimiseranditesse on lisatud veebisait, võivad teatud komponendid, nagu ribareklaamifilter, URL-i nõustaja ja privaatne sirvimine, jätkata krüptitud ühenduste kontrollimist. Turvaliste maksete ja ohutu sirvimise komponendid ei kontrolli eranditesse lisatud veebisait.

Varundamise ja taastamise piirangud

Varundamisel ja taastamisel kehtivad järgmised piirangud.

- Kõvaketta või arvuti asendamise korral ei ole varukoopiate veebihoidla enam saadaval. Pärast riistvara asendamist veebihoidlaga ühenduse taastamise kohta teabe saamiseks külastage Kaspersky tehnilise toe veebisaiti.
- Varuhoidla teenusefailide muutmise korral võib katkeda juurdepääs varuhoidlale ja andmete taastamine ei pruugi enam võimalik olla.

- Kuna rakendus kasutab varundamiseks süsteemi varikooptimeenust, ei kaasata varunduskomplekti Outlooki võrguühendusest andmefaili (.ost), kuna see pole varundamiseks ette nähtud.

Salahoidla funktsioonide piirangud

Kui salahoidla luuakse FAT32 failisüsteemis, ei tohi salahoidlafaili maht kettal ületada 4 GB.

Kaitstud veebilehitseja režiimis tuumamälust juurkrattide otsimise erijooned

Kui kaitstud veebilehitseja režiimis tuvastatakse ebausaldusväärne moodul, avaneb veebilehitsejas uus vahekaart teatega pahavara avastamise kohta. Sel juhul soovitage veebilehitsejast väljuda ja käivitada arvuti täiskontrolli.

Lõikepuhvri andmekaitse erijooned

Kaspersky rakendus lubab rakendusel lõikepuhvri juurde pääseda järgmistel juhtudel.

- Aktiivse aknaga rakendus proovib lõikepuhvrisse andmeid lisada. Aktiivne aken on praegu kasutatav aken.
- Rakenduse usaldusväärne protsess proovib lõikepuhvrisse andmeid lisada.
- Rakenduse usaldusväärne protsess või aktiivse aknaga protsess proovib lõikepuhvrist andmeid tuua.
- Rakenduse protsess, mis on varem lõikepuhvrisse andmeid lisanud, proovib neid andmeid lõikepuhvrist tuua.

Rakenduse komponentide teostatava nakatunud failide töötlemise erijooned

Vaikimisi saab rakendus kustutada nakatunud failid, mida ei saa parandada. Vaikimisi eemaldamine võib toimuda, kui faile töötlevad kontrollitegumite käigus sellised komponendid nagu sissetungitõrje, meilide kaitse, failide kaitse või kui süsteemiseire avastab rakenduste pahatahtliku tegevuse.

Teatud komponentidele kohalduvad piirangud juhul, kui rakendus paigaldatakse koos Kaspersky Fraud Prevention for Endpointsiga

Kui rakendus installitakse koos Kaspersky Fraud Prevention for Endpointsiga, on järgmiste Kaspersky rakenduse komponentide töö kaitstud veebilehitsejas piiratud.

- Ohutu sirvimine, v.a andmepüügivastane kaitse
- URL-i nõustaja
- Ribareklaamifilter

Automaatkäivitusprotsessi töö erijooned

Automaatkäivitusprotsess logib oma töö tulemused. Andmed logitakse tekstifailides, mille nimi on kujul „kl-autorun-<kuupäev><kellaaeg>.log“. Andmete vaatamiseks avage aken **Käivita** ja tippige väljale **Ava** väärtus %TEMP% ning klõpsake nuppu **OK**.

Kõik jäljefailid salvestatakse automaatkäivitusprotsessi käigus alla laaditud seadistusfailide teele. Andmeid talletatakse automaatkäivitusprotsessi käitamise ajal ja pärast protsessi lõpetamist kustutatakse need jäädavalt. Andmeid ei saadeta mitte kuskile.

Kaspersky rakenduse piirangud juhul, kui operatsioonisüsteemis Microsoft Windows 10 RS4 on sisse lülitatud režiim Device Guard

Järgmiste funktsioonide töö on osaliselt piiratud.

- Lõikepuhvri kaitse
- Veebilehitseja kaitse klaviatuuri- ja hiiresisendi emulaatorite vastu (sisendi võltsimine)
- Kaitse kaughaldusrakenduste eest
- Veebilehitseja kaitse (haldamine API kaudu, kaitse veebilehitseja aknatele ohtlikke sõnumeid edastavate rünnakute eest, kaitse teatejärjestuse haldamise vastu)
- Heuristiline analüüs (pahatahtlike rakenduste käivitamise jäljendamine)

Kui Windowsis on sisse lülitatud UMCI-režiim, ei tuvasta Kaspersky rakendus ekraanilukustajaid.

Teave Windowsi sündmuselogisse lõppkasutaja litsentsilepinguga ja Kaspersky Security Networkis seotud sündmuste logimise kohta

Windowsi sündmuselogisse jäädvustatakse sündmused, mis on seotud lõppkasutaja litsentsilepingu tingimustega nõustumise ja neist keeldumisega ning samuti Kaspersky Security Networkis osalemisega nõustumise ja sellest keeldumisega.

Kaspersky Security Networkis kohalike aadresside reputatsioonikontrolli piirangud

Kaspersky Security Networkis ei kontrollita kohalike ressursside linke.

Hoiatus teavet koguvate rakenduste kohta

Kui teie arvutisse on installitud rakendus, mis kogub teavet ja saadab selle töötlemiseks edasi, võib Kaspersky rakendus liigitada selle rakenduse pahavaraks. Selle vältimiseks saate rakenduse kontrollist välja jätta, häälestades Kaspersky rakenduse käesolevas dokumendis antud juhiste järgi.

Hoiatus rakenduse paigaldusaruande loomise kohta

Paigaldusaruande fail luuakse arvutisse rakenduse paigaldamise korral. Kui rakenduse paigaldamine viiakse lõpuni tõrkega, salvestatakse paigaldusaruande fail ja te saate selle saata Kaspersky tehnilisele toele. Paigaldusaruande faili sisu vaatamiseks klõpsake rakendusaknas kuvatavat linki. Kui rakendus on edukalt paigaldatud, kustutatakse paigaldusaruande fail arvutist kohe.

Veebikaamerakontrolli piirangud Microsoft Windows 10 aastapäevavärskendusega (RedStone 1) operatsioonisüsteemis

Pärast rakenduse paigaldamist Microsoft Windows 10 aastapäevavärskendusega (RedStone 1) operatsioonisüsteemi ei ole veebikaamera juurdepääsukontroll tagatud enne arvuti taaskäivitamist.

Veebipõhise varundamise ja varukoopiatest andmete taastamise piirang

Samas arvutis ei saa korraga käivitada Kaspersky varundustegumit ja Kaspersky taastevahendi andmetaastetegumeid.

Tulemüüri piirangud

Tulemüür ei kontrolli kohalikke ühendusi, mille on paigaldanud kontrollitavad rakendused.

Sissetungitõrje komponendi piirangud

Kui teie arvutisse on installitud VeraCrypt, võib Kaspersky rakendus sulguda, kui töötab komponendiga Sissetungitõrje. Selle probleemi lahendamiseks täiendage VeraCrypt versiooniks 1.19 või uuemaks versiooniks.

Piirangud rakenduse esmakäivitamisel pärast Microsoft Windows 7 täiendamist väljalaskeks Microsoft Windows 10

Kui olete täiendanud Microsoft Windows 7 versiooniks Microsoft Windows 8 / 8.1 või Microsoft Windows 10 / RS1 / RS2 / RS3, töötab Kaspersky rakendus esimesel käivituskorral järgmiste piirangutega.

- Töötab ainult failide kaitse (reaalajas kaitse). Rakenduse muud komponendid ei tööta.
- Failide ja süsteemiregistri enesekaitse töötab. Protsesside enesekaitse ei tööta.
- Rakenduse kasutajaliides pole saadaval enne arvuti taaskäivitamist. Rakendus kuvab teate, et mõni rakenduse komponent ei tööta ja et pärast uue operatsioonisüsteemiga kohandamise lõppu tuleb arvuti taaskäivitada.
- Teavitusalal rakenduseikooni kontekstimenüüs on saadaval ainult valik **Välju**.
- Rakendus ei kuva teateid ja valib automaatselt soovitatud toimingut.

Hoiatus rakenduse draiverite kohandamistõrke kohta pärast Windows 7 täiendamist väljalaskeks Windows 10

Pärast Windows 7 täiendamist versiooniks Windows 10 võib Kaspersky rakenduse draiverite kohandamisel ilmned a tõrge. Kuna draivereid kohandatakse taustal, ei saa te selle toimingut edenemise kohta teateid.

Kui draiverite kohandamisel ilmnes tõrge, ei saa kasutada rakenduse järgmisi funktsioone.

- Tulemüür
- Ohutuvastus operatsioonisüsteemi laadimise ajal
- Rakendusprotsesside kaitse Microsoft Corporationi Protected Process Lighti (PPL-i) tehnoloogia abil

Tõrke parandamiseks saate kasutada järgmisi meetodeid.

- Taaskäivitage arvuti ja taaskäivitage teadete keskus kuvatavast teatest rakenduse kohandamine.
- Eemaldage rakendus ja paigaldage see uuesti.

Nutikodu monitori funktsioonide kasutuspiirangud

Etherneti võrgu seadete muutmisel süsteemiregistris võib komponent Nutikodu monitor kuvada Etherneti võrgu tuvastatud Wi-Fi-võrkude loendis ja kuvada selle võrguga ühendatud seadmed.

Piirangud Mozilla Firefox'i veebilehitsejas HTTPS-i kaudu edastatud liikluse kontrollimisel

Versioonis Mozilla Firefox 58.x ja uuemates versioonides ei kontrolli rakendus HTTPS-protokolli kaudu edastatud liiklust, kui veebilehitseja seadete muutmise on kaitstud esmase parooliga. Kui veebilehitsejas tuvastatakse esmane parool, kuvab rakendus teate, mis sisaldab teabebaasiartikli linki. Artikkel sisaldab probleemi lahendamise juhendit.

Kui HTTPS-liiklust ei jälgita, on piiratud järgmiste komponentide töö.

- Ohutu sirvimine
- Andmepüügivastane kaitse
- Vanemakontroll
- Privaatsuse kaitse
- Ribareklaamifilter
- Andmesisestuskaitse
- Turvalised maksed

Kaspersky Kaitse laienduse piirangud Google Chrome'is ja Mozilla Firefoxis

Kaspersky Kaitse laiendus ei tööta Google Chrome'is ja Mozilla Firefoxis, kui teie arvutisse on paigaldatud Windowsi jaoks ette nähtud Malwarebytes.

Erikaalutlused rakenduse paigaldamise korral Microsoft Windows 7 hoolduspaketiga 0 ja hoolduspaketiga 1 operatsioonisüsteemi

Kui rakendus paigaldatakse operatsioonisüsteemi, mis ei toeta SHA256 digiallkirjaga sertifikaate, paigaldab rakendus oma usaldusväärse sertifikaadi.

Teave Kaspersky rakenduste funktsionaalsuse automaatse testimise kohta

Ettevõtte Kaspersky Lab rakendused, sealhulgas Kaspersky rakendus, kasutavad rakendusefunktsioonide automaatseks kontrollimiseks spetsiaalset API-t (rakendusliidest). See API on ette nähtud kasutamiseks ainult Kaspersky arendajatele.

Muud teabeallikad rakenduse kohta

Kaspersky rakenduse teabebaasileht

Teabebaas on tehnilise toe veebisaidi jaotis.

[Kaspersky rakenduse teabebaasilehel](#) saate lugeda artikleid, mis sisaldavad kasulikku teavet, soovitusi ja vastuseid korduma kippuvatele küsimustele rakenduse ostmise, installimise ja kasutamise kohta.

Teabebaasiartiklitest võite leida vastused küsimustele, mis on seotud nii Kaspersky rakenduse kui ka muude Kaspersky rakendustega. Teabebaasi artiklid võivad sisaldada ka tehnilise toe uudiseid.

Kaspersky rakenduste tugi meie foorumis

Saate [meie foorumis](#) kasutajatelt ja Kaspersky ekspertidelt tuge.

Foorumis saate lugeda olemasolevaid teemasid, postitada kommentaare ning luua uusi arutelu- ja toeteemasid.

Väliteenuste ühenduse võrguseaded

Kaspersky rakendus kasutab infovahetuseks väliste teenustega järgmisi võrguseadeid.

Võrgu seaded

Aadress	Kirjeldus
activation- v2.kaspersky.com/activation-service/activation-service.svc Protokoll: HTTPS Port: 443	Rakenduse aktiveerimine
s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com s06.upd.kaspersky.com s07.upd.kaspersky.com s08.upd.kaspersky.com s09.upd.kaspersky.com s10.upd.kaspersky.com s11.upd.kaspersky.com s12.upd.kaspersky.com s13.upd.kaspersky.com s14.upd.kaspersky.com s15.upd.kaspersky.com s16.upd.kaspersky.com s17.upd.kaspersky.com s18.upd.kaspersky.com s19.upd.kaspersky.com cm.k.kaspersky-labs.com Protokoll: HTTPS Port: 443	Andmebaaside ja rakendustarkvara moodulite uuendamine.
downloads.upd.kaspersky.com Protokoll: HTTPS Port: 443	<ul style="list-style-type: none">• Andmebaaside ja rakendustarkvara moodulite uuendamine.• Kaspersky serveritele juurdepääsu kontrollimine. Kui juurdepääs serveritele, mis kasutavad süsteemi DNS-i, pole võimalik, kasutab rakendus avalikku DNS-i. See on vajalik viirusetõrje andmebaaside ajakohastamise

ja arvuti turvalisuse taseme tagamiseks. Kaspersky rakendus kasutab järgmise avalike DNS-serverite loendi servereid järgmises järjekorras.

1. Google'i avalik DNS (8.8.8.8).
2. Cloudflare DNS (1.1.1.1).
3. Alibaba Cloud DNS (223.6.6.6).
4. Quad9 DNS (9.9.9.9).
5. CleanBrowsing (185.228.168.168).

Kuna rakendus loob DNS-serveriga TCP/UDP-ühenduse, võivad rakenduse saadetud päringud sisaldada domeenide aadresse ja kasutaja avalikku IP-aadressi. Seda teavet on vaja näiteks veebiressursi serdi valideerimiseks HTTPS-i kasutamisel. Kui Kaspersky rakendus kasutab avalikku DNS-serverit, reguleerib andmetöötlust vastava teenuse privaatsuspoliitika. Kui soovite takistada Kaspersky rakendusel avaliku DNS-serveri kasutamist, võtke privaatse paiga saamiseks ühendust tehnilise toega.

touch.kaspersky.com

Protokoll: HTTP

- Serdi kehtivusperioodi (TLS-ühendus) kontrollimiseks usaldusväärse kellaaja vastuvõtmine.
- Hoiatus, et juurdepääs veebiressursile on brauseris keelatud, kui ohutu sirvimine on lubatud.

p00.upd.kaspersky.com

Andmebaaside ja

<p>p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com</p> <p>Protokoll: HTTP Port: 80</p>	<p>rakendustarkvara moodulite uuendamine.</p>
<p>ds.kaspersky.com</p> <p>Protokoll: HTTPS Port: 443</p>	<p>Kaspersky Security Networki kasutamine</p>
<p>ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com</p> <p>Protokoll: Ükskõik milline Port: 443, 1443</p>	<p>Kaspersky Security Networki kasutamine</p>
<p>click.kaspersky.com</p> <p>redirect.kaspersky.com</p> <p>Protokoll: HTTPS</p>	<p>Järgige liideses olevaid linke.</p>

Identiteedivarguse kaitse

Kaspersky Premiumi tellimus sisaldab Kaitset identiteedivarguse vastu, mida pakub ülemaailmne identiteedivarguse vastase kaitse ja küberturbe ettevõtte Iris® Powered by Generali.

Kaitse identiteedivarguse vastu pole mõnes piirkonnas saadaval. Selles jaotises kirjeldatud tasulisi teenuseid osutatakse ainult tellimuse omanikule. Need ei ole kättesaadavad kasutajatele, kellega omanik on tellimust jaganud.

Identiteedivarguste kaitse teenused

Kõnekeskus pole mõnes piirkonnas saadaval.

Identiteedivarguse kaitse kõnekeskuse operaatorid töötavad ööpäev läbi, et aidata teil varastatud identiteeti taastada ja vältida edasist kahju sellise varguse tõttu.

- Abi rahakoti varguse või kaotamise korral. Võtame ühendust teie pangaga, et blokeerida ja/või uuesti väljastada teie krediitkaardid ning kui kaotate juhiloa, sotsiaalkindlustuskaardi või passi, võtame nende asendamise protsessi algatamiseks ühendust vastavad dokumendid väljastanud ametiasutustega.
- Vähem laenupakkumisi. Aitame teil kaitsta teie isikuandmeid, vähendades heakskiidetud krediitkaardipakkumiste arvu, mille petturid võivad saata teie identiteedi varastamiseks.
- Eemaldamine reklaamide meilistidest. Aitame teil vähendada krediitkaardipakkumistega meilide arvu ja turunduslikke telefonikõnesid. Sellised pakkumised võivad kujutada endast petturite katseid teie identiteeti varastada.
- Pettusekaitse juhtudel, kui teie nimele laenu võetakse. Kui teie identiteet varastati, saate esitada Internetis taotluse, et aasta jooksul kontrollitaks teie nimel võetud laenusid pettuse suhtes. See hoiab ära petturlike laenude võtmise teie nimel, kasutades teie varastatud identiteeti.
- Kaotatud dokumentide täielik taastamine. Kui teie või teie kindlustusega kaetud pereliige langeb identiteedivarguse või pettuse ohvriks, aitab spetsiaalne töötaja teie isikuandmed taastada (kui esitatud on politseiaruanne, kindlustusseltsile on väljastatud volikiri ja täidetud on identiteedivarguse avaldus). Tähelepanu! Selle teenuse saadavus oleneb teie piirkonnast ja kohaldatavast seadusest.
- Vaidluste lahendamine võlausaldajatega, teavitamine ja tugi. Piirkondades, kus see on võimalik, võtame ühendust teie panga pettuste ennetamise osakonnaga ja saadame neile iga pettusejuhtumi kohta üksikasjaliku aruande. Jälgime iga sellist menetlust ja teavitame teid korrapäraselt kohtuvaidluste tulemustest eriaruannetega.
- Politsei ja ametiasutuste teavitamine. Aitame teil identiteedipettuse korral ühendust võtta politsei ja ametiasutustega ning saadame teie võlausaldajatele pettuse aruande.
- Abi ravikindlustuse teabe varguse korral. Piirkondades, kus see on võimalik, aitame teil teie ravikindlustuse andmete varguse korral probleemi lahendada, kui teile esitatakse ebaseaduslikult meditsiiniteenuste eest arve või kui keegi saab teie ravikindlustust kasutades ebaseaduslikult ravi. Samuti hoolitseme teie raviarvete ja raviandmete parandamise eest, vajaduse korral kaasame oma meditsiinipersonali.
- Abi pikamaareisidel. Kui identiteedivargus leidis aset pikamaareisi ajal (üle 100 miili ehk 160 km kaugusel elukohast), aitame teid lennukipiletite ostmisel, hotellide broneerimisel ja auto rentimisel.

- Rahaline toetus ootamatute asjaolude korral. Kui identiteedivargus leidis aset rohkem kui 100 miili kaugusel teie elukohast, antakse teile 500 dollari suurune rahaline toetus. Võite seda raha kasutada oma äranägemise järgi. Selle teenuse kasutamiseks peab teil olema kehtiv krediitkaart. Kui te ei esitanud kehtivat krediitkaarti ja saite sellise toetuse, esitatakse arve teie krediidasutusele kindlustusseltsi kasuks 30 päeva jooksul alates kuupäevast, mil toetus teile kättesaadavaks tehti, ja te peate selle tagasi maksma krediidasutusele 45 päeva jooksul alates toetuse saamise kuupäevast. Pärast selle tähtaja möödumist maksate võla tasumata jätmise korral summalt intressi 1,5% kuus. Kindlustusseltsil on õigus keelduda teile rahalise toetuse maksmisest, kui teil puudub kehtiv krediitkaart.

Eelnimetatud teenuste saadavus oleneb teie asukohapiirkonnast.

Identiteedivarguse kindlustus

Identiteedivarguse kindlustuse kasutamisega saate kaitsta end isikuandmete taastamisega kaasnevate kulude eest. Saate rahun magada, teades, et kui peaks juhtuma, et teie isikuandmed varastatakse või need lähevad kaotsi, saate varastatud isikuandmete taastamiseks ja kulude katmiseks üks miljon dollarit.

Identiteedivarguse kindlustust pakutakse Generali US Branchi väljastatud põhipoliisi osana Generali Global Assistance, Inc. kasuks. Siin loetletud tingimused on ainult teabelise eesmärgiga ega hõlma kõiki kindlustuslepingu klausleid, tingimusi ja välistusi. Mõnes kohtualluvuses ei pruugita kindlustuskaitset pakkuda. Kindlustusprogrammis osalejad peavad esitama üksikasjaliku teabe tingimuste ja hüvitiste kohta otse kindlustuslepingus. Generali US Branch (New York, NY; NAIC # 11231) tegutseb järgmiste nimede all: Generali Assicurazioni Generali S.P.A. (U.S. Branch) Californias, Assicurazioni Generali – U.S. Branch Colorados, Generali U.S. Branch DBA The General Insurance Company of Trieste & Venice Oregonis ja The General Insurance Company of Trieste and Venice – U.S. Branch Virginias. Generali US Branchil on tegevusluba või muul viisil tegutsemise luba kõigis osariikides ja Columbia ringkonnas.

Eelnimetatud funktsioonide saadavus oleneb piirkonnast. Neid saab kasutada ainult tasulise tellimuse olemasolul.

Abi pettuste ennetamisel

Petturid kasutavad teie raha varastamiseks erinevaid meetodeid. Nad võivad saata teile võltsitud arveid või paluda teil tasuda petturliku veebitellimuse eest. Kui kahtlete, kas konkreetne pakkumine on õiguspärane, võite meile helistada ja me selle üle.

Pettuste ennetamine ja tugi hõlmab järgmist:

- ScamAssist. Kui saate sõnumi või pakkumise, mis tundub kahtlane või liiga hea, et tõsi olla, analüüsivad ScamAssisti töötajad sõnumit või pakkumist ja hoiatavad teid, kui see leitakse olevat petturlik, hoides nii ära teie raha kui ka isikuandmete varguse.

Kindlustusteenuse pakkuja ei vastuta teatud pettuste ennetamise ja toe teenuse raames kasutatavate meetodite, toodete, tööriistade või ressursside kättesaadavuse, turvalisuse, täpsuse ja tõhususe eest. Teie vastutate pettuste ennetamise ja toe kasutamise eest.

Sõnastik

Andmepüügilinkide ja võltsitud krüptovaluutavahetuste andmebaas

Loend veebiaadressidest, mille Kaspersky spetsialistid on määranud andmepüügi veebiaadressideks. Andmebaase uuendatakse regulaarselt ja need kuuluvad Kaspersky rakenduspaketti.

Andmepüük

Internetipettuste tüüp, mille eesmärk on saada loata juurdepääs kasutajate konfidentsiaalsetele andmetele.

Arvatav rämpsmeil

Sõnum, mida ei saa kaheldamatult pidada rämpsmeiliks, kuid millel on mitu rämpsmeilidele iseloomuliku omadust (näiteks teatud tüüpi meililistid ja reklaamsõnumid).

Arvatavalt nakatunud objekt

Objekt, mille kood sisaldab osi teadaoleva ohu modifitseeritud koodist, või objekt, mille käitumine sarnaneb ohu omaga.

Digiallkiri

Dokumenti või rakendusse manustatud krüptitud andmeplokk. Digiallkirja abil tuvastatakse dokumendi või rakenduse autor. Digiallkirja loomiseks peab dokumendi või rakenduse autoril olema autori isikut tõendav digitaalsert.

Digiallkiri võimaldab teil kontrollida andmeallikat ja andmete terviklust ning kaitsta end võltsingute eest.

Eksplloit

Tarkvarakood, mis kasutab ära süsteemi või tarkvara haavatavust. Tihti paigaldatakse eksplloitide abil arvutisse pahavara ilma kasutaja teadmata.

Failimask

Failinime tähistamine metamärkide abil. Failimaskides kasutatakse sageli metamärke „*“ ja „?“: „*“ tähistab mis tahes arvu tähemärke ja „?“ tähistab mis tahes üksikmärki.

Haavatavus

Operatsioonisüsteemi või rakenduse viga, mida pahavaratootjad saavad kasutada operatsioonisüsteemi või rakendusse tungimiseks ja selle tervikluse rikkumiseks. Kui operatsioonisüsteemil on arvukalt haavatavusi, ei ole see töökindel, kuna operatsioonisüsteemi tungivad viirused võivad põhjustada häireid nii operatsioonisüsteemis endas kui ka paigaldatud rakendustes.

Heuristiline analüüs

Tehnoloogia, mis on ette nähtud selliste ohtude tuvastamiseks, mille kohta pole Kaspersky andmebaasidesse veel teavet lisatud. Heuristiline analüüs tuvastab objektid, mille käitumine operatsioonisüsteemis võib kujutada endast turvaohu. Heuristilise analüüsi abil tuvastatud objekte peetakse arvatavalt nakatunuks. Näiteks võib objekti pidada arvatavalt nakatunuks, kui see sisaldab käsujadasid, mis on iseloomulikud pahatahtlikele objektidele (faili avamine, faili kirjutamine).

Hüperviisor

Rakendus, mis toetab ühes arvutis mitme operatsioonisüsteemi paralleelset käitamist.

iCheckeri tehnoloogia

Tehnoloogia, mis võimaldab suurendada viirusekaitsekontrolli kiirust, kuna välistab objektid, mida pole pärast viimast kontrolli muudetud, kui kontrolli parameetrid (andmebaasid ja seaded) on jäänud samaks. Iga faili kohta talletatakse teavet erandmebaasis. Seda tehnoloogiat kasutatakse nii reaajas kaitse kui ka nõudmisel kontrolli režiimides.

Oletagem näiteks, et Kaspersky rakendus on kontrollinud teie arhiivifaili ja määranud sellele *nakatumata* seisundi. Järgmine kord jätab rakendus selle arhiivi vahele, kui kontrolli seadeid ega arhiivi ei ole muudetud. Arhiivi kontrollitakse uuesti, kui olete muutnud selle sisu (lisanud sellesse uue objekti), muutnud kontrolli seadeid või uuendanud rakenduste andmebaase.

iCheckeri tehnoloogia piirangud on järgmised.

- See tehnoloogia ei tööta suurte failidega, kuna faili kontrollimine on kiirem kui kontrollimine, kas faili on pärast viimast kontrolli muudetud.
- Tehnoloogia toetab piiratud arvu failivorminguid.

Jäljed

Rakenduse käitamine silumisrežiimis; pärast iga käsu täitmist rakendus peatatakse ja kuvatakse selle etapi tulemus.

Kaitsekomponendid

Kaspersky rakenduse lahutamatud osad, mis on ette nähtud kaitsma kindlate ohutüüpide eest (näiteks Rämpseilifilter ja Andmepüügivastane kaitse). Kõik komponendid on teistest suhteliselt sõltumatud ja neid saab eraldi välja lülitada või seadistada.

Kaitstud veebilehitseja

Tavaveebilehitseja erirežiim, mis on ette nähtud finantstoiminguteks ja veebiostude sooritamiseks. Kaitstud veebilehitseja kaitseb pankade ja maksesüsteemide veebisaitidele sisestatud konfidentsiaalseid andmeid, näiteks e-panganduses kasutatavaid pangakaardinumbruid või parooli, ning lisaks hoiab veebimaksete sooritamisel ära rahaliste vahendite varguse.

Käivitusobjektid

Operatsioonisüsteemi ja teie arvutisse paigaldatud tarkvara käivitamiseks ja nõuetekohaseks tööks nõutavate programmide komplekt. Need objektid käivitatakse operatsioonisüsteemi igal käivituskorral. On viirusi, mis suudavad nakatada just automaatkäivituvaid objekte ja võivad näiteks blokeerida operatsioonisüsteemi käivitamise.

Karantiin

Erihoidla, kuhu rakendus teisaldab nakkuse eemaldamise käigus muudetud või kustutatud failide varukoopiaid. Failide koopiaid salvestatakse erivormingus, mis pole arvutile ohtlik.

Kaspersky Security Network (KSN)

Kaspersky pilvepõhine teabebaas, mis sisaldab teavet rakenduste ja veebisaitide reputatsiooni kohta. Kaspersky Security Networki andmete kasutamine tagab Kaspersky rakenduste kiirema reageerimise ohtudele, parandab mõne kaitsekomponendi jõudlust ja vähendab valehäirete tõenäosust.

Kaspersky uuendusserverid

Kaspersky HTTP-serverid, kust laaditakse alla andmebaaside ja tarkvaramoodulite uuendused.

Ketta alglaadimissektor

Alglaadimissektor on arvuti kõvaketta, disketi või muu andmekandja eriala. See sisaldab teavet ketta failisüsteemi kohta ja operatsioonisüsteemi käivitamise eest vastutava alglaadurprogrammi kohta.

Alglaadimissektoreid nakatavaid viirusi on mitmeid ja neid nimetatakse seetõttu buudiviirusteks. Kaspersky rakendus võimaldab kontrollida, kas alglaadimissektorites on viiruseid, ja nakkuse avastamise korral selle parandada.

Klaviatuurinuhk

Programm, mis on ette nähtud salvestama salaja teavet kasutaja klahvivajutuste kohta. Klaviatuurinuhid püüavad klaviatuurivajutused kinni.

Liikluse kontrollimine

Reaalajas kontroll, mis kasutab kõigi protokollide (nt HTTP, FTP ja muude protokollide) kaudu edastatud objektide andmebaaside praeguse (uusima) versiooni teavet.

Nakatunud objekt

Objekt, mille koodi osa langeb täielikult kokku teadaoleva pahavara koodiosaga. Kaspersky ei soovita selliseid objekte avada.

Objekti blokeerimine

Kolmanda osapoole rakendustest objektile juurdepääsu keelamine. Blokeeritud objekti ei saa lugeda, käivitada, muuta ega kustutada.

Ohu tase

Indeks, mis näitab tõenäosust, et rakendus on operatsioonisüsteemile ohtlik. Ohutase arvutatakse järgmist kahte tüüpi kriteeriumidel põhineva heuristilise analüüsi abil.

- Staatilised (nt teave rakenduse käivitusfaili kohta: maht, loomiskuupäev jne)
- Dünaamilised, mida kasutatakse virtuaalkeskkonnas rakenduse töö simuleerimisel (rakenduse süsteemikutsete analüüs)

Ohutase võimaldab tuvastada pahavarale omast käitumist. Mida madalam on ohutase, seda rohkem toiminguid on rakendusel lubatud operatsioonisüsteemis teha.

Pahatahtlike veebiaadresside andmebaas

Loend veebiaadressidest, mille sisu võib pidada ohtlikuks. Kaspersky spetsialistide koostatud loendit uuendatakse regulaarselt ja see kuulub Kaspersky rakenduspaketti.

Protokoll

Selgelt määratletud ja standardiseeritud reeglistik, mis reguleerib kliendi ja serveri suhtlust. Tuntud protokollid ja nendega seotud teenused on muu hulgas HTTP, FTP ja NNTP.

Rakenduse aktiveerimine

Rakenduse lülitamine täisfunktsionaalsesse režiimi. Rakenduse aktiveerib rakenduse paigaldamise ajal või pärast seda kasutaja. Rakenduse aktiveerimiseks peab kasutajal olema aktiveerimiskood.

Rakendusemoodulid

Kaspersky paigalduspaketti kuuluvad failid, mis vastutavad vastava rakenduse põhiülesannete täitmise eest. Igale rakenduse täidetavale ülesandetüübile (kaitse, kontroll, viirusekaitse andmebaaside ja rakendusemoodulite uuendused) vastab kindel rakendusemoodul.

Rämpsmail

Soovimatute mailide hulgisaatmine, mis hõlmab kõige sagedamini reklaame.

Rootkit

Programm või programmikomplekt, mis peidab operatsioonisüsteemis sissetungija või pahavara jäljed.

Windowsi-põhistes operatsioonisüsteemides viitab rootkit tavaliselt programmile, mis tungib operatsioonisüsteemi ja sekkub süsteemi funktsioonidesse (Windowsi API-desse). Madala taseme API-funktsioonidesse sekkumine ja nende muutmine on põhimeetodid, mille abil saavad need programmid operatsioonisüsteemis üsna varjatult tegutseda. Rootkit saab tavaliselt lisaks registrivõtmetele varjata ka kettadraivile salvestatud mis tahes protsessi, kausta ja faili, kui neid on kirjeldatud rootkit'i konfiguratsioonis. Paljud rootkit'id paigaldavad operatsioonisüsteemi oma draiverid ja teenused (ka need on n-ö nähtamatud).

Salahoidla

Andmehoidla on andmete erihoidla, milles talletatakse faile krüptitud kujul. Neile failidele juurdepääsemiseks on vaja parooli. Salahoidlad on ette nähtud selleks, et vältida volitamata juurdepääsu kasutajaandmetele.

Skript

Väike arvutiprogramm või programmi (funktsiooni) autonoomne osa, mis reeglina on välja töötatud kindla ülesande täitmiseks. Kõige sagedamini kasutatakse seda koos hüpertexti manustatud programmidega. Skripte kasutatakse näiteks teatud veebisaitide avamisel.

Kui reaajas kaitse on sisse lülitatud, jälgib rakendus skriptide käivitamist, püüab need kinni ja otsib neist viiruseid. Kontrolli tulemustest olenevalt saate skripti blokeerida või lubada seda käitada.

Tegum

Kaspersky rakenduse funktsioone rakendatakse tegumite kujul, nagu täiskontrolli tegum või uuendamise tegum.

Tegumi seaded

Rakenduse tegumitüübikohased seaded.

Tihendatud fail

Tihendatud käivitusfail, mis sisaldab lahtipakkimisprogrammi ja operatsioonisüsteemile ette nähtud juhiseid selle käivitamiseks.

Tundmatu viirus

Uus viirus, mille kohta puudub andmebaasides teave. Üldiselt tuvastab rakendus objektides tundmatud viirused heuristilise analüüsi abil. Need objektid liigitatakse arvatavalt nakatunuks.

Turvatase

Turvatase on rakenduse komponendi seadete eelmääratud kogum.

Ühildumatu rakendus

Kolmandast osapooltest arendaja viirusetõrjerakendus või Kaspersky Labi rakendus, mis ei toeta Kaspersky Small Office Security kaudu haldamist.

Usaldusgrupp

Grupp, millesse Kaspersky Small Office Security määrab rakenduse või protsessi järgmiste kriteeriumide põhjal: digiallkirja olemasolu, reputatsioon Kaspersky Security Networkis, rakenduse allika usaldusväarsuse tase ning rakenduse või protsessi tehtavate toimingute potentsiaalne ohtlikkus. Rakenduse usaldusgrupi põhjal saab Kaspersky Small Office Security piirata toiminguid, mida rakendusel on lubatud operatsioonisüsteemis teha.

Kaspersky rakenduses kasutatakse järgmisi usaldusgruppe: Usaldusväärased, Nõrgad piirangud, Tugevad piirangud või Ebausaldusväärased.

Usaldusväärne protsess

Tarkvaraprotsess, mille failitoiminguid Kaspersky rakendus reaajas kaitse režiimis ei piira. Kui usaldusväärset protsessis tuvastatakse kahtlane tegevus, eemaldab Kaspersky rakendus protsessi usaldusväärsete protsesside loendist ja blokeerib selle toimingud.

Uuendus

Kaspersky uuendusserveritest hangitud uute failide (andmebaaside või rakendusemoodulite) asendamine/lisamine.

Uuenduspakett

Failipakett, mis on ette nähtud andmebaaside ja rakendusemoodulite uuendamiseks. Kaspersky rakendus kopeerib uuenduspaketid Kaspersky uuendusserveritest ning paigaldab ja rakendab need automaatselt.

Valehäire

Olukord, kui Kaspersky rakendus peab nakatamata objekti nakatunuks, kuna objekti kood sarnaneb viiruse omaga.

Varundamine ja taastamine

Loob arvutisse talletatud andmetest varukoopiaid. Varukoopiaid luuakse selleks, et vältida andmete kaotsiminekut varguse, riistvararikete või häkkerirünnakute tõttu.

Viirus

Teisi programme nakatav programm, mis lisab neisse oma koodi, et võtta nakatunud failide käivitamise korral kontroll enda kätte. See lihtne määratlus võimaldab tuvastada mis tahes viiruse põhitoimingu: nakatamise.

Viirusekaitse andmebaasid

Andmebaasid, mis sisaldavad teavet arvutite turvaohutude kohta, mis on Kasperskyle teada viirusekaitse andmebaaside väljaandmise ajal. Viirusekaitse andmebaaside kirjed võimaldavad kontrollitud objektides tuvastada pahatahtlikku koodi. Viirusekaitse andmebaase koostavad Kaspersky spetsialistid ja neid uuendatakse iga tund.

Teave kolmanda osapoole koodi kohta

Teave kolmanda osapoole koodi kohta on rakenduse paigalduskausta failis `legal_notices.txt`.

Kaubamärgiteated

Registreeritud kaubamärgid ja teenindusmärgid kuuluvad nende omanikele.

Adobe, Acrobat, Reader on Adobe registreeritud kaubamärgid või kaubamärgid Ameerika Ühendriikides ja/või teistes riikides.

Apple, macOS, App Store ja Safari on ettevõtte Apple Inc. kaubamärgid, mis on registreeritud Ameerika Ühendriikides ning muudes riikides ja piirkondades.

Dropbox on ettevõtte Dropbox, Inc. kaubamärk.

Google, Google Chrome, Google Play, Chromium, SPDY, YouTube ja Android on ettevõtte Google LLC kaubamärgid.

Intel, Celeron ja Atom on Ameerika Ühendriikides ja/või muudes riikides ettevõtte Intel Corporation kaubamärgid.

IOS on registreeritud kaubamärk või Ameerika Ühendriikides ja teatud muudes riikides ettevõtte Cisco Systems, Inc. ja/või selle sidusettevõtete kaubamärk.

Java ja JavaScript on ettevõtte Oracle ja/või tema sidusettevõtete registreeritud kaubamärgid.

Linux on Linus Torvaldsi kaubamärk, mis on registreeritud Ameerika Ühendriikides ja teistes riikides.

LogMeln Pro ja Remotely Anywhere on ettevõtte LogMeln, Inc. kaubamärgid.

Mail.ru on ettevõtte Mail.ru LLC kaubamärk.

Microsoft, Windows, Windows Mail, Internet Explorer, Outlook, PowerShell, Bing, Skype on Microsofti ettevõtete grupi kaubamärgid.

Mozilla, Thunderbird ja Firefox on mittetulundusühenduse Mozilla Foundation kaubamärgid.

VMware on Ameerika Ühendriikides ja/või muudes kohtualluvustes ettevõtte VMware, Inc. registreeritud kaubamärk.

Teenuste loend, millele parool QR-koodi skannimisel saadetakse

Kui skannite Android-seadmes QR-koodi, saadetakse Google Playle ja AppsFlyerile ühekordne parool teie nutitefonis oleva rakenduse aktiveerimiseks.

Aken „Täienda“

[Prooviversioon](#)

Link käivitab ülemineku proovitellimusele.

[Osta aktiveerimiskood](#)

Selle nupu klõpsamine avab veebilehitsejas veebipoe, kust saate osta tellimuse.

[Sisesta aktiveerimiskood](#)

Klõpsake sellel lingil, et käivitada rakenduse aktiveerimisnõustaja.

Aken „Täienda“

[Osta aktiveerimiskood](#)

Klõpsake sellel lingil, et avada oma brauseris e-poe veebisait, kust saate osta selle rakenduse tellimuse, millele olete üle minemas.

[Sisesta aktiveerimiskood](#)

Klõpsake sellel lingil, et käivitada rakenduse aktiveerimisnõustaja.

[Prooviversioon](#)

Klõpsake seda nuppu teise rakenduse prooviversioonile üleminekuks.

Rakenduse aktiveerimine varuaktiveerimiskoodiga

Varuaktiveerimiskoodi rakendamiseks klõpsake nuppu **Edasi**.

Kui litsents pole veel aegunud, saate rakendada sama aktiveerimiskoodi, mille abil olete varem rakenduse aktiveerinud teises arvutis.

Rakenduse aktiveerimise tühistamiseks klõpsake linki **Tühista**.

[Tühista](#) 

Klõpsake sellel lingil, et tühistada varuaktiveerimiskoodi kasutamine ja naasta aknasse **Litsents**.

Aken „Sisesta aktiveerimiskood“

[Rakenduse aktiveerimiskoodi sisestamiseks mõeldud väljad](#)

Võisite saada aktiveerimiskoodi meili teel või võrguühenduseta poes. Aktiveerimiskood koosneb neljast märgirühmast (näiteks **ABA9C-CDEFG-ABCBC-ABC2D**).

[Taasta tellimus kontolt](#)

Sellel lingil klõpsates avaneb aken vormiga, mis võimaldab teil ühendada seadme oma My Kaspersky halduskonsooli kontoga, et aktiveerida kontole salvestatud tellimus.

[Kust ma aktiveerimiskoodi leian?](#)

Kui klõpsate lingil **Kust ma aktiveerimiskoodi leian?**, avaneb brauseriaken üksikasjaliku teabega rakenduse aktiveerimiskoodi abil aktiveerimise kohta.

[Osta tellimus](#)

Klõpsake seda linki, et avada veebilehitseja aknas e-pood, kust saate osta tellimuse.

[Aktiveeri](#)

Klõpsake seda nuppu, et alustada rakenduse aktiveerimist sisestatud aktiveerimiskoodi abil.

Aktiveerimiskood vastab teisele rakendusele

See aken avaneb, kui sisestatud aktiveerimiskood on ette nähtud muu rakenduse jaoks. Seda rakendust saate hakata kasutama kohe või pärast Kaspersky rakenduse tellimuse aegumist.

[Tühista](#)

Rakenduse aktiveerimise tühistamiseks klõpsake seda linki.

[Jätka](#)

Selle nupu klõpsamise korral alustatakse aktiveerimiskoodile vastava rakenduse paigaldamist ja aktiveerimist.

Teave veebisaidikategooriate kohta

Klõpsake linki, kui soovite [lugeda veebisaitide kategooriate kirjeldusi](#).


DNS-i seadistamine HTTPS-kaitse kaudu

Kui sisestate aadressiribale veebisaidi nime, saadab veebilehitseja teie päringu DNS-serverisse. DNS-server määrab kindlaks soovitud veebisaidi IP-aadressi. Andmed edastatakse teie arvutist DNS-serverisse tavalise krüptimata tekstiprotokolli abil. Sissetungijad saavad püüda kinni teabe teie külastatud veebisaitide kohta ja seda kuritarvitada. Selle vältimiseks tuleb teave edastada turvalise HTTPS-protokolli kaudu. Serverit, mis selliseid päringuid vastu võtab ja analüüsib, nimetatakse HTTPS-i kaudu töötavaks DNS-serveriks (või DoH-serveriks).

Kaspersky võtab automaatselt vastu andmed selle kohta, millist DoH-serverit brauseris Mozilla Firefox kasutatakse. Kui lisate DoH-serveri Kaspersky rakendusse käsitsi ja soovite, et DNS-andmed edastataks selle DoH-serveri kaudu, siis peate selle serveri lisama brauseri Mozilla Firefox seadetes. DoH-serveri seadistamise kohta leiate teavet Mozilla Firefox'i spikrist.

[DoH-serveri lisamine](#)

DoH-serveri lisamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake põhiakna allservas nuppu  .
Avatakse aken **Seaded**.
3. Valige jaotise **Lisaks** alamjaotis **Võrk**.
Avatakse aken **Võrgu seaded**.
4. Akna **Liikluse töötlemine** avamiseks klõpsake plokis **DoH-serverite haldamine** linki **DoH-serverid**.
5. Klõpsake **Lisa**.
6. Avanenud aknas sisestage DoH-serveri nimi või IP-aadress ja klõpsake nuppu **Lisa**.
DoH lisatakse loendisse.

Aken „Informatsioon kehtiva litsentsi kohta on leitud“

[Jah, kasuta <application> ?](#)

Selle valiku korral aktiveerimisnõustaja sulgub. Rakendus töötab tuvastatud aktiivse tellimuse alusel. Kui leitakse Kaspersky Standardi või Kaspersky Plusi tellimus, käivitub üleminekunõustaja.

[Ei, jätkka nõustaja tööd ja sisesta uus aktiveerimiskood ?](#)

Selle suvandi valimisel jätkab aktiveerimisnõustaja tööd ja aktiveerib rakenduse. Teil tuleb sisestada uus aktiveerimiskood, mis on selle rakenduse jaoks kehtiv.

Aken „Registreerimine“

Selles aknas sisestage tehnilise toega ühenduse võtmiseks vajalikud registreerimisandmed.

Internetiühendus puudub

See aken kuvatakse, kui rakenduse aktiveerimine nurjub internetiühenduse probleemide tõttu.

[Proovi uuesti](#)

Selle lingi klõpsamise korral proovib aktiveerimisnõustaja rakendust uuesti aktiveerida. Kui internetiühenduse probleemid on ajutised, võib uuestiproovimine õnnestuda.

Jaotis „Taastatavatele failidele asukohta valimine“

[Algne kaust](#)

Selle valiku korral taastab rakendus failid kaustas, mis oli varukoopia loomise ajal originaalfailide asukoht.

[Määratud kaust](#)

Selle valiku korral taastab rakendus failid väljal **Valige kaust** määratud kaustas.

[Valige kaust](#)

Väli sisaldab selle kausta teed, kus failid tuleb taastada.

See väli on saadaval valiku **Määratud kaust** tegemise korral.

[Sirvi](#)

Selle nupu klõpsamine avab akna **Taastatavatele failidele asukohta valimine**. Selles aknas saate valida kausta, kus failid tuleb taastada.

See nupp on saadaval valiku **Määratud kaust** tegemise korral.

[Kui failinimed on vastuolus](#)

Selles ripploendis saate valida toimingut, mille rakendus peab tegema, kui taastatava faili sihtkaust sisaldab juba samanimelist faili.

- **küsi** – kui failinimed langevad kokku, palub rakendus teil valida ühe järgmistest võimalustest: asendada fail varukoopiaga, salvestada mõlemad failid või jätta fail taastamata.
- **asenda fail varukoopiaga** – Kaspersky rakendus kustutab olemasoleva faili ja asendab selle varukoopiast taastatud failiga.
- **salvesta mõlemad failid** – Kaspersky rakendus jätab olemasoleva faili muutmata ja salvestab varukoopiast taastatud faili samasse kausta uue nimega.
- **ära seda faili taasta** – Kaspersky rakendus jätab olemasoleva faili muutmata ja ei taasta varukoopiast samanimelist faili.

[Taasta](#)

Selle nupu klõpsamise korral alustatakse varukoopiatest failide taastamist.

Aktiveerimisviga

Rakenduse aktiveerimine nurjus. Probleemi kohta teabebaasist teabe lugemiseks klõpsake linki **Põhjused ja võimalikud lahendused**.

[Põhjused ja võimalikud lahendused](#)

Link avab teabebaasi artikli, mis sisaldab teavet tõrke põhjuste ja võimalike lahenduste kohta.

Mõne tõrke korral ei pruugi teabebaasiartiklite lingid saadaval olla.

[Tühista](#)

Rakenduse aktiveerimise tühistamiseks klõpsake seda linki.

Üleminek teisele rakendusele

Ülemineku nõustaja käivitamiseks klõpsake nuppu **Edasi**. Ülemineku nõustaja installib sisestatud aktiveerimiskoodile vastava rakenduse (Kaspersky Standard või Kaspersky Plus).

Kui teie Kaspersky tellimus ei ole veel aegunud, saate Kaspersky aktiveerimiskoodi kasutada teises arvutis.

Kaspersky Standardile või Kaspersky Plusile ülemineku tühistamiseks klõpsake linki **Tühista**.

[Tühista](#)

Klõpsake seda linki, et väljuda ülemineku nõustajast ja naasta eelmisse etappi.

Veendumine, et sisestatav aktiveerimiskood ei oleks tellimuse aktiveerimiskood

Veenduge, et varukoodina sisestatav aktiveerimiskood ei oleks tegelikult ette nähtud rakenduse tellimuspõhiseks kasutamiseks. Rakenduse tellimuspõhise kasutamise eest võetakse tasu tellimuse hankimise hetkel. Kui olete hankinud Kaspersky tellimuse, ärge kasutage rakendust praeguse litsentsi alusel. Selle asemel aktiveerige rakendus tellimuse aktiveerimiskoodiga.

Kuni litsentsi kehtivusaja lõppemiseni saate teises arvutis rakenduse aktiveerida juba kasutatud aktiveerimiskoodi abil.

Aken „Käivitusjärjekord“

[Rakenduste käivitusjärjekord](#)

Loend sisaldab teavet valitud rakenduse käivitatud rakenduste (tütarrakenduste) kohta. Vaikimisi sortitakse tütarrakendused käivitamisaaja järgi, alustades kõige varasemast.

[Käivitus](#)

Selles veerus kuvatakse tütarrakenduse käivitamisaeg.

[Protsessi ID](#)

Selles veerus kuvatakse tütarrakenduse protsessi ID.

[Rakendus](#)

Selles veerus kuvatakse tütarrakenduse nimi.

[Usaldusgrupp](#)

Selles veerus kuvatakse rakenduse usaldusgrupp.

- **Usaldusväärsed.** Rakendus töötab ilma piiranguteta, kuid seda jälgib failide kaitse.
- **Nõrgad piirangud.** Rakendusel on keelatud pääseda juurde kasutaja isiklikele andmetele ja seadetele ning muuta mis tahes avalikke andmeid. Mis tahes katsed muuta süsteemi andmeid või teha õigustepõhiseid toiminguid vajavad kasutaja luba. Selliste rakenduste võrgutegevus on piiratud.
- **Tugevad piirangud.** Rakendusel on keelatud pääseda juurde kasutaja isiklikele andmetele ja seadetele ning samuti kõigile süsteemi või avalikele andmetele. Mis tahes õigustepõhised toimingud vajavad kasutaja luba. Sellise rakenduse võrgutegevus on blokeeritud.
- **Ebausaldusväärsed.** Kogu sellise rakenduse tegevus on täielikult blokeeritud.

Vahekaart „Käivitatud“

Töötavate rakenduste loend [?](#)

Loend sisaldab rakendusi ja protsesse, mis teie arvutis praegu töötavad.

Veerupäise kontekstimenüü avamiseks paremklopsake. Kontekstimenüü võimaldab teil seadistada rakenduste ja protsesside lisateabega veergude kuvamise viisi.

- Rakenduse või protsessi käivitusfaili nimi
- Rakenduse tarnija üksikasjad
- Protsessi ID
- Rakenduse käivitusfaili tee
- Rakenduse või protsessi käivitanud kasutaja nimi
- Rakenduse või protsessi loomise ja käivitamise aeg
- Rakenduse automaatkäivitusseaded

Üksuse **Taasta tulpade vaikekomplekt** abil saate taastada tabeli vaikeilme.

Rakenduse või protsessi rea paremklopsamise korral avaneb kontekstimenüü. Kontekstimenüüs saate teha järgmisi toiminguid.

- Saate avada akna **Rakenduste reeglid**, mis võimaldab seadistada rakenduse tegevuse piiramise reeglid.
- Saate kuvada aknas **Käivitusjärjekord** protsesside käivitamise järjekorra.
- Saate teisaldada rakenduse muusse usaldusgruppi.
- Saate rakendusele rakendada rakenduste õiguste kontrolli vaikeseaded.
- Saate protsessi katkestada.
- Saate avada rakenduse käivitusfaili sisaldava kausta.

Vaade [?](#)

Ripploendis saate süsteemiprotsesside ja Kaspersky algatatud protsesside kuvamise sisse lülitada.

- **Näita süsteemiprotsesse.** Selle üksuse valimise korral kuvatakse rakenduste ja protsesside üldloendis operatsioonisüsteemi nõuetekohaseks toimimiseks vajalikud protsessid.
- **Näita <PRODUCT> protsesse.** Selle üksuse valimise korral kuvatakse rakenduste ja protsesside üldloendis Kaspersky algatatud protsessid.

Ripploendis saate valida rakenduste ja protsesside kuvamisrežiimi.

- **Nimekirjavaade.** Selle valiku korral kuvatakse rakendused ja protsessid loendina.
- **Puuvaade.** Selle valiku korral kuvatakse rakendused ja protsessid hierarhiliselt protsesside kutsumisjärjestuse alusel.

[Rakendus](#)

Selles veerus kuvatakse rakenduse või protsessi nimi.

[Digiallkiri](#)

Selles veerus kuvatakse teave selle kohta, kas rakendus on digiallkirjastatud, ja digiallkirja omaniku kohta.

[Usaldusgrupp](#)

Selles veerus kuvatakse usaldusgrupp, kuhu rakendus kuulub. Rakenduse usaldusgrupist olenevalt sisaldab veerg järgmisi ikooni.

- Punane ikoon tähendab, et rakendus on grupis „Ebausaldusväärsed“.
- Roosa ikoon tähendab, et rakendus on grupis „Tugevad piirangud“.
- Kollane ikoon tähendab, et rakendus on grupis „Nõrgad piirangud“.
- Roheline ikoon tähendab, et rakendus on grupis „Usaldusväärsed“.
- Mõnda eriotstarbelist süsteemiprotsessi (nt System või MemCompression) ei liigitata usaldusgruppidesse ja need ei ole Kaspersky kontrolli all. Sellised protsessid kuvatakse halli ikoonina ja märgitakse tundmatuks.

[Populaarsus](#)

See veerg näitab rakenduse populaarsuse taset Kaspersky Security Networkis (KSN) osalejate seas. Populaarsuse tase kajastab rakendust kasutavate KSN-is osalejate arvu.

[Protsessor](#)

Selles veerus kuvatakse rakenduse või protsessi praegune protsessoriresursside kasutusmäär.

[Mälu](#)

Selles veerus kuvatakse rakenduse või protsessi praegune muutmälu (RAM-i) kasutusmäär.

[Ketas](#)

Selles veerus kuvatakse kogukiirus, millega rakendus või protsess kettal andmeid loeb/kirjutab.

[Võrk](#)

See veerg näitab rakenduse andmeedastuse kogukiirust võrguliidese kaudu.

[Katkesta protsess](#)

Selle nupu klõpsamine sulgeb loendist valitud rakenduse.

Vahekaart „Arvuti käivitamisel käivituvad“

Arvuti käivitamisel käivituvate rakenduste loend [?](#)

See loend sisaldab rakendusi, mis käivitatakse operatsioonisüsteemi käivitamisel.

Veerupäise kontekstimenüü avamiseks paremklõpsake. Kontekstimenüü abil saate seadistada tabeliveergude kuvamisviisi. Üksuse **Taasta tulpade vaikekomplekt** abil saate taastada tabeli vaikeilme.

Rakenduse või protsessi rea paremklõpsamise korral avaneb kontekstimenüü. Kontekstimenüüs saate teha järgmisi toiminguid.

- Saate avada akna **Rakenduste reeglid**, mis võimaldab seadistada rakenduse tegevuse piiramise reeglid.
- Saate teisaldada rakenduse muusse usaldusgruppi.
- Saate rakendusele rakendada rakenduste õiguste kontrolli vaikeseaded.
- Saate avada rakenduse käivitusfaili sisaldava kausta.

Rakendus [?](#)

Selles veerus kuvatakse operatsioonisüsteemi käivitamisel käivituva rakenduse nimi.

Seisund [?](#)

Selles veerus kuvatakse rakenduse seisund: *käivitatud* või *peatatud*.

Digiallkiri [?](#)

Selles veerus kuvatakse teave selle kohta, kas rakendus on digiallkirjastatud, ja digiallkirja omaniku kohta.

Usaldusgrupp [?](#)

Selles veerus kuvatakse usaldusgrupp, kuhu rakendus kuulub. Rakenduse usaldusgrupist olenevalt sisaldab veerg järgmisi ikoone.

- Punane ikoon tähendab, et rakendus on grupis „Ebausaldusväärsed“.
- Roosa ikoon tähendab, et rakendus on grupis „Tugevad piirangud“.
- Kollane ikoon tähendab, et rakendus on grupis „Nõrgad piirangud“.
- Roheline ikoon tähendab, et rakendus on grupis „Usaldusväärsed“.
- Mõnda eriotstarbelist süsteemiprotsessi (nt System või MemCompression) ei liigitata usaldusgruppidesse ja need ei ole Kaspersky kontrolli all. Sellised protsessid kuvatakse halli ikoonina ja märgitakse tundmatuks.

Populaarsus [?](#)

See veerg näitab rakenduse populaarsuse taset Kaspersky Security Networkis (KSN) osalejate seas. Populaarsuse tase kajastab rakendust kasutavate KSN-is osalejate arvu.

Viimane käivitus

Selles veerus kuvatakse rakenduse viimase käivituskorra aeg.

Võrk, mille olete määratlenud koduvõrguna, on tegelikult avalik

Kui loote ühenduse avaliku Wi-Fi-võrguga, näiteks kohvikus, edastatakse andmed ilma krüpteerimata. See tähendab, et teie paroolid, kasutajanimed, sõnumid ja muu konfidentsiaalne teave on sissetungijatele kättesaadav. Teie meiliaadresse saab kasutada rämpsmeilide saatmiseks ja teie sotsiaalmeedia-lehekülgedel olevat teavet saab muuta.

Ohustatud on ka kodune Wi-Fi-võrk. Näiteks WPA2-protokolli saab häkkida, kasutades võtme uuesti installimise rünnakut (KRACK).

Mis tahes Wi-Fi-võrguga ühenduse loomisel järgige alati järgmisi soovitusi.

1. Veenduge, et teil oleks Tulemüür installitud ja sisse lülitatud. See kaitsekomponent kontrollib võrguliiklust ja kaitseb teie arvutit võrgurünnakute eest.
2. Tulemüür on järgmiste Kaspersky rakenduste osa: Kaspersky, Kaspersky Internet Security, Kaspersky Anti-Virus, Kaspersky Total Security, Kaspersky Security Cloud ja Kaspersky Small Office Security.
3. Kasutage turvalist HTTPS-ühendust. Jälgige, et teie brauseri aadressiribal oleks roheline või hall tabaluku-ikoon.
4. Kaitske oma ühendust VPN-i abil. Installige oma seadmesse Kaspersky Secure Connection ja lülitage Secure Connection internetiühenduse loomisel alati sisse.
5. Kui kasutate Windowsi, keelake failide ja printerite jagamise teenus kõigi avalike võrkude puhul, millega loote ühenduse. Juhised leiate [Microsofti toe veebisaidilt](#).
6. Kui võimalik, kasutage avalike Wi-Fi-võrkude asemel mobiilset andmesidet.

Teie koduvõrk kasutab WPS-i

WPS-tehnoloogia eesmärk on seadmete ühendamist Wi-Fi-võrkudega lihtsustada. WPS-i saab kasutada teie ruuteriga ühenduse loomiseks ilma paroolita. Soovitame WPS-i ruuteri seadetes välja lülitada.

Ruuteriliidesed erinevad olenevalt ruuteri tootjast, mudelist ja püsivara versioonist. Ruuteri seadete kohta saate teavet oma mudeli kasutusjuhendist. Kasutusjuhend on tavaliselt ruuteriga kaasas; samuti saate selle alla laadida seadme tootja veebisaidilt.

Alljärgnevalt on toodud ruuteri TP-Link TL-WR841N konfiguratsiooninäide.

WPS-i väljalülitamiseks tehke järgmist.

1. Sisestage brauseri aadressiribale ruuteri IP-aadress.
Avaneb ruuteri konfiguratsiooni veebiliidese autoriseerimislehekülg. Teie ruuteri IP-aadress on kirjas seadme alumisel küljel ja kasutusjuhendis.
2. Sisestage autoriseerimisleheküljele oma kasutajanimi ja parool. Kui neid ei ole kunagi muudetud, leiate need ruuteri alumiselt küljelt.
3. Minge ruuteri seadete lehel jaotisse **Traadita võrk** → **WPS**.
4. Klõpsake nuppu **Lülita välja**.

Teie koduvõrk ei ole parooliga kaitstud

Ilma paroolita on teie Wi-Fi-võrk kõigile juurdepääsetav. Tugev parool takistab teistel isikutel teie võrguga ühendust luua. Tugeva parooli loomiseks järgige [selles artiklis](#) toodud nõuandeid.

Ruuteriliidesed erinevad olenevalt ruuteri tootjast, mudelist ja püsivara versioonist. Ruuteri seadete kohta saate teavet oma mudeli kasutusjuhendist. Kasutusjuhend on tavaliselt ruuteriga kaasas; samuti saate selle alla laadida seadme tootja veebisaidilt.

Alljärgnevalt on toodud ruuteri TP-Link TL-WR841N konfiguratsiooninäide.

Parooli loomiseks tehke järgmist.

1. Sisestage brauseri aadressiribale ruuteri IP-aadress.
Avaneb ruuteri konfiguratsiooni veebiliidese autoriseerimislehekülg. Teie ruuteri IP-aadress on kirjas seadme alumisel küljel ja kasutusjuhendis.
2. Sisestage autoriseerimisleheküljele oma kasutajanimi ja parool. Kui neid ei ole kunagi muudetud, leiate need ruuteri alumiselt küljelt.
3. Minge ruuteri seadete lehel jaotisse **Traadita võrk** → **Traadita võrgu turvalisus**.
4. Valige **WPA/WPA2 – Isiklik**.
5. Looge ja sisestage väljal **Traadita võrgu parool** Wi-Fi-võrgu parool.
6. Klõpsake nuppu **Salvesta**.

Teie koduvõrk kasutab populaarset SSID-d

Üks üldlevinud meetod paroolide häkkimiseks on niinimetatud vikerkaaretabel. Sissetungija kasutab ettevalmistatud vikerkaaretabelit, mis sisaldab miljoneid võimalikke parooli, mis on vastendatud populaarsete SSID-dega. Kui teie SSID ja parool leitakse sellisest tabelist, saab sissetungija eritarkvara abil võrgu parooli kohe taastada.

Koduse traadita võrgu turvalisemaks muutmiseks kasutage haruldast SSID-d.

Ruuteriliidesed erinevad olenevalt ruuteri tootjast, mudelist ja püsivara versioonist. Ruuteri seadete kohta saate teavet oma mudeli kasutusjuhendist. Kasutusjuhend on tavaliselt ruuteriga kaasas; samuti saate selle alla laadida seadme tootja veebisaidilt.

Alljärgnevalt on toodud ruuteri TP-Link TL-WR841N konfiguratsiooninäide.

Wi-Fi-võrgu nime muutmiseks tehke järgmist.

1. Sisestage brauseri aadressiribale ruuteri IP-aadress.

Avaneb ruuteri konfiguratsiooni veebiliidese autoriseerimislehekülg. Teie ruuteri IP-aadress on kirjas seadme alumisel küljel ja kasutusjuhendis.

2. Sisestage autoriseerimisleheküljele oma kasutajanimi ja parool. Kui neid ei ole kunagi muudetud, leiate need ruuteri alumiselt küljelt.

3. Minge ruuteri seadete lehel jaotisse **Traadita võrk** → **Põhiseaded**.

4. Looge ja sisestage väljal **Traadita võrgu nimi** oma Wi-Fi-võrgule nimi.

5. Klõpsake nuppu **Salvesta**.

Teie koduvõrk kasutab nõrka andmekrüpteeringut

Kui kasutate nõrga krüpteeringuga võrku, võivad sissetungijad teie andmed enda valdusse saada. Kui saate koduvõrguga ühendudes teate nõrgast krüpteeringust, minge üle turvalisemale krüpteerimistüübile. Traadita võrkudes kasutatakse tavaliselt järgmisi krüpteerimistüüpe: WEP, TKIP, WPA, WPA2 (AES/CCMP).

Peamine erinevus on nende pakutava kaitse tase. Soovitame kasutada WPA2, mis on kõige turvalisem variant.

Ruuteriliidesed erinevad olenevalt ruuteri tootjast, mudelist ja püsivara versioonist. Ruuteri seadete kohta saate teavet oma mudeli kasutusjuhendist. Kasutusjuhend on tavaliselt ruuteriga kaasas; samuti saate selle alla laadida seadme tootja veebisaidilt.

Alljärgnevalt on toodud ruuteri TP-Link TL-WR841N krüpteeringu konfiguratsiooninäide.

Traadita võrgu jaoks teise krüpteerimistüübi kasutamiseks tehke järgmist.

1. Sisestage brauseri aadressiribale ruuteri IP-aadress.

Avaneb ruuteri konfiguratsiooni veebiliidese autoriseerimislehekülg. Teie ruuteri IP-aadress on kirjas seadme alumisel küljel ja kasutusjuhendis.

2. Sisestage autoriseerimisleheküljele oma kasutajanimi ja parool. Kui neid ei ole kunagi muudetud, leiate need ruuteri alumiselt küljelt.

3. Minge ruuteri seadete lehel jaotisse **Traadita võrk** → **Traadita võrgu turvalisus**.

4. Valige **WPA/WPA2 – Isiklik**.

5. Valige väljal **Autentimise tüüp WPA2-PSK**.

6. Valige väljal **Krüpteerimine AES**.

7. Klõpsake nuppu **Salvesta**.

Teie koduvõrk kasutab nõrka parooli

Soovitame kasutada tugevaid paroole, et kaitsta isikuandmeid ja konfidentsiaalseid teavet. Ärge looge kontosid ilma paroolideta.

Tugeva parooli omadused

- Parool peab olema vähemalt 8 märgi pikkune. Kui kasutate Windowsi, veenduge, et operatsioonisüsteemi seadetes valitud parooli miinimumpikkus oleks vähemalt 8 märki.
- Parool peab sisaldama suur- ja väiketähti, numbreid, tühikuid ja erimärke. Näide: oNQZnz\$Hx2.

Mida parool ei tohi sisaldada

- Isikuandmeid, mida teised võivad hõlpsasti enda valdusse saada. Näiteks ees- või perekonnanimi, sünniaeg.
- Selged ja lihtsad sõnad, fraasid, idioomid või märgijadad, mida on lihtne ära arvata. Näide: parool, parol, abcd, qwerty või asdfg, 1234567.

Paroolide genereerimise tehnikad

- Mõelge välja algoritm paroolide koostamiseks. Võtke näiteks oma lemmikluuletus või kuulus tsitaat. Kirjutage see üles ladina tähestiku väikeste ja suurte tähtedega ning asendage mõned neist sarnase välimusega numbrite ja erimärkidega: @_R0s3 bY_a#y Ot#er n@mE w0u1c|_ \$me11 as_sVV3Et.
- Kasutage parooligeneraatorit. Kaspersky Password Manageriga saate genereerida keerulisi paroole, kontrollida nende tugevust ja hoida neid turvaliselt. Samuti saate installida [Kaspersky Password Manageri](#) brauserilaiendi veebisaitide sisestusväljade automaattäitmiseks.

Kui tihti peaksin oma parooli muutma?

Soovitame muuta oma parooli iga 3 kuu tagant.

Parooli turvamine

- Ärge avaldage ega saatke oma parooli kellelegi.
- Ärge jätke oma paroole paberile kirja panduna kohta, kuhu võib tulla teisi inimesi.
- Kasutage brauserisse sisseehitatud paroolihoidlat või paroolihaldurit.
- Kasutage iga konto jaoks kordumatut parooli. Parooli korduvkasutamine võimaldab sissetungijal, kes saab ühe teie konto parooli teada, pääseda ligi ka kõigile teistele teie kontodele.

Vahekaart „Kõik rakendused“

Rakenduste loend

See loend sisaldab teie arvutisse paigaldatud rakendusi. Iga loendis oleva rakenduse kohta saate vaadata järgmist teavet: seisund, digiallkiri, usaldusgrupp, populaarsus KSN-i kasutajate seas ja viimase käivitamiskorra aeg.

Rakenduse või protsessi rea topeltklõpsamise korral avaneb aken **Rakenduste reeglid**. Selles aknas saate seadistada rakenduse toimingute kontrollimise reeglid.

Rakenduse rea paremklõpsamise korral avaneb kontekstimenüü. Kontekstimenüüs saate teha järgmisi toiminguid.

- Saate avada akna **Rakenduste reeglid**, mis võimaldab seadistada rakenduste tegevuse õigused.
- Saate rakenduse käivitamise lubada või blokeerida.
- Saate teisaldada rakenduse muusse usaldusgruppi.
- Saate rakendusele rakendada rakenduste õiguste kontrolli vaikeseaded (rakenduse seaded lähtestada).
- Saate rakenduse loendist eemaldada.
- Saate avada rakenduse käivitusfaili sisaldava kausta.

Rakendused on loendis lisatud gruppidesse ja alamgruppidesse. Grupi rea paremklõpsamise korral avaneb kontekstimenüü. Kontekstimenüüs saate teha järgmisi toiminguid.

- Saate avada akna **Grupi reeglid**, mis võimaldab seadistada sellesse gruppi kuuluvate rakenduste toimingute vaikeõigused.
- Saate grupis luua alamgrupi. Vaikimisi rakendatakse alamgrupile selle grupi reeglid, millesse alamgrupp kuulub.
- Saate gruppi lisada rakenduse. Vaikimisi rakendatakse rakendusele selle grupi reeglid, millesse rakendus kuulub.
- Saate grupile ning kõigile alamgruppidele ja rakendustele rakendada rakenduste õiguste kontrolli vaikeseaded (grupi seaded lähtestada).
- Saate kõigile gruppi kuuluvatele alamgruppidele ja rakendustele rakendada rakenduste õiguste kontrolli vaikeseaded, kuid jätta grupi seaded muutmata (alamgrupi ja rakenduste seaded lähtestada).
- Saate grupist kustutada alamgrupid ja rakendused.

Rakendus

Selles veerus kuvatakse rakenduse nimi.

Seisund

Selles veerus kuvatakse rakenduse seisund: *käivitatud* või *peatatud*.

[Digiallkiri](#)

Selles veerus kuvatakse teave selle kohta, kas rakendus on digiallkirjastatud, ja digiallkirja omaniku kohta.

[Usaldusgrupp](#)

Selles veerus kuvatakse usaldusgrupp, kuhu rakendus kuulub. Usaldusgrupp määrab arvutis rakenduse kasutamise reeglid: keelab või lubab käivitamise, rakenduse juurdepääsu failidele ja süsteemiregistrile ning rakenduse võrgutegevuse piirangud.

[Populaarsus](#)

See veerg näitab rakenduse populaarsuse taset Kaspersky Security Networkis (KSN) osalejate seas. Populaarsuse tase kajastab rakendust kasutavate KSN-is osalejate arvu.

[Viimane käivitus](#)

Selles veerus kuvatakse rakenduse viimase käivituskorra aeg.

Aken „Ebatsensuurne sõnavara“

Leping

Sisaldab tingimusi, millele peate ebatsensuursete fraaside loendis muudatuste tegemiseks vastama.

Olen täisealine ja nõustun tingimustega

Ruudu märkimine tähendab tingimustega nõustumist. Selle ruudu märkimise korral saab redigeerida ebatsensuursete fraaside loendit.

Ruudust märke eemaldamise korral ei saa ebatsensuursete fraaside loendit redigeerida.

Aken „Rakendused, mille juurdepääs mikrofonile on blokeeritud“

Selles aknas kuvatakse rakendused, mille juurdepääsu mikrofonile olete blokeerinud.

[Luba juurdepääs mikrofonile](#)

Kui klõpsate seda nuppu, lubatakse loendis valitud rakendusel mikrofonile juurde pääseda.

Aken „Saada tagasisidet“

Probleem

Ripploend, millest saate valida tagasiside kategooria. Tagasiside kategooria võib olla seotud kaitstud veebilehitsejas avatud veebisaidi probleemiga.

- **Ma ei kasuta seda.** Valige see üksus, kui te ei kasuta turvaliste maksete komponenti või olete otsustanud turvaliste maksete komponendi kasutamisest loobuda.
- **Veebisait avaneb aeglaselt.** Valige see üksus, kui veebisaidi avamine võtab kauem aega kui tavaveebilehitsejas.
- **Kaitstud veebilehitseja käivitub, kui seda vaja pole.** Valige see üksus, kui kaitstud veebilehitsejas avanevad veebisaidid, mis ei nõua turvaliste maksete komponendi kasutamist.
- **Veebisaidi autoriseerimine ebaõnnestub.** Valige see üksus, kui kaitstud veebilehitsejas avatud veebisaidi autoriseerimiskatsetel ilmneb tõrkeid.
- **Veebisait kuvatakse valesti või see ei avane.** Valige see üksus, kui veebisait ei avata kaitstud veebilehitsejas või kui neid kuvatakse tõrgete või moonutustega.
- **Vead veebisaidi sertifikaadi kinnitamisel.** Valige see üksus, kui veebisaidi sertide valideerimisel kuvatakse tõrketeateid.
- **Ekraanipildi tegemine pole Kaitstud veebilehitseja töötamise ajal võimalik.** Valige see üksus, kui kaitstud veebilehitsejas ei looda ekraanipilte.
- **Vead klaviatuurilt või lõikelaualt andmete sisestamisel.** Valige see üksus, kui kaitstud veebilehitsejas andmete sisestamisel ilmnevad tõrked.
- **Kaitstud veebilehitsejas avatud veebilehte ei saa printida.** Valige see üksus, kui te ei saa printida veebisaidi avatud lehte.
- **Kuvatakse hoiatus, mis ütleb, et olulised operatsioonisüsteemi uuendused on paigaldamata.** Valige see üksus, kui kaitstud veebilehitseja käitamise ajal kuvatakse teade „Kriitilised süsteemi uuendused ei ole paigaldatud“.
- **Kaitstud veebilehitsejana töötab teine veebilehitseja.** Valige see üksus, kui kaitstud veebilehitseja avatakse muus veebilehitsejas kui selles, kus te selle käivitate.
- **Vead töötamisel.** Valige see üksus, kui kaitstud veebilehitseja kuvab tõrkeid, mis puuduvad sellest loendist.
- **Muu.** Valige see üksus, kui teised üksused ei sobi teie probleemi kirjeldamiseks.

Tagasiside kategooriat ei pea määrama.

Üksikasjad

Sellele väljale saate sisestada teavet, mis võib aidata Kasperskyl teie probleemi lahendada. See väli on valikuline.

Saada

Kasperskyle tagasiside saatmine

Turvaliste maksete komponendi toimimise kohta saate tagasisidet saata kuni 10 korda päevas. Kui rakendus ei saa teie tagasisidet saata (näiteks internetiühendus pole saadaval), salvestatakse tagasiside teie arvutisse. Tagasisidet talletatakse avalikult 30 päeva.

Rakenduse kasutamisest lapse poolt

Kui teie arvutisse on installitud rakendus Kaspersky Safe Kids ja kasutate seda, siis saab laps Kaspersky rakenduse abil rakenduse Kaspersky Safe Kids keelata. Selle vältimiseks soovitame [kaitsta juurdepääsu Kaspersky seadetele parooliga](#).

Kui logisite operatsioonisüsteemi sisse konto kaudu, mis on lingitud lapse profiiliga rakenduses Kaspersky Safe Kids, siis ei kuva Kaspersky järgmisi teateid.

- Teated turvauudiste kohta
- Teated operatsioonisüsteemi nõrkade seadete tuvastamise kohta
- Teated hetkel kasutatava seadme Wi-Fi-võrguga ühenduse loomise kohta
- Teated seadme koduse Wi-Fi-võrguga ühenduse loomise kohta
- Brauseri teated veebisaidile sisestatava liiga nõrga parooli kohta
- Teated, mis hoiatavad teid, et veebisaidile sisestatava parooli olete juba teisele veebisaidile sisestanud

Saate teated lubada, märkides märkeruudu **Kuva teateid laste kontodel aknas Seaded** → **Liides**.

Õigused

Parool kaitseb järgmisi rakenduse seadeid kasutaja või grupi tehtavate muudatuste eest. Kui on märgitud toimingu kõrval olev ruut, tähendab see, et kasutajal või kasutajagrupil on lubatud valitud toimingut teha.

Rakenduse seadete konfigureerimine	Rakenduse seadeid saate muuta peaaknas, aknas Seaded , teadete keskses ja teadetes. Rakenduse jäljejälituse lubamine ja keelamine.
Varundamise ja taastamise haldus	Varundamis- ja taastamistegumite loomine, muutmine ja eemaldamine.
Laste kaitsmise haldus	Blokeerige komponendi Host Intrusion Prevention abil rakenduse Kaspersky Safe Kids käivitamine, väljuge Kaspersky rakendusest või häälestage Kaspersky rakendus nii, et kaitse keelataks. Kaspersky Safe Kidsi allalaadimisel, paigaldamisel või käivitamisel parooli ei küsita.
Välju rakendusest	Rakendusest väljumine.
Eemalda / muuda / taasta rakendus	Rakenduse eemaldamine, muutmine ja taastamine.
Eemalda võti	Aktiveerimiskoodi ja varuaktiveerimiskoodi eemaldamine või muutmine.
Kuva aruanded	Avage aken Aruanded .
Kaitsekomponentide väljalülitamine	Keelake või lubage aknas Seaded kuvatavad kaitsekomponendid.

Veaotsing / pööra muudatused tagasi

Selles aknas kuvatakse analüüsi käigus tuvastatud operatsioonisüsteemirikete parandamise edenemine. Kahju parandamine võib aega võtta.

Kui tegite esimeses etapis valiku **Pööra muudatused tagasi**, pöörab Microsoft Windowsi veaotsingu nõustaja tagasi eelmises etapis valitud toimingud.


Tellimuse üksikasjade aken

Selles aknas kuvatakse rakenduse tellimuse kohta järgmine teave.

- Tellimuse olek
- Tellimuse kehtivuse lõpuni jäänud päevade arv
- Tellimusega kaetud seadmete arv
- Aktiveerimise kuupäev
- Tellimuse kehtivuse lõpukuupäev

VPN-i seadistamine valitud veebisaidi jaoks

Valitud veebisaidi jaoks VPN-i seadistamiseks tehke järgmist.

1. Avage rakenduse peaaaken.
2. Klõpsake rakenduse peaaeknas nuppu .
3. Valige **Seaded** → **Veebisaidid**.
4. Klõpsake nuppu **Seaded**.
Avatakse aken **Veebisaitidega ühenduse loomise reeglid**.
5. Klõpsake jaotises **Veebisaitide erandid** nuppu **Seaded**.
Avatakse aken **Veebisaitide erandid**.
6. Veebisaidikategooriate jaoks määratud seadete erandite loendisse veebisaidi lisamiseks klõpsake nuppu **Lisa**.
Avatakse aken **Veebisaidi lisamine**.
7. Sisestage väljale **Veebiaadress (URL)** veebisaidi aadress.
8. Määrake jaotises **Toiming veebisaidi avamisel** toiming, mille rakendus peab tegema veebisaidi külastamise korral.
 - **Aktiveeri VPN.** Rakendus lülitab VPN-i sisse, kui külastate määratud veebisaiti. Näiteks saate rakenduse seadistada VPN-i sisse lülitama siis, kui külastate oma panga veebisaiti. See säte rakendatakse isegi juhul, kui akna **Ignoreeri** jaotises **Ebaturvalisi pankade veebisaitide sirvides** on valitud **Veebisaitidega ühenduse loomise reeglid**.
 - a. Valige ripploendist **Valige VPN-server** piirkond ja linn, mille kaudu soovite selle veebisaidi külastamise korral luua VPN-ühenduse. Kui veebisaidi VPN-i jaoks valitud piirkond erineb veebisaidi kategooria jaoks valitud piirkonnast ja linnast, luuakse ühendus veebisaidiga sellele veebisaidile määratud piirkonna ja linna, mitte veebisaidikategooriale määratud piirkonna ja linna kaudu.
 - b. Märkige ruut **Teavita, kui on sisse lülitatud**, kui soovite saada teateid VPN-i lubamise kohta, kui külastate seda veebisaiti.
 - **Ignoreeri.** Rakendus ei lülita VPN-i sisse, kui külastate määratud veebisaiti.
9. Klõpsake **Lisa**.


Rakendus ei lülita VPN-i sisse, kui veebisaidiga ühenduse loomiseks kasutatakse HTTPS-protokolli.

[Tagasi Kaspersky VPN Secure Connectioni abi lehele](#) .

VPN-i seadistamine veebisaidikategooriate jaoks

Vaikimisi ei loo Kaspersky VPN veebilehitsejas veebisaitide avamise korral turvalist ühendust. VPN-i aktiveerimise saate seada eri veebisaidikategooriate jaoks, kui Kaspersky Plus või Kaspersky Premium on teie arvutisse installitud ja aktiveeritud. Näiteks saate määrata, et VPN tuleb lubada, kui külastate maksesüsteemide või suhtlusvõrkude veebisaite.

Veebisaidikategooriate jaoks VPN-i seadistamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Klõpsake rakenduse peaaknas nuppu .
3. Valige **Seaded** → **Veebisaidid**.
4. Klõpsake nuppu **Seaded**.
Avatakse aken **Veebisaitidega ühenduse loomise reeglid**.
5. Valige veebisaidikategooria.
 - Pangandusveebisaidid. Sellesse kategooriasse kuuluvad pankade veebisaidid.
 - Maksesüsteemid. Sellesse kategooriasse kuuluvad maksesüsteemide veebisaidid.
 - Veebimaksetega internetipoed. Sellesse kategooriasse kuuluvad sisseehitatud maksesüsteemidega veebikaupluste veebisaidid.
 - Suhtlusvõrgud. Sellesse kategooriasse kuuluvad suhtlusvõrkude veebisaidid.
6. Valige toiming, mis tehakse selle veebisaidikategooria külastamise korral.
 - **Aktiveeri VPN**. Selle kategooria veebisaitide külastamise korral aktiveerib rakendus VPN-i.
 - **Küsi**. Selle kategooria mis tahes veebisaidi külastamise korral küsib rakendus teilt, kas selle veebisaidi jaoks tuleb luua VPN. Valige veebilehitseja aknas sobiv toiming ja märkige ruut **Jäta selle veebisaidi valik meelde**. Rakendus teeb valitud toimingu iga kord, kui külastate seda veebisaiti. Kui ruutu ei märgita, jätab rakendus teie valiku meelde üheks tunniks.
 - **Ignoreeri**. Selle kategooria veebisaitide külastamise korral ei loo rakendus VPN-i.
7. Kui suvand **Aktiveeri VPN** on valitud, määrake ripploendis **Valige VPN-server** piirkond ja linn, mille kaudu soovite selle veebisaidikategooria korral VPN-ühenduse luua.
8. Märkige ruut **Teavita, kui on sisse lülitatud**, kui soovite saada teateid turvalise ühenduse lubamise kohta, kui külastate selle kategooria veebisaite.

Vaikimisi ei palu Kaspersky VPN Secure Connection teil VPN-i lubada, kui veebisaidiga ühenduse loomiseks kasutatakse HTTPS-protokolli.

[Tagasi Kaspersky VPN Secure Connectioni abi lehele](#) .

Sissetungitõrje

Jaotises **Rakendused** kuvatakse Kaspersky kontrollitavate rakenduste arv.

[Rakenduste haldus](#)

Selle lingi klõpsamisel avaneb aken **Rakenduste haldus**. Selles aknas saate määrata rakenduste usaldusgrupid, lubada või blokeerida rakenduste käivitamise ja avada valitud rakenduse õiguste seadistamiseks ette nähtud akna.

Jaotises **Praegune tegevus** kuvatakse teave praegu töötavate rakenduste ja protsesside arvu kohta. Graafilisel kujul on esitatud teave protsessori töökoormuse, RAM-i mahu, vaba kettaruumi ja võrgutegevuse kohta.

[Kuva tegevus](#)

Selle lingi klõpsamise korral avaneb aken **Rakenduste tegevus**, kus on kuvatud vahekaart **Käivitatud**. Selles aknas saate vaadata teavet iga praegu töötava rakenduse ressurssikasutuse kohta või avada valitud rakenduse õiguste seadistamiseks ette nähtud akna.

Sissetungitõrje välistamised

[Erandid](#)

Sisaldab isiklike andmetega ressursse, mis on sissetungitõrje kaitseulatusest välja jäetud. Ressurss võib olla fail, kaust või registrivõti.

[Ressurss](#)

Selles veerus kuvatakse ressursi nimi.

[Tee](#)

Selles veerus kuvatakse ressursi asukoht. Tee võib sisaldada maski.

[Seisund](#)

See veerg sisaldab ressursi seisundivalikute ripploendit.

- **Lülita kontroll sisse.** Selle valiku korral kontrollib rakendus ressursikohast tegevust.
- **Lülita kontroll välja.** Selle valiku korral ei kontrolli rakendus ressursikohast tegevust.

Ressursside kontrollimise lubamiseks või keelamiseks vasakklõpsake ripploendis seisundi ikooni.

[Lisa](#)

Selle nupu klõpsamise korral avaneb aken, kus saate määrata isiklike andmetega ressursi, mille lisate loendisse.

[Muuda](#)

Selle nupu klõpsamise korral avaneb aken **Faili või kausta muutmine / Registrivõtme muutmine**. Selles aknas saate muuta ressursi seadeid.

Vaikimisi loendisse lisatud ressursse ei saa muuta.

[Kustuta](#)

Selle nupu klõpsamise korral eemaldatakse valitud ressursid loendist.

Vaikimisi loendisse lisatud ressursse ei saa kustutada.

Vahekaart „Üldine“

[Vahekaart „Üldine“](#) 

Valitud rakendusegrupi kirjeldus.

Vahekaart „Ressursid“

See vahekaart võimaldab teil valida süsteemiressursse või kasutajaressursse ja muuta rakenduste õigust neid ressursse kasutada.

Nupp

Seda nuppu saab kasutada reegliseadete paneeli kuvamiseks või peitmiseks.

Vaade

Selles ripploendis on kaks valitavat ressurside filtreerimisvalikut.

- **Varja süsteemirakendused.** Selle valiku korral peidetakse ressurside loendis süsteemirakenduste ressursid.
- **Varja <PRODUCT>.** Selle valiku korral peidetakse loendis Kaspersky ressursid.

Operatsioonisüsteem

See loend sisaldab valitud kategooria operatsioonisüsteemiseadeid ja ressursse. Ressurss võib olla fail, kaust, registrivõti, võrguteenus või IP-aadress. Sissetungitõrje jälgib teiste rakenduste juurdepääsu loendis olevatele ressursidele.

Vaikimisi sisaldab loend **Operatsioonisüsteem** järgmisi objekte.

- Käivituse seadeid sisaldavad registrivõtmed
- Internetikasutuse seadeid sisaldavad registrivõtmed
- Operatsioonisüsteemi turvalisust mõjutavad registrivõtmed
- Süsteemiteenuse seadeid sisaldavad registrivõtmed
- Süsteemifailid ja -kaustad
- Käivituskaustad

Isiklikud andmed

Sisaldab kasutaja isiklike andmeid, mis on sortitud ressurside ja kategooriate alusel. Ressurss võib olla fail või kaust. Sissetungitõrje analüüsib toiminguid, mida teised rakendused teevad loendis olevate ressursidega.

Vaikimisi sisaldab isiklike andmete loend järgmisi objekte.

- Kasutaja failid (kaust „Minu dokumendid“, küpsisefailid, teave kasutaja tegevuse kohta)
- Failid, kaustad ja registrivõtmed, mis sisaldavad kõige sagedamini kasutatavate rakenduste seadeid ja olulisi andmeid: veebilehitsejad, failihaldurid, meilikliendid, sõnumsidekliendid ja elektroonilised rahakotid.

Ressurss

Selles veerus kuvatakse sissetungitõrje kaitstava operatsioonisüsteemiressursi nimi.

[Tee](#)

Selles veerus kuvatakse ressursi asukoht. Tee võib sisaldada maski.

[Seisund](#)

See veerg sisaldab ressursi seisundivalikute ripploendit.

- **Lülita kontroll sisse.** Selle valiku korral kontrollib rakendus ressursikohast tegevust.
- **Lülita kontroll välja.** Selle valiku korral ei kontrolli rakendus ressursikohast tegevust.

Ressursside kontrollimise lubamiseks või keelamiseks vasakklõpsake ripploendis seisundi ikooni.

[Lisa](#)

Selles ripploendis saate lisada ressursikategooria, ressurssidega faili või kausta või süsteemi registrivõtme.

[Muuda](#)

Selle lingi klõpsamise korral avaneb aken, kus saate muuta valitud ressursi nime ja teed.

[Kustuta](#)

Selle lingi klõpsamise korral eemaldatakse loendist valitud ressursikategooria, ressurssidega fail või kaust või süsteemi registrivõti. Sissetungitõrje ei kontrolli enam teiste rakenduste juurdepääsu sellele ressursile.

[Taasta](#)

Selles ripploendis saate teha ühe järgmistest valikutest.

- **kategooria seaded.** Selle valiku korral määratakse valitud kategooria seadetele vaikeväärtused.
- **alamgruppide ja ressursside seaded.** Selle valiku korral määratakse kategooriasse kuuluvate alamgruppide ja ressursside seadetele vaikeväärtused.

[Rakenduste loend](#)

Selles loendis kuvatakse usaldusgrupid ja neisse usaldusgruppidesse kuuluvad rakendused. Rakenduse või rakendusegrupi juurdepääsuõigused valitud ressursile määravad veerud **Loe**, **Kirjuta**, **Loo** ja **Kustuta**.

Allolevas tabelis on esitatud Kaspersky toimingud juhul, kui rakendus või rakendusegrupp proovib ressursile juurde pääseda.

Kaspersky toimingute kirjeldus

Toiming	Kirjeldus
Päranda	Rakendus või grupp pärib vastuse emagrupilt.
Luba	Kaspersky lubab valitud gruppi kuuluvatel rakendustel ressursile juurde pääseda.
Keela	Kaspersky ei luba valitud gruppi kuuluvatel rakendustel ressursile juurde pääseda.
Küsi kasutajalt	<p>Kui ruut Tee soovitatavad toimingud automaatselt jaotises Seaded → Jõudlusseaded → Arvutiressursside kasutus on märgitud, siis valib Kaspersky ressursi korral tehtava toimingu automaatselt Kaspersky ekspertide loodud reeglite põhjal. Soovi korral saate allmärgusest teada, missugune toiming täpselt valitakse.</p> <p>Ruudust märke eemaldamise korral küsib Kaspersky kasutajalt, kas lubada sellel rakendusel ressursile juurde pääseda või mitte.</p>
Logi sündmusi	Lisaks määratud vastusele logib Kaspersky teabe rakenduse katsete kohta ressursile juurde pääseda ja salvestab selle teabe aruandesse.

Aken „Lõppkasutaja litsentsileping“

Aken sisaldab lõppkasutaja litsentsilepingu teksti. Lõppkasutaja litsentsilepingu lugemiseks kasutage kerimisriba.

Aken „Litsents“

Tellimuse üksikasjad kuvatakse akna ülaservas asuvas jaotises.

- Tellimuse olek
- Tellimuse kehtivuse lõpuni jäänud päevade arv

[Teave litsentsi kohta / Tellimuse teave](#)

Selle lingi klõpsamisel avaneb aken, mis sisaldab teavet praeguse tellimuse kohta.

[Ava My Kaspersky](#)

Selle nupu klõpsamisel avaneb vaikebrauseris My Kaspersky leht.

[Lõppkasutaja litsentsileping](#)

Selle nupu klõpsamise korral avaneb aken, kus kuvatakse litsentsilepingu tekst.

Tellimuse olemasolust ja teie rakenduse versiooni omadustest olenevalt võib aken kuvada mitmesuguseid nuppe, mis on ette nähtud teie tellimusega seotud toimingute algatamiseks. Vaikenuppe on kirjeldatud allpool.

[Uuenda tellimust](#)

Selle nupu klõpsamine avab veebilehitsejas veebipoe, kust saate osta tellimuse.

Nupp muutub nähtavaks, kui tellimus on aegunud või aegub peagi.

[Osta tellimus](#)

Selle nupu klõpsamine avab veebilehitsejas veebipoe, kust saate osta tellimuse.

See nupp on saadaval, kui tellimus on blokeeritud või prooviversioon on aegunud.

[Uuenda andmebaase](#)

Selle nupu klõpsamise korral käivitatakse rakenduste andmebaaside uuendamine.

See nupp on saadaval, kui praeguse litsentsiga seotud probleeme saab lahendada andmebaaside uuendamise teel (näiteks juhul, kui andmebaaside väljalaskeaeg ei ühti litsentsi lõpukuupäevaga).

[Põhjused ja võimalikud lahendused](#)

Selle nupu klõpsamine avab veebilehitseja akna, mis kuvab tehnilise toe veebisaidil lehe, mis sisaldab teavet ilmnenud probleemi kohta.

See nupp on saadaval, kui ilmnevad probleemid seoses tellimusega.

[Uuenda seisundit](#)

Selle nupu klõpsamise korral laaditakse teenusepakkuja serverist alla ajakohane teave tellimuse seisundi kohta. See nupp kuvatakse, kui rakendust kasutatakse tellimuse alusel.

Muud tuvastatud ühildumatud rakendused

[Ühildumatute rakenduste loend](#)

Loend sisaldab rakendusi, mis ei ühildu paigaldatava rakendusega. Paigaldatava rakenduse nõuetekohaseks toimimiseks eemaldage ühildumatud rakendused.

[Eemalda käsitsi](#)

Selle nupu klõpsamise korral avaneb aken, mis sisaldab arvutisse paigaldatud rakenduste loendit. Selles loendis saate valida rakendused, mis ei ühildu installitava rakendusega, et need arvutist eemaldada.

[Jätka](#)

Selle nupu klõpsamise korral jäetakse loendis kuvatud ühildumatud rakendused arvutisse alles ja nõustaja jätkab tööd.

Ühildumatute rakenduste ja paigaldatava rakenduse kooskasutamine võib põhjustada häireid paigaldatava rakenduse töös ja oluliselt kahjustada teie arvuti kaitset.

Leiti ühildumatu tarkvara

Ühildumatute rakenduste loend [?](#)

Loend sisaldab rakendusi, mis ei ühildu paigaldatava rakendusega. Paigaldatava rakenduse nõuetekohaseks toimimiseks eemaldage ühildumatud rakendused.

Kustuta [?](#)

Selle nupu klõpsamise korral eemaldatakse loendis kuvatud ühildumatud rakendused teie arvutist ja nõustaja jätkab tööd.

Jäta [?](#)

Selle nupu klõpsamise korral jäetakse loendis kuvatud ühildumatud rakendused arvutisse alles ja nõustaja jätkab tööd.

Ühildumatute rakenduste ja paigaldatava rakenduse kooskasutamine võib põhjustada häireid paigaldatava rakenduse töös ja oluliselt kahjustada teie arvuti kaitset.

Vajalik on arvuti taaskäivitus

Taaskäivita arvuti

See märkeruut lubab/keelab arvuti taaskäivitamise. Ülemineku nõustaja töö jätkamiseks tuleb arvuti taaskäivitada.

Kui see ruut on märgitud, taaskäivitatakse arvuti pärast nupu **Valmis** klõpsamist, misjärel jätkab ülemineku nõustaja tööd.

Kui sellest ruudust on mäрге eemaldatud, siis arvutit ei taaskäivitata. Ülemineku nõustaja jätkab tööd automaatselt pärast arvuti taaskäivitamist või välja- ja sisselülitamist.

Alustamine

[Näita sertifikaadi infomatsiooni](#)

See link avab akna, mis kuvab teabe Kaspersky sertifikaadi kohta.

[Edasi](#)

Selle nupu klõpsamise korral käivitatakse sertifikaadi paigaldusnõustaja.

Sertifikaadi paigaldus

Selles aknas kuvatakse sertifikaadi automaatse paigaldamise edenemine. Tegumi lõpuleviimine võib pisut aega võtta.

Kaspersky otsib kasutaja arvutisse installitud veebibrausereid ja installib seejärel sertifikaadid automaatselt Microsoft Windowsi sertifikaadisalve.

Sertifikaadi paigaldamise ajal võib ekraanile ilmuda Microsoft Windowsi turvahoiautus, mis palub teil sertifikaadi paigaldamise kinnitada.

Nõustaja lõpuleviimine

[Valmis](#) 

Selle nupu klõpsamise korral sulgeb Kaspersky Sertifikaatide paigaldusnõustaja.

Jaotis „Blokeeritud arvutid“

[Blokeeritud arvutid](#)

Sisaldab teavet nende arvutite kohta, mille korral võrgurünnakute tõrje on keelanud kogu teie arvutile sihitud võrgutegevuse.

[Arvuti aadress](#)

Selles veerus kuvatakse blokeeritud arvuti IP-aadress.

[Aeg, millal blokeerimine algas](#)

Selles veerus kuvatakse arvuti blokeerimisest möödunud aeg.

Vaikimisi blokeerib võrgurünnakute tõrje ründavast arvutist sissetuleva liikluse üheks tunniks.

Loendist valitud arvuti blokeeringu eemaldamiseks avage selle kontekstimenüü.

[Eemalda blokeerimine](#)

Selle nupu klõpsamise korral eemaldab võrgurünnakute tõrje valitud arvuti blokeeringu.

[Eemalda blokeerimine kõigilt arvutitelt](#)

Selle lingi klõpsamise korral eemaldab võrgurünnakute tõrje kõigi blokeeritud arvutite blokeeringu.

Jaotis „Avatud pordid“

Vaade [?](#)

Selle nupu klõpsamise korral avaneb menüü, mis sisaldab järgmisi üksusi.

- **Näita kõiki porte** – loendis kuvatakse kõik arvuti avatud pordid.
- **Peida loopback-porte** – loendis kuvatakse kõik pordid, välja arvatud need, mida kasutab teie operatsioonisüsteemi võrgutarkvara.

Avatud pordid [?](#)

Sisaldab teavet iga protsessi kõigi avatud portide kohta.

Iga pordi kohta kuvatakse järgmine teave.

- Pordi number
- Porti kasutava protsessi (rakenduse, teenuse, serveri) nimi
- Protsessi ID
- Protsessi kohalik IP-aadress
- Pordi kaudu loodud ühenduse protokoll

Loendirea topeltklõpsamise korral avaneb aken **Rakenduste reeglid**, milles on kuvatud vahekaart **Võrgureeglid**. Selles aknas saate seadistada valitud porti kasutava rakenduse võrgureeglid.

Loendiüksuse paremklõpsamise korral avaneb kontekstimenüü, kus saate seadistada võrgureegleid.

Menüü sisaldab järgmisi üksusi.

- **Rakenduste võrgureeglid**. Selle menüüelemendi valimine avab vahekaardil **Rakenduste reeglid** akna **Võrgureeglid**. Selles aknas saate seadistada loendist valitud porti kasutava rakenduse võrgureegli.
- **Kõik võrgureeglid**. Selle menüüelemendi valimine avab akna **Paketireeglid**. Selles aknas saate seadistada loendist valitud porti kasutava rakenduse paketireegleid.

Jaotis „Võrgutegevus“

Vaade [?](#)

Selle nupu klõpsamise korral avaneb menüü. Menüü sisaldab järgmisi üksusi.

- **Näita kohalikke ühendusi** – loendis kuvatakse teave ühenduste kohta, mille teie arvuti on teiste arvutitega loonud samas kohtvõrgus.
- **Näita <PRODUCT> ühendusi** – loendis kuvatakse teave Kaspersky loodud ühenduste kohta.

Võrgutegevus [?](#)

See loend sisaldab kõiki teie arvutis praegu loodud aktiivseid võrguühendusi.

Iga ühenduse kohta kuvatakse järgmine teave.

- Ühenduse algatanud protsessi (rakenduse, teenuse, serveri) nimi
- Ühenduse suund (sissetulev/väljaminev)
- Ühendusprotokoll
- Ühenduse seaded (kaugport ja IP-aadress)
- Edastatud/vastuvõetud andmete hulk (kilobaitides)

Loendiüksuse paremklõpsamise korral avaneb kontekstimenüü, kus saate seadistada võrgureegleid.

Menüü sisaldab järgmisi üksusi.

- **Rakenduste võrgureeglid.** Selle menüüelemendi valimine avab vahekaardil **Rakenduste reeglid** akna **Võrgureeglid**. Selles aknas saate seadistada loendist valitud rakenduse võrgureegli.
- **Kõik võrgureeglid.** Selle menüüelemendi valimine avab akna **Paketireeglid**. Selles aknas saate seadistada loendist valitud rakenduse paketireeglid.

Blokeeri kogu võrgutegevus [?](#)

Lingi klõpsamise korral blokeerib tulemüüri kõigi protsesside võrgutegevuse.

Akna allservas kuvatakse võrguliikluse tabel, mis näitab loendist valitud protsessi sissetuleva ja väljamineva liikluse mahtu. Tabel kajastab liikluse mahtu reaajas. Liikluse maht kuvatakse kilobaitides.

Erikaalutlused võrguadapteri jaoks reegli lisamise korral

Kui loote võrgukaardi lubamisreegli ja/või määratud TTL-iga reegli, võib see reegel olla vastuolus rakenduste keelamisreegliga. Näiteks juhul, kui rakendus on grupis „Tugevad piirangud“, keelatakse sellel võrgule juurde pääseda isegi siis, kui olete loonud võrguadapteri (ja TTL-i) jaoks lubamise paketireegli.

Et seadistada lubamisreegel, mis töötab kõigi rakenduste korral, mis proovivad luua võrguga ühendust selle võrguadapteri kaudu, tuleb teil luua järgmised tähtsuse järjekorras esitatud reeglid (paketireeglite üldises loendis määratakse tähtsus kindlaks ülevalt allapoole, mis tähendab, et kõige ülemisel kirjel on suurim tähtsus ja kõige alumisel väiksem).

1. Valitud võrguadapteri lubamisreegel.
2. Kõigi muude võrguadapterite keelamisreeglid.
3. Lubamisreegel ilma võrguadapterit määramata.

TTL-i kasutava võrguadapteri jaoks lubamisreegli seadistamiseks tuleb teil luua järgmised tähtsuse järjekorras esitatud reeglid.

1. Konkreetse TTL-väärtuse lubamisreegel.
2. 255-ga võrduva TTL-väärtuse keelamisreegel.
3. Lubamisreegel ilma TTL-väärtust määramata.

Jaotis „Võrguliiklus“

Periood

Loend sisaldab võrguliikluse jaotuse kuvamiseks ette nähtud ajavahemikke.

Saadaval on järgmised väärtused.

- **Üheks päevaks.** Selles loendis kuvatakse andmed käesoleva päeva võrguliikluse jaotuse kohta.
- **Eile.** Selles loendis kuvatakse andmed eelmise päeva võrguliikluse jaotuse kohta.
- **Kuu jooksul.** Selles loendis kuvatakse andmed käesoleva kuu võrguliikluse jaotuse kohta.
- **Aasta jooksul.** Selles loendis kuvatakse andmed käesoleva aasta võrguliikluse jaotuse kohta.

Võrguliiklus

Sisaldab teavet kõigi teie arvuti ja teiste arvutite vahel loodud sissetulevate ja väljaminevate ühenduste kohta.

Iga rakenduse (arvuti, teenuse, serveri, protsessi) kohta kuvatakse sissetuleva ja väljamineva liikluse hulk.

Loendis kuvatava rakenduse topeltklõpsamise korral avaneb aken **Rakenduste reeglid**, milles on kuvatud vahekaart **Võrgureeglid**. Selles aknas saate seadistada valitud rakenduse võrgureeglid.

Loendiüksuse paremklõpsamise korral avaneb kontekstimenüü, kus saate seadistada võrgureegleid.

Menüü sisaldab järgmisi üksusi.

- **Rakenduste võrgureeglid.** Selle üksuse valimine avab akna **Rakenduste reeglid** vahekaardi **Võrgureeglid**, kus saate seadistada valitud rakenduse võrgureegli.
- **Kõik võrgureeglid.** Selle üksuse valimine avab akna **Paketireeglid**, kus saate seadistada valitud rakenduse paketireeglid.

Akna allservas kuvatakse diagramm, mis näitab määratud ajavahemikus valitud rakenduse liikluse jaotust aja jooksul.

Võrguühenduste katkestamine

Kui arvuti lülitatakse välja või kaitse peatatakse, kui rakendus jälgib aktiivseid võrguühendusi, kuvatakse teade nende ühenduste katkestamise kohta. See on vajalik rakenduse nõuetekohaseks sulgemiseks. Katkestamine toimub automaatselt 10 sekundi pärast või pärast nupu **Jah** klõpsamist. Enamik katkestatud ühendusi taastatakse lühikese aja jooksul.

Kui ühendus katkeb ajal, mil laadite alla faili ilma allalaadimishaldurita, katkestatakse andmeedastus. Faili allalaadimiseks tuleb allalaadimist uuesti alustama.

Ühenduste katkestamise saate tühistada. Selleks klõpsake teate dialoogiboksis nuppu **Ei**. Rakendus jätkab tööd.

Teave VPN-i täpsemate valikute kohta

VPN-i lisafunktsioonid on saadaval, kui arvutisse on paigaldatud Kaspersky Plus või Kaspersky Premium.

VPN-i lisafunktsioonid on järgmised.

- VPN-i lubamise seaded järgmiste veebisaidikategooriate külastamise korral.
 - pangandusveebisaidid;
 - maksesüsteemid;
 - E-poed ja e-kaubanduse veebisaidid;
 - Suhtlusvõrgud.
- Piirkonna ja linna automaatse vahetamise sätted. Kui määrasite VPN-i sätetes eri kategooriate veebisaitide jaoks eri piirkonnad ja linnad, saate määrata, kas eri kategooriatesse kuuluvate veebisaitide vaheldumisi sirvimise korral tuleb piirkonda ja linna vahetada või mitte.
- VPN-i seaded üksikute veebisaitide jaoks, näiteks sageli külastatavate veebisaitide jaoks.


[Tagasi Kaspersky VPN Secure Connectioni abi lehele](#) .

Avastatud objektid

Lahenda

Selle nupu klõpsamise korral alustab Kaspersky rakendus avastatud objekti töötlemist.

See nupp on saadaval objekti avastamise korral.

Nupu  klõpsamise korral avaneb menüü, kust saate valida soovitud lisatoimingu.

- Käsk **Lisa eranditesse** loob erandi, mille kohaselt ei tohi objekti pahatahtlikuks lugeda.
- Käsk **Ignoreeri** teisaldab teate jaotisse **Ignoreeritud teatised**.
- Käsk **Ava sisaldav kaust** avab kausta, mis algselt faili sisaldas.
- Link **Lisainfo** avab avastatud objekti kirjeldust sisaldava veebilehe.

Kaspersky teateaknad

Tegumiriba teavitusalas kuvatavad teated teavitavad teid rakenduse sündmustest, mis vajavad teie sekkumist. Kui ekraanil kuvatakse teade, tuleb teil teha üks teates pakutavatest valikutest. Optimaalne valik on see, mida Kaspersky eksperdid soovivad vaikevalikuna.

Teave pilvekaitse kohta

Sellest aknast leiate teavet Kaspersky Security Networki kohta.

Aken „Aktiveerimine“

Selles aknas kuvatakse rakenduse aktiveerimise edenemine.

[Tühista](#)

Selle nupu klõpsamise korral saate rakenduse aktiveerimise tühistada.

Registreerimine ja autoriseerimine

[Meiliaadress](#)

Sellele väljale saate sisestada meiliaadressi, et luua ühendus oma My Kaspersky halduskonsooli kontoga või luua uus konto.

[Logi sisse Google'iga](#)

Selle nupu klõpsamine viib teid teie vaikebrauseris Google'i kontole sisselogimise vormile (ei ole saadaval kõigis piirkondades).

[Logi sisse Facebookiga](#)

Selle nupu klõpsamine viib teid teie vaikebrauseris Facebooki kontole sisselogimise vormile (ei ole saadaval kõigis piirkondades).

[Logi sisse Apple'iga](#)

Selle nupu klõpsamine viib teid teie vaikebrauseris Apple'i kontole sisselogimise vormile.

[Mul on aktiveerimiskood](#)

Klõpsamine sellel lingil viib teid aktiveerimiskoodi sisestamise vormile.

[Jätka](#)

Sellel nupul klõpsates avaneb vorm, kuhu saate sisestada My Kaspersky halduskonsooli konto parooli või alustada uue konto loomist.

My Kaspersky halduskonsooli kontole sisselogimisel näitab aken järgmist.

[Parool](#)

Sisestage sellele väljale oma My Kaspersky halduskonsooli konto parool.

[Unustasite oma parooli?](#)

Avage oma My Kaspersky konto unustatud parooli taastamise aken.

[Sisestage teine meiliaadress](#)

Sellel nupul klõpsates avaneb uuesti meiliaadressi sisestamise vorm.

[Logi sisse](#)

Sellel nupul klõpsamine ühendab seadme teie My Kaspersky halduskonsooli kontoga.

My Kaspersky halduskonsooli konto loomise ajal näitab aken järgmist.

[Nõustun Kasperskyle isikupärastatud turunduspakkumiste saamise eesmärgil oma meiliaadressi andma](#)

Kui ruut on märgitud, saadetakse sisestatud meiliaadressile Kaspersky uudiseid.

[Piirkond](#)

Selle lingi klõpsamise korral avaneb piirkonna valimise aken. Paigaldatavad rakendused ja saadaolevad makseviisid olenevad teie valitud piirkonnast.

[Sisestage teine meiliaadress](#)

Sellel nupul klõpsates avaneb uuesti meiliaadressi sisestamise vorm.

[Loo](#)

Selle nupu klõpsamisel registreeritakse My Kaspersky konto. Teie määratud meiliaadressile saadetakse sõnum My Kaspersky halduskonsooli konto parooli loomise lingiga.

[Lisateave My Kaspersky konto kohta](#)

Aken „Võtme valimine registrist“

[Vali](#) 

Selle nupu klõpsamise korral täidetakse akna **Registrivõtme lisamine** väljad valitud võtme väärtustega.

Aken „Salahoidla asukoha valimine“

Selles aknas saate valida loodava salahoidla asukoha.

Vali 

Selle nupu klõpsamise korral saate kinnitada, et määratud tee on õige.

Aken „Faili või kausta valimine“

Vali 

Selle nupu klõpsamise korral kuvatakse akna **Tee väljal Faili või kausta lisamine** faili või kausta tee.

Aken „Usaldusgrupp tundmatutele rakendustele“

Selles aknas kuvatakse rakendused, mida ei saanud lisada olemasolevatesse gruppidesse. Saate valida usaldusgrupi ja klõpsata nuppu **Salvesta**. Rakendused, mida ei saanud lisada teistesse gruppidesse, lisatakse teie määratud gruppi.

Vaikimisi lisatakse need rakendused gruppi **Nõrgad piirangud**.

Aken „Usaldusgrupp rakendustele, mis käivituvad enne kui Kaspersky“

Selles aknas saate valida usaldusgrupi tundmatutele rakendustele, mis käivituvad enne kui Kaspersky rakendus.

[Usaldusgruppide loend](#)

Selle loendi abil saate määrata usaldusgrupi, millesse tuleb määrata enne Kaspersky rakendust käivituvad rakendused. Selliste rakenduste võrgutegevust piiratakse valitud usaldusgrupi reeglite kohaselt. Vaikimisi piiratakse enne Kaspersky rakenduse käivitamist käivituvate rakenduste võrgutegevust Kaspersky ekspertide määratud reeglite kohaselt.

[Vali usaldusgrupp automaatselt](#)

Selle valiku korral lisab komponent Sissetungitõrje enne Kaspersky rakenduse käivitamist käivituvad rakendused usaldusgruppi Kaspersky ekspertide loodud reeglite põhjal.

[Vali usaldusgrupp käsitsi](#)

Selle valiku korral saate käsitsi valida usaldusgrupi, kuhu tuleb lisada enne Kaspersky rakenduse käivitamist käivituvad rakendused.

Privaatse sirvimise erandi lisamise/muutmise aken

Veebiaadressi mask

Sisestage sellele väljale veebisaidi, kus soovite lubada oma veebitegevuse jälgimise, IP-aadress või veebiaadress (URL).

Kategooria lisamise/muutmise aken

Kategooria nimi [?](#)

Sellel väljal saate määrata ressursikategooria nime; sissetungitõrje analüüsib ja kontrollib juurdepääsu sellele ressursikategooriale.

Registrivõtme lisamise/muutmise aken

[Vali](#)

Selle nupu klõpsamise korral avaneb aken **Võtme valimine registrist**, kus saate valida registrivõtme, millele juurdepääsu peab haldama sissetungitõrje komponendi kaudu.

[Nimi](#)

Sellele väljale saab sisestada registrivõtme ressursi nime.

[Tee võtmeni](#)

Sellele väljale saab sisestada registrivõtme tee.

[Kaitse võtme väärtust](#)

Kui see ruut on märgitud, kaitstakse muutmise eest ainult väljale **Võtme väärtus** sisestatud võtmeväärtust.

Kui ruut on märkimata, kaitstakse selle registrivõtme kõiki väärtusi.

Kui väljale **Võtme väärtus** ei ole väärtust sisestatud, kaitstakse vaikimisi registrivõtme vaikeväärtust.

See ruut märgitakse registrivõtme valimise korral automaatselt.

[Võtme väärtus](#)

Sellele väljale saate sisestada registrivõtme väärtuse, mida sissetungitõrje komponent peab muudatuste eest kaitsma.

Seda välja saab muuta, kui märgitud on ruut **Kaitse võtme väärtust**.

[Lisa](#)

Selle nupu klõpsamise korral lisatakse registrivõti ressursside loendisse.

Aken „Ebatsensuurse sõna lisamine/muutmine“

[Ebatsensuurse sõna mask](#)

Sõna või sõnamask, mida peetakse sõnumis tuvastamise korral rämpsmeili tunnuseks.

[Ebatsensuurse sõna kaalukoeffitsient](#)

Arvväärtus, mis tähistab tõenäosust, et roppsõna sisaldav sõnum on rämpsmeil. Mida suurem on kaalukoeffitsient, seda suurem on tõenäosus, et roppsõna sisaldav sõnum on rämpsmeil.

Rämpsmeilifilter märgib sõnumi rämpsmeiliks, kui selles sisalduvate roppsõnade ja blokeeritud fraaside kaalukoeffitsientide summa ületab määratud väärtust.

[Olek](#)

Jaotises **Olek** saate määrata, kas rämpsmeilifilter otsib sõnumitest roppsõna.

- **Aktiivne.** Rämpsmeilifilter kontrollib, kas sõnumites sisaldub roppsõna.
- **Mitteaktiivne.** Rämpsmeilifilter ei kontrolli, kas sõnumites sisaldub roppsõna.

Faili või kausta lisamise/muutmise aken

Nimi [?](#)

Sellel väljal saate määrata selle ressursi nime, mille failile või kaustale juurdepääsu peab sissetungitõrje haldama.

Tee [?](#)

Sellele väljale saate käsitsi sisestada faili- või kaustatee.

Tee käsitsi sisestamisel saate kasutada maski.

Maski `*` abil saate määrata juurdepääsukontrolli valitud kausta kõigile failidele ja alamkaustadele.

Maski `*<failinimelaiend>` abil saate määrata juurdepääsukontrolli valitud kausta kõigile failidele, millel on sisestatud failinimelaiend.

Samuti saate kontrollida rakenduste juurdepääsu kaugarvutis asuvatele failiressurssidele. Selleks sisestage võrguressursi tee UNC-vormingus reegli `\\Server\Ühiskaust\Suhteline` tee kohaselt, mille osadel on järgmine tähendus.

- „Server“ on arvuti domeeninimi või IPv4- või IPv6-vormingus IP-aadress (nõutav).
- „Ühiskaust“ on ühiskausta võrgunimi (nõutav).
- „Suhteline tee“ on kausta- või failitee alates ühiskaustast (valikuline).
Näidisteed on järgmised.
- `\\Server1\Ühiskaust1\test\näide.exe`
- `\\Server1\Ühiskaust1\test*.docx`
- `\\Server1\Ühiskaust1*`

Rakendus ei kontrolli juurdepääsu failiressurssile, kui reeglis määratletud tee erineb taotletud teest.

Vali [?](#)

Selle nupu klõpsamise korral avaneb aken, kus saate valida faili või kausta.

Lisa [?](#)

Selle nupu klõpsamise korral lisatakse fail või kaust ressursside loendisse.

Aken „Aktiveerimine lõppes“

See aken avaneb, kui rakendus on edukalt aktiveeritud.

Valmis 

Selle nupu klõpsamise korral viiakse rakenduse aktiveerimine lõpule ja avatakse litsentsimisaken.

Aken „Blokeeritud ja lubatud rakendused“

Selles aknas kuvatakse loend rakendustest, millel on lubatud või keelatud muuta operatsioonisüsteemi seadeid. Tühi loend tähendab, et te pole operatsioonisüsteemi seadete muutmist veel ühegi rakenduse jaoks lubanud ega blokeerinud.

[Rakenduste loend](#)

Rakenduste loend sisaldab järgmisi andmeid.

- **Rakendus.** Selles veerus kuvatakse rakenduse nimi.
- **Faili nimi.** Selles veerus kuvatakse rakenduse käivitusfaili nimi.
- **Tee.** Selles veerus kuvatakse teie arvuti kõvakettal oleva rakenduse käivitusfaili tee.
- **Tootja.** Selles veerus kuvatakse rakenduse väljaandja digiallkiri.
- **Muudatused.** Selles veerus kuvatakse, kas operatsioonisüsteemi seadete, veebilehitseja seadete ja võrguseadete muutmine on rakenduse jaoks blokeeritud või lubatud.

Aken „Privaatsuse kaitse“

Selles aknas saate lülitada sisse või välja järgmised komponendid.

[Veebikaamera ja mikrofoni kontroll](#)

[Andmelekkekontroll](#)

[Privaatne sirvimine](#)

Rakenduseuuendaja. Erandid

Erandid

Paigaldatud rakenduste vahelejäetud uuendused lisatakse loendisse **Erandid**. Saate vahele jätta nii üksikuid uuendusi kui ka kindla arvutisse paigaldatud rakenduse kõik uuendused.

Loend **Erandid** koosneb järgmistest veergudest.

- **Rakendus** – selles veerus kuvatakse rakenduse nimi.
- **Jäta vahele** – see veerg võib sisaldada järgmisi väärtusi.
 - **Uuenduse versioon** – see kuvatakse, kui olete vahele jätnud paigaldatud rakenduse üksiku uuenduse.
 - **Kõik uuendused** – see kuvatakse, kui olete otsustanud rakendust mitte uuendada.

Kustuta

Selle nupu klõpsamise korral eemaldatakse valitud rakendused erandite loendist. Nupp on saadaval, kui loendist on valitud rakendus.

Kaspersky teavitab teid loendist eemaldatud rakendustele saadaolevatest värskendustest.

Aken „Privaatse sirvimise erandid“

[Erandite loend](#)

See loend sisaldab nende veebisaitide aadresse, kus on lubatud jälgida teie veebitegevust. Nendel veebisaitidel tuvastab privaatse sirvimise komponent andmekogumiskatseid, kuid ei blokeeri neid isegi juhul, kui komponent on seadistatud blokeerima neisse kategooriatesse kuuluvate jälgimisteenuste andmekogumist.

Loendisse saate lisada veebiaadressi või aadressimaski.

[Muuda](#)

See avab akna, kus saate muuta valitud veebiaadressi / veebiaadressi maski.

[Kustuta](#)

Eemaldab valitud veebiaadressi / aadressimaski loendist

[Lisa](#)

See avab akna, kus saate lisada veebiaadressi / veebiaadressi maski.

Aken „Rakenduse kasutus“

Rakendused

Veerg näitab rakendusi ja rakendusegruppe, mille kasutamist saate piirata.

Kasutus

See veerg näitab, kas kasutajal on lubatud rakendust või rakendusegruppi kasutada.

- **Lubatud** – kasutaja saab seda rakendust või rakendusegruppi kasutada.
- **Blokeeritud** – kasutajal ei ole lubatud seda rakendust või rakendusegruppi kasutada.
- **Piirangutega** – kasutaja võib seda rakendust või rakendusegruppi kasutada piiratud aja jooksul.

Valitud kasutaja jaoks rakenduse või rakendusegrupi kasutamise lubamiseks, blokeerimiseks või piiramiseks valige ripploendist soovitud üksus.

Tee

See veerg näitab rakenduse käivitusfaili teed.

Reeglid

Selle nupu klõpsamise korral avaneb aken, kus saate piirata valitud rakenduse kasutusaega.

Kustuta

Selle nupu klõpsamise korral kustutatakse valitud rakendus loendist. Pärast rakenduse loendist kustutamist lõpetab Kaspersky rakenduse kasutamise jälgimise ja kasutaja saab seda rakendust piiranguteta kasutada.

Lisa rakendus

Selle nupu klõpsamise korral avaneb dialoogiboks, kus saate valida loendisse lisatava rakenduse käivitusfaili. Vanemakontroll lisab rakenduse loendis vastavasse kategooriasse.

Aken „Karantiin“

[Karantiinis olevate objektide loend](#)

Sisaldab karantiini pandud failide loendit. Karantiin on ette nähtud nakkuse eemaldamise või parandamise käigus kustutatud või muudetud failide varukoopiate talletamiseks.

[Fail](#)

Selles veerus kuvatakse karantiini pandud faili nimi.

Paremklõps avab kontekstimenüü, kus saate teha karantiini pandud failide jaoks saadaolevaid toiminguid: need taastada, eemaldada või avada algses kaustas.

[Tee](#)

Selles veerus kuvatakse failitee.

[Avastatud](#)

Selles veerus kuvatakse avastatud objekti tüüp, näiteks *Võrgurünnak*.

[Kuupäev ja kellaeg](#)

Selles veerus kuvatakse faili karantiini teisaldamise kuupäev ja kellaeg.

[Taasta](#)

Selle nupu klõpsamise korral tagastab Kaspersky loendist valitud faili kausta, kus seda talletati enne karantiini teisaldamist.

[Kustuta](#)

Selle nupu klõpsamise korral kustutab Kaspersky loendist valitud faili.

[Eemalda kõik](#)

Selle nupu klõpsamise korral kustutab Kaspersky kõik karantiini pandud failide varukoopiad.

Kaspersky ei eemalda nakkusi Windows Store'i rakendustest. Kui kontrollitulemused näitavad, et selline rakendus on ohtlik, kustutatakse see teie arvutist. Kui Windows Store'i rakendus kustutatakse, ei loo Kaspersky sellest varukoopiat. Selliste objektide taastamiseks peate kasutama operatsioonisüsteemi taastetööriistu (üksikasjaliku teabe saamiseks lugege arvutisse paigaldatud operatsioonisüsteemi dokumentatsiooni) või uuendama rakendusi Windows Store'i kaudu.

Aken „Ebatsensuurne sõnavara“

Selles aknas kuvatakse ebatsensuurse sõnavara loend. Kui sõnumis on mõni neist sõnadest, märgib Kaspersky sõnumi rämpsmeiliks.

Nupp

Selle nupu klõpsamise korral avaneb menüü, kus saab valida järgmised toimingud.

- Impordi ja lisa olemasolevatele. Selle valiku korral saate importida ebatsensuursete fraaside loendi CSV-failist. Praeguseid fraase ei kustutata.
- Impordi ja asenda olemasolevad. Selle valiku korral saate importida ebatsensuursete fraaside loendi CSV-failist. Praegused fraasid kustutatakse.
- Ekspordi. Selle valiku korral saate eksportida ebatsensuursete fraaside loendi CSV-faili.

Ebatsensuurne sõnavara

Selles veerus kuvatakse sõna või fraas. See sõna või fraas võib tähendada, et sõnum on rämpsmeil.

Kaalukoeffitsient

Veerg näitab ebatsensuursele sõnale määratud kaalukoeffitsienti. Kui sõnum sisaldab mitut ebatsensuurset sõna, mille kombineeritud kaalukoeffitsient on üle 100, märgitakse see sõnum rämpsmeiliks.

Seisund

See veerg näitab, kas rämpsmeilifilter kasutab seda sõna sõnumitest ebatsensuurse sõnavara otsimisel.

- **Aktiivne.** Rakendus otsib sõnumitest seda sõna.
- **Mitteaktiivne.** Rakendus ei otsi sõnumitest seda sõna.

Muuda

Selle nupu klõpsamise korral avaneb aken, kus saate muuta loendis valitud ebatsensuurset sõna või sõnamaski.

Kustuta

Nupu klõpsamise korral saate ebatsensuurse sõna kustutada.

Lisa

Selle nupu klõpsamise korral avaneb aken, kus saate loendisse lisada ebatsensuurse sõna või sõnamaski.

Aken „Uudised“

[Uudiste loend](#)

Uudised kuvatakse aknas loendina. Märgitud on iga uudise pealkiri, teadaanne ja avaldamisaeg. Selle nupu klõpsamise korral avaneb uudise teksti kuvav aken.

Aken „Uudised“

[Lingid Twitterisse ja sotsiaalvõrgustikesse](#)

Linkidele klõpsamisel avanevad teie leheküljed Twitteris või sotsiaalvõrgustikes uudiste postitamiseks. Postitavat teksti saab muuta.

Kui te pole sisse loginud, kuvatakse vastava sotsiaalvõrgustiku veebisaidi sisselogimisleht.

Lingid sotsiaalvõrgustikele kuvatakse, kui teil on lubatud selliseid saite külastada.

[Nupud](#)

Nupud, mida klõpsates saate uudiseid sirvida.

Aken „Rakendushalduri seaded“

[Lülita sisse/välja](#) [Rakendushaldur](#)

Rakendushalduri sisselülitamine. Kui see lüliti on sisse lülitatud, kontrollib Kaspersky rakendus lisarakenduste installimist ja eemaldamist, samuti reklaame sisaldavate installimisetappide kuvamist.

Rakendushalduri sisselülitamine. Kui see lüliti on sisse lülitatud, kontrollib Kaspersky rakendus lisarakenduste installimist ja eemaldamist, samuti reklaame sisaldavate installimisetappide kuvamist.

[Tühjenda rakenduste paigaldamisel automaatselt lisatarkvara paigaldamise märkeruudud. Hoiata lisatarkvara paigaldamise katsete korral](#)

Kui see ruut on märgitud, siis blokeerib Kaspersky rakendus arvutisse rakenduste installimise ajal lisarakenduste installimise.

Kui ruudust eemaldati mäрге pärast kindla rakenduse paigaldamise alustamist, jätkab soovimatute rakenduste installimise blokeerija töötamist kuni poolelioleva paigaldamise lõpuni. Paigaldamiseks pakutavate lisarakenduste vastas kuvatavatest ruutudest eemaldatakse märged ja lisarakendusi ei paigaldata. Funktsioon lülitatakse välja järgmisel paigalduskorral. Lisarakendused paigaldatakse koos põhirakendusega.

[Ära kuva paigaldusetappe, mis sisaldavad reklaame ja pakkumisi lisaprogrammide paigaldamiseks](#)

Kui see ruut on märgitud, blokeerib Kaspersky arvutisse rakenduste installimise ajal reklaamide ja lisaprogrammide installimispakkumiste kuvamise.

Aken „Rakenduseuuendaja seaded“

[Luba rakenduseuuenduste otsing](#)

Kui see ruut on märgitud, otsib Kaspersky installitud rakenduste värskendusi ning palub teil need alla laadida ja installida.

[Häälesta uuenduste otsingurežiim](#)

Selle lingi klõpsamise korral avaneb aken, kus saate määrata arvutisse paigaldatud rakenduste uuenduste automaatotsingu režiimi.

[Laadib uuendused automaatselt alla ja paigaldab, kui sellega ei kaasne litsentsilepinguga nõustumist](#)

Kui see ruut on märgitud, otsib Kaspersky rakendus installitud rakenduste värskendusi automaatselt ning laadib alla ja installib saadaolevad värskendused, kui see ei nõua teie nõustumist uute lõppkasutaja litsentsilepingutega.

[Rakenduseuuenduste otsimine](#)

Seadetes peate valima, millised rakenduse uuendused tuleb installida.

- **Olulised uuendused, mis parandavad arvuti turvalisust** tähendab, et installitakse ainult olulised uuendused, mis parandavad tarkvara haavatavusi ja teie arvuti turvalisust.
- **Kõik tuntud rakenduste uuendused** tähendab, et installitakse kõik uuendused.

[Erandid](#)

Selle lingi klõpsamise korral avaneb erandite loendit sisaldav aken **Erandid**. Paigaldatud rakenduste vahelejäetud uuendused lisatakse erandite loendisse. Saate vahele jätta nii üksikuid uuendusi kui ka kindla arvutisse paigaldatud rakenduse kõik uuendused.

Uuenduste otsingu režiim / ajakava

Tabelis kirjeldatakse seadeid, mis määravad rakenduseuuendaja ja rakendushalduri komponentide ajakava.

Seaded	Kirjeldus
<p>Uuenduste otsingu režiim (rakenduseuuendaja)</p> <p>Teosta analüüs (rakendushaldur)</p>	<p>automaatselt. Kaspersky käivitab tegumi üks kord 24 tunni jooksul vastavalt rakendusesisestele seadetele.</p> <p>iga minut / iga tund / iga päev / iga nädal / Iga kuu / määratud ajal. Kaspersky käivitab tegumi vastavalt teie määratud ajakavale, mille saab määrata minutilise täpsusega. Kui teha üks neist valikutest, on saadaval loend Lükka käitamine pärast rakenduse käivitust edasi N minutit.</p> <p>pärast rakenduse käivitust. Pärast Kaspersky käivitumist käivitab see tegumi pärast väljal Käivita järgmise aja möödudes N minutit määratud minutite möödumist.</p> <p>pärast iga uuendust. Kaspersky käivitab tegumi pärast uue uuenduspaketi allalaadimist ja installimist.</p>
<p>Kui arvuti on välja lülitatud, otsi uuendusi järgmisel päeval (rakenduseuuendaja)</p> <p>Kui arvuti on välja lülitatud, teosta objektianalüüs järgmisel päeval (rakendushaldur)</p>	<p>Kui arvuti väljalülitamise tõttu jääb vahele ajastatud rakendusevärskenduste otsing või objektianalüüs, käivitab Kaspersky tegumi pärast arvuti sisselülitamist.</p> <p>See märkeruut kuvatakse, kui valitud on üks järgmistest käivitusrežiimidest: iga päev / iga nädal / Iga kuu / määratud ajal.</p>
<p>Otsi rakenduseuuendusi vaid siis, kui ekraanisäästja on aktiivne või arvuti on lukustatud (rakenduseuuendaja)</p> <p>Teosta objektianalüüsi vaid siis, kui ekraanisäästja on aktiivne ja arvuti on lukustatud (rakendushaldur)</p>	<p>Kaspersky käivitab tegumi, kui olete arvutiga töötamise lõpetanud. See tähendab, et tegum ei kasuta teie töö ajal süsteemiressursse.</p> <p>See märkeruut kuvatakse, kui valitud on käivitusrežiim pärast iga uuendust.</p>

Uuenduste seaded

Seaded	Kirjeldus
Andmebaaside uuendamise graafik	<p>Selle lingi klõpsamise korral avaneb aken Andmebaaside uuendamisgraafik, kus saate valida ühe järgmistest andmebaasiuuenduste käivitusrežiimidest.</p> <p>automaatselt. Uuendamistegumi käivitusrežiim, mille korral kontrollib Kaspersky rakendus uuenduspaketti uuendusallikas kindla sagedusega. Kontrolli sagedust saab suurendada viiruspuhangute ajal ja vähendada nende puudumise korral. Pärast värsket uuenduspaketi tuvastamist laadib Kaspersky rakendus selle alla ja installib uuendused arvutisse.</p> <p>käsitsi. See tegumi käivitusrežiim režiim võimaldab teil uuendamise tegumi käivitada käsitsi.</p> <p>iga minut / iga tund / iga päev / iga nädal / Iga kuu / määratud ajal / pärast rakenduse käivitust. Uuendamistegumi käivitusrežiim, mille korral käivitab Kaspersky rakendus uuendamistegumi teie loodud ajakava järgi. Kui valite uuendamistegumile selle käivitusrežiimi, saate Kaspersky rakenduse uuendamistegumi käivitada ka käsitsi.</p>
Uuendusallikate valimine	<p>Selle lingi klõpsamise korral avaneb uuendusallikate loendi aken.</p> <p><i>Uuendusallikas</i> on avalik HTTP- või FTP-server või ühiskaust (kohalik või võrgus), kust rakendus saab uuendatud andmebaasid ja moodulid alla laadida.</p> <p>Vaikimisi sisaldab uuendusallikate loend Kaspersky uuendusservereid. Loendisse saate lisada muid uuendusallikaid.</p> <p>Kui loendist on valitud mitu uuendusallikat, esitab Kaspersky rakendus neisse üksikshaaval päringuid, kuni leiab esimese saadaoleva uuendusallika, kust saab alla laadida uuenduspaketi.</p>
Käivita andmebaasiuuendused	<p>Lingi klõpsamise korral avaneb aken, kus saate andmebaasiuuenduse käivitada konkreetse kasutaja õigustega.</p> <p>Vaikimisi käivitub Kaspersky rakenduse uuendamistegum selle kasutaja nimel, kelle õigustega olete operatsioonisüsteemis registreeritud. Sellegipoolest saab Kaspersky rakendust värskendada uuendusallikast, millele kasutajal pole juurdepääsuõigust (näiteks uuenduspaketti sisaldavast ühiskaustast) või mille jaoks ei ole puhverserveris seatud autentimist. Rakenduse seadetes saate määrata nõutavate õigustega kasutaja ja käivitada Kaspersky rakenduse uuendamistegumi selle kasutaja nimel.</p>

Aken „Rakenduse haavatavuste kontroll“

[Käivita kontroll](#)

Selle nupu klõpsamise korral käivitatakse rakenduse haavatavuste kontroll.

[Peata](#)

Selle nupu klõpsamine peatab rakenduse haavatavuste kontrolli.
Nupp on saadaval rakenduse haavatavuste kontrolli käitamise ajal.

[N haavatavat rakendust](#)

Selle lingi klõpsamise korral avaneb aken **Haavatavad rakendused**, mis sisaldab kontrolli käigus tuvastatud haavatavate rakenduste loendit. Link on saadaval rakenduste haavatavuste kontrolli käitamise ajal.

Aken „Kaitse peatamine“

[Peata](#)

Kaitsekomponentide töö jätkamise režiim, mille korral lubatakse kaitse pärast teie määratud ajavahemikku automaatselt.

Ajavahemiku saate määrata allpool oleva rippmenüü abil.

[Peata, kuni rakendus taaskäivitub](#)

Kaitsekomponentide töö jätkamise režiim, mille korral lubatakse kaitse pärast rakenduse sulgemist ja uuesti käivitamist või operatsioonisüsteemi taaskäivitamist (kui lubatud on rakenduse automaatne käivitamine).

[Peata](#)

Kaitsekomponentide töö jätkamise režiim, mille korral lubatakse kaitse alles siis, kui otsustate selle taastada.

Parooli kontrollimise aken

[Parool](#)

Kaspersky rakenduse haldamiseks ette nähtud parool.

[Salvesta parool praeguseks seansiks](#)

Kui see ruut on märgitud, jätab Kaspersky sisestatud parooli käimasoleva seansi ajaks meelde ega küsi seda enam.

Aken „Rakendused, mille juurdepääs veebikaamerale on blokeeritud“

Selles aknas kuvatakse rakendused, mille juurdepääsu veebikaamerale olete blokeerinud.

[Luba juurdepääs veebikaamerale](#) 

Selle nupu klõpsamise korral lubatakse loendis valitud rakendusel veebikaamerale juurde pääseda.

Soovitatud seade aken

[Lülita sisse reklaamidevastane kaitse, et paigaldataks vaid soovitud tarkvara ja blokeeritaks lisapaigaldused](#) 

Kui see ruut on märgitud, blokeerib Kaspersky arvutisse mistahes tarkvara paigaldamise ajal reklaamide kuvamise. Samuti on blokeeritud reklaamitava lisatarkvara paigaldamine.

[Valmis](#) 


Selle nupu klõpsamise korral avaneb rakenduse peaaaken.


Aken „Aruanded“


Aruannete hõlpsamaks haldamiseks saate kasutada järgmisi võimalusi.

- Kuupäeva järgi filtreerimine.
- Mis tahes lahtri väärtuse järgi filtreerimine.
- Sündmusekirje teksti järgi otsimine.
- Loendi sortimine iga aruandeveru järgi.
- Aruandes kuvatavate veergude järjestuse ja paigutuse muutmine.

Aruannetes kasutatakse järgmisi sündmuste olulisustasemeid.

 **Informatiivsed sõnumid.** Infosündmused, mis üldiselt ei sisalda olulist teavet.

 **Hoiatused.** Sündmused, millele teil tuleb tähelepanu pöörata, kuna need sisaldavad teavet oluliste olukordade kohta, mis ilmnevad Kaspersky rakenduse töös.

 **Kriitilised sündmused.** Kriitiliselt olulised sündmused, mis näitavad, et Kaspersky rakendusel on ilmnenud probleeme, mis mõjutavad selle töövõimet, või haavatavusi, mis mõjutavad kasutaja arvuti kaitsetaset.

Kui klõpsate nuppu **Salvesta aruanne**, saate aruande salvestada TXT- või CSV-vormingus failina.

Aken Konto seaded

[Käivita andmebaasiuuendused](#)

Kaspersky uuendamistegumid käivitatakse teie valitud kasutajakonto õigustega. See funktsioon on saadaval Kaspersky uuendamistegumi käivitamiseks nii käsitsi kui ka ajakava järgi.

Saadaval on järgmised valikud.

- **Praegune kasutaja.** Uuendamise tegumitele kehtivad praeguse konto õigused (selle operatsioonisüsteemikonto omad, millesse olete sisse logitud).
- **teise kasutajana.** Uuendamise tegumid käivitatakse määratud kasutajakontol. Selle valiku korral määrake väljadel **Konto** ja **Parool** vastavalt konto nimi ja parool.

Aruande saatmine

[Operatsioonisüsteemi informatsioon](#)

See märkeruut võimaldab tehnilise toe serverisse saadetavasse aruandesse lisada teabe operatsioonisüsteemi seisundi kohta.

[Analüüsiks saadud andmed](#)

Ruudu märkimise korral saate tehnilise toe serverisse saadetavale aruandele lisada [jälgfailid](#) ja [tõmmised](#). Nendes failidesse on salvestatud rakenduse käskude täitmise ajalugu ja teave rakenduse seisundi kohta.

Märkeruudu kõrval kuvatava lingi **<failide arv>**, **<andmete maht>** klõpsamise korral avaneb aken **Analüüsiks saadud andmed**. Aknas kuvatakse tehnilise toe serverisse edastatavate failide loend ja andmete koguhulk.

[Salvesta aruanne arvutisse](#)

Lingi klõpsamise korral avaneb faili salvestamiseks ette nähtud dialoogiboks.

[Sisestage päringu number](#)



Number, mis määratakse teie päringule My Kaspersky veebisaidi kaudu tehnilise toega ühenduse võtmise korral.

[Saada aruanne](#)

Selle nupu klõpsamise korral laaditakse valitud failid üles tehnilise toe FTP-serverisse.

Aken „Analüüsiks saadud andmed“

Andmefailide loend

Loend failidest, mille Kaspersky lisab tehnilise toe serverisse saadetavale aruandele. Loend sisaldab [jälje-](#)  ja [tõmmisefaiile](#) . Nendes failidesse on salvestatud rakenduse käskude täitmise ajalugu ja teave rakenduse seisundi kohta.

Kui on failirea ruut on märgitud, laaditakse fail üles tehnilise toe serverisse. Enne üleslaadimist valmistatakse andmefailid ette ja arhiivitakse.

Kui failirea ruudust mäрге eemaldada, ei laadita faili tehnilise toe serverisse üles.

Fail

Selles veerus kuvatakse tehnilise toe serverisse saatmiseks valmis oleva faili nimi.

Maht

Aruandele määratud faili lisamise korral tehnilise toe serverisse saadetavate andmete hulk. Rakendus lisab faili aruandele, kui failireas kuvatav ruut on märgitud.

Skripti käivitamine

[Käivitatava skripti tekst](#)

Tehniliselt toelt saadud skripti tekst.

Kaspersky spetsialistid soovivad teil skripti teksti mitte muuta.

[Käivita](#)

Selle nupu klõpsamise korral algab skripti käitamine.

AVZ skriptide käivitamine

Selles aknas kuvatakse AVZ skripti käitamise protsess. Skripti käitamine võib pisut aega võtta.

Skripti käitamise tulemus

Viga

Tõrketeade. Kuvatakse, kui AVZ skriptis leitakse vigu. AVZ skripti käitamisnõustaja seiskub.

Valmis

Selle nupu klõpsamise korral sulgub AVZ skripti käitamisnõustaja.

Skripti käitamise tulemus

Sule

Selle nupu klõpsamise korral sulgub AVZ skripti käitamisõustaja.

Muuda

Selle nupu klõpsamise korral saate lisada skripti ja proovida skripti uuesti käitada.

Aken „Haavatavad rakendused“

[Haavatavad rakendused](#)

Loetleb rakendustest leitud haavatavused.

Mõne uuendusteenuse käitumise tõttu võidakse mõne rakenduse haavatavusi tuvastada mitu korda.

Iga haavatavuse jaoks on saadaval järgmised nupud.

- **Üksikasjad**

Selle nupu klõpsamine suunab teid tehnilise toe veebisaidile, kust leiate ohu kirjelduse. Veebisaidilt saate alla laadida ja paigaldada oma rakenduseversiooni jaoks nõutavad uuendused.

- **Lisa eranditesse**

Selle nupu klõpsamisel lisatakse rakendus usaldusväärsesse tsooni.

ZIP-faili või kausta valimine

Kohandatud kujundusteemad pole kõigis piirkondades saadaval.

Teema valimisel võtke arvesse järgmisi piiranguid.

- Kaspersky ei saa valitud teemat kasutada järgmistel juhtudel.
 - Arhiivis olevatel failidel on kaustastruktuuris nimi või tee, mis erineb vaiketeema omast.
 - Rakenduse akende tekstidele vastavad arhiivitud failid on rikutud.
- Teemad on kujundatud Kaspersky kindla versiooni jaoks ja neid ei saa rakendada teistes versioonides ega muudes rakendustes. Rakenduse uueks versiooniks täiendamise või seda asendava muu rakenduse paigaldamise korral asendatakse teema vaiketeemaga.

Kui alternatiivse teema valimisel esineb probleeme ja te ei saa vaiketeemat ettenähtud meetodi abil installida (näiteks juhul, kui ei saa eemaldada märget ruudust **Kasuta kohandatud kujundusteemat** aknas **Liidese seaded**, kuna kiri on taustaga ühte värvi ja vajalikke halduselemente ei saa eristada), soovitame Kaspersky uuesti installida.

Arvutiklaviatuuri erandi lisamise/muutmise aken

[Veebiaadressi mask](#)

Loendisse lisatava veebisaidi veebiaadress. Saate määrata veebiaadressi või aadressimaski.

Jaotises **Ulatus** saate määrata klaviatuurikaitse erandireegli rakendamisalala.

[Rakenda tervele veebisaidile](#)

Klaviatuurikaitse on sisse lülitatud väljal **Veebiaadressi mask** määratud veebisaidi kõigil lehtedel.

[Rakenda määratud lehele](#)

Klaviatuurikaitse on sisse lülitatud ainult väljal **Veebiaadressi mask** määratud veebilehel.

Jaotises **Klaviatuurikaitse** saate määrata, kas Kaspersky kaitseb valitud saidile või veebilehele arvutiklaviatuuri abil sisestatud andmeid.

[Kaitse](#)

Kaspersky kaitseb valitud saidile või veebilehele arvutiklaviatuuri abil sisestatud andmeid.

[Ära kaitse](#)

Kaspersky ei kaitse valitud saidile või veebilehele arvutiklaviatuuri abil sisestatud andmeid.

Ekraaniklaviatuuri erandi lisamise/muutmise aken

[Veebiaadressi mask](#)

Loendisse lisatava veebisaidi veebiaadress. Saate määrata veebiaadressi või aadressimaski.

Jaotises **Ulatus** saate määrata, millele ekraaniklaviatuuri ikooni kuvamise seadeid rakendatakse: tervele veebisaidile või määratud lehele.

[Rakenda tervele veebisaidile](#)

Ekraaniklaviatuuri kiirkäivitusikoon kuvatakse väljal **Veebiaadressi mask** määratud veebilehe kõigi veebilehtede sisestusväljadel.

[Rakenda määratud lehele](#)

Ekraaniklaviatuuri kiirkäivitusikoon kuvatakse ainult väljal **Veebiaadressi mask** määratud veebilehe sisestusväljadel.

Jaotises **Ekraaniklaviatuuri ikoon** saate määrata, kas rakendusel tuleb määratud veebiaadressi maskile vastavatel lehtedel kuvada ekraaniklaviatuuri ikoon või mitte.

[Näita veebilehitseja aknas ikooni](#)

Kaspersky kuvab sisestusväljadel ekraaniklaviatuuri kiirkäivitusikooni.

[Ära näita veebilehitseja aknas ikooni](#)

Kaspersky ei kuva sisestusväljadel ekraaniklaviatuuri kiirkäivitusikooni.

Aruannete ja karantiini seaded

Jaotises **Aruanded** saate seadistada aruannete loomise ja talletamise seadeid.

Säilita aruandeid mitte kauem kui

See märkeruut lubab/keelab aruannete säilitusperioodi piiramise valiku. Aruandeid saab säilitada üks päev, üks nädal, üks või kuus kuud või üks aasta.

Kui määratud väärtus on saavutatud, kustutab rakendus kõik aruandekirjed, mis on vanemad kui määratud päevade arv miinus 10%. Kui väärtuseks on sisestatud 30 päeva ja aruandes esineb sündmus, mis on vanem kui 30 päeva, kustutatakse aruandest kõik sündmused, mida on hoitud kauem kui 27 päeva.

Kui see ruut on märkimata, on aruannete säilitusaeg piiramata.

Piira aruandefailide mahtu

See märkeruut lubab/keelab aruandefailide maksimummahu piiramise valiku. Maksimaalne failimaht on määratud megabaitides.

Kui see ruut on märgitud, on aruande maksimummaht vaikselt 1024 MB. Kustutamine toimub siis, kui on jõutud pooleni määratud mahust. Aruandefaili tegelikust mahust kustutatakse 10%. Kui väärtuseks on määratud 1024 MB, siis hakatakse aruandefaili vanemaid kirjeid kustutama, kui fail jõuab 512 MB-ni, ja faili mahtu vähendatakse 10% võrra selle tegelikust mahust, kustutades vanimad kirjed.

Kui see ruut on märkimata, pole aruandefaili maht piiratud.

Tühjenda

Selle nupu klõpsamise korral eemaldab Kaspersky aruannete kaustast andmed.

Vaikselt kustutab Kaspersky kontrollimistegumid, uuendamistegumite aruanded ja Tulemüüri reeglite kohaldamise aruanded.

Jaotises **Karantiin** saate muuta karantiini seadeid.

Säilita objekte mitte kauem kui

Märkeruut lubab/keelab karantiinis objektide säilitusperioodi piiramise valiku. Aruandeid saab säilitada üks päev, üks nädal, üks või kuus kuud või üks aasta.

Kui see ruut on märgitud, säilitatakse objekte ruudu kõrval asuvas ripploendis valitud perioodi jooksul.

Kui see ruut on märkimata, on objektide säilitusaeg piiramata.

Määra karantiini mahupiirang

See märkeruut lubab/keelab karantiini maksimummahu piiramise valiku. Karantiini maht on määratud megabaitides.

Kui see ruut on märgitud, on hoidla maksimummaht vaikselt 100 MB. Maksimummahu ületamise korral eemaldatakse uute objektide lisamiseks hoidlast vanimad objektid.

Kui see ruut on märkimata, on hoidlal piiramatut mahtu.

Enesekaitse seaded

Lülita Enesekaitse sisse [?](#)

See märkeruut lülitab sisse/välja Kaspersky rakenduse mehhanismi, mis kaitseb rakendust selle kõvakettafailide, mälu protsesside ja süsteemiregistikirjete muutmise ja kustutamise eest.

Selle ruudu märkimise korral keelatakse ka võimalus juhtida süsteemiteenust väljastpoolt. Kui süsteemiteenuse väline juhtimine on välja lülitatud, blokeerib Kaspersky rakendus kõik katsed hallata rakenduse teenuseid kaugteel. Kui tuvastatakse katse rakendust kaugteel hallata, kuvatakse operatsioonisüsteemi Microsoft® Windowsi® tegumiriba teavitusalal Kaspersky rakenduse ikooni kohal teade (kui teated pole välja lülitatud).

Luba toote <PRODUCT> seadete haldamine kaugjuhtimisrakenduste kaudu [?](#)

Selle ruudu märkimise korral saavad usaldusväärsed kaughaldusrakendused (näiteks TeamViewer, LogMeIn Pro ja Remotely Anywhere) muuta Kaspersky Small Office Security seadeid.

Ebausaldusväärsed kaugjuhtimisrakendused ei tohi Kaspersky Small Office Security seadeid muuta isegi juhul, kui ruut on märgitud.

Puhverserveri seaded

[Ära kasuta puhverserverit ?](#)

Selle lülitiga saate internetiühenduste jaoks puhverserveri kasutamise sisse/välja lülitada. Internetiühendus on vajalik Kaspersky teatud kaitsekomponentide toimimiseks, aga ka andmebaaside ja rakendusemoodulite uuendamiseks.

[Määra puhverserveri seaded automaatselt ?](#)

Kaspersky tuvastab puhverserveri seaded automaatselt, kasutades WPAD-protokolli (veebiproksi automaatotsingu protokoll).

Kui selle protokolliga ei saa aadressi kindlaks määrata, kasutab Kaspersky Chromium-põhises brauseris Microsoft Edge määratud puhverserveriseadeid. Kaspersky ei võta arvesse teiste kasutaja arvutisse installitud brauserite jaoks määratud puhverserveriseadeid.

[Kasuta puhverserveri täpsustatud seadeid ?](#)

Kaspersky kasutab puhverserverit, mis erineb brauseri ühenduseseadetes määratud.

[Aadress ?](#)

Sisaldab puhverserveri IP-aadressi või sümbolset nime (URL).

Välja saab muuta seade **Kasuta puhverserveri täpsustatud seadeid** valimise korral (näiteks IP 192.168.0.1).

[Port ?](#)

Puhverserveri port.

Väli on saadaval seade **Kasuta puhverserveri täpsustatud seadeid** valimise korral.

[Kasuta puhverserveri autentimist ?](#)

Autentimine on kasutaja sisselogimiseabe kontrollimine.

See märkeruut lubab/keelab kasutada puhverserveris autentimist.

Kui see ruut on märgitud, proovib Kaspersky esmalt teha NTLM-autentimise ja seejärel BASIC-autentimise.

Kui see ruut on märkimata või kui puhverserveri seaded pole määratud, proovib Kaspersky teha NTLM-autentimist selle konto abil, millel tegum (näiteks uuendamise tegum) käivitati.

Kui puhverserver nõuab autentimist ning kasutajanime ja parooli ei sisestatud või kui puhverserver ei aktsepteerinud edastatud andmeid, avaneb aken, kus küsitakse kasutajanime ja parooli. Kui autentimine õnnestub, kasutab Kaspersky edaspidi määratud kasutajanime ja parooli. Vastasel juhul küsib Kaspersky uuesti autentimisseadeid.

[Kasutajanimi ?](#)

Puhverserveris autentimiseks kasutatav kasutajanimi.

Parool

Määratud kasutajanime parool.

Ära kasuta puhverserverit kohalike aadresside korral

Kui see ruut on märgitud, siis ei kasuta Kaspersky kohalikust kaustast või võrgukaustast andmebaaside ja rakendusemoodulite uuendamisel puhverserverit.

Kui see ruut on märkimata, kasutab Kaspersky kohalikust kaustast või võrgukaustast andmebaaside ja rakenduse tarkvaramoodulite uuendamisel puhverserverit.

Jaotis „Kaitse“

[Kaitsekomponentide loend](#)

See loend sisaldab kaitsekomponente, mis on loodud kaitsma eri tüüpi digitaalsete ohtude vastu.

Iga ohutüübiga tegeleb selleks ette nähtud kaitsekomponent. Komponente saab lubada või keelata üksteisest sõltumatult ning nende seadeid saab seadistada.

Veebikaamera ja mikrofoni kontroll

[Lülita veebikaamera ja mikrofoni kontroll sisse/välja](#)

Selle lülitiga saate veebikaamera ja mikrofoni kontrolli sisse/välja lülitada.

Veebikaamera seaded alt saate muuta järgmisi seadeid.

[Blokeeri kõikide rakenduste juurdepääs veebikaamerale](#)

Kui see suvand on valitud, siis on juurdepääs veebikaamerale kõigi teie arvutisse installitud rakenduste jaoks blokeeritud.

[Teavita, kui rakendus kasutab veebikaamerat](#)

Kui see suvand on valitud, kuvab Kaspersky teate, kui veebikaamerat kasutab juurdepääsuloaga rakendus. Teateaknas saate muuta rakenduse veebikaamerajuurdepääsu seadeid või määrata, et ei soovi selle kohta rohkem teateid saada.

Mikrofoni seaded alt saate muuta järgmisi seadeid.

[Blokeeri kõikide rakenduste juurdepääs mikrofoni](#)

Kui see suvand on valitud, siis on juurdepääs mikrofoni kõigi teie arvutisse installitud rakenduste jaoks blokeeritud.

[Teavita, kui rakendus kasutab mikrofoni](#)

Kui see suvand on valitud, kuvab Kaspersky teate, kui mikrofoni kasutab juurdepääsuloaga rakendus. Teatise aknas saate rakenduse mikrofoni juurdepääsu seadeid muuta või valida, et ei soovi rohkem teatise saada.

[Lisateave veebikaamerale ja mikrofoni juurdepääsu kohta](#)

Avastati kahtlane ümbersuunamine

[Kustuta salvestused](#)

Kaspersky kustutab failist hosts kõik kahtlased kirjed.

[Jäta vahele](#)

Kaspersky ei kustuta failist hosts neid kahtlasi kirjeid, mis on loendis.

[Kahtlaste kirjete loend](#)

See loend sisaldab pahatahtlike või tundmatute veebiserverite aadresse, kuhu teid ümber suunatakse, kui rakendus üritab luua ühendust Kaspersky serveritega.

Soovitame kahtlased kirjed failist hosts kustutada.

Parooli sisestamise aken

[Kehtiv parool](#)

Kaspersky haldamise jaoks ette nähtud kehtiv parool.

[Salvesta parool praeguseks seansiks](#)

Kui see ruut on märgitud, jätab Kaspersky sisestatud parooli käimasoleva seansi ajaks meelde ega küsi seda enam.

Aken „Parooliga kaitse“

Link **Muuda või eemalda parool** on saadaval siis, kui Kaspersky funktsioonidele juurdepääsu kaitsmiseks on määratud parool.

[Muuda või eemalda parool](#)

Selle lingi klõpsamise korral tehakse kättesaadavaks uue parooli määramise ja kinnitamise sisestusväljad.

[Uus parool](#)

Kaspersky haldamiseks ette nähtud parool.

[Kinnitage parool](#)

Sisestage väljale **Uus parool** sisestatud parool uuesti.

Jaotises **Parooli ulatus** saate määrata, milliseid rakenduse halduse osi soovite parooliga kaitsta.

[Rakenduse seadete konfigureerimine](#)

Märkeruut lülitab sisse/välja kasutajale parooliviiba kuvamise, kui ta proovib salvestada rakenduse seadetes tehtud muudatusi.

[Varundamise ja taastamise haldus](#)

See märkeruut lülitab sisse/välja kasutajalt akna **Varundamine ja taastamine** avamiseks parooli küsimise.

[Rakendusest väljumine](#)

Märkeruut lülitab sisse/välja kasutajale parooliviiba kuvamise, kui ta proovib rakendust sulgeda.

[Rakenduse eemaldamine](#)

Märkeruut lülitab sisse/välja kasutajale parooliviiba kuvamise, kui ta proovib rakendust eemaldada.

Kontrolli seaded

Tabelis kirjeldatakse järgmiste kontrollitüüpide seadeid: täiskontroll, kiirkontroll, valikuline kontroll ja kiire failide kontroll.

Seaded	Kirjeldus
Turvalisuse tase	<p>Kaspersky kasutab kontrollimiseks mitmesuguseid seadete komplekte. Rakendusse salvestatud seadekomplekte kutsutakse <i>turbetasemeteks</i>.</p> <ul style="list-style-type: none">• Äärmuslik. Kaspersky rakendus kontrollib kõiki failitüüpe. Liitfailide kontrollimisel kontrollib rakendus ka meilivormingus faile.• Optimaalne. Kaspersky rakendus kontrollib arvuti kõigil kõvaketastel, võrguketastel ja irdketastel ainult määratud failivorminguid ning manustatud OLE-objekte. Rakendus ei kontrolli arhiive ega paigalduspakette.• Madal. Kaspersky rakendus kontrollib arvuti kõigil kõvaketastel, irdketastel ja võrguketastel ainult kindlate failinimelaienditega uusi ja muudetud faile. Rakendus ei kontrolli liitfaile.
Toiming ohu avastamisel	<ul style="list-style-type: none">• Küsi kasutajalt. Kui Kaspersky rakendus tuvastab kontrolli käigus nakatunud või tõenäoliselt nakatunud objekti, teavitab ta teid sellest viivitamatult ja küsib, mida tuvastatud objektiga teha. See valik on saadaval, kui menüüs Seaded → Jõudlusseaded → Arvutiressursside kasutus on märkeruudust Tee soovitatavad toimingud automaatselt märges eemaldatud.• Vali toiming automaatselt. Nakatunud või tõenäoliselt nakatunud objekti tuvastamise korral teeb Kaspersky toimingut, mida on soovitanud Kaspersky spetsialistid.<ul style="list-style-type: none">• Esmalt proovib Kaspersky nakatunud objekti parandada. Kui nakkuse eemaldamine nurjub, siis see kustutab faili.• Kaspersky kustutab tõenäoliselt nakatunud objekti, kui märgitud on ruut Kustuta pahatahtlikud tööriistad, reklaamvara, väljahelistusprogrammid ja kahtlased pakkijad. Kui ruudust on märges eemaldatud, ei kustuta rakendus arvatavalt nakatunud objekti. Selle asemel kuvatakse teadete keskuses teade objekti tuvastamise kohta (selle avamiseks klõpsake rakenduse peaaknas nuppu Üksikasjad).See valik on saadaval, kui menüüs Seaded → Jõudlusseaded → Arvutiressursside kasutus on märgitud ruut Tee soovitatavad toimingud automaatselt.• Paranda; kui parandamine nurjub, siis kustuta. Selle valiku korral proovib rakendus automaatselt parandada kõik tuvastatud nakatunud failid. Kui nakkuse eemaldamine nurjub, siis rakendus kustutab objektid.• Paranda; kui parandamine nurjub, siis blokeeri. Selle toimingut valimise korral proovib Kaspersky automaatselt parandada kõik leitud nakatunud failid. Kui nakkuse eemaldamine nurjub, siis lisab rakendus teabe leitud nakatunud failide kohta tuvastatud objektide loendisse.• Teata. Selle valiku korral lisab Kaspersky rakendus teabe leitud nakatunud failide kohta tuvastatud objektide loendisse.

	<p>Enne nakatunud faili parandamise või kustutamise katset loob rakendus varukoopia juhuks, kui teil hiljem on vaja fail taastada või avaneb võimalus sellest nakkus eemaldada.</p>
<p>Muuda kontrolli ulatust (pole saadaval kontekstimenüükontrolli seadetes)</p>	<p>Lingil klõpsamisel avaneb aken loendiga objektidest, mida Kaspersky rakendus saab kontrollida. Kontrolli tüübist (täiskontroll, kiirkontroll või valikuline kontroll) olenevalt lisatakse loendisse vaikimisi erinevad objektid.</p> <p>Loendis saate objekte lisada või enda lisatud objekte kustutada.</p> <p>Kontrollist objekti eemaldamiseks ei pea objekti loendist kustutama. Piisab objektinime kõrval kuvatavast ruudust märke eemaldamisest.</p>
<p>Kontrollimise ajakava (pole saadaval kontekstimenüükontrolli seadetes)</p>	<p>käsitsi. Käivitusrežiim, mille korral saate kontrolli teile sobival ajal käivitada käsitsi.</p> <p>Ajakava järgi. Kontrolli käivitusrežiim, mille korral käivitab rakendus kontrolli tegumi teie loodud ajakava järgi. Kui valite kontrollile selle käivitusrežiimi, saate kontrolli tegumi käivitada ka käsitsi.</p>
<p>Käivita kontroll kui</p>	<p>Lingi klõpsamise korral avaneb aken, kus saate kontrolli käivitada konkreetse kasutaja õigustega.</p> <p>Vaikimisi käivitatakse kontrolli tegum selle kasutaja nimel, kelle õigustega olete operatsioonisüsteemis registreeritud. Kaitse ulatus võib hõlmata võrgukettaid või muid objekte, millele juurdepääsemiseks on vaja eriõigusi. Rakenduse seadetes saate määrata nõutavate õigustega kasutaja ja käivitada kontrolli tegumi selle kasutaja nimel.</p>
<p>Failitüübid</p>	<p>Kaspersky rakendus käsitleb nimelaiendita faile täitmisfailidena. Rakendus kontrollib neid alati, sõltumata kontrollimiseks valitud failitüüpidest.</p> <p>Kõik failid. Kui see seade on sisse lülitatud, kontrollib Kaspersky eranditult kõiki faile (kõiki vorminguid ja failinimelaiendeid).</p> <p>Vormingu järgi kontrollitud failid. Selle seade valimise korral kontrollib rakendus ainult potentsiaalselt nakatunud faile. Enne failist pahatahtliku koodi otsimist analüüsitakse failivormingu (näiteks TXT, DOC, EXE) kindlaksmääramiseks faili sisemist päist. Kontroll otsib ka kindlate failinimelaienditega faile.</p> <p>Laiendi järgi kontrollitud failid. Selle seade valimise korral kontrollib rakendus ainult potentsiaalselt nakatunud faile. Failivorming määratakse kindlaks failinimelaiendi põhjal.</p>
<p>Kontrolli ainult uusi ja muudetud faile</p>	<p>Kontrollib ainult uusi faile ja faile, mida on pärast viimast kontrollimiskorda muudetud. See võimaldab teil kontrollimisel aega kokku hoida. See kontrollimisrežiim rakendatakse nii tava- kui ka liitfailidele.</p>
<p>Ära kontrolli faile kauem kui N sekundit</p>	<p>Piirab ühe objekti kontrollimise kestust. Pärast määratud aja möödumist lõpetab rakendus faili kontrollimise. See võimaldab teil kontrollimisel aega kokku hoida.</p>
<p>Kontrolli arhiive</p>	<p>Kontrollitakse ZIP-, GZIP-, BZIP-, RAR-, TAR-, ARJ-, CAB-, LHA-, JAR-, ICE- ja muudes vormingutes arhiive. Rakendus kontrollib arhiive nii failinimelaiendi kui ka vormingu järgi.</p>
<p>Kontrolli levituspakette</p>	<p>Märkeruut lülitab sisse/välja kolmanda osapoole levituspakettide kontrollimise.</p>
<p>Kontrolli Microsoft Office'i vormingus faile</p>	<p>Kontrollib Microsoft Office'i faile (DOC, DOCX, XLS, PPT ja muud Microsofti faililaiendid). Office'i vormingus failid hõlmavad ka OLE-objekte.</p>

<p>Kontrolli meilivorminguid</p>	<p>See märkeruut lubab/keelab Kasperskyl meilivormingutes ja meiliandmebaasides failide kontrollimise.</p> <p>Rakendus skannib täielikult ainult Microsoft Outlooki, Windows Maili / Microsoft Outlook Expressi ja EML-i meilifailivorminguid ning ainult juhul, kui arvutil on Microsoft Outlooki x86-meiliklient.</p> <p>Kui see ruut on märgitud, liigendab Kaspersky meilivormingus faili ja analüüsib iga selle komponenti (sisu, manuseid) viiruste suhtes.</p> <p>Kui sellest ruudust on mäрге eemaldatud, kontrollib Kaspersky meilivormingus faili ühe objektina.</p>
<p>Kontrolli parooliga kaitstud arhiivid</p>	<p>Kui ruut on märgitud, kontrollib rakendus parooliga kaitstud arhiive. Enne kui arhiivis olevaid faile saab kontrollida, küsitakse ekraanil parooli.</p> <p>Kui ruut pole märgitud, jätab rakendus parooliga kaitstud arhiivide kontrollimise vahele.</p>
<p>Ära paki lahti suuri liitfaile</p> <p>Faili maksimaalne suurus</p>	<p>Kui ruut on märgitud, ei kontrolli rakendus liitfaile, mis on määratud väärtusest suuremad.</p> <p>Kui sellest ruudust on mäрге eemaldatud, kontrollib rakendus kõiki liitfaile nende mahust olenemata.</p> <p>Rakendus kontrollib kõiki arhiividest lahtipakitud suuri faile ruudu märkimisest või märkimata jätmisest olenemata.</p>
<p>Heuristiline analüüs</p>	<p>Tehnika, mis on ette nähtud selliste ohtude avastamiseks, mida ei saa tuvastada Kaspersky rakenduste andmebaaside praeguse versiooni abil. See võimaldab teil leida faile, mis võivad sisaldada tundmatut pahavara või teadaoleva pahavaraprogrammi uut modifikatsiooni.</p> <p>Failidest pahatahtliku koodi otsimisel täidab heuristiline analüüs käivitusfailides sisalduvaid juhiseid. Heuristilise analüüsi täidetavate juhiste arv on heuristilise analüüsi jaoks määratud tasemest. Heuristilise analüüsi tase määrab uute ohtude otsingu põhjalikkuse, operatsioonisüsteemiressursside koormuse ja heuristilise analüüsi kestuse vahelise tasakaalu.</p>
<p>iSwifti tehnoloogia</p>	<p>See tehnoloogia on NTFS-failisüsteemi kasutavate arvutite jaoks ette nähtud iCheckeri tehnoloogia edasiarendus.</p> <p>iSwifti tehnoloogial on piirangud: see on seotud konkreetse faili asukohaga failisüsteemis ja töötab ainult NTFS-failisüsteemis olevate objektidega.</p> <p>Kui viite Kaspersky Small Office Security rakenduse üle uuele versioonile, lülitatakse iSwifti tehnoloogia kõigi kontrollimistüüpide jaoks sisse ka siis, kui see oli varem välja lülitatud.</p>
<p>iCheckeri tehnoloogia</p>	<p>See tehnoloogia võimaldab kontrolli kiirendada, kuna jätab kindlad failid kontrollist välja. Kontrollist failide väljajätmiseks kasutatakse erialgoritmi, mis võtab arvesse Kaspersky Small Office Security andmebaaside väljalaskekuupäeva, faili viimase kontrollimise kuupäeva ja kõiki kontrolli seadetes tehtud muudatusi. iCheckeri tehnoloogial on piirangud: see ei tööta suurte failidega ja rakendatakse ainult failidele, mille struktuuri rakendus ära tunneb (näiteks EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ja RAR).</p>

Irdketaste kontrolli seaded

Seaded	Kirjeldus
Toiming irdketta ühendamise korral	<ul style="list-style-type: none">• Kiirkontroll. Kui teete selle valiku, siis kontrollib Kaspersky pärast välisseadme ühendamist ainult teatud vormingus faile, mis on nakkustele kõige vastuvõtlikumad ja asuvad juurkaustas. Samuti ei hõlma kiirkontroll arhiivide lahtipakkimist ega kontrollimist.• Detailne kontroll. Kui see ruut on märgitud, siis kontrollib Kaspersky pärast välisseadme ühendamist välisseadme igas kaustas kõiki faile. Samuti pakib see lahti arhiivid ja kontrollib neid, välja arvatud juhul, kui need on parooliga kaitstud.
Suurim irdketta maht	<p>Kui see ruut on märgitud, kontrollib Kaspersky kõiki välisseadmeid, mis ei ületa kindlaksmääratud maksimummahtu.</p> <p>Kui sellest ruudust on märges eemaldatud, kontrollib Kaspersky kõiki välisseadmeid nende mahust olenemata.</p>
Kuva kontrolli edenemine	<p>Kui see ruut on valitud, kuvab Kaspersky välisseadmekontrolli edenemist eraldi aknas ja poolelioleva kontrolli aknas.</p>
Blokeeri kontrollimistegumi peatamine	<p>Kui see ruut on valitud, ei ole välisseadmekontrolli korral poolelioleva kontrolli aknas saadaval nupp Peata.</p>

Taustal tehtava kontrolli seaded

Kui taustal toimuv kontroll on lubatud, teeb Kaspersky taustal kontrolli. Taustal toimuv kontroll on automaatne kontrollimisrežiim, milles ei kuvata teateid. See kontroll nõuab vähem arvutiressursse kui muud tüüpi kontrollid (näiteks täiskontroll). Selles režiimis kontrollib Kaspersky süsteemimälu, süsteemimahte, alglaadimissektoreid ja käivitusobjekte ning otsib rootkit'e.

Kui arvuti töötab akutoitel, ei tee Kaspersky arvuti jõudeolekus taustal kontrolle.

Rakenduse haavatavuste kontrolli seaded

Seaded	Kirjeldus
Muuda otsingu ulatust	<p>Lingil klõpsamise korral avaneb aken Rakenduse haavatavuste kontrolli ulatus koos loendiga objektidest, mille haavatavusi rakendustest otsitakse.</p> <p>Loendis saate objekte lisada või enda lisatud objekte kustutada.</p> <p>Kontrollist objekti eemaldamiseks ei pea objekti loendist kustutama. Piisab objektinime kõrval kuvatavast ruudust märke eemaldamisest.</p>
Otsi ajakava	<p>käsitsi. Käivitusrežiim, mille korral saate rakenduse haavatavuste kontrolli endale sobival ajal käsitsi käivitada.</p> <p>Ajakava järgi. Kontrolli käivitusrežiim, mille korral käivitab rakendus kontrolli tegumi teie loodud ajakava järgi. Kui valite kontrollile selle käivitusrežiimi, saate kontrolli tegumi käivitada ka käsitsi.</p>

Konto seaded

[Käivita kontroll kui ?](#)

Valige konto, mille õigusi Kaspersky kontrollimistegumite käivitamiseks kasutab. See funktsioon on saadaval nii käsitsi kui ka ajastatud kontrollide käivitamiseks.

Saadaval on järgmised valikud.

- **praeguse kasutajana.** Kontrollitegumid käivitatakse praeguse konto õigustega.
- **teise kasutajana.** Kontrollitoimingute käivitamiseks kasutatakse määratud kasutajakontot. Selle valiku korral tippige väljadele **Konto** ja **Parool** vastavalt konto nimi ja parool.

Ribareklaamifiltri seaded

[Lülita Ribareklaamifilter sisse/välja](#)

Selle lülitiga saate ribareklaamifiltri sisse/välja lülitada.

Kui nupp on roheline, blokeerib ribareklaamifilter teie külastatud veebisaitidel ja mõne rakenduse liideses ribareklaamide kuvamise. Vaikimisi blokeerib ribareklaamifilter veebisaitide ribareklaamid teadaolevate ribareklaamide loendi põhjal. See loend on lisatud Kaspersky andmebaasidesse.

[Filtrite loend](#)

Selle lingi klõpsamise korral avaneb aken **Filtrite loend**, kus saate erifiltrite abil täpsemalt määrata, millised ribareklaamid tuleb blokeerida.

[Lubatud ribareklaamidega veebilehed](#)

Selle lingi klõpsamise korral avaneb aken, kus on loend veebisaitidest, kus olete lubanud ribareklaame kuvada.

[Blokeeritud ribareklaamid](#)

Selle lingi klõpsamisel avaneb aken **Blokeeritud ribareklaamid**. Selle akna abil saate luua blokeeritavate ribareklaamide loendi.

[Lubatud ribareklaamid](#)

Selle lingi klõpsamisel avaneb aken **Lubatud ribareklaamid**. Selles aknas saate luua lubatavate ribareklaamide loendi.

[Luba ribareklaame Kaspersky veebilehtedel](#)

Kui ruut on märgitud, ei blokeeri ribareklaamifilter ribareklaame Kaspersky veebisaitidel ega meie partnerite veebisaitidel, kus hostitakse Kaspersky reklaame. Nende veebisaitide loendi kuvamiseks klõpsake linki **Kaspersky veebisaidid**.

[Kaspersky veebisaidid](#)

Selle lingi klõpsamise korral avaneb Kaspersky veebisaitide loendi aken.

See link on saadaval, kui märgitud on ruut **Luba ribareklaame Kaspersky veebilehtedel**.

Ribareklaami lisamise/muutmise aken

[Veebiaadressi mask \(URL\) ?](#)

IP-aadress, veebiaadress (URL) või veebiaadressi mask.

Veebiaadressi maski sisestamisel saate kasutada metamärke * ja ?; *tähistab mis tahes tähemärgijada ja ? tähistab mis tahes üksikmärki.

[Olek ?](#)

Jaotises **Olek** saate määrata, kas ribareklaamifilter kasutab seda aadressi ribareklaamide kontrollimisel.

Saadaval on järgmised valikud.

- **Aktiivne.** Ribareklaamifilter kasutab seda aadressi ribareklaamide kontrollimisel.
- **Mitteaktiivne.** Ribareklaamifilter ei kasuta seda aadressi ribareklaamide kontrollimisel.

Aken „Veebisaidi lisamine/muutmine“

[Veebileht](#)

Veebisaidi veebiaadress (URL).

[Olek](#)

Jaotises **Olek** saate määrata, kas ribareklaamifilter peab kindlal veebisaidil ribareklaamide kuvamise lubama või mitte.

Saadaval on järgmised valikud.

- **Aktiivne.** Ribareklaamifilter lubab määratud veebisaidil kuvada ribareklaame.
- **Mitteaktiivne.** Ribareklaamifilter ei luba määratud veebisaidil kuvada ribareklaame.

Aken „Blokeeritud ribareklaamid“

Nupp

Nupu klõpsamine avab menüü, mis sisaldab järgmisi üksusi.

- **Impordi ja lisa olemasolevatele.** Selle üksuse valimise korral avaneb aken, mis võimaldab importida blokeeritud aadresside loendi CSV-failist. Praeguseid aadresse ei kustutata.
- **Impordi ja asenda olemasolevad.** Selle üksuse valimise korral avaneb aken, mis võimaldab importida blokeeritud aadresside loendi CSV-failist. Praegused aadressid kustutatakse.
- **Ekspordi.** Selle üksuse valimise korral avaneb aken, mis võimaldab eksportida blokeeritud aadresside loendi CSV-faili.

Blokeeritud ribareklaamide loend

Talletab blokeeritud ribareklaamide aadresse või aadressimaski. Ribareklaamifilter blokeerib ribareklaami, kui selle aadress on blokeeritud ribareklaamide loendis.

Loendisse saate lisada aadressi või aadressimaski.

Kui veerus **Seisund** on aadressireale seatud väärtus *Aktiivne*, kasutab ribareklaamifilter seda aadressi ribareklaamide kontrollimisel.

Kui veerus **Seisund** on aadressireale seatud väärtus *Mitteaktiivne*, ei kasuta ribareklaamifilter seda aadressi ribareklaamide kontrollimisel.

Veebiaadressi mask (URL)

Selles veerus kuvatakse blokeeritud ribareklaami aadress või aadressimask.

Seisund

See veerg näitab, kas ribareklaamifilter kasutab seda aadressi ribareklaamide kontrollimisel.

Kui aadressireale on seatud väärtus *Aktiivne*, kasutab ribareklaamifilter seda aadressi ribareklaamide kontrollimisel.

Kui aadressireale on seatud väärtus *Mitteaktiivne*, ei kasuta ribareklaamifilter seda aadressi ribareklaamide kontrollimisel.

Muuda

Selle nupu klõpsamise korral avaneb blokeeritud ribareklaamide loendisse kuuluva ribareklaami aadressi või aadressimaski muutmise aken.

Kustuta

Selle nupu klõpsamise korral eemaldab ribareklaamifilter valitud ribareklaami aadressi/aadressimaski loendist.

Lisa

Selle nupu klõpsamise korral avaneb blokeeritud ribareklaamide loendisse ribareklaami aadressi või aadressimaski lisamise aken.

Aken „Lubatud ribareklaamid“

Nupp

Nupu klõpsamine avab menüü, mis sisaldab järgmisi üksusi.

- **Impordi ja lisa olemasolevatele.** Selle üksuse valimise korral saate importida lubatud aadresside loendi CSV-failist. Praeguseid aadresse ei kustutata.
- **Impordi ja asenda olemasolevad.** Selle üksuse valimise korral saate importida lubatud aadresside loendi CSV-failist. Praegused aadressid kustutatakse.
- **Ekspordi.** Selle üksuse valimise korral saate eksportida aadresside loendi CSV-faili. Saate eksportida kogu aadressiloendi või loendist valitud üksikud aadressid.

Lubatud ribareklaamide loend

Talletab lubatud ribareklaamide aadresse või aadressimaski. Ribareklaamifilter ei blokeeri ribareklaami, kui selle aadress on lubatud aadresside loendis.

Loendisse saate lisada aadressi või aadressimaski.

Kui veerus **Seisund** on aadressireale seatud väärtus *Aktiivne*, kasutab ribareklaamifilter seda aadressi ribareklaamide kontrollimisel.

Kui veerus **Seisund** on aadressireale seatud väärtus *Mitteaktiivne*, ei kasuta ribareklaamifilter seda aadressi ribareklaamide kontrollimisel.

Veebiaadressi mask (URL)

Selles veerus kuvatakse lubatud ribareklaami aadress või aadressimask.

Seisund

See veerg näitab, kas ribareklaamifilter kasutab seda aadressi ribareklaamide kontrollimisel.

Kui aadressireale on seatud väärtus *Aktiivne*, kasutab ribareklaamifilter seda aadressi ribareklaamide kontrollimisel.

Kui aadressireale on seatud väärtus *Mitteaktiivne*, ei kasuta ribareklaamifilter seda aadressi ribareklaamide kontrollimisel.

Muuda

Selle nupu klõpsamise korral avaneb lubatud ribareklaamide loendis ribareklaami aadressi või aadressimaski muutmise aken.

Kustuta

Selle nupu klõpsamise korral eemaldab ribareklaamifilter valitud ribareklaami aadressi/aadressimaski lubatud ribareklaamide loendist.

Lisa

Selle nupu klõpsamise korral avaneb lubatud ribareklaamide loendisse ribareklaami aadressi või aadressimaski lisamise aken.

Aken „Lubatud ribareklaamidega veebilehed“

[Nupp](#)

Nupu klõpsamine avab menüü, mis sisaldab järgmisi üksusi.

- **Impordi ja lisa olemasolevatele.** Selle üksuse valimise korral saate importida lubatud aadresside loendi CSV-failist. Praeguseid aadresse ei kustutata.
- **Impordi ja asenda olemasolevad.** Selle üksuse valimise korral saate importida lubatud aadresside loendi CSV-failist. Praegused aadressid kustutatakse.
- **Ekspordi.** Selle üksuse valimise korral saate eksportida aadresside loendi CSV-faili. Saate eksportida kogu aadressiloendi või loendist valitud üksikud aadressid.

[Lubatud ribareklaamidega veebisaitide loend](#)

Sisaldab nende veebisaitide aadresse, kus olete lubanud kuvada ribareklaame. Ribareklaamifilter ei blokeeri veebisaidi ribareklaame, kui selle aadress on loendis.

Kui veerus **Seisund** on aadressireale seatud väärtus *Aktiivne*, lubab ribareklaamifilter sellel veebisaidil kuvada ribareklaame.

Kui veerus **Seisund** on aadressireale seatud väärtus *Mitteaktiivne*, blokeerib ribareklaamifilter selle veebisaidi ribareklaamid.

[Muuda](#)

Selle nupu klõpsamise korral avaneb loendis valitud aadressi muutmise aken.

[Kustuta](#)

Selle nupu klõpsamise korral eemaldab ribareklaamifilter valitud veebisaidiaadressi loendist.

[Lisa](#)

Selle nupu klõpsamise korral avaneb loendisse veebisaidiaadressi lisamise aken.

Aken „Kaspersky veebisaidid“

Selles aknas kuvatakse loend Kaspersky veebisaitidest ja meie partnerite veebisaitidest, kus hostitakse Kaspersky reklaame.

Loendi on koostanud ja seda uuendavad Kaspersky eksperdid. Loend uueneb andmebaaside ja rakendusemoodulite uuendamisel automaatselt.

Rämpseilifiltri seaded

[Lülita Rämpseilifilter sisse/välja](#)

Selle lülitiga saate rämpseilifiltri sisse/välja lülitada.

Kui nupp on sisse lülitatud, tuvastab rämpseilifilter soovimatu meili (rämpsmeili) ja töötleb seda vastavalt teie meilikliendi reeglitele.

[Turvalisuse tase](#)

Jaotises **Turvalisuse tase** saate rämpseilifiltri jaoks valida ühe eelmääratud seadekogumitest (turvasemetest). Asjakohane turvatase tuleb valida töötingimuste ja hetkeolukorra põhjal.

Saadaval on järgmised turvasemed.

- **Äärmuslik.** Sellel turvasemel rakendab rämpseilifilter rämpseili filtreerimisel maksimaalset rangust.

Kõrge turvatase on soovitatav valida ohtlikus keskkonnas töötamise korral (näiteks tasuta meiliteenuse kasutamisel).

Kõrge turvatase seadmise korral võidakse tavameilid sagedamini liigitada rämpseilideks.

- **Optimaalne.** See turvatase tagab optimaalse tasakaalu jõudluse ja turvalisuse vahel. See tase sobib enamikus olukordades.

- **Madal.** Sellel turvasemel rakendab rämpseilifilter rämpseili filtreerimise minimaalset rangust.

Madal turvatase on soovitatav määrata turvalises keskkonnas töötamise korral (näiteks ettevõtte krüpteeritud meiliteenuse kasutamisel).

Madala turvatase seadmise korral liigitatakse tavameilid harvemini rämpseilideks või arvatavateks rämpseilideks.

[Optimaalse turvatase taastamine](#)

Selle lingi klõpsamise korral rakendab rakendus turvatase **Optimaalne**. Link kuvatakse, kui olete muutnud seadeid akna **Rämpseilifiltri täpsemad seaded** jaotises **Ära liigita sõnumit rämpseiliks**.

[Täpsemad seaded](#)

Lingi klõpsamise korral avaneb aken „Rämpseilifiltri täpsemad seaded“.

Rämpseilifiltri täpsemad seaded

Jaotises **Liigita sõnum rämpsmeiliks** saate määrata meili filtreerimise tingimused, mille järgi rämpsmeilifilter rämpsmeilid ära tunneb.

[kui see sisaldab andmepüügielemente](#)

See märkeruut lubab/keelab kontrollida, kas meilisõnumi tekst sisaldab andmepüügielemente või URL-e, mis on lisatud andmepüügi veebiaadresside loendisse.

Kui see ruut on märgitud, liigitab rämpsmeilifilter rämpsmeiliks meilid, mis sisaldavad andmepüügi veebiaadresside loendis leiduvaid URL-e.

Kui see ruut on märkimata, ei võrdle rämpsmeilifilter meilides sisalduvaid URL-e andmepüügi veebiaadresside loendiga.

[kui see sisaldab URL-e kahjur-URL-ide andmebaasist](#)

See märkeruut lubab/keelab kontrollida, kas meilides olevad lingid on lisatud kahjurlinkide loendisse.

[kui see on blokeeritud saatjalt](#)

See märkeruut lubab/keelab filtreerida meile blokeeritud saatjate loendi alusel; rämpsmeilifilter liigitab nende saatjate meilisõnumid rämpsmeiliks.

[Vali](#)

Selle lingi klõpsamise korral avaneb aken **Blokeeritud saatjad**, kus saate luua blokeeritud saatjate loendi.

Loendi loomisel saate määrata nii blokeeritud saatjate aadressid kui ka aadressimaskid.

See link on saadaval, kui märgitud on ruut **kui see on blokeeritud saatjalt**.

[kui see sisaldab blokeeritud fraase](#)

See märkeruut lubab/keelab filtreerida, kasutades loendit blokeeritud fraasidest, mille esinemine meilisõnumis näitab, et see on rämpsmeil.

[Vali](#)

Selle nupu klõpsamise korral avaneb aken **Blokeeritud fraasid**, kus saate luua blokeeritud fraaside loendi.

Loendi loomisel saate määrata nii blokeeritud fraasid kui ka fraasimaskid.

See link on saadaval, kui märgitud on ruut **kui see sisaldab blokeeritud fraase**.

[Kui see sisaldab vulgaarset sõnavara](#)

Selle lingi klõpsamisel avaneb aken **Ebatsensuurne sõnavara**. Selles aknas saate luua vulgaarsete sõnade loendi. Selliste sõnade esinemine meilisõnumis näitab, et see on rämpsmeil.

See link on saadaval, kui märgitud on ruut **Kui see sisaldab vulgaarset sõnavara**.

Jaotises **Ära liigita sõnumit rämpsmeiliks** saate määrata tunnused, mille järgi rämpsmeilifilter tunneb ära tavameilid.

[kui see on lubatud saatjalt](#)

See märkeruut lubab/keelab kontrollida, kas saatja aadress on lisatud lubatud saatjate loendisse.

Kui see ruut on märgitud, liigib rämpsmeilifilter lubatud saatjatelt saadud meilisõnumid tavameiliks.

Kui see ruut on märkimata, ei liigita rämpsmeilifilter lubatud saatjate meilisõnumeid tavameiliks. Lubatud saatjate loendis olevate saatjate saadetud meilisõnumeid ei filtreerita.

[Vali](#)

Selle lingi klõpsamise korral avaneb aken **Lubatud saatjad**, kus saate luua lubatud saatjate loendi.

Loendi loomisel saate määrata nii lubatud saatjate aadressid kui ka aadressimaskid.

See link on saadaval, kui märgitud on ruut **kui see on lubatud saatjalt**.

[kui see sisaldab lubatud fraase](#)

See märkeruut lubab/keelab meilisõnumi kontrollimise lubatud fraaside loendi alusel.

Kui see ruut on märgitud, liigib rämpsmeilifilter selle loendi lubatud fraase sisaldavad meilisõnumid tavameiliks.

Kui see ruut on märkimata, ei kasuta rämpsmeilifilter meilisõnumite filtreerimiseks lubatud fraaside loendit ega liigita loendi väljendeid sisaldavaid meilisõnumeid tavameiliks.

[Vali](#)

Selle lingi klõpsamise korral avaneb aken **Lubatud fraasid**, kus saate luua lubatud fraaside loendi.

Loendi loomisel saate määrata nii üksikfraasid kui ka lubatud fraaside maskid.

See link on saadaval, kui märgitud on ruut **kui see sisaldab lubatud fraase**.

Jaotises **Toimingud sõnumitega** saate määrata sildid, mis lisatakse nende sõnumite teemariidadele, millele rämpsmeilifilter määrab oleku *Rämpsmeil* või *Arvatav rämpsmeil*.

[Lisa märgistus \[!! RÄMPSMEIL\] rämpsmeilina liigitatud sõnumite teemareale](#)

Märgistus lisatakse automaatselt nende sõnumite teemale, mille rämpsmeilifilter tuvastab *rämpsmeilina*.

Sildi tekst kuvatakse märkeruudu kõrval oleval väljal. Vaikimisi lisab rämpsmeilifilter märgistuse [!! RÄMPSMEIL].

[Lisa märgistus \[?? Arvatav RÄMPSMEIL\] arvatava rämpsmeilina liigitatud sõnumite teemareale](#)

Märgistus lisatakse automaatselt nende sõnumite teemale, mille rämpsmeilifilter tuvastab *arvatava rämpsmeilina*.

Sildi tekst kuvatakse märkeruudu kõrval oleval väljal. Vaikimisi lisab rämpsmeilifilter märgistuse [?? Arvatav RÄMPSMEIL].

Aken „Blokeeritud fraasi lisamine/muutmine“

Fraasi mask [?](#)

Fraas või fraasimask, mida peetakse sõnumis tuvastamise korral rämpsmeili tunnuseks.

Fraasi kaalukoeffitsient [?](#)

Arvväärtus, mis tähistab tõenäosust, et blokeeritud fraasi sisaldav sõnum on rämpsmeil. Mida suurem on kaalukoeffitsient, seda suurem on tõenäosus, et blokeeritud fraasi sisaldav sõnum on rämpsmeil.

Rämpsmeilifilter märgib sõnumi rämpsmeiliks, kui selles sisalduvate blokeeritud fraaside kaalukoeffitsientide summa ületab määratud väärtust.

Olek [?](#)

Jaotises **Olek** saate määrata, kas soovite, et rämpsmeilifilter otsiks sõnumitest blokeeritud fraase.

- **Aktiivne.** Rämpsmeilifilter kontrollib, kas sõnumites sisaldub blokeeritud fraase.
- **Mitteaktiivne.** Rämpsmeilifilter ei kontrolli, kas sõnumites sisaldub blokeeritud fraase.

Aken „Blokeeritud saatjad“

Nupp [?](#)

Selle nupu klõpsamise korral avaneb menüü, kus saab valida järgmised toimingud.

- **Impordi ja lisa olemasolevatele.** Selle valiku korral saate importida blokeeritud saatjate loendi CSV-failist. Praegust saatjate loendit ei kustutata.
- **Impordi ja asenda olemasolevad.** Selle valiku korral saate importida blokeeritud saatjate loendi CSV-failist. Praegune saatjate loend kustutatakse.
- **Ekspordi.** Selle valiku korral saate eksportida blokeeritud saatjate loendi CSV-faili.

Blokeeritud saatjate loend [?](#)

Sisaldab loendit aadressidest, mille rämpsmeilifilter liigitab rämpsmeilialliketeks.

Loendisse saate lisada aadressi või aadressimaski.

Kui veerus **Seisund** on aadressireale seatud väärtus *Aktiivne*, liigitab rämpsmeilifilter aadressi blokeerituks.

Kui veerus **Seisund** on aadressireale seatud väärtus *Mitteaktiivne*, arvab rämpsmeilifilter aadressi loendist välja.

Saatja aadress [?](#)

Selles veerus kuvatakse blokeeritud saatja meiliaadress või meiliaadressi mask.

Seisund [?](#)

See veerg näitab, kas rämpsmeilifilter liigitab sellelt aadressilt saabunud sõnumid rämpsmeiliks.

Kui aadressireale on seatud väärtus *Aktiivne*, liigitab rämpsmeilifilter sellelt aadressilt saadud sõnumid rämpsmeiliks.

Kui aadressireale on seatud väärtus *Mitteaktiivne*, arvab rämpsmeilifilter valitud aadressi loendist välja.

Muuda [?](#)

Selle nupu klõpsamise korral avaneb loendis valitud URL-i või URL-i maski muutmise aken.

Kustuta [?](#)

Selle nupu klõpsamise korral eemaldab rämpsmeilifilter valitud aadressi või aadressimaski loendist.

Lisa [?](#)

Selle nupu klõpsamise korral avaneb loendisse URL-i või URL-i maski lisamise aken.

Aken „Blokeeritud fraasid“

Nupp

Selle nupu klõpsamise korral avaneb menüü, kus saab valida järgmised toimingud.

- **Impordi ja lisa olemasolevatele.** Selle valiku korral saate importida blokeeritud fraaside loendi CSV-failist. Praeguseid fraase ei kustutata.
- **Impordi ja asenda olemasolevad.** Selle valiku korral saate importida blokeeritud fraaside loendi CSV-failist. Praegused fraasid kustutatakse.
- **Ekspordi.** Selle valiku korral saate eksportida blokeeritud fraaside loendi CSV-faili.

Blokeeritud fraaside loend

Sisaldab põhifraase, mis näitavad, et neid sisaldav sõnum on rämpsmeil.

Loendisse saate lisada fraasi või fraasimaski.

Kui veerus **Seisund** on fraasireale seatud väärtus *Aktiivne*, kasutab rämpsmeilifilter seda fraasi meilisõnumite filtreerimisel.

Kui veerus **Seisund** on fraasireale seatud väärtus *Mitteaktiivne*, arvab rämpsmeilifilter fraasi loendist välja ja ei kasuta seda meilisõnumite filtreerimisel.

Muuda

Selle nupu klõpsamise korral avaneb aken, kus saate muuta loendis valitud fraasi või fraasimaski.

Kustuta

Selle nupu klõpsamise korral eemaldab rämpsmeilifilter valitud fraasi või fraasimaski loendist.

Lisa

Selle nupu klõpsamise korral avaneb aken, kus saate loendisse lisada fraasi või fraasimaski.

Meiliaadressi lisamise/muutmise aken

Meiliaadressi mask [?](#)

Selles aknas saate määrata meiliaadressi või meiliaadressi maski.

Maski sisestamisel saate kasutada metamärke * ja ?; * tähistab mis tahes tähemärgijada ja ? tähistab mis tahes üksikmärki.

Olek [?](#)

Jaotises **Olek** saate määrata, kas soovite, et lubatud/blokeeritud saatjate loendi alusel sõnumite kontrollimisel blokeeriks rämpsmeilifilter sellelt aadressilt saadetud sõnumid.

- **Aktiivne.** Rämpseilifilter blokeerib sellelt aadressilt saadetud sõnumid.
- **Mitteaktiivne.** Rämpseilifilter ei blokeeri sellelt aadressilt saadetud sõnumeid.

Aken „Lubatud fraasi lisamine/muutmine“

Fraasi mask [?](#)

Fraas või fraasimask, mille esinemine sõnumis näitab, et see pole rämpsmeil.

Fraasi kaalukoeffitsient [?](#)

Arvväärtus, mis tähistab tõenäosust, et lubatud fraasi sisaldav sõnum ei ole rämpsmeil. Mida suurem on kaalukoeffitsient, seda suurem on tõenäosus, et lubatud fraasi sisaldav sõnum ei ole rämpsmeil.

Rämpsmeilifilter ei märgi sõnumit rämpsmeiliks, kui selles sisalduvate lubatud fraaside kaalukoeffitsientide summa ületab määratud väärtust.

Olek [?](#)

Jaotises **Olek** saate määrata, kas rämpsmeilifilter otsib sõnumitest konkreetset lubatud fraasi.

- **Aktiivne.** Rämpsmeilifilter kontrollib, kas lubatud fraas sisaldub sõnumites.
- **Mitteaktiivne.** Rämpsmeilifilter ei kontrolli, kas lubatud fraas sisaldub sõnumites.

Aken „Lubatud saatjad“

Nupp

Selle nupu klõpsamise korral avaneb menüü, kus saab valida järgmised toimingud.

- **Impordi ja lisa olemasolevatele.** Selle valiku korral saate importida lubatud saatjate loendi CSV-failist. Praegust saatjate loendit ei kustutata.
- **Impordi ja asenda olemasolevad.** Selle valiku korral saate importida lubatud saatjate loendi CSV-failist. Praegune saatjate loend kustutatakse.
- **Ekspordi.** Selle valiku korral saate eksportida lubatud saatjate loendi CSV-faili.

Lubatud saatjate loend

Sisaldab nende saatjate aadresside loendit, kelle sõnumid liigitab rämpsmeilifilter tavameiliks.

Loendisse saate lisada aadressi või aadressimaski.

Kui veerus **Seisund** on aadressireale seatud väärtus *Aktiivne*, liigitab rämpsmeilifilter kõik selle saatja sõnumid tavameiliks.

Kui veerus **Seisund** on aadressireale seatud väärtus *Mitteaktiivne*, ei liigita rämpsmeilifilter kõiki selle saatja sõnumeid tavameiliks ja kontrollib neid tavapärase meetodite abil.

Saatja aadress

Selles veerus kuvatakse lubatud saatja meiliaadress või meiliaadressi mask.

Seisund

See veerg näitab, kas rämpsmeilifilter liigitab sellelt aadressilt saabunud sõnumid tavameiliks.

Kui aadressireale on seatud väärtus *Aktiivne*, liigitab rämpsmeilifilter sellelt aadressilt saadud sõnumid tavameiliks.

Kui aadressireale on seatud väärtus *Mitteaktiivne*, arvab rämpsmeilifilter valitud aadressi loendist välja.

Muuda

Selle nupu klõpsamise korral avaneb aken, kus saate muuta lubatud saatjate loendis sisalduvad URL-i või URL-i maski.

Kustuta

Selle nupu klõpsamise korral eemaldab rämpsmeilifilter valitud aadressi või aadressimaski loendist.

Lisa

Selle nupu klõpsamise korral avaneb aken, kus saate lubatud saatjate loendisse lisada URL-i või URL-i maski.

[Lisa minu meilisõnumite saajad lubatud saatjate hulka](#)

Kui see ruut on märgitud, lisab rakendus teie saadetud meilide saajad lubatud saatjate loendisse.

Aken „Lubatud fraasid“

Nupp

Selle nupu klõpsamise korral avaneb menüü, kus saab valida järgmised toimingud.

- **Impordi ja lisa olemasolevatele.** Selle valiku korral saate importida lubatud fraaside loendi CSV-failist. Praeguseid fraase ei kustutata.
- **Impordi ja asenda olemasolevad.** Selle valiku korral saate importida lubatud fraaside loendi CSV-failist. Praegused fraasid kustutatakse.
- **Ekspordi.** Selle valiku korral saate eksportida lubatud fraaside loendi CSV-faili.

Lubatud fraaside loend

Sisaldab põhiväljendeid, mille esinemine sõnumis näitab, et see pole rämpsmeil.

Loendisse saate lisada fraasi või fraasimaski.

Kui veerus **Seisund** on fraasireale seatud väärtus *Aktiivne*, kasutab rämpsmeilifilter seda fraasi meilisõnumite filtreerimisel.

Kui veerus **Seisund** on fraasireale seatud väärtus *Mitteaktiivne*, ei kasuta rämpsmeilifilter seda fraasi meilisõnumite filtreerimisel.

Muuda

Selle nupu klõpsamise korral avaneb aken, kus saab muuta loendis valitud fraasi või fraasimaski.

Kustuta

Selle nupu klõpsamise korral eemaldab rämpsmeilifilter valitud fraasi või fraasimaski loendist.

Lisa

Selle nupu klõpsamise korral avaneb aken, kus saate loendisse lisada fraasi või fraasimaski.

Turvaliste maksete seaded

[Lülita Turvalised maksed sisse/välja](#)

Selle lülitiga saate turvalised maksed sisse/välja lülitada.

Kui nupp on roheline, jälgib rakendus kõiki katseid pääseda juurde pankade või maksesüsteemide veebisaitidele ja teeb vaikimisi määratud või kasutaja seadistatud toiminguid. Turvaliste maksete režiimis töötamisel küsib rakendus kasutajalt kaitstud veebilehitseja käivitumisel kinnitust.

Kui nupp on punane, lubab rakendus külastada pankade või maksesüsteemide veebisaitide tavalises veebilehitsejas.

[Lisainfo](#)

Selle lingi klõpsamise korral avaneb veebilehitseja aknas komponendi üksikasju sisaldav leht.

Jaotises **Pankade ja maksesüsteemide esmasel külastamisel toimi järgmiselt** saate valida toiminguid, mille rakendus teeb, kui avate pankade või maksesüsteemide veebisaitide esimest korda.

[Käivita Kaitstud veebilehitseja](#)

Kui rakendus tuvastab katse pääseda juurde määratud veebisaidile, avab see veebisaidi kaitstud veebilehitsejas. Veebisaidile juurdepääsemiseks kasutatav tavaline veebilehitseja kuvab teate, mis teavitab teid kaitstud veebilehitseja käivitamisest.

[Küsi kasutajalt](#)

Kui rakendus tuvastab katse pääseda juurde määratud veebisaidile, küsib see teilt, kas käivitada kaitstud veebilehitseja või avada veebisait tavalises veebilehitsejas.

[Ära käivita Kaitstud veebilehitsejat](#)

Kui proovite pääseda juurde määratud veebisaidile, ei kasuta rakendus kaitstud veebilehitsejat. Veebisait avatakse tavalises veebilehitsejas.

Jaotises **Lisaks** saate seadistada turvaliste maksete lisaseadeid.

[Veebisaitide avamiseks Turvaliste maksete aknast kasuta järgmist Vaikeveebilehitseja](#)

Ripploendist saate valida veebilehitseja, milles rakendus avab aknas „Turvalised maksed“ valitud pankade või maksesüsteemide veebisaidid.

Turvalised maksed on saadaval järgmistel veebilehitsejate kasutajatele: Microsoft Internet Explorer, Chromiumpõhine Microsoft Edge, Mozilla Firefox, Google Chrome ja Yandex.Browser.

Vaikimisi kasutavad turvalised maksed operatsioonisüsteemi vaikeveebilehitsejat.






[Loo Turvaliste maksete otsetee](#)

Selle lingi klõpsamise korral luuakse turvaliste maksete käivitamiseks töölauale otsetee. See otsetee võimaldab avada akna, mis sisaldab nende pankade või maksesüsteemide veebisaitide loendit, millele juurdepääsemiseks kasutatakse kaitstud veebilehitsejat.

[Windows 8, Windows 8.1 ja Windows 10 64-bitistes versioonides kasutatakse brauseri kaitsmiseks riistvara virtualiseerimist.](#)

Ohutu sirvimise seaded

Seaded	Kirjeldus
<p>Turvalisuse tase</p>	<p>Rakendus kasutab turvalise sirvimise käitamiseks mitmesuguseid seadegruppe. Rakendusse salvestatud seadekomplekte kutsutakse <i>turbetasemeteks</i>.</p> <ul style="list-style-type: none"> • Äärmuslik. Veebiliikluse turbetase, mille korral kontrollib ohutu sirvimise funktsioon arvutisse HTTP- ja FTP-protokollide kaudu saabuvat veebiliiklust väga põhjalikult. Ohutu sirvimine kontrollib rakenduste andmebaaside täiskomplekti abil üksikasjalikult kõiki veebiliikluse objekte ja teeb ka kõige sügavama heuristilise analüüsi. • Optimaalne. Veebiliikluse turvatase, mis tagab Kaspersky rakenduse jõudluse ja veebiliikluse turvalisuse optimaalse tasakaalu. Ohutu sirvimine teeb keskmise põhjalikkustasemega heuristilise analüüsi. Seda veebiliikluse turvataset soovitavad Kaspersky spetsialistid. • Madal. Veebiliikluse turvatase, mille seaded tagavad kõige kiirema veebiliikluse kontrolli. Ohutu sirvimine teeb madala põhjalikkustasemega heuristilise analüüsi.
<p>Toiming ohu avastamisel</p>	<ul style="list-style-type: none"> • Teata. Ohutu sirvimise funktsioon teavitab teid nakatunud või arvatavalt nakatunud objekti avastamisest ning küsib teilt, mida sellega teha. See valik on saadaval, kui menüüs Seaded → Jõudlusseaded → Arvutiressursside kasutus on märkeruudust Tee soovitatavad toimingud automaatselt märges eemaldatud. • Soorita toiming automaatselt. Ohutu sirvimine valib toimingu praeguste seadete põhjal automaatselt. Kui veebiressurss on erandite loendis või sisalda ühtki nakatunud ega arvatavalt nakatunud objekti, lubab ohutu sirvimine sellele juurdepääsu. Kui ohutu sirvimise kontroll tuvastab veebiressurssis nakatunud või arvatavalt nakatunud objekti, siis juurdepääs veebiressurssile blokeeritakse. See valik on saadaval, kui menüüs Seaded → Jõudlusseaded → Arvutiressursside kasutus on märgitud ruut Tee soovitatavad toimingud automaatselt. • Blokeeri allalaadimine. Kui teete selle valiku, siis veebiliiklusest nakatunud objekti avastamise korral blokeerib ohutu sirvimise funktsioon sellele objektile juurdepääsu ja kuvab veebilehitsejas teate.
<p>Kontrollimismeetodid</p> <p>Kontrolli, kas veebiaadress on pahatahtlike veebiaadresside andmebaasis</p>	<p>Kui kontrollite, kas lingid on pahatahtlike linkide andmebaasis, saate jälgida keelunimekirja lisatud veebisaitide. Pahatahtlike linkide andmebaasi on koostanud Kaspersky spetsialistid. See kuulub tarkvara levituskomplekti ja seda uuendatakse koos Kaspersky rakenduse andmebaasiga.</p>
<p>Kontrolli, kas veebiaadress on reklaamprogramme sisaldavate veebiaadresside andmebaasis</p>	<p>Üheks näiteks on tarkvara, mis suunab internetis teie otsingupäringu reklaamveebisaidile. Seetõttu satute reklaamveebisaidile, mitte teie otsingupäringu suhtes kõige asjakohasema veebiressursi juurde.</p>

<p>Kontrolli, kas veebiaadress on selliste legitiimseid rakendusi sisaldavate veebiaadresside andmebaasis, mida sissetungijad võivad kasutada teie arvuti või isiklike andmete kahjustamiseks</p>	<p>Sellesse kategooriasse kuulub näiteks kaughaldustööriist, mida süsteemiadministraatorid kasutavad õiguspäraselt tõrkeotsinguks. Kurjategija võib sellise tööriista arvutisse paigaldada ilma teie teadmata, et pääseda juurde teie arvutile ja kasutada seda kuritegelikel eesmärkidel.</p> <p>Kaspersky rakendus lubab selliste rakenduste allalaadimist veebilehtedel asuvate linkide klõpsamisega. Erandiks on ühekordsed lingid. Te ei saa neid linke kasutada selliste õiguspärase rakenduste allalaadimiseks, mida häkkerid võivad kasutada teie arvuti või andmete kahjustamiseks.</p>
<p>Kasuta heuristilist analüüsi</p>	<p>Tehnika, mis on ette nähtud selliste ohtude avastamiseks, mida ei saa tuvastada Kaspersky rakenduste andmebaaside praeguse versiooni abil. See võimaldab teil leida faile, mis võivad sisaldada tundmatut pahavara või teadaoleva pahavaraprogrammi uut modifikatsiooni.</p> <p>Veebiliiklusest viiruste ja muude ohtlike rakenduste otsimise käigus täidab heuristiline analüüs käivitusfailides sisalduvaid juhiseid. Heuristilise analüüsi täidetavate juhiste arv on heuristilise analüüsi jaoks määratud tasemest. Heuristilise analüüsi tase määrab uute ohtude otsingu põhjalikkuse, operatsioonisüsteemiresursside koormuse ja heuristilise analüüsi kestuse vahelise tasakaalu.</p>
<p>Andmepüügivastane kaitse Kontrolli, kas veebiaadress on andmepüügi- ja võltsitud krüptovaluuta kauplemisplatvormide veebiaadresside andmebaasis (mõnedes tellimuslepingutes Kontrolli, kas veebiaadress on andmepüügiveebiaadresside andmebaasis)</p>	<p>Andmepüügilinkide ja võltsitud krüptovaluutavahetuste andmebaas sisaldab praegu teadaolevate andmepüügirünnakuteks kasutatavate veebisaitide veebiaadresse. Kaspersky täiendab seda andmebaasi rahvusvaheliselt andmepüügivastasel tööühmalt (Anti-Phishing Working Group) saadud aadressidega. Andmepüügilinkide ja võltsitud krüptovaluutavahetuste andmebaas kuulub tarkvara levituskomplekti ning seda uuendatakse koos Kaspersky rakenduse andmebaasiga.</p>
<p>Kasuta heuristilist analüüsi</p>	<p>Tehnika, mis on ette nähtud selliste ohtude avastamiseks, mida ei saa tuvastada Kaspersky rakenduste andmebaaside praeguse versiooni abil. See võimaldab andmepüügi avastada ka siis, kui URL-i pole andmepüügi veebiaadresside andmebaasis.</p>
<p>Kontrolli URL-e</p>	<p>URL-i nõustaja komponent kontrollib linke Chromium-i-põhises Microsoft Edge'is, Google Chrome'is või Mozilla Firefoxis avatud veebilehel. Kaspersky rakendus kuvab kontrollitud lingi kõrval ühte järgmistest ikoonidest.</p> <ul style="list-style-type: none">  – kui lingitud veebileht on Kaspersky andmetel turvaline  – kui teave lingitud veebilehe ohutuse kohta puudub  – kui Kaspersky andmetel saavad häkkerid teie arvutit või andmeid kahjustada, kasutades veebilehte, millele link viib  – kui Kaspersky andmetel võib veebileht, millele link viib, olla nakatunud või häkitud  – kui lingitud veebileht on Kaspersky andmetel ohtlik Lingi kohta üksikasju sisaldava hüpikakna kuvamiseks viige hiirekursor vastavale ikoonile.
<p>Kõigil veebisaitidel peale määratute Halda erandeid</p>	<p>Selle valiku korral kontrollib rakendus linke kõigil veebisaitidel, välja arvatud aknas Erandid määratud saitidel.</p> <p>Akna Erandid avamiseks tuleb klõpsata linki Halda erandeid.</p>

<p>Ainult määratud veebisaitidel Konfigureeri kontrollitavad veebisaidid</p>	<p>Selle valiku korral kontrollib Kaspersky linke ainult veebisaitidel, mis on määratud aknas Kontrollitud veebisaidid.</p> <p>Akna Kontrollitud veebisaidid avamiseks tuleb klõpsata linki Konfigureeri kontrollitavad veebisaidid.</p>
<p>Konfigureeri URL-i nõustaja</p>	<ul style="list-style-type: none"> • Kõik URL-id. Rakendus kontrollib linke igat tüüpi veebilehtedel. • Ainult URL-id otsingutulemustes. Rakendus kontrollib linke veebilehtedel, mis sisaldavad otsingumootoritest saadud otsingutulemusi.
<p>Veebisaitide kategooriad</p>	<p>Kui märgitud on ruut Näita informatsiooni veebisaitide sisu kategooriate kohta, lisab rakendus lingikommentaaridesse teabe, mis näitab, kas veebisait kuulub määratud kategooriatesse (näiteks Vägivald või Täiskasvanutele mõeldud sisu).</p> <p>Hoiatusi mittevajavate kategooria kõrval kuvatavatest ruutudest saate märke eemaldada.</p>
<p>Ära kontrolli veebiliiklust järgmisest allikast usaldusväärset URL-id</p>	<p>Kui ruut on märgitud, ei kontrolli ohutu sirvimise funktsioon sisu veebilehtedel/veebisaitidel, mille aadressid on usaldusväärsete veebiaadresside loendis. Usaldusväärsete veebiaadresside loendisse saate lisada nii kindlaid veebilehti/veebisaidiaadresse kui ka veebilehe-/veebisaidiaadressi maske. Usaldusväärsete veebiaadresside loend on saadaval aknas Usaldusväärset URL-id, mille avamiseks saate klõpsata usaldusväärset URL-id linki.</p>

Aken „Kaspersky ja tema partnerite veebisaidid“

Selles aknas kuvatakse Kaspersky ja meie partnerite veebisaitide loend.

Loendi on koostanud ja seda uuendavad Kaspersky eksperdid. Loend uueneb andmebaaside ja rakendusemoodulite uuendamisel automaatselt.

Võrgurünnakute tõrje seaded

Võrgurünnakute tõrje laaditakse operatsioonisüsteemi käivitamisel ja jälgib, kas sissetulevas võrguliikluses leidub võrgurünnakutele iseloomulikke tegevust. Kui Kaspersky rakendus tuvastab võrgurünnakukatse kasutaja arvutile, blokeerib see võrguühenduse ründava arvutiga. Praegu teadaolevate võrgurünnakutüüpide kirjeldused ja nende neutraliseerimismeetodid sisalduvad Kaspersky rakenduse andmebaasides. Võrgurünnakute tõrje tuvastatavate võrgurünnakute loendit uuendatakse rakenduste andmebaaside ja moodulite uuendamisel.

Võrgurünnakute tõrje seaded

Seaded	Kirjeldus
Kohtle pordi skannimist ja võrgu ummistumist rünnakutena	<p><i>Võrgu ummistamine</i> on rünnak organisatsiooni võrguressursside (näiteks veebiserverite) vastu. Selle rünnaku korral saadetakse väga suures koguses liiklust, et ammendada võrgu läbilaskevõime. Selle tulemusel ei pääse kasutajad organisatsiooni võrguressurssidele juurde.</p> <p><i>Pordi skannimise rünnaku</i> korral skannitakse UDP- ja TCP-porte, samuti arvuti võrguteenuseid. See rünnak võimaldab enne ohtlikumaid võrgurünnakuid määrata kindlaks arvuti haavatavustaseme. Pordi skannimine võimaldab häkkeritel määrata kindlaks ka arvuti operatsioonisüsteemi ja valida selle jaoks operatsioonisüsteemipõhiseid rünnakuid.</p> <p>Kui lüliti on sisse lülitatud, blokeerib võrgurünnakute tõrje komponent portide skannimise ja võrgu ummistamise.</p>
Lisa ründav arvuti blokeeritud arvutite nimekirja N minutiks	<p>Kui lüliti on sisse lülitatud, lisab võrgurünnakute tõrje komponent ründava arvuti blokeeritud seadmete loendisse. See tähendab, et pärast esimest võrgurünnakukatset blokeerib võrgurünnakute tõrje määratud aja jooksul võrguühenduse ründava arvutiga, et kaitsta kasutaja arvutit automaatselt samalt aadressilt pärinevate võimalike tulevaste võrgurünnakute eest. Ründava arvuti saab blokeerimisloendisse lisada kõige vähem üheks minutiks. Maksimaalne kestus on 32 768 minutit.</p>
Halda erandeid	<p>Loend sisaldab IP-aadresse, millelt pärinevaid võrgurünnakuid võrgurünnakute tõrje ei blokeeri.</p> <p>Rakenduse aruandluses ei kajastata teavet erandite loendis olevatelt IP-aadressidelt pärinevate võrgurünnakute kohta.</p>

Sissetungitõrje seaded

[Lülita sissetungitõrje sisse/välja](#)

Selle lülitiga saate sissetungide vältimise sisse/välja lülitada.

[Lisainfo](#)

Selle lingi klõpsamise korral avaneb veebilehitseja aknas komponendi üksikasju sisaldav leht.

[Usalda digiallkirjaga rakendusi](#)

Kui see ruut on märgitud, liigitab sissetungitõrje digiallkirjaga rakendused usaldusväärseteks. Sissetungitõrje teiselaldab need rakendused gruppi **Usaldusväärsed** ega kontrolli nende tegevust.

Kui see ruut on märkimata, ei liigita sissetungitõrje digiallkirjaga rakendusi usaldusväärseteks ja kontrollib nende tegevusi. Sissetungitõrje liigitab usaldusväärsete tarkvaratootjate (näiteks Microsofti) rakendused usaldusväärseteks olenemata sellest, kas see ruut on märgitud või mitte.

[Laadi rakenduste reeglid Kaspersky Security Networki \(KSN\) andmebaasist](#)

Kui see ruut on märgitud, saadab sissetungitõrje rakendusegrupi määratlemiseks päringu Kaspersky Security Networki andmebaasi.

Kui see ruut on märkimata, ei otsi sissetungitõrje rakenduse usaldusgrupi kindlaks määramiseks teavet Kaspersky Security Networki andmebaasist.

[Usaldusgrupp rakendustele, mida polnud olemasolevatele rühmadele võimalik lisada](#)

Selle lingi klõpsamisel avaneb aken **Usaldusgrupp rakendustele, mida polnud olemasolevatele rühmadele võimalik lisada**. Selles aknas saate valida [usaldusgruppi](#), millesse määratakse tundmatud rakendused.

Saate teha ühe järgmistest valikutest.

- Usaldusväärsed.
- Nõrgad piirangud.
- Tugevad piirangud.
- Ebausaldusväärsed.

[Usaldusgrupp rakendustele, mis käivituvad enne kui <PRODUCT>](#)

Selle lingi klõpsamise korral avaneb aken **Usaldusgrupp rakendustele, mis käivituvad enne kui <PRODUCT>**. Selles aknas saate muuta nende rakenduste [usaldusgruppi](#), mis käivituvad enne kui Kaspersky. Enne Kaspersky käivitamist käivituvate rakenduste võrgutegevust kontrollitakse valitud usaldusgrupi reeglite järgi.

Vaikimisi määratakse enne Kaspersky käivitamist käivituvate rakenduste usaldusgrupp Kaspersky loodud reeglite alusel.

[Rakenduste haldus](#)

Selle lingi klõpsamisel avaneb aken **Rakenduste haldus**. Selles aknas saate muuta rakenduste reeglite loendi.

[Ressursside haldus](#)

Selle lingi klõpsamisel avaneb aken **Ressursside haldus**. Selles aknas saate luua isiklike andmete loendi ning operatsioonisüsteemi seadete ja ressursside loendi. Sissetungitõrje kontrollib juurdepääsu nendele üksustele.

Aken „Veebimajakad“

Selles aknas kuvatakse veebimajakate loend.

Loendi on koostanud ja seda uuendavad Kaspersky eksperdid. Loend uueneb andmebaaside ja rakendusemoodulite uuendamisel automaatselt.

Privaatse sirvimise kategooriad ja erandid

[Veebianalüüsiteenused](#)

Kui ruut on märgitud, blokeerib privaatse sirvimise komponent veebianalüüsiteenused, mis analüüsivad tegevuse jälgimise teel teie veebitegevust.

Lingi **Kuva nimekiri** klõpsamise korral avaneb aken, mis sisaldab tegevuse jälgimise teel teie veebitegevust analüüsivate veebianalüüsiteenuste loendit.

[Reklaamiagentuurid](#)

Kui ruut on märgitud, blokeerib privaatse sirvimise komponent reklaamibüroodel reklaamieesmärgil teie veebitegevuse jälgimise.

Lingi **Kuva nimekiri** klõpsamise korral avaneb aken, mis sisaldab reklaamieesmärgil teie veebitegevust jälgivate reklaamiagentuuride loendit.

[Veebimajakad](#)

Kui ruut on märgitud, blokeerib privaatse sirvimise komponent teie veebitegevuse jälgimise veebimajakade abil. Veebimajakad on veebilehtedesse manustatud ja kasutajate jaoks nähtamatud objektid.

Lingi **Kuva nimekiri** klõpsamise korral avaneb aken, mis sisaldab veebimajakate loendit.

[Sotsiaalvõrgustikud](#)

Kui see ruut on märgitud, blokeerib privaatse sirvimise komponent suhtlusvõrkude külastamise ajal andmekogumise, välja arvatud nende suhtlusvõrkude endi teostatava andmekogumise. Andmekogumise blokeerimine ei takista funktsioonide „Märgi meeldivaks“, „+1“ ja sarnaste funktsioonide kasutamist.

Suhtlusvõrkude nimedega märkeruudud võimaldavad teil määrata suhtlusvõrgud, mille veebisaitidel peab rakendus andmekogumise blokeerima.

[Erandid](#)

Selle lingi klõpsamise korral avaneb aken, milles saate määrata veebisaidid, kus teie veebitegevuse jälgimine on lubatud.

Aken „Ühildumatud veebisaidid“

Selles aknas on kuvatud loend veebisaitidest, mis Kaspersky andmetel ei pruugi andmekogumise blokeerimise korral olla kasutatavad.

Loendi on koostanud ja seda uuendavad Kaspersky eksperdid. Loend uueneb andmebaaside ja rakendusemoodulite uuendamisel automaatselt.

Aken „Privaatse sirvimise seaded“

[Lülita privaatne sirvimine sisse/välja](#)

Kui lüliti on sisse lülitatud, tuvastab privaatse sirvimise komponent veebi sirvimise ajal jälgimisteenuste andmekogumiskatsed. Jälgimisteenused analüüsivad saadud teabe abil teie tegevust ja näitavad analüüsitulemuste põhjal teile asjakohaseid reklaame.

[Kogu vaid statistikat](#)

Selle valiku korral töötab privaatse sirvimise komponent *avastamise režiimis*, mis võimaldab teil vaadata aruandeid avastatud andmekogumiskatsete kohta.

[Blokeeri andmete kogumine](#)

Selle valiku korral töötab privaatse sirvimise komponent *blokeerimise režiimis*, mis tuvastab ja blokeerib andmete kogumise katsed. Teave nende katsete kohta kirjutatakse aruandesse.

[Kategooriad ja erandid](#)

Selle lingi klõpsamise korral avaneb aken, kus saate määrata jälgimisteenuste kategooriad, mis tuleb blokeerida või millel tuleb lubada andmeid koguda. Selles aknas saate alustada loendi loomist veebisaitidest, mille jälgimistegevuse soovite lubada.

[Blokeeri jälgimine](#)

Kui ruut on märgitud ja blokeerimise režiim on sisse lülitatud, saadab veebilehitseja veebisaidi külastamise korral veebisaidile HTTP-päise „Ära jälgi“, mis tähendab, et teie tegevust pole lubatud jälgida.

[Luba andmete kogumine Kaspersky ja tema partnerite veebisaitidel](#)

Kui see ruut on märgitud, lubab Kaspersky andmeid koguda Kaspersky ja oma partnerite veebisaitidel.

[Kaspersky ja tema partnerite veebisaidid](#)

Selle lingi klõpsamise korral avaneb Kaspersky ja meie partnerite veebisaitide loendi aken.

[Luba andmete kogumine ühildumatutel veebisaitidel](#)

Kui see ruut on märgitud, lubab Kaspersky andmeid koguda veebisaitidel, mis ei pruugi andmete kogumise blokeerimise korral olla kasutatavad.

[Ühildumatud veebisaidid](#)

Selle lingi klõpsamise korral avaneb aken, mis sisaldab loendit veebisaitidest, mis ei pruugi andmete kogumise blokeerimise korral olla kasutatavad.

Aken „Reklaamiagentuurid“

Selles aknas on kuvatud loend reklaamiagentuuridest, mis jälgivad teie veebitegevust reklaamieesmärgil.

Loendi on koostanud ja seda uuendavad Kaspersky eksperdid. Loend uueneb andmebaaside ja rakendusemoodulite uuendamisel automaatselt.

Aken „Veebianalüüsiteenused“

Selles aknas on kuvatud loend veebianalüüsiteenustest, mis analüüsivad tegevuse jälgimise teel teie veebitegevust.

Loendi on koostanud ja seda uuendavad Kaspersky eksperdid. Loend uueneb andmebaaside ja rakendusemoodulite uuendamisel automaatselt.

Meilide kaitse seaded

Seaded	Kirjeldus
<p>Turvalisuse tase</p>	<p>Kaspersky rakendus kasutab Meilide kaitse käitamiseks erinevaid seadete gruppe. Rakendusse salvestatud seadekomplekte kutsutakse <i>turbetasemeteks</i>.</p> <ul style="list-style-type: none"> • Äärmuslik. Selle meilikaitse turvataseme valimise korral rakendab meilide kaitse sõnumite kontrollimisel maksimaalset rangust. Meilide kaitse kontrollib sissetulevaid ja väljaminevaid sõnumeid ning teeb ka väga põhjaliku heuristilise analüüsi. Kõrge meilide turbetase rakendatakse ohtlikus arvutikeskkonnas töötamisel. Selline keskkond on näiteks keskse meilikaitseta koduvõrgus tasuta meiliteenusega loodud ühendus. • Optimaalne. Meilikaitse turvatase, mis tagab Kaspersky rakenduse jõudluse ja meilikaitse optimaalse tasakaalu. Meilide kaitse kontrollib sissetulevaid ja väljaminevaid sõnumeid ning teeb ka keskmise põhjalikkusega heuristilise analüüsi. Seda meilikaitse turvataset soovitavad Kaspersky spetsialistid. • Madal. See on meilikaitse turvatase, mille korral kontrollib meilide kaitse ainult sissetulevaid meilisõnumeid ja teeb põgusa heuristilise analüüsi. Sellel tasemel ei kontrollita sõnumitele manustatud arhiive. Selle meilikaitse turvataseme valimise korral kontrollib meilide kaitse meilisõnumeid võimalikult kiiresti ja kasutab kõige vähem operatsioonisüsteemiresursse. Meilikaitse turbetaset „Madal“ on soovitatav kasutada kindlalt kaitstud keskkonnas töötamise korral. Selline keskkond on näiteks keskse meilikaitsega kohtvõrk.
<p>Toiming ohu avastamisel</p>	<ul style="list-style-type: none"> • Küsi kasutajalt. Meilide kaitse teavitab teid nakatunud või arvatavalt nakatunud objekti avastamisest ja küsib teilt, millised toimingud soovite selle objektiga teha. See valik on saadaval, kui menüüs Seaded → Jõudluseaded → Arvutiressursside kasutus on märkeruudust Tee soovitatavad toimingud automaatselt märges eemaldatud. • Vali toiming automaatselt. Nakatunud või arvatavalt nakatunud objektide tuvastamise korral teeb meilide kaitse automaatselt toimingut, mida on soovitanud Kaspersky spetsialistid. Nakatunud objektide korral on see toiming „Paranda“. See väärtus on valitud vaikimisi. Enne nakatunud objekti parandamise või kustutamise katset loob meilide kaitse varukoopia juhaks, kui hiljem on vaja objekt taastada või avaneb võimalus sellest nakkus eemaldada. See valik on saadaval, kui menüüs Seaded → Jõudluseaded → Arvutiressursside kasutus on märgitud ruut Tee soovitatavad toimingud automaatselt. • Paranda; kui parandamine nurjub, siis kustuta. Kui sissetulevast või väljaminevast sõnumist avastatakse nakatunud objekt, proovib Kaspersky rakendus avastatud objekti parandada. Kasutaja saab juurdepääsu turvalise manusega sõnumile. Kui Kaspersky rakendus ei saa objekti parandada, siis see kustutatakse. Kaspersky rakendus lisab teabe tehtud toimingut kohta sõnumi teemareale järgmisel kujul: <i>[Sõnum on töödeldud] <sõnumi teema></i>. • Paranda; kui parandamine nurjub, siis blokeeri. Kui sissetulevast sõnumist avastatakse nakatunud objekt, proovib Kaspersky rakendus avastatud objekti parandada. Kasutaja saab juurdepääsu turvalise manusega sõnumile. Kui objekti ei saa parandada, lisab Kaspersky rakendus sõnumi teemareale hoiatuse. Kasutaja saab juurdepääsu algse manusega sõnumile. Kui väljaminevast sõnumist avastatakse nakatunud objekt, proovib Kaspersky rakendus avastatud objekti parandada. Kui Kaspersky rakendus ei saa objekti parandada, blokeerib see sõnumi saatmise ja meiliklient kuvab tõrketeadet. • Blokeeri. Kui sissetulevast sõnumist avastatakse nakatunud objekt, lisab Kaspersky rakendus sõnumi teemareale hoiatuse. Kasutaja saab juurdepääsu algse manusega

	sõnumile. Kui väljaminevast sõnumist avastatakse nakatunud objekt, blokeerib Kaspersky rakendus sõnumi saatmise ja meiliklient kuvab tõrke.
Kaitse ulatus	<p><i>Kaitse ulatus</i> hõlmab objekte, mida komponent käivitumise korral kontrollib: saabuvad ja väljuvad sõnumid või ainult saabuvad sõnumid.</p> <p>Enda arvutite kaitsmiseks tuleb teil kontrollida ainult sissetulevaid sõnumeid. Väljaminevate sõnumite kontrollimise saate sisse lülitada vältimaks arhiivides sisalduvate nakatunud failide saatmist. Samuti saate väljaminevate sõnumite kontrollimise sisse lülitada, kui soovite takistada teatud vormingus failide (näiteks heli- ja videofailide) saatmist.</p>
Kontrolli POP3-, SMTP-, NNTP- ja IMAP-liiklust	See märkeruut lülitab sisse/välja POP3-, SMTP-, NNTP- ja IMAP-protokolli kaudu saadetud meililiikluse kontrollimise meilide kaitse abil.
Ühenda Microsoft Outlooki laiendus	<p>Ruudu märkimise korral kontrollitakse POP3-, SMTP-, NNTP- ja IMAP-protokolli kaudu edastatud meilisõnumeid Microsoft Outlooki integreeritud laienduse abil.</p> <p>Kui meili kontrollitakse Microsoft Outlooki laienduse abil, on soovitatav kasutada Exchange'i vahemälurežiimi. Üksikasjalikku teavet Exchange'i vahemälurežiimi kohta ja soovitused selle kasutamiseks leiate Microsofti teabebaasist.</p>
Heuristiline analüüs	<p>Tehnika, mis on ette nähtud selliste ohtude avastamiseks, mida ei saa tuvastada Kaspersky rakenduste andmebaaside praeguse versiooni abil. See võimaldab teil leida faile, mis võivad sisaldada tundmatut pahavara või teadaoleva pahavaraprogrammi uut modifikatsiooni.</p> <p>Failidest pahatahtliku koodi otsimisel täidab heuristiline analüüs käivitusfailides sisalduvaid juhiseid. Heuristilise analüüsi täidetavate juhiste arv oleneb heuristilise analüüsi jaoks määratud tasemest. Heuristilise analüüsi tase määrab uute ohtude otsingu põhjalikkuse, operatsioonisüsteemiresursside koormuse ja heuristilise analüüsi kestuse vahelise tasakaalu.</p>
Kontrolli Microsoft Office'i vormingus manustatud faile	Kontrollib Microsoft Office'i faile (DOC, DOCX, XLS, PPT ja muud Microsofti faililaiendid). Office'i vormingus failid hõlmavad ka OLE-objekte.
Kontrolli manustatud arhiive	Kontrollitakse ZIP-, GZIP-, BZIP-, RAR-, TAR-, ARJ-, CAB-, LHA-, JAR-, ICE- ja muudes vormingutes arhiive. Rakendus kontrollib arhiive nii failinimelaiendi kui ka vormingu järgi.
Ära kontrolli arhiive, mis on suuremad kui	Kui see ruut on märgitud, jätab e-posti kaitse kontrollimata e-posti sõnumitele manustatud arhiivid, kui nende maht ületab teie määratud väärtust. Kui ruut on märkimata, kontrollib e-posti kaitse kõiki e-posti sõnumitele manustatud arhiive nende mahust olenemata.
Ära kontrolli arhiive kauem kui	Kui ruut on märgitud, piiratakse e-posti sõnumitele manustatud arhiivide kontrollimise kestus määratud ajavahemikuga.
Manuste filter	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;">Manuste filter ei tööta väljaminevate meilisõnumite korral.</div> <p>Lülita filtreerimine välja. Selle valiku korral ei filtreeri meilide kaitse meilisõnumitele manustatud faile.</p>

Nimeta valitud tüüpi manused ümber. Selle valiku korral asendab meilide kaitse määratud tüüpi manustatud failide nimelaiendi viimase tähemärgi allkriipsuga (näiteks manus.doc_). Seetõttu peab kasutaja faili avamiseks selle ümber nimetama.

Kustuta valitud tüüpi manused. Selle valiku korral kustutab meilide kaitse määratud tüüpi failid, kui need on manustatud meilisõnumitele.

Failimaskide loendis saate määrata manustatud failide tüübid, mis tuleb meilisõnumites ümber nimetada või kustutada.

Aken „Võrgu omadused“ (adapter)

[Nimi](#) ?

Võrguadapteri nimi.

[Ühenduse tüüp](#) ?

Võrguadapteri tüüp, näiteks Etherneti võrk, juhtmeta võrk või modemiühendus.

[Seisund](#) ?

Võrguühenduse hetkeseisund: kas *ühendatud* või *ühendus katkestatud*.

Jaotises **Uued ühendused** saate valida toimingu, mille tulemüür teeb selle adapteri kaudu uue ühenduse tuvastamise korral.

[Küsi gruppi](#) ?

Kui tulemüür tuvastab uue võrguühenduse, teavitab see teid ja palub valida uue võrgu seisundi.

[Teisalda uued võrgud automaatselt gruppi](#) ?

Kui tulemüür tuvastab uue võrguühenduse, määrab see võrgule automaatselt ripploendis valitud seisundi. Ripploendis saate määrata võrguseisundi, mille tulemüür uutele võrkudele automaatselt määrab.

Süsteemiseire seaded

[Lülita sisse/välja](#)

Selle lülitiga saate süsteemiseire sisse/välja lülitada.

Kui nupp on roheline, kogub ja salvestab süsteemiseire andmeid kõigi operatsioonisüsteemis toimuvate sündmuste kohta (näiteks faili muutmine, registrivõtmete muutmine, draiverite käivitamine või arvuti sulgemise katsed). Neid andmeid kasutatakse rakenduse (sh lunavara) pahatahtliku ja muu tegevuse jälgimiseks ning operatsioonisüsteemi sellise seisundi taastamiseks, mis oli enne rakenduse installimist (pahavara või rakenduse muu tegevuse tagajärgede tagasipööramiseks). Mõnel juhul ei saa rakenduste tegevust tagasi pöörata, näiteks kui rakenduse avastab sissetungitõrje.

Süsteemiseire kogub andmeid erinevatest allikatest, sealhulgas Kaspersky muudest komponentidest. Süsteemiseire analüüsib rakenduste tegevust ja edastab sündmuste kohta kogutud teabe Kaspersky teistele komponentidele.

Jaotises **Eksploitide tõkestus** saate seadistada toimingud, mille rakendus teeb, kui käivitusfaile käivitavad haavatavad rakendused.

[Jälgi katseid teha volitamata operatsioone](#)

Selle märkeruudu abil saate [eksploitide](#) tõkestuse lubada/keelata.

Kui see ruut on märgitud, jälgib Kaspersky täitmisfaile, mille käivitavad haavatavad rakendused. Kui Kaspersky tuvastab haavatavast rakendusest täitmisfaili käivitamise katse, mida kasutaja ei algatanud, teeb rakendus ripploendis **Ohu avastamisel toimi järgmiselt** valitud toimingu.

[Ohu avastamisel toimi järgmiselt](#)

Selles ripploendis saate valida toimingu, mille süsteemiseire teeb, kui jälgitavast haavatavast rakendusest käivitatakse käivitusfail.

See loend võimaldab valida järgmiste toimingute vahel.

- **Küsi kasutajalt.** Süsteemiseire küsib tegevust kasutajalt. See valik on saadaval, kui menüüs **Seaded** → **Jõudlusseaded** → **Arvutiressursside kasutus** on märkeruudust **Tee soovitatavad toimingud automaatselt** märges eemaldatud.
- **Vali toiming automaatselt.** Süsteemiseire teeb Kaspersky seadetes valitud toimingu automaatselt ja lisab aruandesse teabe valitud toimingu kohta. See valik on saadaval, kui menüüs **Seaded** → **Jõudlusseaded** → **Arvutiressursside kasutus** on märgitud ruut **Tee soovitatavad toimingud automaatselt**.
- **Luba toiming.** Süsteemiseire lubab käivitusfaili käivitada.
- **Blokeeri toiming.** Süsteemiseire blokeerib käivitusfaili.

[Pahatahtliku või muu tegevuse avastamisel toimi järgmiselt](#)

Selles ripploendis saate toimingut, mille süsteemiseire teeb, kui avastab rakenduste tegevuse analüüsimise põhjal pahatahtliku või muu tegevuse.

- **Küsi kasutajalt.** Süsteemiseire küsib tegevust kasutajalt. See valik on saadaval, kui menüüs **Seaded** → **Jõudlusseaded** → **Arvutiressursside kasutus** on märkeruudust **Tee soovitatavad toimingud automaatselt** märgi eemaldatud.
- **Vali toiming automaatselt.** Süsteemiseire teeb automaatselt Kaspersky ekspertide poolt soovitatud toimingut. See valik on saadaval, kui menüüs **Seaded** → **Jõudlusseaded** → **Arvutiressursside kasutus** on märgitud ruut **Tee soovitatavad toimingud automaatselt**.
- **Kustuta rakendus.** Süsteemiseire kustutab rakenduse.
- **Katkesta rakenduse tegevus.** Süsteemiseire katkestab kõik rakenduse protsessid.
- **Katkesta rakenduse tegevus.** Süsteemiseire ei tee rakendusega mitte ühtegi toimingut.

[Kui pahatahtlikku või muud tegevust saab tagasi pöörata, toimi järgmiselt](#)

Selles ripploendis saate valida toimingut, mille süsteemiseire teeb, kui rakenduse pahatahtlikku või muud tegevust on võimalik tagasi pöörata.

- **Küsi kasutajalt.** Kui süsteemiseire, failide kaitse või kontrollitegumi tulemused kinnitavad, et tagasipööramine on vajalik, küsib süsteemiseire kasutajalt, mida teha. See valik on saadaval, kui menüüs **Seaded** → **Jõudlusseaded** → **Arvutiressursside kasutus** on märkeruudust **Tee soovitatavad toimingud automaatselt** märgi eemaldatud.
- **Vali toiming automaatselt.** Kui süsteemiseire analüüsib rakenduse tegevust ja leiab, et see on pahatahtlik, siis pöörab see rakenduse tegevuse tagasi ja teavitab sellest sündmusest kasutajat. See valik on saadaval, kui menüüs **Seaded** → **Jõudlusseaded** → **Arvutiressursside kasutus** on märgitud ruut **Tee soovitatavad toimingud automaatselt**.
- **Pööra muudatused tagasi.** Süsteemiseire pöörab tagasi rakenduse pahatahtliku või muu tegevuse.
- **Ära pööra muudatusi tagasi.** Süsteemiseire salvestab teabe pahatahtliku või muu tegevuse kohta, kuid ei pööra rakenduse toiminguid tagasi.

Jaotises **Kaitse ekraanilukustajate eest** saate valida toimingud, mis tehakse ekraanilukustaja tegevuse tuvastamisel. Ekraanilukustajad on pahatahtlikud programmid, mis piiravad arvutis kasutaja tegevust, lukustades ekraani ja klaviatuuri või blokeerides juurdepääsu tegumiribale ja otseteedele. Ekraanilukustajad võivad operatsioonisüsteemile juurdepääsu taastamise eest proovida lunaraha välja pressida. Kasutades kaitset ekraanilukustajate eest, saate kindla klahvikombinatsiooni abil sulgeda kõik ekraanilukustajad.

[Avasta ja sule ekraanilukustajad](#)

See märkeruut lubab/keelab kaitse ekraanilukustajate eest.

Kui see ruut on märgitud, saate ekraanilukustaja tegevuse avastamise korral selle peatamiseks vajutada märkeruudu all olevas ripploendis määratud klahvikombinatsiooni.

[Ekraanilukustajate käsitsi sulgemiseks kasutage klahvikombinatsiooni](#)

Ripploendist saate valida klahvi või klahvikombinatsiooni, mille vajutamise korral käivitatakse ekraanilukustaja tuvastamiseks ja kustutamiseks kaitse ekraanilukustaja eest.

Vaikimisi kasutatakse järgmist klahvikombinatsiooni: CTRL+ALT+SHIFT+F4.

Failide kaitse seaded

Seaded	Kirjeldus
Turvalisuse tase	<p>Kaspersky rakendus kasutab Failide kaitse käitamiseks erinevaid seadete gruppe. Rakendusse salvestatud seadekomplekte kutsutakse <i>turbetasemeteks</i>.</p> <ul style="list-style-type: none"> • Äärmuslik. Selle failikaitse turvaseme valimise korral rakendab failide kaitse komponent kõigile avatud, salvestatud ja käivitatud failidele kõige rangemat kontrolli. Failide kaitse komponent kontrollib arvuti kõigil kõvaketastel, võrguketastel ja irdketastel kõiki failitüüpe. Lisaks kontrollib see arhiive, paigalduspakette ja manustatud OLE-objekte. • Optimaalne. Seda failikaitse turvaset soovitavad Kaspersky Labi eksperdid. Failide kaitse komponent kontrollib arvuti kõigil kõvaketastel, võrguketastel ja irdketastel ainult määratud failivorminguid ning manustatud OLE-objekte. Failide kaitse komponent ei kontrolli arhiive ega paigalduspakette. • Madal. Selle failikaitse turvaseme seaded tagavad kõige kiirema kontrolli. Failide kaitse komponent kontrollib arvuti kõigil kõvaketastel, võrguketastel ja irdketastel ainult määratud failinimelaienditega faile. Failide kaitse komponent ei kontrolli liitfaile.
Toiming ohu avastamisel	<ul style="list-style-type: none"> • Küsi kasutajalt. Failide kaitse teavitab teid nakatunud või arvatavalt nakatunud objekti avastamisest ning küsib teilt, mida sellega teha. See valik on saadaval, kui menüüs Seaded → Jõudlusseaded → Arvutiressursside kasutus on märkeruudust Tee soovitatavad toimingud automaatselt märgi eemaldatud. • Vali toiming automaatselt. Nakatunud või arvatavalt nakatunud objekti avastamise korral teeb failide kaitse automaatselt toimingut, mida on objekti kohta soovitanud Kaspersky eksperdid. Nakatunud objektide korral on see toiming „Paranda“. See väärtus on valitud vaikimisi. Enne nakatunud objekti parandamise või kustutamise katset loob failide kaitse sellest varukoopia, mille saab taastada või parandada hiljem. See valik on saadaval, kui menüüs Seaded → Jõudlusseaded → Arvutiressursside kasutus on märgitud ruut Tee soovitatavad toimingud automaatselt. • Paranda; kui parandamine nurjub, siis kustuta. Selle toimingut valimise korral proovib rakendus automaatselt parandada kõik nakatunud failid, mille see leiab. Kui nakkuse eemaldamine nurjub, siis rakendus kustutab objektid. • Paranda; kui parandamine nurjub, siis blokeeri. Selle toimingut valimise korral proovib rakendus automaatselt parandada kõik nakatunud failid, mille see leiab. Kui nakkuse eemaldamine nurjub, siis lisab rakendus teabe leitud nakatunud failide kohta tuvastatud objektide loendisse. • Blokeeri. Selle valiku korral blokeerib failide kaitse komponent automaatselt kõik nakatunud failid, ilma et prooviks neist nakkust eemaldada. <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Enne nakatunud faili parandamise või kustutamise katset loob rakendus varukoopia juhaks, kui teil hiljem on vaja fail taastada või avaneb võimalus sellest nakkus eemaldada.</p> </div>
Failitüübid	<p>Kõik failid. Selle seade sisselülitamise korral kontrollib rakendus eranditult kõiki faile (kõiki vorminguid ja failinimelaiendeid).</p>

	<p>Vormingu järgi kontrollitud failid. Selle seade valimise korral kontrollib rakendus ainult potentsiaalselt nakatunud faile . Enne failist pahatahtliku koodi otsimist analüüsitakse failivormingu (näiteks TXT, DOC, EXE) kindlaksmääramiseks faili sisemist päist. Kontroll otsib ka kindlate failinimelaienditega faile.</p> <p>Laiendi järgi kontrollitud failid. Selle seade valimise korral kontrollib rakendus ainult potentsiaalselt nakatunud faile . Failivorming määratakse kindlaks failinimelaiendi põhjal.</p>
Muuda kaitse ulatust	<p>Selle lingi klõpsamise korral avaneb aken Failide kaitse ulatus, mis sisaldab failide kaitse kontrollitavate objektide loendit.</p> <p>Loendis saate objekte lisada või enda lisatud objekte kustutada.</p> <p>Kontrollist objekti eemaldamiseks ei pea objekti loendist kustutama. Piisab objektinime kõrval kuvatavast ruudust märke eemaldamisest.</p>
Heuristiline analüüs	<p>Tehnika, mis on ette nähtud selliste ohtude avastamiseks, mida ei saa tuvastada Kaspersky rakenduste andmebaaside praeguse versiooni abil. See võimaldab teil leida faile, mis võivad sisaldada tundmatut pahavara või teadaoleva pahavaraprogrammi uut modifikatsiooni.</p> <p>Failidest pahatahtliku koodi otsimisel täidab heuristiline analüüs käivitusfailides sisalduvaid juhiseid. Heuristilise analüüsi täidetavate juhiste arv on heuristilise analüüsi jaoks määratud tasemest. Heuristilise analüüsi tase määrab uute ohtude otsingu põhjalikkuse, operatsioonisüsteemiressursside koormuse ja heuristilise analüüsi kestuse vahelise tasakaalu.</p>
Kontrolli ainult uusi ja muudetud faile	<p>Kontrollib ainult uusi faile ja faile, mida on pärast viimast kontrollimiskorda muudetud. See võimaldab teil kontrollimisel aega kokku hoida. See kontrollimisrežiim rakendatakse nii tava- kui ka liitfailidele.</p>
Kontrolli arhiive	<p>Kontrollitakse ZIP-, GZIP-, BZIP-, RAR-, TAR-, ARJ-, CAB-, LHA-, JAR-, ICE- ja muudes vormingutes arhiive. Rakendus kontrollib arhiive nii failinimelaiendi kui ka vormingu järgi.</p>
Kontrolli levituspakette	<p>Märkeruut lülitab sisse/välja kolmanda osapoole levituspakettide kontrollimise.</p>
Kontrolli Microsoft Office'i vormingus faile	<p>Kontrollib Microsoft Office'i faile (DOC, DOCX, XLS, PPT ja muud Microsofti faililaiendid). Office'i vormingus failid hõlmavad ka OLE-objekte.</p>
Ära paki lahti suuri liitfaile Faili maksimaalne suurus	<p>Kui ruut on märgitud, ei kontrolli rakendus liitfaile, mis on määratud väärtusest suuremad.</p> <p>Kui sellest ruudust on märged eemaldatud, kontrollib rakendus kõiki liitfaile nende mahust olenemata.</p> <p>Rakendus kontrollib kõiki arhiividest lahtipakitud suuri faile ruudu märkimisest või märkimata jätmisest olenemata.</p>
Paki liitfailid taustal lahti Minimaalne faili suurus	<p>Kui see ruut on märgitud, võimaldab rakendus määratud väärtusest suurematele liitfailidele juurdepääsu enne nende failide kontrollimist. Sel juhul pakib Kaspersky rakendus liitfailid lahti ja kontrollib neid taustal.</p> <p>Sellest väärtusest väiksematele liitfailidele võimaldab rakendus juurdepääsu alles pärast nende failide lahtipakkimist ja kontrollimist.</p> <p>Kui see ruut on märkimata, võimaldab rakendus liitfailidele juurdepääsu alles pärast failide lahtipakkimist ja kontrollimist nende suurusest olenemata.</p>
Kontrollimisrežiim	<p>Nutikas režiim. Selles režiimis kontrollib failide kaitse objekti selle objektiga tehtud toimingute analüüsi põhjal. Näiteks Microsoft Office'i dokumendiga töötamise korral kontrollib Kaspersky rakendus faili esimest korda, kui see avatakse, ja viimast korda, kui see suletakse. Pärast faili üle kirjutavaid vahetoiminguid seda ei kontrollita.</p>

	<p>Avamisel ja muutmisel. Selles režiimis kontrollib failide kaitse objekte alati, kui neid proovitakse avada või muuta.</p> <p>Avamisel. Selles režiimis kontrollib failide kaitse objekte ainult juhul, kui neid proovitakse avada.</p> <p>Käivitamisel. Selles režiimis kontrollib failide kaitse objekte ainult juhul, kui neid proovitakse käivitada.</p>
iSwifti tehnoloogia	<p>See tehnoloogia on NTFS-failisüsteemi kasutatavate arvutite jaoks ette nähtud iCheckeri tehnoloogia edasiarendus.</p> <p>iSwifti tehnoloogial on piirangud: see on seotud konkreetse faili asukohaga failisüsteemis ja töötab ainult NTFS-failisüsteemis olevate objektidega.</p> <p>Kui viite Kaspersky Small Office Security rakenduse üle uuele versioonile, lülitatakse iSwifti tehnoloogia kõigi kontrollimistüüpide jaoks sisse ka siis, kui see oli varem välja lülitatud.</p>
iCheckeri tehnoloogia	<p>See tehnoloogia võimaldab kontrolli kiirendada, kuna jätab kindlad failid kontrollist välja. Kontrollist failide väljajätmiseks kasutatakse erialgoritmi, mis võtab arvesse Kaspersky Small Office Security andmebaaside väljalaskekuupäeva, faili viimase kontrollimise kuupäeva ja kõiki kontrolli seadetes tehtud muudatusi. iCheckeri tehnoloogial on piirangud: see ei tööta suurte failidega ja rakendatakse ainult failidele, mille struktuuri rakendus ära tunneb (näiteks EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ja RAR).</p>
Erandid	<p>Kontrollidest välja jäetud objektid.</p> <p>Erandite määramiseks klõpsake aknas Halda erandeid linki Erandid.</p>
Failide kaitse peatamine	<p>See peatab määratud ajal või määratud rakenduste kasutamise ajal ajutiselt ja automaatselt failide kaitse töö.</p> <p>Selle seadistamiseks tuleb klõpsata linki Failide kaitse peatamine.</p>

AMSI kaitse seaded

Seaded	Kirjeldus
Kontrolli arhiive	Kontrollitakse ZIP-, GZIP-, BZIP-, RAR-, TAR-, ARJ-, CAB-, LHA-, JAR-, ICE- ja muudes vormingutes arhiive. Rakendus kontrollib arhiive nii failinimelaiendi kui ka vormingu järgi.
Kontrolli levituspakette	Märkeruut lülitab sisse/välja kolmanda osapoole levituspakettide kontrollimise.
Kontrolli Microsoft Office'i vormingus faile	Kontrollib Microsoft Office'i faile (DOC, DOCX, XLS, PPT ja muud Microsofti faililaiendid). Office'i vormingus failid hõlmavad ka OLE-objekte.
Ära paki lahti suuri liitfaile Faili maksimaalne suurus	<p>Kui ruut on märgitud, ei kontrolli rakendus liitfaile, mis on määratud väärtusest suuremad.</p> <p>Kui sellest ruudust on mäрге eemaldatud, kontrollib rakendus kõiki liitfaile nende mahust olenemata.</p> <p>Rakendus kontrollib kõiki arhiividest lahtipakitud suuri faile ruudu märkimisest või märkimata jätmisest olenemata.</p>

Aken „Isiklike andmete lisamine/muutmine“

[Isiklike andmete tüübid](#)

Kui klõpsate väljal **Välja nimi** linke, kuvatakse vastavat tüüpi isiklikud andmed.

[Välja nimi](#)

Isiklike andmete kirjete loendis kuvatav kirjeldus (näiteks *Kodutelefon*, *Töötelefon* või *Sihtnumber*).

Isiklike andmete kirjelduse automaatseks kopeerimiseks saate klõpsata vastavat isiklike andmete tüübi linki.

[Väärtus](#)

Isiklikud andmed, mille saatmine on blokeeritud või lubatud.

Isiklike andmete edastamise aruanne

Akna ülaservas kuvatakse selle kasutajakonto nimi, mille toimingute kohta on aruanne esitatud.

Kontrollimine sisse lülitatud / välja lülitatud

See lüliti võimaldab lubada/keelata vanemakontrolli kaudu kasutaja toimingute jälgimise.

Olenevalt sellest, kas vanemakontroll jälgib kasutaja toiminguid, on nupul järgmine ilme.

 – vanemakontroll jälgib kasutaja toiminguid.

 – vanemakontroll ei jälgi kasutaja toiminguid.

Kasutaja toimingute jälgimine toimub kasutajale määratud vanemakontrolli seadete alusel.

Selles aknas saate vaadata teavet valitud kasutaja võtmesõnakasutuse ja isiklike andmete edastamiskatsete kohta.

Täna

Selle nupu klõpsamise korral avaneb aruanne kasutaja tänase tegevuse kohta.

Nupud

Nende nuppude klõpsamine avab eelmise ja järgmise ajavahemiku aruanded.

Päev/nädal/kuu

Ajavahemik, mille kohta aruanne luuakse. Aruande saate luua järgmiste ajavahemike kohta: päev, nädal ja kuu.

Nupp

Selle nupu klõpsamisel avaneb vanemakontrolli seadete akna jaotis **Vanemakontroll**. Selles jaotises saate seada isiklike andmete saatmise piirangud.

Blokeeritud isiklike andmete loend

Sisaldab valitud ajavahemikul kasutaja saadetud ja vastuvõetud sõnumites leidunud isiklike andmete loendit.

Andmed

See veerg sisaldab saadetud või vastuvõetud sõnumitest pärinevaid isiklike andmeid.

Blokeeritud isiklike andmete korral on täpsustatud teabetüüp, mille edastamine on blokeeritud.

Ressurss

Selles veerus kuvatakse veebisait, mille kaudu proovis kasutaja saata või vastu võtta sõnumit, mis sisaldas isiklike andmeid, mille edastamine on blokeeritud.

Seisund

Kui vanemakontroll on sõnumi saatmise blokeerinud, kuvatakse veerus väärtus *Blokeeritud*.

Kuupäev

Selles veerus kuvatakse kuupäev, mil võeti vastu või saadeti sõnum, mis sisaldas isiklikke andmeid, mille edastamine on blokeeritud.

Kasutajaprofili valimine

[Andmete kogumine](#)

Selle nupu klõpsamise korral rakendatakse valitud kasutajakontole vaikeseadetega profiil. See profiil kogub statistikat ainult valitud kasutaja toimingute kohta. Rakenduse- ja internetikasutusele piiranguid ei seata.

[Valikulised piirangud](#)

Valitud kasutajakontole rakendatakse käsitsi seadistatud seaded.

[Laps \(4+\)](#)

Selle nupu klõpsamisel rakendatakse valitud kasutajakontole 4–12 aasta vanustele lastele mõeldud profiil. See profiil sisaldab interneti- ja rakendusekasutuse kohta järgmisi reegleid.

- Interneti kasutamine on lubatud.
- Sirvida on lubatud ainult veebisaitide, mis on loetletud kategooriates „Interneti-suhtlus“ ja „Arvutimängud“.
- Igat tüüpi failide allalaadimine on blokeeritud.
- Arvutikasutuse jälgimine on sisse lülitatud; arvutikasutusele piiranguid ei seata.
- Rakendusekasutuse jälgimine on sisse lülitatud; arvutikasutuspiirangud puuduvad.
- Mängukasutuse jälgimine on sisse lülitatud; piirangud seatakse hindamissüsteemi kohaselt.

[Teismeline \(12+\)](#)

Selle nupu klõpsamisel rakendatakse valitud kasutajakontole üle 12 aasta vanustele lastele mõeldud profiil. See profiil sisaldab interneti- ja rakendusekasutuse kohta järgmisi reegleid.

- Interneti kasutamine on lubatud.
- Sirvida on lubatud ainult veebisaitide, mis on loetletud kategooriates „Internetisuhtlus“, „Poed, pangad, maksesüsteemid“ ja „Arvutimängud“.
- Arvutikasutuse jälgimine on sisse lülitatud; arvutikasutusele piiranguid ei seata.
- Rakendusekasutuse jälgimine on sisse lülitatud; arvutikasutuspiirangud puuduvad.
- Mängukasutuse jälgimine on sisse lülitatud; piirangud seatakse hindamissüsteemi kohaselt.

[Vaikeseaded](#)

Selle nupu klõpsamise korral rakendatakse valitud kasutajakontole vaikeseadetega profiil. See profiil sisaldab interneti- ja rakendusekasutuse kohta järgmisi reegleid.

- Interneti kasutamine on lubatud.
- Sirvida on lubatud ainult veebisaite, mis on loetletud kategooriates „Internetisuhtlus“, „Poed, pangad, maksesüsteemid“ ja „Arvutimängud“.
- Ohutu otsing on sisse lülitatud.
- Arvutikasutuse jälgimine on sisse lülitatud; arvutikasutusele piiranguid ei seata.
- Rakendusekasutuse jälgimine on sisse lülitatud; arvutikasutuspiirangud puuduvad.
- Mängu käivitamise jälgimine on sisse lülitatud; käivituspiiranguid pole seatud.
- Veebilehitsejates krüpteeritud SSL ühenduste jälgimine on sisse lülitatud.

[Impordi](#)

Selle lingi klõpsamisel avaneb vanemakontrolli seadeid sisaldava faili valimiseks ette nähtud aken. Pärast faili valimist rakendatakse need seaded valitud kasutaja kontole.

[Ekspordi](#)

Selle lingi klõpsamisel avaneb vanemakontrolli praeguste seadete failina salvestamiseks ette nähtud aken.

Veebiaadressi lisamise/muutmise aken

Veebiaadressi mask [?](#)

Veebisaidi veebiaadress või aadressimask, millele juurdepääs tuleb lubada või blokeerida.

Toiming [?](#)

Selle abil blokeeritakse või lubatakse kasutaja juurdepääs veebisaitidele.

Saate teha ühe järgmistest valikutest.

- **Luba.** Selle valiku korral lubab vanemakontroll kasutajal veebisaidile juurde pääseda isegi juhul, kui see kuulub blokeeritud kategooriasse või sisse on lülitatud kõigi veebisaitide blokeerimine.
- **Blokeeri.** Selle valiku korral blokeerib vanemakontroll kasutaja juurdepääsu veebisaidile isegi juhul, kui see kuulub lubatud kategooriasse.

Tüüp [?](#)

Saate määrata veebisaidi juurdepääsuseadete rakendamise ulatuse.

Saate teha ühe järgmistest valikutest.

- **Veebisaidi mask.** Selle valiku korral lubab või blokeerib vanemakontroll kasutaja juurdepääsu kõigile määratud veebisaidi veebilehtedele.
Näiteks juhul, kui väli **Veebiaadressi mask** sisaldab aadressi example.com, lubab või blokeerib vanemakontroll juurdepääsu kõigile veebisaidi example.com veebilehtedele, sealhulgas news.example.com, market.example.com ja mail.example.com.
- **Määratud veebiaadress.** Selle valiku korral lubab või blokeerib vanemakontroll kasutaja juurdepääsu ainult määratud veebisaidilehele, mis on märgitud väljale **Veebiaadressi mask**.
Näiteks juhul, kui sisestate väljale **Veebiaadressi mask** URL-i mail.example.com/login, lubab või blokeerib vanemakontroll juurdepääsu ainult määratud sisselogimislehele, mida kasutatakse veebimeiliteenuse kontosse sisselogimiseks. Seda reeglit ei rakendata veebisaidi teistele lehtedele.

Rakenda mall [?](#)

Võimaldab rakendada erandile mõne olemasoleva malli, mis sisaldab määratud seadekomplekti.

Saate teha ühe järgmistest valikutest.

- **Kogu veebisait** – selle valiku korral lubab või blokeerib vanemakontroll juurdepääsu väljal **Veebiaadressi mask** määratud domeenile. Näiteks juhul, kui väli **Veebiaadressi mask** sisaldab aadressi example.com, lubab või blokeerib vanemakontroll juurdepääsu kõigile domeeni example.com veebilehtedele, sealhulgas news.example.com, market.example.com ja mail.example.com.
- **Määratud veebileht** – selle valiku korral lubab või blokeerib vanemakontroll juurdepääsu väljal **Veebiaadressi mask** määratud konkreetsele lehele ja kõigile seda lehte sisaldavatele veebiaadressidele. Näiteks juhul, kui väli **Veebiaadressi mask** sisaldab aadressi example.com/hl, lubab või blokeerib vanemakontroll juurdepääsu nii sellele lehele kui ka seda sisaldavatele veebiaadressidele, näiteks example.com/hl/example1.html.
- **Määratud veebiaadress** – selle valiku korral lubab või blokeerib vanemakontroll juurdepääsu väljal **Veebiaadressi mask** määratud kindlale veebiaadressile. Näiteks juhul, kui sisestate väljale **Veebiaadressi mask** URL-i mail.example.com/login, lubab või blokeerib vanemakontroll juurdepääsu ainult määratud sisselogimislehele, mida kasutatakse veebimeiliteenuse kontosse sisselogimiseks. Seda reeglit ei rakendata veebisaidi teistele lehtedele.

Vanemakontrolli erandid

Selles aknas saate luua konfigureeritud vanemakontrolli seadete erandite loendi. Erandite loendisse lisatud veebisaitide mõjutavad juurdepääsuseaded rakendatakse nii veebisaitide blokeerimisel kategooriate alusel (nupp **Blokeeri juurdepääs veebisaitidele valitud kategooriates**) kui ka kõigi veebisaitide blokeerimise korral (nupp **Blokeeri juurdepääs kõigile veebisaitidele**).

Näiteks saate lubada juurdepääsu internetisuhtluse kategooria veebisaitidele, kuid lisada erandite loendisse veebisaidi `www.example.com`, et blokeerida juurdepääs sellele konkreetsele veebisaidile. Sellisel juhul lubab vanemakontroll juurdepääsu kõigile suhtlusvõrkudele, välja arvatud suhtlusvõrgule `example.com`. Samuti saate blokeerida kõik veebisaidid ja lisada erandite loendisse juurdepääsu veebimeiliteenuse veebisaidile, mille soovite lubada. Sellisel juhul lubab vanemakontroll kasutajal juurde pääseda ainult veebimeiliteenuse veebisaidile.

Erandite loend

Loend sisaldab veebiaadresse, millele juurdepääs on lubatud või blokeeritud hoolimata vanemakontrolli seadetest.

Loendis sisalduva veebiaadressi kontekstimenüüs saate muuta veebiaadressi või eemaldada selle loendist ning samuti lubada või blokeerida juurdepääsu veebisaidile.

Veebiaadressi mask

Veebisaidi veebiaadress või aadressimask, millele juurdepääs on lubatud või blokeeritud.

Tüüp

Veerg näitab veebisaidi juurdepääsuseadete rakendamise ulatust.

Kui veerus on kuvatud tüüp *Veebisaidi mask*, on juurdepääs lubatud või blokeeritud veebisaidi kõigile lehtedele.

Kui veerus on kuvatud tüüp *Määratud veebiaadress*, on juurdepääs lubatud või blokeeritud ainult veebisaidi kindlale (määratud) veebilehele.

Toiming

See veerg näitab, kas juurdepääs veebisaidile on lubatud või blokeeritud.

Kui veerus on kuvatud sõna *Lubatud*, lubab vanemakontroll veebisaidile juurde pääseda.

Kui veerus on kuvatud sõna *Blokeeritud*, blokeerib vanemakontroll juurdepääsu veebisaidile.

Muuda

Selle nupu klõpsamise korral avaneb aken **Muuda**, kus saate muuta erandite loendist valitud veebisaidi veebiaadressi maski või veebiaadressi ja veebisaidi juurdepääsuseadeid.

Nupp on saadaval, kui erandite loendis on valitud veebiaadressi mask.

Kustuta

Selle nupu klõpsamise korral eemaldatakse valitud veebiaadressi mask erandite loendist.

Nupp on saadaval, kui erandite loendis on valitud veebiaadressi mask.

Selle nupu klõpsamise korral avaneb veebisaidiaadressi maski lisamise aken, kus saate erandite loendisse lisada veebisaidiaadressi või veebisaidiaadressi maski.

Aken „Rakenduse kasutamise piirang“

Selles aknas saate seada valitud rakenduse kasutusajapiirangud.

Jaotises **Tööpäevad** saate piirata rakenduse kasutusaega tööpäevadel.

[Luba juurdepääs mitte rohkem kui <N> tundi päevas](#)

See märkeruut lülitab sisse/välja rakenduse kasutusajapiirangu tööpäevadel.

Kui see ruut on märgitud, piirab vanemakontroll valitud kasutaja jaoks rakenduse kogukasutusaega. Rakenduse kasutusajapiirang seatakse (tundides) märkeruudu kõrval kuvatavas ripploendis.

Kui see ruut on märkimata, ei piira vanemakontroll tööpäevadel rakenduse kasutamist.

Jaotises **Nädalalõpud** saate piirata rakenduse kasutusaega nädalalõppudel.

[Luba juurdepääs mitte rohkem kui <N> tundi päevas](#)

See märkeruut lülitab sisse/välja rakenduse kasutusajapiirangu nädalalõppudel.

Kui see ruut on märgitud, piirab Vanemakontroll valitud kasutaja jaoks rakenduse kogukasutusaega. Rakenduse kasutusajapiirang seatakse (tundides) märkeruudu kõrval kuvatavas ripploendis.

Kui see ruut on märkimata, ei piira vanemakontroll nädalalõppudel rakenduse kasutamist.

Jaotises **Vaheajad** saate seadistada rakendusele päeva jooksul korrapäraseid juurdepääsupiiranguid.

[Tee vaheaeg iga <N> tunni järel kestusega <N> minutit](#)

See märkeruut lülitab sisse/välja rakenduse korrapärase blokeerimise määratud ajavahemiku järel, et kasutaja teeks kindlasti vaheaja.

Kui see ruut on märgitud, blokeerib vanemakontroll rakenduse ripploendis <TT:MM> seatud ajavahemiku järel. Juurdepääs on blokeeritud ripploendis <N> minutit valitud aja jooksul.

Jaotises **Täpne kasutamise aeg** kuvatakse rakenduse kasutaja tabel. Selle tabeli abil saate tunnikaupa seadistada rakenduse kasutamise ajakava kogu nädalaks.

[Rakenduse kasutaja tabel](#)

Selle tabeli abil saate määrata nädalapäevad ja kellaajad, millal kasutajal on lubatud rakendust kasutada.

Tabeliread vastavad nädalapäevadele ja tabeliveerud ajaskaala ühetunnistele ajavahemikele.

Operatsioonisüsteemi piirkonnaseadetest olenevalt võib ajaskaala olla kuvatud 24-tunnises või 12-tunnises vormingus. Tabelilahtrite värvid tähistavad kehtivaid piiranguid: punane tähendab, et rakenduse kasutamine on blokeeritud, ja hall tähendab, et rakenduse kasutamine on lubatud. Tabelilahtri klõpsamine muudab selle värvi. Kui kerite lahtri kohal hiirekursorit, kuvatakse tabeli all lahtrile vastav ajavahemik.

Aken „Isiklike andmete nimekiri“

[Isiklike andmete nimekiri](#)

See loend sisaldab kasutaja isiklike andmeid, mille saatmist tuleb kontrollida.

[Välja nimi](#)

Selles veerus kuvatakse isiklike andmete tüüp (näiteks *Pangakaardi number* või *Kodu telefoninumber*).

[Väärtus](#)

See veerg sisaldab isiklike andmeid (näiteks pangakaardi numbrit või telefoninumbrit), mida soovite sõnumites jälgida.

[Muuda](#)

Selle nupu klõpsamise korral avaneb aken, kus saate muuta isiklike andmete kirjet.

[Kustuta](#)

Selle nupu klõpsamise korral saate valitud kirje loendist eemaldada.

[Lisa](#)

Selle nupu klõpsamise korral avaneb aken, kus saate isiklike andmete loendisse lisada uue kirje.

Blokeeritud veebisaitide ja allalaadimiste aruanne

Täna

Selle nupu klõpsamise korral avaneb aruanne kasutaja tänase tegevuse kohta.

Nupud

Nende nuppude klõpsamine avab eelmise ja järgmise ajavahemiku aruanded.

Päev/nädal/kuu

Ajavahemik, mille kohta aruanne luuakse. Aruande saate luua järgmiste ajavahemike kohta: päev, nädal ja kuu.

Nupp

Selle nupu klõpsamisel avaneb vanemakontrolli seadete akna jaotis **Internet**. Selles jaotises saate valitud kasutaja jaoks kehtestada internetikasutuse aja-, veebisaitide juurdepääsu- ja failide allalaadimispiirangud.

Blokeeritud veebisaidid ja allalaadimised

See loend sisaldab vanemakontrolli blokeeritud veebisaitide ja failide, mille allalaadimine on blokeeritud.

Loend sisaldab järgmisi andmeid.

- Blokeeritud veebisaidi või faili nimi
- Kasutaja juurdepääsukatse blokeerimise põhjus (näiteks *veebisait on blokeeritute kategoorias*)
- Veebisaidi avamise või faili allalaadimise kuupäev

Rakenduste kasutuse aruanne

Akna ülaservas kuvatakse selle kasutajakonto nimi, mille toimingute kohta on aruanne esitatud.

Kontrollimine sisse lülitatud / välja lülitatud

See lüliti võimaldab lubada/keelata vanemakontrolli kaudu kasutaja toimingute jälgimise.

Olenevalt sellest, kas vanemakontroll jälgib kasutaja toiminguid, on nupul järgmine ilme.

 – vanemakontroll jälgib kasutaja toiminguid.

 – vanemakontroll ei jälgi kasutaja toiminguid.

Kasutaja toimingute jälgimine toimub kasutajale määratud vanemakontrolli seadete alusel.

Aknas **Rakenduste kasutuse aruanne** saate vaadata teavet valitud kontol kindla ajavahemiku jooksul rakenduste käivitamise kohta.

Täna

Selle nupu klõpsamise korral avaneb aruanne kasutaja tänase tegevuse kohta.

Nupud

Nende nuppude klõpsamine avab eelmise ja järgmise ajavahemiku aruanded.

Päev/nädal/kuu

Ajavahemik, mille kohta aruanne luuakse. Aruande saate luua järgmiste ajavahemike kohta: päev, nädal ja kuu.

Nupp

Selle nupu klõpsamisel avaneb vanemakontrolli seadete akna jaotis **Rakendused**. Selles jaotises saate seada rakenduste käivitus- ja kasutuspiiranguid.

Sageli kasutatavad rakendused

Sisaldab loendit rakendustest, mida kasutaja on määratud ajavahemiku jooksul kõige sagedamini käivitanud. Loendis kirjeldatakse ka iga rakenduse kasutamise kestust.

Blokeeritud rakendused


Sisaldab loendit rakendustest, mille käivitamine on vanemakontroll blokeeritud. Rakendused on esitatud kronoloogilises järjestuses, kõige hiljutisemad rakendused on kuvatud ülaservas.

Kui klõpsate lingil **<N> veel**, näete ka teisi rakendusi, mille käivitamine on blokeeritud.

Kõik kasutatud rakendused

Sisaldab loendit kõigist rakendustest, mille kasutaja on määratud ajavahemiku jooksul käivitanud. Loendis kirjeldatakse ka iga rakenduse kasutamise kestust.

Rakendused on rühmitatud kategooriate kaupa (näiteks „Mängud“ või „IM-kliendid“).

Nupu  klõpsamine võimaldab vaadata kindla kategooria rakenduste loendit.

Nupu  klõpsamine minimeerib kategooriasse kuuluvate rakenduste loendi ühele reale.

Mängude blokeerimine kategooriate järgi

Selles aknas saate lülitada sisse või välja mängude blokeerimise nende sisu alusel. Mängusisu klassifikatsioon (märkeruutude kogum) vastab PEGI või ESRB hindamissüsteemile. Mänguklassifikatsiooni tüüp valitakse automaatselt olenevalt teie asukohast. Vajaduse korral saate mänguklassifikatsiooni tüübi vanemakontrolli komponendi seadetes valida käsitsi.

Kui kategooria kõrval olev ruut on märgitud, blokeerib vanemakontroll kategooriasse kuuluvad mängud.

Kui kategooria kõrval olev ruut on märkimata, lubab vanemakontroll selle kategooria mängu käivitada.

Mängu käivitamine on lubatud, kui kõik mängu sisule vastavad kategooriad on lubatud.

Aken „Parooli ulatus“

[Varundamise ja taastamise haldus](#)

See märkeruut lülitab sisse/välja kasutajalt akna **Varundamine ja taastamine** avamiseks parooli küsimise.

[Rakenduse seadete konfigureerimine](#)

Märkeruut lülitab sisse/välja kasutajale parooliviiba kuvamise, kui ta proovib salvestada rakenduse seadetes tehtud muudatusi.

[Rakendusest väljumine](#)

Märkeruut lülitab sisse/välja kasutajale parooliviiba kuvamise, kui ta proovib rakendust sulgeda.

[Rakenduse eemaldamine](#)

Märkeruut lülitab sisse/välja kasutajale parooliviiba kuvamise, kui ta proovib rakendust eemaldada.

[Loo parool](#)

Selle nupu klõpsamine lülitab sisse parooliga kaitse, mis piirab juurdepääsu määratud rakendusefunktsioonidele.

Üldine statistika

Akna ülaservas kuvatakse selle kasutajakonto nimi, mille toimingute kohta on aruanne esitatud.

Kontrollimine sisse lülitatud / välja lülitatud

See lüliti võimaldab lubada/keelata vanemakontrolli kaudu kasutaja toimingute jälgimise.

Olenevalt sellest, kas vanemakontroll jälgib kasutaja toiminguid, on nupul järgmine ilme.

 – vanemakontroll jälgib kasutaja toiminguid.

 – vanemakontroll ei jälgi kasutaja toiminguid.

Kasutaja toimingute jälgimine toimub kasutajale määratud vanemakontrolli seadete alusel.

Profiil: <profiili seaded>

Selle lingi klõpsamine võimaldab konfigurierida praegusele kontole rakendatavaid vanemakontrolli seadeid.

Jaotises **Arvuti** saate vaadata valitud kasutaja arvutikasutusaega, vaadata arvutikasutuse aruannet ja konfigurierida vanemakontrolli seadeid. Arvutikasutuse statistika kuvatakse arvutikasutuse aruande jaoks määratud ajavahemiku kohta. Vaikimisi kuvatakse viimase 24 tunni statistika.

Üksikasjad

Selle lingi klõpsamise korral avaneb aken **Arvutikasutuse aruanne**. Selles aknas saate vaadata teavet valitud kasutaja arvutikasutusaja kohta.

Seaded

Selle lingi klõpsamise korral avaneb aken. Selles aknas saate määrata ajavahemiku, mille jooksul saab valitud kasutaja arvutit kasutada.

Jaotises **Rakendused** saate vaadata üksikasju valitud kasutaja hiljuti kasutatud rakenduste kohta. Rakenduste kasutuse statistika kuvatakse rakenduste kasutuse aruandes määratud ajavahemiku kohta. Vaikimisi kuvatakse viimase 24 tunni statistika.

Üksikasjad

Selle lingi klõpsamise korral avaneb aken **Rakenduste kasutuse aruanne**. Selles aknas kuvatakse üksikasjad valitud kasutaja käivitatud rakenduste ja nende kasutusaja kohta.

Seaded

Selle lingi klõpsamise korral avaneb aken. Selles aknas saate määrata rakendused, mida valitud kasutaja saab kasutada.

Jaotis **Internet** sisaldab veebisaidikülastuste statistikat ja aruannet aja kohta, mille kasutaja on nendel veebisaitidel veetnud. Samuti saate vaadata blokeeritud veebisaitide blokeeritud külastuskatsete koguarvu.

Külastatud veebiressursside statistika kuvatakse internetikasutusaja aruandes määratud ajavahemiku kohta. Vaikimisi kuvatakse viimase 24 tunni statistika.

Üksikasjad

Selle lingi klõpsamise korral avaneb aken **Internetikasutuse aruanne**. Selles aknas saate vaadata teavet valitud kasutaja külastatud veebiressursside kohta.

Seaded

Selle lingi klõpsamise korral avaneb aken. Selles aknas saate määrata ajavahemiku, mille jooksul saab valitud kasutaja internetti kasutada.

Jaotises **Sisu kontroll** kuvatakse teave isiklike andmete edastamise blokeeritud katsete arvu kohta.

Seda statistikat kuvatakse sisukontrolli aruandes määratud ajavahemiku kohta. Vaikimisi kuvatakse ühe nädala statistika.

Üksikasjad

Selle lingi klõpsamise korral avaneb aken. Selles aknas saate teavet selle kohta, milliseid isiklike andmeid proovis valitud kasutaja suhtlusvõrkudes suhtlemise ajal edastada.

Seaded

Selle lingi klõpsamise korral avaneb aken. Selles aknas saate määrata isiklikud andmed, mille kasutamist soovite valitud kasutaja suhtluses jälgida.

Internetikasutuse aruanne

Akna ülaservas kuvatakse selle kasutajakonto nimi, mille toimingute kohta on aruanne esitatud.

Kontrollimine sisse lülitatud / välja lülitatud

See lüliti võimaldab lubada/keelata vanemakontrolli kaudu kasutaja toimingute jälgimise.

Olenevalt sellest, kas vanemakontroll jälgib kasutaja toiminguid, on nupul järgmine ilme.

 – vanemakontroll jälgib kasutaja toiminguid.

 – vanemakontroll ei jälgi kasutaja toiminguid.

Kasutaja toimingute jälgimine toimub kasutajale määratud vanemakontrolli seadete alusel.

Aknas **Internetikasutuse aruanne** saate vaadata teavet veebisaitide kohta, mida valitud kasutaja on määratud ajavahemikus külastanud.

Täna

Selle nupu klõpsamise korral avaneb aruanne kasutaja tänase tegevuse kohta.

Nupud

Nende nuppude klõpsamine avab eelmise ja järgmise ajavahemiku aruanded.

Päev/nädal/kuu

Ajavahemik, mille kohta aruanne luuakse. Aruande saate luua järgmiste ajavahemike kohta: päev, nädal ja kuu.

Nupp

Selle nupu klõpsamisel avaneb vanemakontrolli seadete akna jaotis **Internet**. Selles jaotises saate valitud kasutaja jaoks kehtestada internetikasutuse aja-, veebisaitide juurdepääsu- ja failide allalaadimispiirangud.

Enim vaadatud veebisaidid

Selles aruandes kuvatakse aruande ajavahemikus kasutaja sageli külastatud veebisaitide loend ja külastuskordade arv.

Veedetud aeg

Kogu aeg, mille valitud kasutaja on määratud ajavahemikus internetis veetnud.

Blokeeritud veebiressursid

Vanemakontrolli blokeeritud veebisaitide loend ja loend failidest, mille allalaadimine on blokeeritud.

Näita kõiki

Selle lingi klõpsamise korral avaneb aken, mis sisaldab teavet blokeeritud failiallalaadimiste ja veebisaidiküllastuste arvu kohta.

[Veebisaitide kategooriad](#)

See sisaldab veebisaitide kategooriate loendit. Iga veebisaidikategooria korral on kuvatud küllastuste arv, mille vanemakontroll on blokeeritud või lubanud.

- Vanemakontrolli blokeeritud veebisaitidele juurdepääsemiskatsete arv on kuvatud punase värviga.
- Vanemakontrolli lubatud veebisaitidele juurdepääsemiskatsete arv on kuvatud halli värviga.

Arvutikasutuse aruanne

Akna ülaservas kuvatakse selle kasutajakonto nimi, mille toimingute kohta on aruanne esitatud.

[Kontrollimine sisse lülitatud / välja lülitatud](#)  / 

See lüliti võimaldab lubada/keelata vanemakontrolli kaudu kasutaja toimingute jälgimise.

Olenevalt sellest, kas vanemakontroll jälgib kasutaja toiminguid, on nupul järgmine ilme.

 – vanemakontroll jälgib kasutaja toiminguid.

 – vanemakontroll ei jälgi kasutaja toiminguid.

Kasutaja toimingute jälgimine toimub kasutajale määratud vanemakontrolli seadete alusel.

Aknas **Arvutikasutuse aruanne** saate vaadata teavet valitud konto arvutikasutusaja kohta määratud ajavahemikul.

[Täna](#) 

Selle nupu klõpsamise korral avaneb aruanne kasutaja tänase tegevuse kohta.

[Nupud](#)   

Nende nuppude klõpsamine avab eelmise ja järgmise ajavahemiku aruanded.

[Päev/nädal/kuu](#) 

Ajavahemik, mille kohta aruanne luuakse. Aruande saate luua järgmiste ajavahemike kohta: päev, nädal ja kuu.

[Nupp](#)  

Selle nupu klõpsamisel avaneb vanemakontrolli seadete akna jaotis **Arvuti**. Selles jaotises saate seada arvutikasutuse ajapiirangud.

[Arvutikasutuse aruanne](#) 

Sisaldab teavet arvutikasutuse ajavahemike ja kestuse kohta määratud ajavahemikul.

Ajavahemikud, mil valitud konto kasutas arvutit, on tähistatud roosa värviga.

Praegune ajavahemik (päev, nädal või kuu) on esile tõstetud rohelise värviga.

Praegune kellaeg (kui valitud ajavahemik on *päev* või *nädal*) on tähistatud punase joonega.

Aken „Rakenduste haldus“

[Käivitus / Piirangud](#)

Loendis rakenduste kuvamisviisi muutmiseks klõpsake järgmisi linke.

- Lingi **Käivitus** klõpsamise korral sortitakse rakendused loendis kahte gruppi: **Blokeeritud** ja **lubatud**.
- Lingi **Piirangud** klõpsamise korral sortitakse rakendused loendis usaldusgruppide järgi. Näiteks on usaldusväärsed rakendused loetletud grupis **Usaldusväärsed**.

[Tühjenda](#)

Selle lingi klõpsamise korral eemaldab Kaspersky loendist rakendused, mida enam pole.

[Vaade](#)

Ripploendist saate valida rakenduste ja protsesside kuvamisrežiimi.

- **Laienda kõik.** Selle üksuse valimise korral kuvatakse loendis kõik arvutisse paigaldatud rakendused.
- **Ahenda kõik.** Selle üksuse valimise korral kuvatakse loendis usaldusgruppid.

Ripploendis saate valida rakenduste ja protsesside kuvamisrežiimi.

- **Nimekirjavaade.** Selle valiku korral kuvatakse rakendused ja protsessid loendina.
- **Puuvaade.** Selle valiku korral kuvatakse rakendused ja protsessid hierarhiliselt protsesside kutsumisjärjestuse alusel.

See ripploend võimaldab lülitada välja ka süsteemirakenduste, Kaspersky rakenduste ja muude mittevõrgurakenduste kuvamise.

- **Varja süsteemirakendused.** Selle üksuse valimise korral ei kuvata rakenduste ja protsesside üldloendis operatsioonisüsteemi nõuetekohaseks toimimiseks vajalikke rakendusi. Süsteemirakendused on vaikimisi peidetud.
- **Varja <PRODUCT>.** Selle üksuse valimise korral ei kuvata rakenduste ja protsesside üldloendis Kaspersky rakendusi. Kaspersky rakendused on vaikimisi peidetud.
- **Näita ainult võrgurakendusi.** Selle üksuse valimise korral kuvatakse rakenduste ja protsesside üldloendis ainult võrgurakendused. Võrgurakendused on rakendused, mis on ette nähtud eri arvutite kasutajate grupikoostöö korraldamiseks.

[Rakenduste loend](#)

See loend sisaldab teie arvutisse paigaldatud rakendusi. Iga loendis oleva rakenduse kohta saate vaadata järgmist teavet: seisund, digiallkiri, usaldusgrupp, populaarsus KSN-i kasutajate seas ja viimase käivitamiskorra aeg.

Rakenduse või protsessi rea topeltklõpsamise korral avaneb aken **Rakenduste reeglid**. Selles aknas saate seadistada rakenduse toimingute kontrollimise reeglid.

Rakenduse rea paremklõpsamise korral avaneb kontekstimenüü. Kontekstimenüüs saate teha järgmisi toiminguid.

- Saate avada akna **Rakenduste reeglid**, mis võimaldab seadistada rakenduste tegevuse õigused.
- Saate rakenduse käivitamise lubada või blokeerida.
- Saate teisaldada rakenduse muusse usaldusgruppi.
- Saate rakendusele rakendada rakenduste õiguste kontrolli vaikeseaded (rakenduse seaded lähtestada).
- Saate rakenduse loendist eemaldada.
- Saate avada rakenduse käivitusfaili sisaldava kausta.

Rakendused on loendis lisatud gruppidesse ja alamgruppidesse. Grupi rea paremklõpsamise korral avaneb kontekstimenüü. Kontekstimenüüs saate teha järgmisi toiminguid.

- Saate avada akna **Grupi reeglid**, mis võimaldab seadistada sellesse gruppi kuuluvate rakenduste toimingute vaikeõigused.
- Saate grupis luua alamgrupi. Vaikimisi rakendatakse alamgrupile selle grupi reeglid, millesse alamgrupp kuulub.
- Saate gruppi lisada rakenduse. Vaikimisi rakendatakse rakendusele selle grupi reeglid, millesse rakendus kuulub.
- Saate grupile ning kõigile alamgruppidele ja rakendustele rakendada rakenduste õiguste kontrolli vaikeseaded (grupi seaded lähtestada).
- Saate kõigile grupi kuuluvatele alamgruppidele ja rakendustele rakendada rakenduste õiguste kontrolli vaikeseaded, kuid jätta grupi seaded muutmata (alamgrupi ja rakenduste seaded lähtestada).
- Saate grupist kustutada alamgrupid ja rakendused.

[Rakendus](#)

Selles veerus kuvatakse rakenduse nimi.

[Piirangud](#)

Selles veerus kuvatakse usaldusgrupp, kuhu rakendus kuulub. Usaldusgrupp määrab arvutis rakenduse kasutamise reeglid: keelab või lubab käivitamise, rakenduse juurdepääsu failidele ja süsteemiregistrile ning rakenduse võrgutegevuse piirangud.

[Populaarsus](#)

See veerg näitab rakenduse populaarsuse taset Kaspersky Security Networkis (KSN) osalejate seas. Populaarsuse tase kajastab rakendust kasutavate KSN-is osalejate arvu.

Võrk

Selles veerus saate valida toimingu, mis tuleb rakendusel teha, kui rakendus proovib võrgule juurde pääseda.

Allolevas tabelis on esitatud Kaspersky toimingud juhul, kui rakendus või rakendusegrupp proovib võrgule juurde pääseda.

Kaspersky toimingute kirjeldus

Toiming	Kirjeldus
Päranda	Rakendus või grupp pärib vastuse emagrupilt.
Luba	Kaspersky lubab valitud gruppi kuuluvatel rakendustel võrgule juurde pääseda.
Keela	Kaspersky ei luba valitud gruppi kuuluvatel rakendustel võrgule juurde pääseda.
Küsi kasutajalt	Kui ruut Tee soovitatavad toimingud automaatselt jaotises Seaded → Jõudlusseaded → Arvutiressursside kasutus on märgitud, siis valib Kaspersky ressursi korral tehtava toimingu automaatselt Kaspersky ekspertide loodud reeglite põhjal. Soovi korral saate allmärkusest teada, missugune toiming täpselt valitakse. Sellest ruudust märke eemaldamise korral küsib rakendus kasutajalt, kas lubada sellel rakendusel võrgule juurde pääseda või mitte.
Logi sündmusi	Lisaks määratud reaktsioonile logib Kaspersky teabe rakenduse katsete kohta võrgule juurde pääseda ja salvestab selle teabe aruandesse.

Käivitus

Selles veerus saate valitud rakenduse käivitamise lüliti abil lubada või blokeerida. Vaikimisi on rakenduse käivitamine lubatud või blokeeritud olenevalt piirangutest, mis on seatud grupile, kuhu rakendus kuulub.

Arvuti kaitsmine

Kaspersky rakendus pakub igakülgset kaitset viiruste, võrgurünnakute, andmepüügi, isikuandmetega seotud rikkumiste ja muude küberturbeohtude eest. Kaspersky rakenduse osadena on saadaval mitmesugused funktsioonid ja kaitsekomponendid, mis pakuvad igakülgset kaitset.

Iga ohutüübiga tegeleb selleks ette nähtud kaitsekomponent. Saate lubada ja keelata kaitsekomponente ning konfigurereida nende seadeid.

Lisaks turvakomponentide pakutavale reaajas kaitsele tuginemisele soovime korrapäraselt kontrollida viiruste ja muu pahavara olemasolu teie arvutis. See on vajalik selleks, et vältida selliste pahatahtlike programmide võimalikku levikut, mida kaitsekomponendid pole avastanud näiteks madala turbetaseme tõttu või muudel põhjustel.

Kaspersky rakenduse ajakohasena hoidmiseks tuleb andmebaase ja rakendusemooduleid regulaarselt uuendada.

Failide kaitse

Failide kaitse hoiab ära arvuti failisüsteemi nakatumise. Komponent käivitub koos operatsioonisüsteemiga, asub pidevalt arvuti RAM-is ja skannib kõiki arvutis avatud, salvestatud või käivitatud faile ning kõiki ühendatud kettaid. Kaspersky rakendus tabab iga juurdepääsukatse failile ning kontrollib faili teadaolevate viiruste ja muu pahavara osas. Edasine juurdepääs failile on lubatud ainult juhul, kui fail pole nakatunud või rakendus on selle edukalt desinfitseerinud. Kui faili ei saa mingil põhjusel desinfitseerida, siis see kustutatakse. Kui see juhtub, teisaldatakse faili koopiat karantiini. Kui nakatunud fail paigutatakse samasse kohta, kus varem asus sama nimega kustutatud fail, salvestab karantiin ainult viimase faili koopiat. Varasema sama nimega faili koopiat ei salvestata.

Võrgurünnakute tõrje

Võrgurünnakute tõrje laaditakse operatsioonisüsteemi käivitamisel ja jälgib, kas sissetulevas võrguliikluses leidub võrgurünnakutele iseloomulikke tegevusi. Kui tuvastatakse katse teie arvutit rünnata, blokeerib Kaspersky rakendus kogu ründavast arvutist teie arvutile suunatud võrgutegevuse.

Ohutu sirvimine

Ohutu sirvimine katkestab ja blokeerib skriptide käivitamise veebisaitidel, juhul kui need on ohtlikud. Ohutu sirvimine jälgib ka kogu veebiliiklust ja blokeerib juurdepääsu ohtlikele veebisaitidele.

Meilide kaitse

Meilide kaitse skannib teie arvutisse laekuvaid ja väljaminevaid meile. Meilisõnum on adressaadile saadaval ainult juhul, kui see ei sisalda ohtlikku sisu.

Tulemüür

Tulemüür tagab teie turvalisuse, kui kasutate kohalikke võrke ja Interneti. Komponent filtreerib kõiki võrgutegevusi kahte tüüpi reeglite abil: rakenduste reeglid ja paketiireeglid.

Tulemüür on saadaval ainult pakettides Kaspersky Standard, Kaspersky Plus ja Kaspersky Premium.

Süsteemiseire

Süsteemiseire komponent pöörab tagasi pahatahtliku rakenduse või muu tegevuse kaudu operatsioonisüsteemis tehtud muudatused.

Komponent kaitseb pahavara eest, sealhulgas:

- Eksploidid
- Ekraanilukustajad
- Krüptorid, mis krüpteerivad andmeid
- Volitamata krüptoraha kaevandamine
- Lunavara, mis krüpteerib andmeid või blokeerib juurdepääsu failidele või süsteemile ning nõuab failide taastamise või neile juurdepääsu eest lunaraha

Selle komponendi keelamine pole soovitatav.

Andmepüügivastane kaitse

Kaspersky rakendus kaitseb teid andmepüügiveebisaitide küllastamise eest. Andmepüügiveebisait on petturlik veebisait, mis näeb välja nagu panga või maksesüsteemi veebisait, krüptovaluuta kauplemisplatvorm või mõni muu seaduslik veebisait. Andmepüügiveebisaiti võib selle välimuse põhjal olla üsna raske eristada seaduslikust veebisaidist. Andmepüügiveebisaidi küllastamine võib kaasa tuua paroolide, pangakaarditeabe ja muude tundlike isiklike andmete varguse.

Privaatsete jälgede eemaldaja / muudatuste tagasipööramine

Selles aknas kuvatakse operatsioonisüsteemist teie tegevuse jälgede eemaldamise edenemine. Puhastamisprotsess võib pisut aega võtta. Mõne tegevusjälje eemaldamiseks tuleb arvuti võib-olla taaskäivitada.

Kui olete esimeses etapis teinud valiku **Pööra muudatused tagasi**, pöörab privaatsete jälgede eemaldamise nõustaja tagasi eelmises etapis valitud toimingud.

Arvutiressursside tarbimine

Seaded	Kirjeldus
Tee soovitatavad toimingud automaatselt	<p>Kui mäрге on ruudust eemaldatud, töötavad Kaspersky rakenduse põhikomponendid interaktiivses režiimis. See tähendab, et Kaspersky rakendus palub teil otsustada, millised toimingud tuvastatud objektide ja ohtude korral teha, kui Failide kaitse, Turvalise sirvimise, Meilide kaitse, Süsteemiseire ja Sissetungitõrje seadetes on tehtud valik Küsi kasutajalt.</p> <p>Kui see ruut on märgitud, valib Kaspersky rakendus toimingu automaatselt Kaspersky ekspertide määratud reeglite põhjal.</p>
Kustuta pahatahtlikud tööriistad, reklaamvara, väljahelistusprogrammid ja kahtlased pakkijad	<p>Kui see ruut on märgitud, kustutab Kaspersky rakendus automaatse kaitse režiimis pahatahtlikud tööriistad, reklaamvara, väljahelistusprogrammid ja kahtlased pakkijad.</p> <p>Funktsioon on saadaval, kui märgitud on ruut Tee soovitatavad toimingud automaatselt.</p>
Akusäästja	<p>Kui ruut on märgitud, on energiasäästurežiim lubatud. Kaspersky rakendus lükkab ajastatud tegumid edasi. Vajaduse korral saate kontrolli ja uuendamise tegumid käivitada käsitsi.</p>
Mängurežiim	<p>Kui see ruut on märgitud, siis ei käivita Kaspersky rakendus kontrollimis- ega uuendamistegumeid ning ei kuva teateid, kui mängite mängu või käitate rakendusi täisekraanrežiimis.</p>
Režiim Ära sega	<p>Kui see ruut on märgitud, ei kuva Kaspersky rakendus videokõnede ja videote vaatamise ajal sündmuseteateid.</p>
Kui protsessor ja kettasüsteemid on suure koormuse all, lükka arvuti kontrollimistoimingud edasi	<p>Kui Kaspersky rakendus käitab ajastatud tegumeid, võib see suurendada protsessori ja ketta alamsüsteemide töökoormust, mis mõjutab muude rakenduste jõudlust.</p> <p>Kui see ruut on märgitud, peatab Kaspersky rakendus ajastatud tegumid, kui tuvastab suurenenud koormuse, ja vabastab operatsioonisüsteemi ressursid kasutaja rakenduste jaoks.</p>
Otsi operatsioonisüsteemi nõrku seadeid	<p>Kui see ruut on märgitud, otsib Kaspersky rakendus automaatselt operatsioonisüsteemi nõrku seadeid.</p>
Käivita <PRODUCT> arvuti sisselülitamisel (soovitatav)	<p>Kui see ruut on märgitud, käivitub Kaspersky rakendus pärast operatsioonisüsteemi laadimist, kaitstes nii arvutit kogu seansi vältel.</p> <p>Kui ruudust on mäрге eemaldatud, ei käivitu Kaspersky rakendus pärast operatsioonisüsteemi laadimist enne, kui kasutaja selle käsitsi käivitab. Arvutikaitse on keelatud ja kasutaja andmed võivad olla ohus.</p>
Kasuta tehnoloogiat Aktiivse nakkuse eemaldus (nõuab märgatavalt arvutiressursse)	<p>Kui see ruut on märgitud, kuvatakse ekraanil hüpikteade, kui operatsioonisüsteemis tuvastatakse kahjulik tegevus. Selles teates pakub Kaspersky rakendus kasutajale võimalust teha arvutile aktiivse nakkuse eemaldus. Kui kasutaja selle toimingu kinnitab, neutraliseerib Kaspersky rakendus ohu. Pärast aktiivse nakkuse eemalduse lõpuleviimist taaskäivitab Kaspersky rakendus arvuti. Aktiivse nakkuse eemalduse tehnoloogia kasutab märkimisväärses koguses andmetöötlusressursse, mis võib aeglustada muid rakendusi.</p> <p>Kui rakendus tuvastab aktiivset nakkust, ei pruugi osa operatsioonisüsteemi funktsioone olla samal ajal saadaval. Operatsioonisüsteemi käideldavus taastatakse pärast aktiivse nakkuse eemaldamise lõpuleviimist ja arvuti taaskäivitamist.</p>

Arvuti töö kiirendamise viiside automaatotsing	Kui märkeruut on märgitud, otsitakse automaatselt võimalusi arvuti kiiremaks muutmiseks.
Lülita Enesekaitse sisse	Kui see ruut on märgitud, takistab Kaspersky kõvakettal olevate rakendusefailide, mälu protsesside ja süsteemiregistri kirjade muutmist ning kustutamist.
Luba toote <PRODUCT> seadete haldamine kaugjuhtimisrakenduste kaudu	Selle ruudu märkimise korral saavad usaldusväärsed kaughaldusrakendused (näiteks TeamViewer, LogMeIn Pro ja Remotely Anywhere) muuta Kaspersky Small Office Security seadeid. Ebausaldusväärsed kaugjuhtimisrakendused ei tohi Kaspersky Small Office Security seadeid muuta isegi juhul, kui ruut on märgitud.
Lülita sisse süsteemiteenuste väline haldamine	Kui see ruut on märgitud, lubab Kaspersky rakenduse teenuseid kaugarvutist hallata. Kui rakenduse teenuseid proovitakse kaugteel hallata, kuvatakse Microsoft Windowsi tegumiribal rakenduseikooni kohal teade (välja arvatud juhul, kui kasutaja on teavitusteenuse keelanud).
Lülita sisse tõmmise kirjutamine	Kui see ruut on märgitud, jäädvustab Kaspersky kraahi korral tõmmised. Kui ruudust on märke eemaldatud, ei jäädvusta Kaspersky tõmmiseid. Samuti kustutab rakendus arvuti kõvakettalt olemasolevad tõmmisefailid.
Lülita sisse tõmmise- ja jäljefailide kaitse	Kui see ruut on märgitud, antakse juurdepääs tõmmisefailidele nii süsteemiaministraatorile ja kohalikule administraatorile kui ka kasutajale, kes lubas tõmmiste kirjutamise. Jäljefailidele pääsevad juurde ainult süsteemiaministraatorid ja kohalikud administraatorid. Kui märke on ruudust eemaldatud, on tõmmisefailidele ja jäljefailidele juurdepääs igal kasutajal.

Ohud ja erandid

Seaded	Kirjeldus
Avastatavate objektide tüübid	<p>Rakendus tuvastab erinevat tüüpi objekte, näiteks viirused ja ussid, trooja programmid ja reklaamprogrammid. Üksikasjalikumat teavet leiate Kaspersky entsüklopeediast.</p> <p>Saate keelata järgmist tüüpi objektide tuvastamise.</p> <ul style="list-style-type: none">Muu tarkvara, mida kurjategijad võivad kasutada arvuti ja isiklike andmete kahjustamiseks. See tarkvara hõlmab kaughaldusrakendusi, mida süsteemadministratoorid saavad kasutada jälgimis- või halduseesmärgil kaugarvuti kasutajaliidesele juurdepääsemiseks.Mitmekordselt pakendatud failid. Failid, mis on pakitud mitu korda, sealhulgas eri pakkijatega. Mitmekordne pakkimine raskendab objektide kontrollimist.
Halda erandeid	<p>Selle lingi klõpsamise korral avaneb kontrollimiserandite loendit sisaldav aken Erandid. <i>Kontrollimise erand</i> on tingimuste kogum, mille täitmise korral ei kontrolli rakendus konkreetset objekti viiruste ega muude ohtude suhtes.</p> <p>Loendis saate erandeid lisada, muuta või kustutada.</p> <p>Erandi lisamise või muutmise aknas saate määrata konkreetset tingimused, mille täitmise korral takistatakse objektide kontrollimist (rakendus ei kontrolli neid).</p> <ul style="list-style-type: none">Kontrollidest väljajätav fail või kaust (saate välja jätta ka rakenduste ja protsesside käivitusfailid). Maske saate kasutada järgmiste reeglite kohaselt.<ul style="list-style-type: none">Märk * (tärn) asendab mis tahes märgikomplekti, välja arvatud märgid \ ja / (faili- ja kaustateedes faili- ja kaustanimede eraldajad). Näiteks mask C:**.txt sisaldab kõiki teid ketta C: kaustades (kuid mitte alamkaustades) asuvate TXT-laiendiga failide juurde.Kaks järjestikust märki * asendavad faili- või kaustanimel mis tahes märgikomplekti (sealhulgas tühja komplekti), sealhulgas märke \ ja / (faili- ja kaustateedes faili- ja kaustanimede eraldajad). Näiteks mask C:\Kaust***.txt hõlmab kõiki teid TXT laiendusega kaustas nimega Kaust, v.a Kausta ennast. Mask peab sisaldama vähemalt ühte pesastustaset. Mask C:***.txt ei ole sobilik mask.Märk ? (küsimärk) asendab mis tahes üksikmärgi, välja arvatud märgid \ ja / (faili- ja kaustateedes faili- ja kaustanimede eraldajad). Näiteks mask C:\Kaust\???.txt sisaldab kõiki teid kaustas nimega Kaust asuvate TXT-laiendiga ja kolmest märgist koosneva nimega failide juurde.Kontrollidest väljajätavate objektide tüüp. Sisestage objektitüübi nimi vastavalt objekti liigitusele Kaspersky entsüklopeedias (näiteks Email-Worm, Rootkit või RemoteAdmin). Saate kasutada maske, mis sisaldavad märki ? (asendab mis tahes üksikmärgi) ja märki * (asendab mis tahes arvul märke). Näiteks juhul, kui määratud on mask Client*, jätab rakendus kontrollimata objektid Client-IRC, Client-P2P ja Client-SMTP.Objekti kontrollsumma. Objekti kontrollsumma võrdlemine selles seades tähistatud kontrollsummaga võimaldab kontrollist välja jätta objekti, mida pole pärast viimast kontrolli muudetud.Kaitsekomponendid, milles erandit rakendatakse. <p>Loendist erandi kustutamise asemel saate erandi seada olekusse Mitteaktiivne (erandi lisamise või muutmise aknas). Mitteaktiivset erandit ei rakendata.</p>

<p>Määra usaldusväärseid rakendusi</p>	<p>Selle lingi klõpsamise korral avaneb usaldusväärsete rakenduste loendi aken. Kaspersky rakendus ei jälgi usaldusväärsete rakenduste (sh pahatahtlike) faili- ja võrgutegevust ega ka nende rakenduste päringuid süsteemiregistrisse.</p> <p>Loendis saate usaldusväärseid rakendusi lisada, muuta või kustutada.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Isegi kui rakendus on usaldusväärsete üksuste loendis, jätkab Kaspersky rakendus selle täitmisfailist ja protsessist viiruste ning muude ohtude otsimist. Kui te ei soovi usaldusväärse rakenduse käivitusfaili ja protsessi kontrollida, lisage rakendus erandite loendisse.</p> </div> <p>Usaldusväärse rakenduse lisamisel või muutmisel saate aknas Erandid rakendusele määrata reeglid, mida Kaspersky rakendus kasutab usaldusväärse rakenduse tegevuse jälgimiseks.</p> <p>Aknas Erandid rakendusele on saadaval järgmised reeglid.</p> <ul style="list-style-type: none"> • Ära kontrolli avatud faile. • Ära jälgi rakenduse tegevust. Sissetungitõrje ei jälgi mitte ühtegi rakenduse tegevust. • Ära pärandi (rakenduse) emaprotsessi piiranguid. Kui emaprotsessi või -rakenduse piiranguid ei pärita, jälgitakse rakenduse tegevust vastavalt teie määratud reeglitele või rakenduse usaldusgrupi reeglitele. • Ära kontrolli tütarakenduste tegevust. • Ärge blokeerige infovahetust Kaspersky rakenduse liidesega. Rakendus tohib Kaspersky rakendust hallata selle graafilise kasutajaliidese abil. Kui soovite kasutada kaugtöölaauühenduse rakendust või andmesisestusseadme tööd toetavat rakendust, võib olla vaja lubada rakendusel hallata Kaspersky rakenduse liidest. Selliste seadmete hulka kuuluvad näiteks puuteplaadid ja graafikatahvlid. • Ära kontrolli kogu liiklust (või krüpteeritud liiklust). Olenevalt tehtud valikust (Ära kontrolli kogu liiklust või Ära kontrolli krüpteeritud liiklust) jätab Kaspersky rakendus kontrollimata rakenduse kogu võrguliikluse või SSL-i kaudu edastatava liikluse. Selle seade väärtus ei mõjuta tule müüri tööd: tule müür kontrollib rakenduste liiklust vastavalt tule müüri seadetele. Erandid mõjutavad meilide kaitset, ohutut sirvimist ja rämpsmeilifiltrit. Saate määrata IP-aadressid või võrgupordid, millele liikluskontrolli piirang tuleb rakendada. <p>Kui määrate rakendusele oleku Mitteaktiivne (aknas Erandid rakendusele), ei kohtle Kaspersky rakendus seda rakendust usaldusväärseks. Nii saate rakenduse ajutiselt usaldusväärsete üksuste loendist välja arvata ilma seda tegelikult loendist kustutamata.</p>
<p>Usaldusväärne süsteemi serdisalv</p>	<p>Kui valitud on üks usaldusväärne süsteemi serdisalv, jätab Kaspersky rakendus kontrollimata rakendused, mis on allkirjastatud usaldusväärse digiallkirjaga. Kaspersky määrab sellised rakendused automaatselt gruppi Usaldusväärsed.</p> <p>Valiku Ära kasuta korral kontrollib Kaspersky rakendusi sellest hoolimata, kas neil on digiallkiri või mitte. Kaspersky rakendus lisab rakenduse usaldusgruppi olenevalt sellest, kui suurt ohtu võib rakendus arvuti jaoks kujutada.</p>

Võrgu seaded

Seaded	Kirjeldus
Piira liiklust mahupõhistel ühendustel	<p>Kui see ruut on märgitud, piirab rakendus oma võrguliiklust, kui internetiühendus on piiratud. Kaspersky rakendus loeb kiire mobiilse internetiühenduse piiratud ühenduseks ja Wi-Fi-ühenduse piiramata ühenduseks.</p> <p>Kuluteadlik võrgundus töötab arvutites, milles töötab Windows 8 või uuem versioon.</p>
Süsti skript veebiliiklusesse, et suhelda veebilehtedega	<p>Kui see ruut on märgitud, sisestab Kaspersky rakendus veebilehe infovahetusskripti veebiliiklusesse. See skript tagab selliste komponentide töö nagu turvalised maksed, privaatne sirvimine, ribareklaamifilter ja URL-i nõustaja.</p>
Toeta DoH-protokolli (DNS over HTTPS)	<p>Kui ruut on märgitud, töötleb rakendus HTTPS-i kaudu edastatud DNS-andmed õigesti.</p> <p>Me ei soovita sellest ruudust märget eemaldada.</p>
DoH-serverite haldamine	<p>Link avab akna, kus saate käsitsi lisada DoH-serveri, mille kaudu edastatakse DNS-andmed veebilehitsejasse. Siit saate lugeda teavet DoH (DNS over HTTPS) ja DoH-serveri lisamise kohta.</p>
Jälgitavad pordid	<p>Jälgi kõiki võrguporte. Selles pordijälgimisrežiimis jälgivad meilide kaitse, rämpsmeilifilter ja ohutu sirvimise funktsioon kõiki avatud arvutiporte.</p> <p>Jälgi ainult valitud võrguporte. Selles pordijälgimisrežiimis jälgivad meilide kaitse, rämpsmeilifilter ja ohutu sirvimise funktsioon valitud arvutiporte. Jälgitavad võrgupordid saate määrata aknas Võrgupordid, mille avamiseks klõpsake linki Vali. Samuti saate määrata konkreetseid rakendused, mille korral tuleb lubada kõigi kasutatavate võrguportide jälgimine.</p> <ul style="list-style-type: none"> • Kaspersky soovitatud loendis olevate rakenduste kõikide portide jälgimine. Nende rakenduste loend on määratud vaikimisi ja lisatud Kaspersky rakenduse tarkvarapaketti. <p>Kui see ruut on märgitud, jälgib Kaspersky rakendus kõiki järgmiste rakenduste porte.</p> <ul style="list-style-type: none"> • Adobe Acrobat Reader. • Apple Application Support. • Google Chrome. • Microsoft Edge. • Mozilla Firefox. • Internet Explorer. • Java. • mIRC. • Opera. • Pidgin. • Safari.

	<ul style="list-style-type: none"> • Mail.ru Agent. • Yandexi veebilehitseja. • Määratletud rakenduste kõigi portide jälgimine. Rakendused saate määrata aknas Rakendused, mille avamiseks klõpsake linki Vali.
Võrgupordid	<p>Kaspersky rakenduse levituskomplekti on lisatud loend portidest, mida meilide ja veebiliikluse edastamiseks tavaliselt kasutatakse. Vaikimisi jälgib Kaspersky rakendus kõiki selle loendi porte läbivat liiklust. Saate loendisse porte lisada või neid loendist kustutada.</p> <p>Kui veerus Seisund on pordireale seatud väärtus <i>Aktiivne</i>, siis jälgib Kaspersky rakendus seda porti läbivat liiklust. Kui veerus Seisund on pordireale seatud väärtus <i>Mitteaktiivne</i>, siis jätab Kaspersky rakendus selle pordi kontrollimata, kuid ei eemalda seda pordiloendist. Aknas saate seisundi ja muude pordiseadete muutmiseks klõpsata nuppu Muuda.</p>
Krüpteeritud ühenduste kontroll	<p>SSL-i kaudu krüptitud ühenduste kontrollimiseks saate valida ühe järgmistest režiimidest.</p> <ul style="list-style-type: none"> • Ära kontrolli krüpteeritud ühendusi. • Kontrolli krüpteeritud ühendusi, kui seda nõuab kaitsekomponent. • Kontrolli alati krüpteeritud ühendusi. <p>Kui suvand Kontrolli krüpteeritud ühendusi, kui seda nõuab kaitsekomponent on valitud, kontrollib Kaspersky rakendus SSL-ühenduste turvalisust installitud Kaspersky sertifikaadi abil, kui seda nõuavad kaitsekomponendid Turvaline sirvimine ja URL-i nõustaja. Kui need komponendid on välja lülitatud, ei kontrolli Kaspersky rakendus SSL-ühenduste turvalisust.</p> <p>Pärast seda, kui Kaspersky rakendus on SSL-ühendust kontrollinud, ei pruugi veebisaitide sertifikaadid kuvada veebisaidi registreerinud organisatsiooni nime.</p> <p>Kui te ei soovi, et rakendus kontrolliks veebisaidiga loodud SSL-ühendust, klõpsake veebisaidi erandite loendisse lisamiseks linki Usaldusväärsed aadressid.</p>
Krüptitud ühenduste kontrollimise vigade esinemise korral	<p>Ripploendis saate valida toimingut, mille rakendus teeb, kui veebisaidil ilmneb turvaliste ühenduste kontrollimisel tõrge.</p> <ul style="list-style-type: none"> • Ignoreeri. Rakendus katkestab ühenduse veebisaidiga, millel on ilmnenud kontrollitõrge. • Küsi. Rakendus kuvab teile teate, milles saate veebisaidiaadressi lisada kontrollimistõrgetega veebisaitide loendisse. Veebisaidiaadressi kontrollitakse pahatahtlike objektide andmebaasi alusel. • Lisa domeen eranditesse. Rakendus lisab veebisaidiaadressi kontrollimistõrgetega veebisaitide loendisse. Veebisaidiaadressi kontrollitakse pahatahtlike objektide andmebaasi alusel.
Kontrollimisvigadega domeenid	<p>Loend domeenidest, mida ei saanud kontrollida ühenduse loomisel ilmnenud tõrgete tõttu. Domeenide aadresse on kontrollitud pahatahtlike objektide andmebaasi alusel.</p>
Usaldusväärsed aadressid	<p>Klõpsake seda linki, et avada aken Usaldusväärsed aadressid, mis sisaldab ohutu sirvimise ja URL-i nõustaja komponentide jaoks erandina lisatud veebisaitide loendit.</p>
Usaldusväärsed rakendused	<p>Loend rakendustest, mille tegevust Kaspersky rakendus oma töö ajal ei jälgi. Saate valida rakenduste tegevuse tüübid, mida Kaspersky rakendus ei jälgi (näiteks saab</p>

	<p>kontrollimata jätta võrguliikluse). Kaspersky rakendus toetab keskkonnamuutujaid ning maske * ja ?.</p>
<p>Blokeeri SSL 2.0 ühendused (soovitatav)</p>	<p>Kui ruut on märgitud, blokeerib rakendus SSL 2.0 protokollu kaudu loodud võrguühendused.</p> <p>Kui märkeruut on tühi, ei blokeeri rakendus SSL 2.0 protokollu kaudu loodud võrguühendusi ega jälgi nende ühenduste kaudu edastatud võrguliiklust.</p>
<p>Dekrüpteeri krüptitud ühendus veebisaidiga, mis kasutab EV-sertifikaati</p>	<p>EV-sertifikaadid (laiendatud valideerimisega sertifikaadid) kinnitavad veebisaitide autentsust ja parandavad ühenduse turvalisust. Veebisaidi EV-sertifikaadi olemasolu tähistamiseks kuvavad veebilehitsejad aadressiribal lukuikooni. Samuti võivad veebilehitsejad kuvada aadressiriba kas üleni või osaliselt rohelisena.</p> <p>Kui see ruut on märgitud, dekrüpteerib rakendus EV-sertifikaadiga veebisaitidega loodud krüptitud ühendused ja jälgib neid.</p> <p>Kui märkeruut on tühi, pole rakendusel juurdepääsu HTTPS-liikluse sisule. Seetõttu jälgib rakendus HTTPS-liiklust ainult veebisaidi aadressi (näiteks https://bing.com) põhjal.</p> <p>Kui avate EV-sertifikaadiga veebisaidi esimest korda, dekrüpteeritakse krüptitud ühendus hoolimata sellest, kas ruut on märgitud või mitte.</p>
<p>Puhverserveri seaded</p>	<p>Klientarvutite kasutajate internetipääsu puhverserveri seaded. Kaspersky rakendus kasutab neid seadeid teatud kaitsekomponentide jaoks, sealhulgas andmebaaside ja rakendusemoodulite uuendamiseks.</p> <p>Puhverserveri automaatseks häälestamiseks kasutab Kaspersky rakendus WPAD-protokollu (veebiproksi automaatotsingu protokollu). Kui puhverserveri IP-aadressi ei saa selle protokollu abil kindlaks teha, kasutab rakendus puhverserveri aadressi, mis on määratud Microsoft Internet Exploreri veebilehitseja seadetes.</p>
<p>Kasuta Mozilla rakendustes krüptitud ühenduste kontrollimiseks valitud sertifikaadisalve</p>	<p>Kui see ruut on märgitud, kontrollib rakendus krüptitud liiklust Mozilla Firefoxis veebilehitsejas ja Thunderbirdi meilikliendis. Mõnele saidile võib juurdepääs HTTPS-protokollu kaudu olla blokeeritud.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Mozilla Firefoxis ja Thunderbirdis liikluse kontrollimiseks peate sisse lülitama krüpteeritud ühenduste kontrolli. Kui krüpteeritud ühenduste kontroll on välja lülitatud, ei kontrolli rakendus krüptitud liiklust Mozilla Firefoxis ja Thunderbirdis.</p> </div> <p>Rakendus kasutab krüptitud liikluse dekrüpteerimiseks ja analüüsimiseks Kaspersky juursertifikaati. Saate valida sertifikaadisalve, kuhu Kaspersky juursertifikaat talletatakse.</p> <ul style="list-style-type: none"> • Kasuta Windowsi sertifikaadisalve (soovitatav). Kaspersky juursertifikaat lisatakse sellesse salve Kaspersky rakenduse installimise käigus. • Kasuta Mozilla sertifikaadisalve. Mozilla Firefox ja Thunderbird kasutavad oma sertifikaadisalvesid. Kui valite Mozilla sertifikaadisalve, peate veebilehitseja atribuutide kaudu lisama Kaspersky juuresertifikaadi sellesse salve käsitsi.

Rakenduse seadete haldamine

Seaded	Kirjeldus
Impordi	Ekstraktige rakenduse seaded CFG-vormingus failist ja rakendage need.
Ekspordi	Salvestage rakenduse praegused seaded CFG-vormingus faili.
Taasta	Saate igal ajal taastada Kaspersky ekspertide soovitatud rakenduse seaded. Seadete taastamise korral seatakse kõigile kaitsekomponentidele turbetase Optimaalne .

Tulemüür

Seaded	Kirjeldus
<p>Teata haavatavustest Wi-Fi-võrkudes</p>	<p>Kui see ruut on märgitud, kuvab Kaspersky rakendus Wi-Fi-võrgus haavatavuste tuvastamisel teateid.</p> <p>Sellele märkeruudule pääseb juurde juhul, kui arvutisse ei ole paigaldatud Kaspersky VPN Secure Connectionit.</p> <p>Kui ruut Blokeeri paroolide ebaturvaline edastus internetis ja kuva hoiatus on märgitud, siis blokeerib Kaspersky rakendus internetis välja Parool täitmisel krüptimata tekstivormingus paroolide edastamise.</p> <p>Lingi Vali kategooriad klõpsamise korral avaneb aken Kategooriad, kus saate määrata Wi-Fi-võrkude haavatavuste tüübid. Rakendus annab teile märku, kui proovite luua ühenduse Wi-Fi-võrguga, millel on määratud haavatavus.</p>
<p>Kuva minu võrkudega ühendatud seadmed</p>	<p>Kui see ruut on märgitud, on Nutikodu monitor sisse lülitatud ja toimib.</p>
<p>Luba aktiivse FTP-režiimi jaoks ühendused juhuslikes portides</p>	<p>Kui ruut on märgitud, lubab tulemüür luua teie arvutiga ühenduse juhuslike portide kaudu, kui hostühenduses tuvastati lülitumine aktiivsele FTP-režiimile.</p>
<p>Ära lülita Tulemüüri välja enne, kui operatsioonisüsteem on täielikult välja lülitunud</p>	<p>Selle ruudu märkimise korral ei lakka tulemüür töötamast enne, kui operatsioonisüsteem täielikult välja lülitub.</p>
<p>Blokeeri võrguühendused, kui kasutajalt ei saa küsida tegevuskinnitust</p>	<p>Kui see ruut on märgitud, ei peata Tulemüür tööd, kui Kaspersky rakenduse liidest pole laaditud.</p>
<p>Rakenduste reeglid</p>	<p>Selle lingi klõpsamisel avaneb aken Rakenduste võrgureeglid. Selles aknas kuvatakse teave, mis on seotud rakenduste ja rakendusegruppide võrgutegevuse juhtimisega.</p> <div data-bbox="470 1438 1493 1563" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Sissetungitõrje komponent reguleerib rakenduste võrgutegevust vastavalt rakenduste ja rakendusegruppide võrgureeglitele.</p> </div> <p>Rakenduse või rakendusegrupi võrgutegevusõigusi saate seadistada veeru Võrk lahtrimenüüs. Menüüelemente on kirjeldatud jaotises Sissetungitõrje reeglid.</p> <p>Rea kontekstimenüüs valiku Üksikasjad ja reeglid tegemise korral saate jätkata rakenduse või rakendusegrupi võrgureeglite seadistamist.</p>
<p>Paketireeglid</p>	<p>Selle lingi klõpsamisel avaneb aken Paketireeglid. Vaikimisi kuvatakse aknas eelmääratud võrgupaketireegleid, mida Kaspersky eksperdid soovivad Microsoft Windowsi operatsioonisüsteemiga arvutite võrguliikluse optimaalseks kaitsmiseks.</p> <p>Võrgupaketireeglite eesmärk on seada võrgupakettidele piirangud rakendusest olenemata. Sellised reeglid piiravad sissetulevat ja väljaminevat võrguliiklust valitud andmeprotokolli konkreetsete portide kaudu.</p> <div data-bbox="470 2040 1493 2130" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Võrgupaketireeglitel on rakenduste võrgureeglitest kõrgem prioriteet.</p> </div>

Paketireegli lisamisel või muutmisel saate määrata järgmised seaded.

- Toiming:
 - **Luba.** Kaspersky rakendus lubab võrguühendust.
 - **Blokeeri.** Kaspersky rakendus blokeerib võrguühenduse.
 - **Rakendusereeglitele vastavalt.** Kaspersky rakendus ei töötle andmevoogu paketireegli järgi, vaid kasutab selle asemel rakendusereeglit (vt eespool jaotist **Rakendusereeglid**).
- Nimi.
- Suund:
 - **Sissetulev.** Kaspersky rakendus rakendab reeglit kaugarvuti poolt avatud võrguühendustele.
 - **Väljaminev.** Kaspersky rakendus rakendab reeglit teie arvuti poolt avatud võrguühendusele.
 - **Sissetulev/väljaminev.** Kaspersky rakendus rakendab reeglit nii sissetulevatele kui ka väljaminevatele andmepakettidele või -voogudele, hoolimata sellest, milline arvuti (teie arvuti või kaugarvuti) võrguühenduse algatas.
 - **Sissetulev (pakett).** Kaspersky rakendus rakendab reeglit teie arvuti poolt vastu võetud andmepakettidele.
 - **Väljaminev (pakett).** Kaspersky rakendus rakendab reeglit teie arvuti poolt saadetud andmepakettidele.
- Protokoll.
- ICMP seaded. Saate määrata kontrollitavate andmepakettide tüübi ja koodi. Seadete jaotis on saadaval, kui on valitud ICMP või ICMPv6 protokollid.
- Kaugpordid (kaugarvuti pordid).
- Kohalikud pordid (teie arvuti pordid).

Saate määrata kaugportide või kohalike portide vahemiku (näiteks 6660–7000), loetleda mitu komaga eraldatud porti või kasutada mõlemat meetodit korraga (näiteks 80–83, 443, 1080).

- Aadress:
 - **Suvaline aadress.**
 - **Alamvõrgu aadressid.** Kaspersky rakendus rakendab reeglit kõigi hetkel ühendatud ja määratud tüüpi võrkude (*Avalik, Kohalik* või *Usaldusväärne*) IP-aadressidele. Võrgu tüübi saab valida allpool kuvatavast ripploendist valiku **Alamvõrgu aadressid** tegemise korral.

- **Aadressid nimekirjast.** Kaspersky rakendus rakendab reeglit määratud vahemikus olevatele IP-aadressidele. IP-aadressid saate määrata allpool kuvataval väljadel **Kaugaadressid** ja **Kohalikud aadressid**, kui olete teinud valiku **Aadressid nimekirjast**. Lisatud IP-aadressid tuleb eraldada komaga.
- Seisund. Tulemüür rakendab ainult paketireegleid, millel on **Aktiivne** seisund. Saate seada seisundi **Mitteaktiivne**, kui soovite paketireegli ajutiselt keelata ilma seda loendist kustutamata.
- Võrgupakettide läbitavad võrguadapterid.
- Kasuta TTL-i. Kaspersky rakendus kontrollib võrgupakettide edastamist, mille eluiga (TTL) ei ületa määratud väärtust.
- Sündmuste logimine Kaspersky rakenduse aruandesse.

Reegli kiiristamiseks saate akna allosas kuvatavast ripploendist valida soovitud eelmääratud malli.

Kättesaadavad võrgud

Selle lingi klõpsamise korral avaneb aken **Võrgud**, mis sisaldab loendit võrguühendustest, mille tulemüür on arvutis tuvastanud.

Loendis saate muuta võrgu tüüpi (*Avalik*, *Usaldusväärne* või *Kohalik*), kasutades lahtri **Võrgu tüüp** menüüd. Võrguseadeid saate muuta aknas **Võrgu omadused**, mille avamiseks saab topeltklõpsata võrgu rida.

Internetile on vaikimisi määratud tüüp *Avalik*. Te ei saa muuta interneti võrgutüüpi ega muid seadeid.

Aknas **Võrgu omadused** saate muuta järgmisi võrguseadeid.

- Võrgu nimi.
- Võrgu tüüp.
- Järgmiste teadete kuvamine.
 - Ühendus võrguga.
 - Muudetud MAC-aadress (näiteks võrguadapteri asendamise korral).
 - Muudetud MAC-aadressi/IP-aadressi paar (näiteks juhul, kui DHCP-teenus määrab erineva IP-aadressi).
- Selle võrguga ühenduse loomisel vaikimisi soovitatud printeri valimine. See seade kuvatakse juhul, kui teie arvuti operatsioonisüsteemi on paigaldatud printer.
- LISAALAMVÕRKUDE loend (eraldatud komadega).

Rakenduste reeglid / grupi reeglid

Seaded	Kirjeldus
Fail (ainult aknas Rakenduste reeglid)	Viiteteave rakenduse ja rakenduse käivitusfaili kohta. Kaspersky rakendus saab teavet rakenduse kohta selle täitmisfailist ja Kaspersky Security Networkist .
Failid ja süsteemiregister	Operatsioonisüsteemi tööga või teie isiklike andmetega seotud süsteemi registrivõtmetele ja failidele juurdepääsemise reeglid. Lugemis-, kirjutamis-, loomis- ja kustutamistoimingute üksikud juurdepääsuseaded saab määrata ühekaupa vastavate tabeliveergude lahtrites asuva menüü abil. Menüüelemente on kirjeldatud jaotises Sissetungitõrje reeglid .
Õigused	Operatsioonisüsteemi ressurssidele ja protsessidele juurdepääsemise õigused ning käivitusõigused. Juurdepääsuõigused saate määrata veeru Toiming lahtrites oleva menüü abil. Menüüelemente on kirjeldatud jaotises Sissetungitõrje reeglid .
Võrgureeglid	Kaspersky rakenduse kasutatavad reeglid rakenduse või rakendusegrupi võrgutegevuse reguleerimiseks. Vaikimisi kuvatakse loendis rakenduste jaoks eelmääratud võrgureeglid, mida soovivad Kaspersky eksperdid. Eelmääratud võrgureegleid ei saa kustutada ega muuta (välja arvatud toimingu muutmine veerus Luba ; saadaolevate toimingute kirjelduse leiate jaotisest Sissetungitõrje reeglid). Reegli lisamisel või muutmisel saate määrata järgmised seaded. <ul style="list-style-type: none"> • Toiming: <ul style="list-style-type: none"> • Luba. Kaspersky rakendus lubab võrguühendust. • Blokeeri. Kaspersky rakendus blokeerib võrguühenduse. • Küsi kasutajalt. Kui ruudust Tee soovitatavad toimingud automaatselt jaotises Seaded → Jõudlusseaded → Arvutiressursside kasutus on märke eemaldatud, palub Kaspersky rakendus kasutajal otsustada, kas võrguühendus lubada või keelata. Kui ruut on märgitud, valitakse toiming automaatselt. Soovi korral saate rakenduse aknas kuvatavast allmärgusest teada, missugune toiming täpselt valitakse. • Nimi. • Suund: <ul style="list-style-type: none"> • Sissetulev. Kaspersky rakendus rakendab reeglit kaugarvuti poolt avatud võrguühendustele. • Väljaminev. Kaspersky rakendus rakendab reeglit teie arvuti poolt avatud võrguühendusele. • Sissetulev/väljaminev. Kaspersky rakendus rakendab reeglit nii sissetulevatele kui ka väljaminevatele andmepakettidele või -voogudele, hoolimata sellest, milline arvuti (teie arvuti või kaugarvuti) võrguühenduse algatas. • Protokoll. • ICMP seaded. Saate määrata kontrollitavate andmepakettide tüübi ja koodi. Seadete jaotis on saadaval, kui on valitud ICMP või ICMPv6 protokollid.

- Kaugpordid (kaugarvuti pordid).
- Kohalikud pordid (teie arvuti pordid).

Saate määrata kaugportide või kohalike portide vahemiku (näiteks 6660–7000), loetleda mitu komaga eraldatud porti või kasutada mõlemat meetodit korraga (näiteks 80–83, 443, 1080).

- Aadress:
 - **Suvaline aadress.**
 - **Alamvõrgu aadressid.** Kaspersky rakendus rakendab reeglit kõigi hetkel ühendatud ja määratud tüüpi võrkude (*Avalik, Kohalik* või *Usaldusväärne*) IP-aadressidele. Võrgu tüübi saab valida allpool kuvatavast ripploendist valiku **Alamvõrgu aadressid** tegemise korral.
 - **Aadressid nimekirjast.** Kaspersky rakendus rakendab reeglit määratud vahemikus olevatele IP-aadressidele. IP-aadressid saate määrata allpool kuvataval väljal **Kaugaadress**, kui olete teinud valiku **Aadressid nimekirjast**.
- Võrgupakettide läbitavad võrguadapterid.
- Kasuta TTL-i. Kaspersky rakendus kontrollib võrgupakettide edastamist, mille eluiga (TTL) ei ületa määratud väärtust.
- Sündmuste logimine Kaspersky rakenduse aruandesse.

Reegli kiirlisamiseks saate akna allosas kuvatavast ripploendist valida soovitud eelmääratud malli.

Erandid (ainult aknas **Rakenduste** **reeglid**)

Saate valida reeglid, mille alusel jäetakse rakendused kontrollimata:

- Ära kontrolli avatud faile.
- Ära jälgi rakenduse tegevust. Sissetungitõrje ei jälgi mitte ühtegi rakenduse tegevust.
- Ära pärandi (rakenduse) emaprotsessi piiranguid. Kui emaprotsessi või -rakenduse piiranguid ei pärita, jälgitakse rakenduse tegevust vastavalt teie määratud reeglitele või rakenduse usaldusgrupi reeglitele.
- Ära kontrolli tütarrakenduste tegevust.
- Ärge blokeerige infovahetust Kaspersky rakenduse liidesega. Rakendus tohib Kaspersky rakendust hallata selle graafilise kasutajaliidese abil. Kui soovite kasutada kaugtööolauaühenduse rakendust või andmesisestusseadme tööd toetavat rakendust, võib olla vaja lubada rakendusel hallata Kaspersky rakenduse liidest. Selliste seadmete hulka kuuluvad näiteks puuteplaadid ja graafikatahvlid.
- Ära kontrolli kogu liiklust (või krüpteeritud liiklust). Olenevalt tehtud valikust (**Ära kontrolli kogu liiklust** või **Ära kontrolli krüpteeritud liiklust**) jätab Kaspersky rakendus kontrollimata rakenduse kogu võrguliikluse või SSL-i kaudu edastatava liikluse. Selle seade väärtus ei mõjuta tulemüüri tööd: tulemüür kontrollib rakenduste liiklust vastavalt tulemüüri seadetele. Erandid mõjutavad meilide kaitset, ohutut sirvimist ja rämpsmeilifiltrit. Saate määrata IP-aadressid või võrgupordid, millele liikluskontrolli piirang tuleb rakendada.

Ajalugu (ainult aknas Rakenduste reeglid)	Viiteteave rakendusega tehtud toimingute kohta, näiteks rakenduse käivitamine või usaldusgruppi määramine.
--	--

Sissetungitõrje reeglid

Reegel on sissetungitõrje reaktsioonikomplekt vastuseks toimingutele, mida mõni rakendus teeb teatud kategooriatesse kuuluvate operatsioonisüsteemi ressursside ja isiklike andmetega.

Sissetungitõrje oskab rakenduste toimingutele reageerida järgmiselt.

- **Päranda.** Rakenduse tegevusele reageerimiseks rakendab sissetungitõrje reegli, mis on konfigureeritud selle oleku jaoks, mille sissetungitõrje on rakendusele määratud.
Vaikimisi rakendatakse see reaktsioon. Vaikimisi pärib sissetungitõrje juurdepääsuõigused olekust, mille sissetungitõrje on rakendusele määratud.
Kui muutsite mõne rakenduse reeglit, on rakenduse reeglil rakendusele määratud olekureegluga võrreldes kõrgem prioriteet.
- **Luba.** Sissetungitõrje lubab rakendusel toimingut teha.
- **Keela.** Sissetungitõrje ei luba rakendusel seda toimingut teha.
- **Küsi kasutajalt.** Kui jaotises **Seaded** → **Jõudlusseaded** → **Arvutiressursside kasutus** on eemaldatud märged ruudust **Tee soovitatavad toimingud automaatselt**, palub sissetungitõrje kasutajal otsustada. Kui ruut on märgitud, valitakse toiming automaatselt. Soovi korral saate Kaspersky rakenduse aknas kuvatavast allmärgusest teada, missugune toiming täpselt valitakse.
- **Logi sündmusi.** Sissetungitõrje logib teabe rakenduse tegevuse ja sellele reageerimise kohta aruandesse. Teabe saab aruandesse lisada lisaks mis tahes muule sissetungitõrje tehtud toimingule.

Andmesisestuskaitse seaded

Seaded	Kirjeldus
<p>Kasuta riistvara virtualiseerimist, kui see on saadaval</p>	<p>Kui ruut on märgitud, kasutatakse kaitstud veebilehitseja käitamisel riistvara virtualiseerimist (hüperviisor). Rakendus kasutab hüperviisori tehnoloogiat lisakaitseks keeruka pahavara vastu, mis võib teie isiklike andmeid lõikepuhvri või andmepüügi teel abil kinni püüda. See märkeruut kuvatakse, kui rakendus on paigaldatud 64-bitisesse Windows 8, Windows 8.1 ja Windows 10 operatsioonisüsteemi.</p> <p>Riistvara virtualiseerimise ja selle tööpõhimõtte kohta üksikasjalikuma teabe saamiseks klõpsake seda linki.</p>
<p>Riistvara virtualiseerimist kasutav kaitse</p>	<p>Klaviatuurikaitse aitab teil veebisaitide külastamisel takistada klaviatuuri abil sisestatud andmete kinnipüüdmist küberkurjategijate poolt (üksikasjalikumat teavet leiate jaotisest Teave klaviatuurikaitse kohta).</p> <p>Märkige nende veebisaidikategooriate ruudud, millel soovite kaitsta klaviatuuri abil sisestatud andmeid.</p> <p>Et luua loendeid veebisaitidest, kus soovite klaviatuurikaitse lubada või keelata hoolimata valitud veebisaidi kategooriast, klõpsake linki Halda erandeid. Erandite lisamisel saate kasutada maske.</p>
<p>Ekraaniklaviatuur</p>	<p>Paljud nuhkvaraks liigitatud programmid saavad jäädvustada ekraanipilte, mis edastatakse seejärel automaatselt sissetungijale edasiseks analüüsiks, et varastada kasutaja isiklike andmeid. Ekraaniklaviatuur kaitseb sisestatud isiklike andmeid ekraanipiltide kaudu kinnipüüdmise eest. (Üksikasjalikumat teavet leiate jaotisest Teave ekraaniklaviatuuri kohta.)</p> <div data-bbox="416 1059 1493 1182" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Ekraaniklaviatuuri lubamise tagamiseks tuleb pärast Kaspersky rakenduse installimist arvuti taaskäivitada.</p> </div> <p>Saate valida, kuidas soovite ekraaniklaviatuuri avada.</p> <ul style="list-style-type: none"> • Ava ekraaniklaviatuur, vajutades klahvikombinatsiooni CTRL+ALT+SHIFT+P. • Näita andmesisestusväljadel kiirkäivitusikooni. Ekraaniklaviatuuri kiirkäivitusikoon kuvatakse veebilehtede paroolisisestusväljadel. Märkige nende veebisaidikategooriate ruudud, millel soovite kaitsta ekraaniklaviatuur kaudu sisestatud andmeid. <p>Et luua loendeid veebisaitidest, kus soovite ekraaniklaviatuuri kiirkäivitusikooni kuvamise lubada või keelata hoolimata valitud veebisaidi kategooriast, klõpsake aknas Halda erandeid linki Ekraaniklaviatuuri erandid. Erandite lisamisel saate kasutada maske.</p>
<p>Näita nõuandeid tugeva parooli loomiseks</p>	<p>Kui see ruut on märgitud, kontrollib Kaspersky rakendus brauserisse esmakordselt sisestatava parooli tugevust ja teavitab teid sellest.</p>
<p>Kaitse sama parooli kasutamise vastu</p>	<p>Kui sisestate parooli veebisaidile, kus parooli turvalisus on eriti oluline (näiteks suhtlusvõrgus), palub Kaspersky rakendus lubada kaitse sama parooli kasutamise vastu.</p> <p>Ruudu Hoiata sama parooli kasutamise eest veebisaitidel märkimise korral lubatakse kaitse sama parooli kasutamise vastu. Saate valida veebisaidikategooriad, mida tuleb kaitsta sama parooli kasutamise vastu. Need kategooriad hõlmavad pankade ja maksesüsteemide veebisaitide, suhtlusvõrkude veebisaitide ja meiliteenuse veebisaitide.</p> <p>Kõigi varem salvestatud paroolide kustutamiseks saate klõpsata linki Kustuta salvestatud andmed.</p>

Aken „Kustutatavate failide kustutamine“

[Faili- või kaustatee sisestusväli](#)

Väli sisaldab jäädavalt kustutatava faili või kausta teed. Faili või kausta saate valida sisestusvälja kohal olevast puust või määrata käsitsi.

Aken „Krüpteeritavate andmete valimine“

[Faili- või kaustatee sisestusväli](#)

Väli sisaldab salahoidlasse lisatava faili või kausta teed. Faili või kausta saate valida sisestusvälja kohal olevast puust või määrata käsitsi.

Salahoidla avamise aken

[Salahoidlale juurdepääsu parool](#)

Salahoidla failidele juurdepääsu parool.

[Ava Windows Exploreris](#)

Selle nupu klõpsamise korral avaneb Exploreris kaust, mis sisaldab salahoidlas talletatavate failide ja kaustade loendit.

Salahoidla kustutamise aken

[Salahoidlale juurdepääsu parool](#)

Salahoidla failidele juurdepääsu parool.

[Kustuta salahoidla](#)

Selle nupu klõpsamise korral kustutab Kaspersky rakendus salahoidla ja kõik sinna salvestatud failid.

Salahoidla failid ja kaustad kustutatakse jäädavalt.

Salahoidla ümbernimetamise aken

Hoidla uus nimi

Salahoidlale määratav uus nimi.

Salvesta

Selle nupu klõpsamise korral määrab Kaspersky rakendus salahoidlale uue nime.

Salahoidla parooli muutmise aken

[Vana parool](#)

Salahoidla praegune parool.

[Uus parool](#)

Salahoidla uus parool.

[Kinnitage parool](#)

Sisestage väljale **Uus parool** sisestatud parool uuesti.

[Salvesta](#)

Selle nupu klõpsamise korral asendatakse salahoidla praegune parool uue parooliga.

Faili või salahoidla valimise aken

[Failitee sisestusväli](#)

Väli sisaldab salahoidla teed. Salahoidla saate valida sisestusvälja kohal olevast puust või sisestada salahoidla tee käsitsi.

Aken „Varundamine ja taastamine“

[Vali failid](#)




Nupu klõpsamise korral käivitub varundustegumi loomise nõustaja.

[Taasta faile mu varukoopiate komplektist](#)

Selle lingi klõpsamise korral avaneb varuhoidlate loendi aken. Selles aknas saate valida varem loodud varukoopiakomplekti sisaldava hoidla.

[Nupud](#) / /

Nende nuppude abil saab varundamistoimingut hallata.

-  – varundustegumi lõpetamine. See nupp kuvatakse, kui varundustegum on pooleli või peatatud.
-  – varundustegumi peatamine. See nupp kuvatakse, kui varundustegum on pooleli.
-  – varundustegumi käivitamine või peatatud varundustegumi jätkamine. See nupp on saadaval, kui varundustegum on lõpule viidud või peatatud.

[Käivita](#)

Nupu klõpsamise korra käivitatakse failide varukoopiate loomistoiming. See nupp kuvatakse, kui puudub pooleliolev varundustegum.

Nupu  klõpsamise korral avaneb menüü, kust saate valida määratud varundamisseadete lisatoimingu.

- **Muuda seadeid** – käivitab varundamisseadete redaktori nõustaja.
- **Kustuta seaded** – kustutab varundamisseaded.

[Failide taastamine](#)

Selle nupu klõpsamine avab akna **Failide taastamine varukoopiatest**. Selles aknas saate valida varukoopiad, kust failid taastada.

[Logi sisse Dropboxi](#)

Selle nupu klõpsamise korral avaneb Dropboxi veebisaidi sisselogimisaken. Kui teil pole veel kontot, saate registreeruda Dropboxi veebisaidil.

Nupp kuvatakse, kui te pole juba selles arvutis Dropboxi veebisaiti sisse logitud.

[Uuenda seisundit](#)

Selle nupu klõpsamise korral loob Kaspersky rakendus ühenduse veebihoidlaga ning uuendab teavet veebihoidla mahu ja sellesse talletatud failide suuruse kohta.

See nupp kuvatakse, kui rakenduse varasem katse hankida veebihoidla kohta teavet on nurjunud (näiteks juhul, kui arvutil puudus internetiühendus).

[Üksikasjad](#)

Selle lingi klõpsamisel avaneb aken **Aruanded**. Selles aknas kuvatakse üksikasjalik teave lõpuleviidud varundustegumite kohta.

[Käivitusrežiim](#)

Selle lingi klõpsamisel avaneb aken **Varundamise ajakava**. Selles aknas saate muuta varundustegumi käivitusrežiimi.

[Tühjenda](#)

Selle nupu klõpsamise korral avaneb aken **Hoidla tühjendamine**, kus saate varuhoidlast eemaldada soovimatud varukoopiaid.

[Loo varukoopiaid teistest failidest](#)

Selle nupu klõpsamise korral avaneb varundustegumi loomise nõustaja aken, kus saate lisada varundatavad failid.

[Taasta faile varukoopiakomplektist, mis ei ole nimekirjas](#)

Selle lingi klõpsamisel avaneb aken **Otsi varukoopiaid**. Selles aknas saate määrata varem loodud varukoopiaid sisaldava varuhoidla.

[Halda hoidlaid](#)

Selle lingi klõpsamise korral avaneb saadaolevate varuhoidlate loendi aken. Selles aknas saate taastada faile valitud hoidlas talletatavatest varukoopiatest, muuta valitud hoidla seadeid või kustutada selle hoidla ja ka lisada loendisse hoidla.

Aken „Varundatava kausta valimine“

[Kaustatee sisestusväli](#)

Väli sisaldab varundatava kausta teed. Kausta saate valida sisestusvälja kohal olevast puust või määrata käsitsi.

Taastevahendi aken

[Kopeeri Kaspersky taastevahendi hoidlasse](#)

Kui see ruut on märgitud, kopeerib rakendus varundamistoimingu ajal Kaspersky taastevahendi hoidlasse. Selle vahendiga saab faile varukoopiatest taastada juhul, kui Kaspersky rakendus on rikutud või installimata.

Aken „Varundamiseks valitud failid“

Failitüüpide loend [?](#)

Sisaldab failitüüpide nimesid ja igat tüüpi failide arvu.

Loendiüksuse valimise korral kuvatakse kõik seda tüüpi failid loendina.

Valitud tüüpi failide loend [?](#)

Sisaldab teavet varundamiseks valitud kindlat tüüpi failide kohta: faili nime, asukohta ja mahtu.

Kui failinime kõrval olev märkeruut on märgitud, varundab rakendus selle faili.

Kui failinime kõrval olev märkeruut on märkimata, ei varunda rakendus seda faili.

Jaotis „Võrguketas“

[Ketas](#)

Varuhoidlana kasutatava võrgukausta tee.

[Sirvi](#)

Selle nupu klõpsamine avab akna **Vali kaust**. Selles aknas saate valida varuhoidlana kasutatava võrgukausta.

[Kasutajanimi](#)

Võrgukaustale juurdepääsemiseks ette nähtud konto nimi. Kasutajanimi tuleb sisestada vormingus *<arvuti nimi>\<kasutajanimi>* (näiteks *kl-12345\ivanov*).

[Parool](#)

Võrgukaustale juurdepääsemiseks ette nähtud parool.

Jaotis „Kohalik ketas“

[Kohalike ketaste loend](#)

Loend sisaldab arvuti kohalikke kettaid. Ühe kohaliku ketta saate määrata varukoopiate hoidlaks.

Kui kohalikku ketast ei kuvata loendis, saate sisestada selle tee allpool kuvatavale väljale või klõpsata nuppu **Sirvi** ja valida avanenud aknas **Varundatava kausta valimine** soovitud kohaliku ketta.

[Sirvi](#)

Selle nupu klõpsamine avab akna **Varundatava kausta valimine**. Selles aknas saate valida varuhoidlana kasutatava kohaliku ketta.

Jaotis „Irdketas“

[Ühendatud irdketaste loend](#)

Loend sisaldab arvutiga ühendatud irdkettaid. Ühe irdketta saate määrata varukoopiate hoidlaks.

Kui irdketast ei kuvata loendis, saate sisestada selle tee allpool kuvatavale väljale või klõpsata nuppu **Sirvi** ja valida avanenud aknas **Vali kaust** soovitud irdketta.

[Sirvi](#)

Selle nupu klõpsamine avab akna **Vali kaust**. Selles aknas saate valida varuhoidlana kasutatava irdketta.

Jaotis „Veebihoidla“

Veebihoidla kasutamiseks logige sisse veebisaidil dropbox.com. Nupu **OK** klõpsamise korral avaneb automaatselt veebisaidi dropbox.com sisselogimisvormi veebileht.

Aken „Hoidlad“

[Hoidlate loend](#)

Loetleb loodud varuhoidlad. Iga hoidla kohta kuvatav teave hõlmab kogu ja kasutatud hoidlaruumi, hoidla asukohta, hoidlat kasutavaid tegumeid ja saadaolevaid toiminguid.

[Failide taastamine](#)

Selle nupu klõpsamise korral avaneb aken, mis sisaldab hoidlasse talletatud varukoopiakomplektide loendit. Selles aknas saate valida varukoopiakomplekti, kust failid taastada.

Nupu klõpsamise korral avaneb menüü, kust saate valida soovitud lisatoimingu.

- **Muuda seadeid** – käivitab hoidlaseadete redaktori nõustaja.
- **Hoidla kustutamine** – lõpetab valitud ketta või veebiressursside kasutamise failide varukoopiate hoidlana ja kustutab hoidlast kõik failide varukoopiad.
- **Hoidla tühjendamine** – avab akna **Hoidla tühjendamine** window. Selles aknas saate hoidlaruumi vabastamiseks valida hoidlast eemaldatavad failide varukoopiad.

[Lisa võrguhoidla](#)

Selle lingi klõpsamisel avaneb aken **Lisa võrguhoidla**. Selles aknas saate määrata hoidlate loendisse lisatava võrguketta seaded.

[Ühendu olemasoleva hoidlaga](#)

Selle lingi klõpsamisel avaneb aken **Hoidlaga ühendamine**. Selles aknas saate määrata hoidlate loendisse lisatava kohaliku ketta, irdketta, võrguketta või veebihoidla seaded.

Hoidla varukoopiakomplektide loendi aken

[Varukoopiakomplektide loend](#)

Sisaldab hoidlasse talletatud varukoopiakomplektide kohta järgmist teavet.

- Varukoopiakomplekti nimi
- Sellest komplektist failide taastamiseks nõutav kettaruum

[Failide taastamine](#)

Selle nupu klõpsamine avab akna **Failide taastamine varukoopiatest**. Selles aknas saate valida varukoopiad, kust failid taastada.

Toe aken

Jaotis **Kaspersky tehniline tugi** sisaldab Kaspersky tehnilise toega ühenduse võtmiseks vajalikku teavet: Kaspersky Small Office Security versiooninumber, andmebaaside ja rakendusemoodulite väljalaskekuupäev ja -kellaeg, operatsioonisüsteemi versioon ja võti.

[Litsentsivõti](#)

Klõpsates lingil **<key>**, avaneb aken **Litsentsi üksikasjad**, mis annab teavet kehtiva litsentsi kohta.

[Muud versioonid](#)

Sellel lingil klõpsates avaneb veebisait, kust saate alla laadida teie piirkonnas kasutamiseks mõeldud rakenduseversiooni. See link pole saadaval kõigis rakenduseversioonides.

[Vastused korduma kippuvatele küsimustele](#)

Selle lingi klõpsamisel avaneb brauseriaknas interaktiivse toe leht. Lehelt leiate vastused küsimustele, mida kasutajad Kaspersky tehnilise toe spetsialistidelt kõige sagedamini küsivad.

[Rakenduse konfigureerimise näpunäited](#)

Sellel lingil klõpsates avaneb brauseriaknas tehnilise toe veebileht, kus kuvatakse artiklid Kaspersky konfigureerimise ja kasutamise kohta.

[Foorum](#)

Sellel lingil klõpsates avaneb brauseriaknas Kaspersky foorum, kus saate vaadata postitatud teemalõngu, jätta kommentaare, luua uusi teemalõngu ja otsida teavet.

[Kasutajatoe tööriistad](#)

Selle lingi klõpsamisel avaneb aken **Kasutajatoe tööriistad**. Aknas saate koguda tehnilist teavet rakenduse töö kohta ja koostada süsteemi seisundi aruande.

Aken „Hoidla tühjendamine“

[Varukoopiad, mis on loodud varem kui](#)

Funktsioon, mis eemaldab hoidlast failide varukoopiad, mis on loodud enne märkeruudu kõrval kuvatavale väljale sisestatud kuupäeva.

[Varukoopiate eelmised versioonid](#)

Kui see märkeruut on märgitud, kustutatakse varukoopiate hoidla puhastamisel varukoopiate vanad versioonid. Varukoopiate alleshoitavate uusimate versioonide arv tuleb sisestada väljale **Varukoopiate säilitatavate versioonide arv**.

[Varukoopiad failidest, mille originaalid kustutati](#)

See märkeruut lülitab sisse/välja funktsiooni, mis eemaldab arvutist kustutatud failide varukoopiad hoidlast.

Aken „Vali taastamiseks varukoopia versioon“

[Varukoopia versioonide loend](#)

Sisaldab teavet faili varukoopiate saadaolevate versioonide kohta. Iga loendiüksus sisaldab failinime, versiooninumbrit ja varukoopia versiooni loomiskuupäeva.

Loendiüksuse paremklõpsamise korral avaneb järgmisi üksusi sisaldav kontekstimenüü.

- **Ava** – faili varukoopia versioon avatakse failivormingule vastava rakenduse aknas.
- **Taasta varukoopia versioon** – avaneb aken **Taastatavatele failidele asukoha valimine**. Selles aknas saate valida kausta, kuhu taastatud fail teisaldatakse.

[Taasta](#)

Selle nupu klõpsamise korral avaneb aken, kus saate muuta failide taastamise seadeid.

Aken „Kausta valimine“

[Kaustatee sisestusväli](#)

Väli sisaldab selle kausta teed, kus failid tuleb taastada. Kausta saate valida sisestusvälja kohal olevast puust või sisestada kaustatee käsitsi.

Aken „Failide taastamine“

Peata

Selle nupu klõpsamise korral peatab Kaspersky rakendus varukoopiatest failide taastamise.

Aken „Taastatav fail on juba olemas“

[Asenda fail varukoopiaga](#)

Kaspersky rakendus kustutab olemasoleva faili ja asendab selle varukoopiast taastatud failiga.

[Ära seda faili taasta](#)

Kaspersky rakendus jätab olemasoleva faili muutmata ja ei taasta varukoopiast samanimelist faili.

[Salvesta mõlemad failid](#)

Kaspersky rakendus jätab olemasoleva faili muutmata ja salvestab varukoopiast taastatud faili samasse kausta uue nimega.

[Rakenda seda valikut kõigil sarnastel juhtudel](#)

Kui see ruut on märgitud, teeb Kaspersky rakendus valitud toiminguga kõigi taastatavate failide korral.

Aken „Failide taastamine“

Peata 

Selle nupu klõpsamise korral peatab Kaspersky rakendus varukoopiatest failide taastamise.

Aken „Hoidla seaded“

[Hoidla nimi](#) 

See väli sisaldab varuhoidla nime.

Aken „Kaspersky taastevahend“

Varundustegum

Selles ripploendis saate valida taastatavad andmed.

Varundamise kuupäev ja kellaeg

See rippmenüü võimaldab teil valida kuupäeva ja kellaaja, millal on varundatud failid, mida soovite taastada. Valitud failid taastatakse olekus, milles need olid sellel kuupäeval ja kellaajal.

Otsing



Failinime järgi faili varukoopia otsimise väli. Otsing toimub tähemärkide sisestamisega üheaegselt.

Nupp /

See lüliti muudab failide varukoopiate loendi vaadet: kaustapuu või tähestikulises järjestuses faililoend.

Failide nimekiri

Loend sisaldab failide varukoopiaid, mida saab taastada.

Olenevalt lüliti  /  asendist kuvatakse aknas kaustapuu või kõik failide varukoopiad tähestikulises järjestuses.

Selles loendis kuvatakse teave faili varukoopia nime, lähtefaili asukoha, failitüübi, failinimelaiendi, failimahu ja faili varukoopiate arvu kohta. Veerus **Versioon** kuvatava lingi klõpsamise korral avaneb aken **Vali taastamiseks varukoopia versioon**. Selles aknas saate valida varukoopia versiooni, kust fail taastada.

Kui faili varukoopia nime vastas olev märkeruut on märgitud, taastab rakendus selle faili.

Kui faili varukoopia nime vastas olevast märkeruudust on märke eemaldatud, ei taasta rakendus seda faili.

Loendiüksuse paremklõpsamise korral avaneb järgmisi üksusi sisaldav kontekstimenüü.

- **Ava fail** – fail avatakse seda tüüpi failide haldamiseks ette nähtud rakenduses.
- **Taasta faili värskem varukoopia versioon** – avab akna **Taastatavatele failidele asukoha valimine**, kus saate määrata faili varukoopia värskemast versioonist taastatava faili sihtkausta.
- **Faili varukoopiate versioonid** – avaneb aken **Vali taastamiseks varukoopia versioon**. Selles aknas saate valida varukoopia versiooni, kust fail taastada.

Versioon

Selle lingi klõpsamise korral avaneb aken **Vali taastamiseks varukoopia versioon**, mis võimaldab teil vaadata valitud faili kõiki versioone, mida saab taastada.

Vali teine hoidla ?

Selle lingi klõpsamise korral avaneb varuhoidla valimise aken.

Taasta valitud andmed ?

Selle nupu klõpsamise korral avaneb aken, kus saate muuta failide taastamise seadeid.

Vanemakontrolli kasutamine

Vanemakontroll võimaldab jälgida toiminguid, mida kasutajad teevad kohalikus arvutis ja veebis. Vanemakontrolli abil saate piirata juurdepääsu internetiressurssidele ja rakendustele ning vaadata aruandeid kasutajate tegevuse kohta.

Üha rohkem lapsi ja teismelisi pääseb juurde arvutitele ja veebiressurssidele. Arvutite ja Interneti kasutamine kujutab endast lastele mitmeid väljakutseid ja ohte:

- Aja ja/või raha kaotamine jututubade, mänguressursside, veebipoodide ja oksjonite külastamisel
- Juurdepääs täiskasvanutele mõeldud veebisaitidele, nagu need, mis sisaldavad pornograafiat, ekstremismi, tulirelvi, narkootikumide kasutamist ja selgesõnalist vägivalda
- Pahavaraga nakatunud failide allalaadimine
- Arvuti liigsest kasutamisest põhjustatud terviseprobleemid
- Kokkupuude võõrastega, kes võivad end esitleda eakaaslastena, et saada alaealistelt kasutajatelt teavet, nagu tegelik nimi, füüsiline aadress või kellaaeg, mil kedagi kodus pole

Vanemakontroll võimaldab teil vähendada arvuti- ja internetikasutusega seotud riske. Selleks on saadaval järgmised funktsioonid.

- Arvutikasutus- ja internetikasutusaja piiramine
- Lubatud ja blokeeritud mängude ja rakenduste loendite loomine, samuti lubatud rakenduste kasutamise ajutine piiramine
- Lubatud ja blokeeritud veebisaitide loendite loomine ning sobimatu sisuga veebisaidikategooriate valikuline blokeerimine
- Otsingumootorites ohutu otsingu režiimi sisselülitamine (otsingutulemite hulgas ei kuvata küsitava sisuga veebisaitide linke)
- Internetist failide allalaadimise piiramine
- Teatud isiklike andmete saatmise blokeerimine

Vanemakontrolli funktsioonid saate kõigi arvuti kasutajakontode jaoks konfigureerida eraldi. Kui kasutaja kasutab kahte kontot, näiteks operatsioonisüsteemi kohalikku kontot ja Microsofti kasutajakontot, tuleb vanemakontrolli seaded konfigureerida Microsofti kasutajakonto jaoks.

Samuti saate vaadata vanemakontrolli aruandeid jälgitavate kasutajate tegevuse kohta.

Kui ajavöönd muutub või minnakse üle suveajale ja talveajale, rakendatakse arvuti- ja internetikasutusele ning mängude ja rakenduste käivitamisele järgmisi reegleid.

- Kui ajavööndi muutumisel ei muudeta kuupäeva, jätkub käimasolev loendus blokeerimisajani ilma muudatusteta. Sama reegel kehtib ka suveajale või talveajale ülemineku korral.
- Kui ajavööndi muutumisel nihutatakse kuupäeva edasi või tagasi, nullitakse kasutaja veedetud aeg ja loendus blokeerimisajani algab otsast peale.

Vanemakontrolli seadete avamine

Vanemakontrolli seadete avamiseks tehke järgmist.

1. Avage rakenduse peaaken.
2. Avage jaotis **Turvalisus**.
3. Klõpsake jaotises **Vanemakontroll** nuppu **Lülita sisse**.
4. Kui juurdepääs vanemakontrolli seadetele pole parooliga kaitstud, palub rakendus kasutajal parooli seada. Tehke üks järgmistest valikutest.
 - Vanemakontrolli seadetele juurdepääsu kaitsmiseks parooliga tehke järgmist.
 - a. Täitke väljad **Parool** ja **Kinnitage parool** ning klõpsake nuppu **Jätka**.
 - b. Klõpsake aknas **Parooli ulatus** nuppu **Loo parool**.
 - c. Kinnitage aknas **Sisestage parool** parool ja klõpsake nuppu **Logi sisse**.
 - Kui te ei soovi juurdepääsu vanemakontrolli seadetele parooliga kaitsta, klõpsake vanemakontrolli seadete avamiseks linki **Jäta vahele**.




Avaneb aken **Vanemakontroll**.

5. Vanemakontrolli seadete akna avamiseks valige kasutajakonto ja klõpsake linki **Konfigureeri piiranguid**.

Arvutikasutuse kontrollimine

Vanemakontroll võimaldab teil piirata kasutaja arvuti taga veedetud aega. Saate määrata ajavahemiku, mille jooksul peab vanemakontroll blokeerima juurdepääsu arvutile (magamaminekuaja), samuti kogu igapäevase arvutikasutuse ajapiirangu. Tööpäevade ja nädalalõppude jaoks saate määrata erineva suurusega piirangud.

Arvutikasutusaja piirangute seadistamiseks tehke järgmist.

1. Avage [Vanemakontrolli seadete aken](#).
2. Valige vanemakontrolli seadete aknas jaotis **Arvuti**.
3. Et määrata ajavahemik, mil vanemakontroll peab juurdepääsu arvutile blokeerima, märkige jaotistes **Tööpäevad** ja **Nädalalõpud** ruut **Blokeeri juurdepääs alates N kuni N**.
4. Määrake märkeruudu **Blokeeri juurdepääs alates N** kõrval kuvatavas ripploendis blokeeringu algusaeg.
5. Määrake ripploendis **kuni N** blokeeringu lõppaeg.
Vanemakontroll blokeerib määratud ajavahemikus kasutaja juurdepääsu arvutile.
6. Samuti saate tabeli abil seadistada arvutikasutuse ajakava. Tabeli kuvamiseks klõpsake nuppu  .
- Vanemakontroll blokeerib kasutaja juurdepääsu arvutile tabelis määratud **ajakava järgi**.
7. Kogu päevase arvutikasutusaja piirangu seadmiseks märkige jaotistes **Tööpäevad** ja **Nädalalõpud** ruut **Luba juurdepääs mitte rohkem kui: N tundi päevas** ja valige siis märkeruudu kõrval kuvatavast ripploendist ajavahemik.
Vanemakontroll blokeerib kasutaja juurdepääsu arvutile, kui arvutikasutusaeg ületab kogu päeva jaoks määratud ajahulga.
8. Kasutaja arvutikasutusseansside vaheaegade seadistamiseks märkige jaotises **Vaheajad** ruut **Tee vaheaeg <aeg> kestusega <kestus>** ning seejärel valige märkeruudu kõrval kuvatavates ripploendites vaheaegade sageduse (näiteks iga tunni järel) ja kestuse (näiteks 10 minutit) väärtused.
9. Seadke akna ülaservas kuvatav lüliti asendisse **Kontroll on sisse lülitatud** .


Vanemakontroll blokeerib kasutaja juurdepääsu arvutile kooskõlas määratud seadetega.

Internetikasutuse kontrollimine

Vanemakontrolli abil saate piirata internetis veedetud aega ning keelata kasutajate juurdepääsu teatud veebisaidikategooriatele või määratud veebisaitidele. Samuti saate keelata kasutajal internetist teatud tüüpi failide (näiteks arhiivide või videote) allalaadimise.

[Internetikasutusaja piiramine](#)

Internetikasutusaja piiramiseks tehke järgmist.

1. Avage [Vanemakontrolli seadete aken](#).
2. Valige vanemakontrolli seadete aknas jaotis **Internet**.
3. Kui soovite piirata interneti kogukasutusaega tööpäevadel, märkige jaotises **Internetile juurdepääsu piirang** ruut **Piira juurdepääs tööpäevadel N tunnile päevas** ja seejärel valige märkeruudu kõrval kuvatavast ripploendist ajapiirangu väärtus.
4. Kui soovite piirata interneti kogukasutusaega nädalavahetustel, märkige ruut **Piira juurdepääs nädalavahetustel N tunnile päevas** ja seejärel valige märkeruudu kõrval kuvatavast ripploendist ajapiirangu väärtus.
5. Seadke akna ülaservas kuvatav lüliti asendisse **Kontroll on sisse lülitatud** .

Vanemakontroll piirab kasutaja internetis veedetud aja koguhulka teie määratud väärtuste kohaselt.

[Konkreetsete veebisaitide külastuste piiramine](#)

Konkreetsete veebisaitide külastuste piiramiseks tehke järgmist.

1. Avage [Vanemakontrolli seadete aken](#).

2. Valige vanemakontrolli seadete aknas jaotis **Internet**.

3. Et täiskasvanutele mõeldud sisu ei kuvataks otsingutulemites, märkige jaotises **Veebikülastuste kontroll** ruut **Lülita ohutu otsing sisse otsingumootorites**.

Kui otsite teavet sellistelt veebisaitidelt nagu Google™, YouTube™ (ainult kasutajad, kes pole veebisaidil youtube.com oma konto abil sisse loginud), Bing®, Yahoo!™ ja Yandex, ei kuvata otsingutulemites täiskasvanutele mõeldud sisu.

4. Kindlate kategooriate veebisaitidele juurdepääsu blokeerimiseks tehke järgmist.

a. Märkige jaotises **Veebikülastuste kontroll** ruut **Halda juurdepääsu veebisaitidele**.

b. Valige **Blokeeri juurdepääs veebisaitidele valitud kategooriates** ja klõpsake akna **Veebisaidikategooriatele juurdepääsu blokeerimine** avamiseks linki **Vali veebisaitide kategooriad**.

c. Märkige ruudud nende veebisaidikategooriate kõrval, mille soovite blokeerida.

Vanemakontroll blokeerib kõik kasutaja katsed veebisaiti avada, kui selle sisu on liigitatud mis tahes blokeeritud kategooriasse.

5. Konkreetsetele veebisaitidele juurdepääsu blokeerimiseks tehke järgmist.

a. Märkige jaotises **Veebikülastuste kontroll** ruut **Halda juurdepääsu veebisaitidele**.

b. Akna **Erandid** avamiseks klõpsake linki **Halda erandeid**.

c. Klõpsake akna allservas nuppu **Lisa**.

Avaneb uue veebiaadressi maski lisamiseks ette nähtud aken.

d. Sisestage väljale **Veebiaadressi mask** selle veebisaidi aadress, mille külastamise soovite keelata.

e. Määrake jaotises **Ulatus** blokeeringu ulatus: terve veebisait või ainult määratud veebileht.

f. Kui soovite määratud veebisaidi blokeerida, tehke **Toiming** valik **Blokeeri**.

g. Klõpsake nuppu **Lisa**.


Määratud veebisait kuvatakse akna **Erandid** loendis. Sulgege aken **Erandid**.

6. Seadke akna ülaservas kuvatav lüliti asendisse **Kontroll on sisse lülitatud** .

Vanemakontroll blokeerib veebisaitide avamiskatsed kooskõlas määratud seadetega.

[Kindlate failitüüpide allalaadimise blokeerimine](#) 

Internetist kindlate failitüüpide allalaadimise keelamiseks tehke järgmist.

1. Avage [Vanemakontrolli seadete aken](#).
2. Valige vanemakontrolli seadete aknas jaotis **Internet**.
3. Märkige jaotises **Blokeeri failide allalaadimine** ruudud nende failitüüpide kõrval, mille allalaadimise soovite blokeerida.
4. Seadke akna ülaserivas kuvatav lüliti asendisse **Kontroll on sisse lülitatud** .


Vanemakontroll blokeerib internetist määratud tüüpi failide allalaadimise.

Mängude ja rakenduste käivitamise kontrollimine

Vanemakontrolli abil saate kasutajal lubada või keelata mängude käivitamise neile antud vanuserühmahinnangu põhjal. Samuti saate kasutajal keelata teatud rakenduste (nt mängude või IM-klientide) käivitamise või piirata rakenduste lubatud kasutusaega.

[Vanusele sobimatu sisuga mängude blokeerimine](#)

Vanusele sobimatu sisuga mängude blokeerimiseks tehke järgmist.

1. Avage [Vanemakontrolli seadete aken](#).
2. Valige vanemakontrolli seadete aknas jaotis **Rakendused**.
3. Kui soovite blokeerida kõik mängud, mis sisaldavad kasutaja vanusele sobimatut sisu, märkige ruut **Piira mängude käivitamist kasutajate puhul, kes on nooremad kui** ja valige märkeruudu kõrval kuvatavast ripploendist soovitud vanusepiirang.
4. Kui soovite blokeerida teatud kategooriasse kuuluva sisuga mängu, tehke järgmist.
 - a. Märkige ruut **Blokeeri täiskasvanute kategooria mängud**.
 - b. Akna **Mängude blokeerimine kategooriate järgi** avamiseks klõpsake linki **Vali mängude kategooriaid**.
 - c. Märkige ruudud nende sisukategooriate kõrval, mida sisaldavad mängud soovite blokeerida.
5. Naaske jaotisse **Rakendused**.
6. Kui soovite mängude blokeerimiseks kasutada hindamissüsteemi, valige ripploendist **Kasuta mängude blokeerimiseks seda hindamissüsteemi** hinnangute ja mängusisu liigitamise tüüp.
 - **Tuvasta automaatselt** – vanemakontroll valib teie asukoha põhjal ühe kahest järgmisest mänguhinnangute tüübist: üleeuroopalise mänguteabe süsteemi (PEGI) sisuhindamissüsteem või Ameerika Ühendriikide ja Kanada hindamissüsteem (ESRB).
 - **PEGI** – vanemakontroll konfigureerib mängukäivitusõigused Euroopa hindamissüsteemi alusel.
 - **ESRB** – vanemakontroll konfigureerib mängukäivitusõigused Ameerika Ühendriikide ja Kanada hindamissüsteemi alusel.
7. Seadke akna ülaserivas kuvatav lüliti asendisse **Kontroll on sisse lülitatud** .

[Konkreetse rakenduse käivitamise piiramine](#)

Konkreetsse rakenduse käivitamise piiramiseks tehke järgmist.

1. Avage [Vanemakontrolli seadete aken](#).

2. Valige vanemakontrolli seadete aknas jaotis **Rakendused**.

3. Akna **Rakenduste kasutus** avamiseks klõpsake linki **Konfigureeri**.

4. Akna **Ava** avamiseks klõpsake nuppu **Lisa rakendus** ja valige rakenduse käivitusfail.

Valitud rakendus kuvatakse loendis **Rakenduste kasutus**. Kaspersky lisab selle rakenduse automaatselt teatud kategooriasse, näiteks *Mängud*.

5. Tehke järgmised toimingud.

- Rakenduse käivitamise blokeerimiseks valige rakenduse nime kõrval kuvatavas ripploendis üksus **Blokeeri**.
- Kõigi määratud kategooriasse kuuluvate rakenduste blokeerimiseks märkige loendis selle kategooria nime kõrval kuvatav ruut (näiteks saate blokeerida rakendused, mis kuuluvad kategooriasse *Mängud*).
- Rakenduse käivitamise lubamiseks valige rakenduse nime kõrval kuvatavas ripploendis üksus **Luba**.
- Rakenduse kasutusajapiirangute seadmiseks valige rakenduse nime kõrval kuvatavas ripploendis üksus **Piira**.

Avaneb aken **Rakenduse kasutamise piirang**.

Tehke järgmised toimingud.

a. Kui soovite seada rakenduse kasutusele ajapiirangu tööpäevadel ja nädalalõppudel, märkige jaotises **Tööpäevad** ja **Nädalalõpud** ruut **Luba juurdepääs mitte rohkem kui <N> tundi päevas** ja määrake ripploendis tundide arv, mille jooksul on kasutajal lubatud rakendust iga päev kasutada. Lisaks saate tabeli **Täpne kasutamise aeg** abil määrata aja, millal kasutajal on lubatud/keelatud rakendust kasutada.

b. Kui soovite määrata perioode, millal rakendus on peatatud, märkige jaotises **Vaheajad** märkeruut **Tee paus <time> kestusega <interval>** ning valige ripploenditest väärtused, kui sageli ja kui pikk see ajavahemik peab olema.

c. Klõpsake nuppu **Salvesta**.

6. Sulgege aken **Rakenduste kasutus**.

7. Seadke akna ülaservas kuvatav lüliti asendisse **Kontroll on sisse lülitatud** .

Vanemakontroll rakendab määratud piirangud, kui kasutaja rakenduse avab.

Sõnumi sisu jälgimine

Vanemakontrolli abil saate jälgida ja keelata kasutaja katseid sisestada sõnumitesse kindlaksmääratud isiklike andmeid (nt nimesid, telefoninumbreid, pangakaardinumbreid).

[Isiklike andmete edastamise kontrolli seadistamine](#)

Isiklike andmete edastamise kontrolli seadistamiseks tehke järgmist.

1. Avage [Vanemakontrolli seadete aken](#).
2. Valige vanemakontrolli seadete aknas jaotis **Sisu kontroll**.
3. Märkige jaotises **Isiklike andmete edastamise kontroll** ruut **Blokeeri isiklike andmete edastamine kolmandatele osapooltele**.
4. Akna **Isiklike andmete nimekiri** avamiseks klõpsake linki **Muuda isiklike andmete nimekirja**.
5. Klõpsake akna allservas nuppu **Lisa**.
Avaneb isiklike andmete lisamiseks ette nähtud aken.
6. Isiklike andmete tüübi (näiteks „telefoninumber“) valimiseks klõpsake vastavat linki või sisestage väljale **Välja nimi** kirjeldus.
7. Sisestage väljale **Väärtus** isiklikud andmed (nt teie perekonnanimi või telefoninumber).
8. Klõpsake nuppu **Lisa**.
Isiklikud andmed kuvatakse aknas **Isiklike andmete nimekiri**.
9. Sulgege aken **Isiklike andmete nimekiri**.
10. Seadke akna ülaservas kuvatav lüliti asendisse **Kontroll on sisse lülitatud** .

Vanemakontroll jälgib ja blokeerib kasutaja katseid kasutada määratud isiklike andmeid interneti vahendusel toimivas sõnumisides.

Kasutaja tegevuse kohta aruande vaatamine

Teil on juurdepääs kõigi vanemakontrolli kontrollitavate kasutajakontode tegevusaruannetele ning kõiki kontrollitavaid sündmusi kajastatakse aruandluses eraldi.

Kontrollitud kasutajakonto tegevusaruande vaatamiseks tehke järgmist.

1. Avage [Vanemakontrolli seadete aken](#).
2. Aruannete akna avamiseks valige kasutajakonto ja klõpsake linki **Kuva aruanne**.
3. Jälgitavate toimingute aruande avamiseks klõpsake asjakohast piirangutüüpi sisaldavas jaotises (näiteks **Internet**) linki **Üksikasjad**.

Aknas kuvatakse jälgitavate kasutajatoimingute aruanne.

Veebisaidi kategooriate aken

[Internetipangad ja maksesüsteemid](#)

Kui see ruut on märgitud, kuvab rakendus hoiatuse, kui loote või sisestate Internetis parooli, mida olete varem pankade ja maksesüsteemide veebisaitidel kasutanud.

[Suhtlusvõrgud](#)

Kui see ruut on märgitud, kuvab rakendus hoiatuse, kui loote või sisestate Internetis parooli, mida olete varem suhtlusvõrkudes kasutanud.

[Meiliteenused](#)

Kui see ruut on märgitud, kuvab rakendus hoiatuse, kui loote või sisestate Internetis parooli, mida olete varem meiliteenuste veebisaitidel kasutanud.

Aidake meil paremaks saada! Tagasiside jätmise aken

Selles aknas olev parameetrite komplekt oleneb hinnangust, mille komponendile andsite. Kategooria parameeter Probleem on saadaval, kui andsite komponendile hinnangu 1 kuni 2.

Teema [?](#)

Ripploend, millest saate valida tagasiside kategooria. Tagasisidekategooria võib tegeleda komponendi Nutikodu monitor probleemidega.

- **Tüütu kasutada.** Valige see üksus, kui komponendi Nutikodu monitor kasutamisel tekib ebamugavusi.
- **Rakendusel võtab võrgust seadmete otsimine kaua aega.** Valige see üksus, kui komponent Nutikodu monitor töötab liiga aeglaselt.
- **Rakendus tuvastab võrgus asuvaid seadmeid valesti.** Valige see üksus, kui rakendus määrab võrku ühendatud seadmete nimed ja/või tüübid valesti.
- **Uute seadmete kohta võrgus on liiga palju teateid.** Valige see üksus, kui rakendus kuvab teile võrgus olevate uute seadmete kohta liiga palju teateid.
- **Arvuti jõudlus on halvenenud.** Valige see üksus, kui komponendi Nutikodu monitor kasutamine halvendab teie arvuti jõudlust.
- **Komponenti ei saa konfigureerida.** Valige see üksus, kui komponendi Nutikodu monitor konfigureerimisel tekib probleeme.
- **Muu.** Valige see üksus, kui teised üksused ei sobi teie probleemi kirjeldamiseks.

Üksikasjad [?](#)

Sellele väljale saate sisestada teavet, mis võib aidata Kasperskyl teie probleemi lahendada. See väli on valikuline.

Saada [?](#)

Kasperskyle tagasiside saatmine

Komponendi Nutikodu monitor kohta saate tagasisidet saata kuni 10 korda päevas. Kui rakendus ei saa teie tagasisidet saata (näiteks internetiühendus pole saadaval), salvestatakse tagasiside teie arvutisse. Tagasisidet talletatakse avalikult 30 päeva.

Teave lõppkasutaja litsentsilepingu kohta

Lõppkasutaja litsentsileping on teie ja ettevõtte AO Kaspersky Lab vahel sõlmitud siduv leping, milles on sätestatud tingimused, mille kohaselt on teil lubatud rakendust kasutada.

Enne rakenduse kasutamist lugege hoolikalt läbi litsentsilepingu tingimused.

Nõustute litsentsilepingu tingimustega, kui kinnitate rakenduse paigaldamisel litsentsilepinguga nõustumist. Kui te ei nõustu litsentsilepingu tingimustega, peate rakenduse paigaldamise katkestama ja ei tohi rakendust kasutada.

Teave piiratud funktsionaalsuse režiimi kohta

Alltoodud tabel näitab, millised Kaspersky rakenduse funktsioonid on saadaval ja millised mitte, kui rakendus on piiratud funktsionaalsusega režiimis. Kui veerus „Piiratud funktsionaalsuse režiim“ on väärtus „jah“, on asjakohane funktsioon piiratud funktsionaalsuse režiimis saadaval. Kui veerus „Piiratud funktsionaalsuse režiim“ on väärtus „ei“, pole asjakohane funktsioon saadaval. Lisateavet leiate veerust „Piirangud“.

Kaspersky rakenduse funktsioonid piiratud funktsionaalsusega režiimis

Funktsioon	Piirangud	Piiratud funktsionaalsuse režiim
Viirusekontroll		jah
Viirusekaitse andmebaaside ja rakendusemoodulite uuendamine	Saadaval on ainult kriitilised uuendused.	ei
Rakenduse haavatavuste kontroll		jah
Ohutu sirvimine		jah – Windows 7, 8 / ei – Windows 10, 11
Failide kaitse		jah – Windows 7, 8 / ei – Windows 10, 11
Meilide kaitse		jah – Windows 7, 8 / ei – Windows 10, 11
Süsteemiseire		jah – Windows 7, 8 / ei – Windows 10, 11
Kaspersky Security Networkis failide reputatsiooni kontrollimine		ei
Andmesisestuskaitse		ei
Hädaabitaaste	Kaspersky Rescue Diski saab alla laadida rakenduse liidese kaudu.	jah
Ohud ja erandid		jah
Võrgu seaded		jah
Aruanded ja karantiin		jah
Rakenduse kuvamise seaded		jah
Mängurežiim		ei
Režiim „Mitte segada“		ei
Sissetungitõrje		jah – Windows 7, 8 / ei – Windows 10, 11
Tulemüür		jah
Võrgurünnakute tõrje		jah
Rämpsemailifilter		jah
Ribareklaamifilter		jah
Turvalised maksed		ei
Privaatne sirvimine		jah

Privaatsete jälgede eemaldaja		ei
Nutikodu monitor		ei
Veebikaamera ja mikrofoni kontroll		jah – Windows 7, 8 / ei – Windows 10, 11
Võrguseire		jah
Rakendushaldur		ei
Paroolihaldur		jah
Failipurustaja		jah
Salahoidla	Saadaval on juurdepääs ainult varem loodud salahoidlates talletatavatele andmetele.	ei
Varundamine ja taastamine	Saadaval on ainult varem loodud varukoopiatest andmete taastamine.	ei
Rakenduseuuendaja		ei
Arvutipuhastus		ei
Arvuti kiirendamine		ei
Kaspersky VPN		jah
Andmelekkedekontroll		ei
Microsoft Windowsi veaotsing		jah
Kiirkäivitus		ei
Nõrkade seadete kontroll		ei
Duplikaadid		ei
Suured failid		ei
Kasutamata rakendused		ei
Kõvaketta seisundi jälgimisfunktsioon		ei
Praegune tegevus		ei
Akusäästja		ei
Nuhkvara tuvastamine		ei
Soovimatute rakenduste installimise blokeerija		ei
Reklaamprogrammide eemaldaja		ei
AMSI kaitse		jah, ainult Windows 10, 11
Seadete haldus		jah
Rakenduse seadete parooliga kaitse		jah
Arvutiressursside tarbimise seaded		jah
Ajalugu		jah
Soovitused		jah

Vanemakontroll	Saadaval on ainult aruannete vaatamine.	ei
Tehnilise toega ühenduse võtmine		jah

Andmepüügist

Andmepüük on isikuandmete vargust hõlmav internetipettuse liik; seda levitatakse meili ja muude kanalite kaudu.

Meilid võivad olla pankade, internetiteenuse osutajate, e-poodide, elektrooniliste maksesüsteemide või muude subjektide võltsitud teatised. Meilide abil püütakse adressaati veenda petturite veebisaiti külastama valed ettekäändel, nt kutsega uuendada sisselogimisandmeid või saada toote või teenuse kohta lisateavet.

Pahaaimamatud andmepüügimeili saajad võivad lingile klõpsates leida end andmepüügiveebisaidilt, mis näeb välja täpselt samasugune nagu vastava ettevõtte veebisait.

Internetikasutaja võib sattuda andmepüügisaidile muul viisil, näiteks klõpsates otsingumootoris lingil.

Petturid võivad püüda saavutada erinevaid eesmärke. Üks neist eesmärkidest on meelitada kasutajaid avaldama oma konfidentsiaalseid andmeid, nagu sisselogimisnime, konto või krüptorahakoti parooli või muid registreerimisandmeid, pangakonto numbrit ja pangakaardi andmeid. Kasutajad sisestavad selle teabe petturliku veebisaidi veebivormile, andes petturitele juurdepääsu oma rahale. Teine lõks, kuhu kasutaja võib andmepüügilingil klõpsates sattuda, on arvutite nakatamine viiruste ja pahavaraga.

Petturlike meilide ja veebisaitide tuvastamine

Petturlikud (andmepüügi) meilid ja veebisaidid võivad esmapilgul tunduda usaldusväärsed. Ehtsana väljanägevate ettevõtetelogeode või tegelike kontakttelefoninumbrite lisamine võib tekitada kasutajates vale turvatunde. Meil võib sisaldada ka linke ettevõtte tegelikule veebisaidile, välja arvatud peamine andmepüügilink, mis viib kasutaja kurjategijate veebisaidile.

Järgmised andmepüüki reetvad märgid võivad kasutajat hoiatada.

- Kuigi andmepüügiveebisaitide domeenid võivad tunduda tegelike legitiimsete ettevõtete veebidomeenidena, võib kasutaja tähelepanelikumal vaatlusel märgata domeeninimes lisasõnu (näiteks ettevõtte ametlik domeen www.example.com võidakse muuta nimeks www.login-example.com) või punkte või kriipse kaldkriipsude asemel (www.example.com/personal/login võib olla muudetud aadressiks www.example.com.personal.login või www.example.com-personal.login). Pange tähele, et meili sisus võib küll olla ettevõtte tegelik domeeniaadress, kuid kui kasutaja sellel lingil klõpsab, kuvatakse brauseri aadressiribal teistsugune domeen.
- Meilis kasutatakse mitteisikulist pöördumist, näiteks „Kallis kasutaja“ või „Tere“.
- Graafika meilis või veebisaidil näeb välja ebaprofessionaalne, tekst sisaldab kirjavigu või halba grammatikat.
- Meili saajal palutakse lingil klõpsates viivitamatult tõestada oma konfidentsiaalsed andmed või mõnikord sisestada oma andmed e-kirja sisus olevasse vormi. Meilis võidakse sellist kiireloomulisust seletada konto blokeerimise või häkkimise või andmete kaotamise ohuga.

Andmepüügi kontroll

Kaspersky rakendus kontrollib meilide ja veebisaitide sisu andmepüügilinkide suhtes. Linke võrreldakse andmepüügi-veebiaadresside ja võltsitud krüptovaluutavahetuste andmebaasiga, mida regulaarselt uuendatakse.

Täiendava kaitse tagamiseks kasutab Kaspersky heuristlikku analüüsi ja saadab kontrolli ajal päringuid [Kaspersky Security Networki \(KSN\)](#) pilveteenustesse. Kaspersky Security Network sisaldab uusimat teavet äsjaselgunud ohtude, sealhulgas andmepüügiga tegelevate veebisaitide kohta, mida pole veel Kaspersky andmebaasidesse lisatud. KSN-i laekunud andmeid analüüsivad viiruselabori töötajad reaalsajas.

Kui olete andmepüügiveebisaidi avanud, saate sellest Kaspersky Security Networkile teada anda, kasutades [laiendit Kaspersky Kaitse](#).

Profil

Seadme ühendamine My Kasperskyga

Tellimuse haldamiseks, tellimuse aktiveerimiseks erinevates seadmetes ja selliste seadmete kaitse kaughaldamiseks on teil tarvis My Kaspersky kontot. My Kaspersky konto võimaldab teil vaadata kõigi kontoga ühendatud seadmete olekut, kuhu rakendus on installitud; samuti saate hallata tellimusi ja salvestada aktiveerimiskood turvalisse kohta.

[Logi sisse](#)

Sellel nupul klõpsates avaneb aken seadme ühendamiseks teie My Kaspersky kontoga. Nupp on saadaval, kui te pole seadet oma My Kaspersky kontoga ühendanud või kui te pole kinnitanud, et seade kuulub teile.

Olenevalt teie tellimusest ei pruugi mõned rakenduse funktsioonid olla saadaval, kui seadet pole My Kaspersky kontoga ühendatud.

[Halda kontot](#)

Nupul klõpsates suunatakse teid vaikebrauseris teie kontole My Kaspersky veebisaidil. Nupp muutub kättesaadavaks pärast seda, kui olete selles seadmes kontole sisse loginud.

[Nupp](#)

Sellel nupul klõpsamine katkestab seadme ühenduse teie My Kaspersky halduskonsooli kontoga. Nupp on saadaval, kui seade on teie My Kaspersky halduskonsooli kontoga ühendatud.

Sõltuvalt teie tellimusest võib olla vajalik seadme ühendamine teie My Kaspersky kontoga. Sellisel juhul ei saa te pärast seadme kontost lahutamist enam rakendust kasutada.

[Lisateave My Kaspersky konto kohta](#)


Tellimuse üksikasjad

Siit leiate üldist teavet teie rakenduse kasutatava tellimuse kohta. Näete tellimuse olekut, tasutud perioodi lõppemiseni jäänud päevade arvu, automaatse uuendamise olekut ja tellimuse omaniku nime, kui te pole omanik.

[Üksikasjad](#)

Sellel nupul klõpsates avaneb aken **Tellimuse üksikasjad** üksikasjaliku teabega teie tellimuse kohta. Siit leiate järgmise teabe.

- Tellimuse olek
- Automaatse uuendamise olek
- Litsentsivõti, mida võib vaja minna tehnilise toe poole pöördumisel
- Lõppkasutaja litsentsilepingu link
- Veebiportaali avalduse link
- Seadmete koguarv, mida oma tellimusega saab kaitsta
- Seadmete arv, mida te hetkel oma tellimusega kaitsete
- Aktiveerimise kuupäev
- Tasutud perioodi lõpukuupäev

Muude toimingute nägemiseks, mida saab oma tellimusega teha, klõpsake nuppu . Sõltuvalt teie tellimusest ja selle olekust võib saadaolevate toimingute loend varieeruda.

[Uuenda olekut](#)

Sellel nupul klõpsates saate teavet oma tellimuse oleku kohta.

[Sisestage aktiveerimiskood](#)

Sellel nupul klõpsates avaneb aken, kuhu saate sisestada aktiveerimiskoodi. Sõltuvalt teie tellimusest ei pruugi see nupp olla saadaval.

Aktiveerimiskoodide kohta lisateabe saamiseks vaadake jaotisi [Kui ostsite karbi või aktiveerimiskaardi](#) ja [Tellimuse uuendamine reservi varuaktiveerimiskoodiga](#).

[Muu tellimuse valimine](#)

Sellel nupul klõpsates avaneb aken teie My Kaspersky kontol saadaolevate tellimuste loendiga, mis ühilduvad teie rakendusega.

Nupp on saadaval, kui seade on teie My Kaspersky halduskonsooli kontoga ühendatud.

[Halda tellimust](#)

Sellel nupul klõpsates avaneb teie My Kaspersky halduskonsooli konto ja teid suunatakse tellimuse haldamise lehele. Nupp on saadaval, kui seade on teie My Kaspersky halduskonsooli kontoga ühendatud.

[Uuenda kohe / Osta kohe](#)

Olenevalt teie tellimuse olekust saate praegust tellimust uuendada või osta uue tellimuse.

Nupp on saadaval, kui teie tellimus on aegunud, te pole aktiveerinud automaatset uuendamist ja te pole rakendusele lisanud varuaktiveerimiskoodi.

Jätka

Nupp on saadaval, kui olete tellimuse tühistanud. Teatud aja vältel pärast tellimuse tühistamist saate seda jätkata.

Praeguse tellimuse jätkamine ei pruugi teie piirkonnas saadaval olla.

[Lisateave tellimuse haldamise kohta](#)

Kaitske rohkem seadmeid

Siin näeb, kui palju seadmeid saab oma tellimusega kaitsta, kui palju seadmeid te hetkel kaitsete; samuti saab alustada uue seadme kaitsmist. Kui olete seadme oma My Kaspersky kontoga ühendanud, värskendatakse teavet rakenduse käivitamisel.

Seadmete arv, millega saab oma tellimust kasutada, sõltub tellimusplaanist ja lõppkasutaja litsentsilepingus sätestatud tingimustest.

Nupp

Nupul klõpsamisel avaneb aken **Kaitske rohkem seadmeid**, kus saab valida eelistatud meetodi tellimuse seadmesse saatmiseks.

Nupp on saadaval, kui teie tellimus võimaldab teil kaitsta rohkem kui ühte seadet.

Olenevalt teie tellimusest ei pruugi see nupp olla kuvatud.

 nupule klõpsamine võimaldab valida ühe järgmistest toimingutest.

[Kaitse seadet](#)

Nupul klõpsamisel avaneb aken **Kaitske rohkem seadmeid**, kus saab valida eelistatud meetodi tellimuse teise seadmesse saatmiseks.

Nupp on saadaval, kui teie tellimus võimaldab teil kaitsta rohkem kui ühte seadet.

[Halda seadmeid](#)

Sellel nupul klõpsates avaneb teie My Kaspersky halduskonsooli konto ja teid suunatakse jaotises **Minu seadmed** asuvale tellimuse haldamise lehele. Siin näete kõiki seadmeid, mis kasutavad teie tellimust, ja saate jälgida nende seadmete olekut.

Kui te ei ole veel seadet oma My Kaspersky kontoga ühendanud, avaneb aken, mis võimaldab teil ühendada seadme oma kontoga.

Lisateavet seadmete kaughaldamise kohta leiate jaotisest [My Kaspersky spikker !\[\]\(291e070cef6c4d5e78fefe4696ef53be_img.jpg\)](#).

Sõltuvalt teie tellimusest võidakse kuvada ainult üldist teavet kaitstavate seadmete koguarvu kohta.

[Lisateave teiste seadmete kaitsmise kohta teie tellimusega](#)

Lahendused teile

Sellel lehel pakume teile huvipakkuvaid Kaspersky lahendusi ja meie partnerite pakutavaid lahendusi. Siit saate osta teie vajadustele vastava lahenduse, sirvida varem ostetud rakendusi ja teenuseid, jälgida oma liitumisolekut, jätkata rakenduse installimist või lugeda kasutusjuhendit.

Klõpsates jaotisel **Osta** viiakse teid veebipoodi, kus saate oma valitud lahenduse kohta rohkem teada saada ja ostuga tutvuda. Saate e-kirja, mis sisaldab teavet ostu ja aktiveerimisjuhiste kohta.

Ostetud tellimusi saate hallata oma My Kaspersky kontol.