

Paroolihaldurid

Siit juhendist leiad juhised Tartu Ülikooli poolt soovitatud paroolihaldurite kohta.

 [In English](#)



Tartu Ülikool soovib salvestatud paroolid veebilehitsejatest välja eksportida ja need soovitud paroolihaldurisse eksportida (vt [Paroolide eksportimine ja importimine](#)).

Tartu Ülikooli süsteemidesse sisselogimiseks mõeldud andmeid on soovituslik hoida paroolihalduris. Paroolihaldurid on turvalised tarkvararakendused, mida saab kasutada paroolide haldamiseks ja turvaliseks salvestamiseks. Need rakendused pakuvad võimalust luua tugevaid paroole ning salvestada neid turvaliselt, nii et ei pea enam muretsema paroolide meeldejätmise või nende kaotamise pärast.

Tartu Ülikool soovib paroolihaldureid **Bitwarden**, **LastPass**, **KeePassXC** ja **iCloud Keychain**.

Enne paroolihalduri valimist tuleks uurida nende eeliseid ja piiranguid ning veenduda, et valitud paroolihaldur vastab teie vajadustele ja eelistustele.



LastPass ja Bitwarden on mõlemad populaarsed paroolihaldurid, kuid oluline on meeles pidada, et need on pilvepõhised lahendused. See tähendab, et paroolid salvestatakse LastPass/Bitwarden serveritesse, mis võib tekitada teatud turvariske.

Tugevaima kaitse tagamiseks soovime kasutada paroolihaldurit KeePassXC.

Plussid, miinused ja kokkuvõte

Plussid:

- avatud lähtekoodiga
- tasuta versioonis enamus funktsioonid olemas
- sünkroonib seadmete vahel
- saab kasutada võrguühenduseta
- nutiseadme rakendused saadaval
- chrome'i, Firefoxi, Edge'i ja Safari laiendused saadaval

Miinused:

- keskmise raskusastmega kasutajaliides
- mõnel funktsioonil on piiratud tugi

Kokkuvõte: Bitwarden sobib ideaalselt kasutajatele, kes soovivad avatud lähtekoodiga ja läbipaistvat valikut, mis pakub head tasakaalu funktsioonide ja kulude vahel. Sellel on enamike funktsioonidega tasuta versioon, mis võimaldab sünkroonimist seadmete vahel.

Plussid:

- kasutajasõbralik liides ja lihtne seadistamine
- toetab mitmeastmelist autentimist
- täidab veebilehtedel ja rakendustes paroolid automaatselt
- sünkroonib seadmete vahel
- nutiseadme rakendused saadaval
- Chrome'i, Firefoxi, Edge'i ja Safari laiendused saadaval

Miinused:

- varem on esinenud tõrkeid teenuse kasutamises
- tasuta versioon võimaldab kasutada ainult ühte seadme tüüpi (nt ainult arvutid või ainult nutiseadmed)

- tasuline versioon võib olla kulukas
- võrguühenduseta kasutamine pole võimalik

Kokkuvõte: LastPass sobib kõige paremini kasutajatele, kes seavad esikohale kasutismugavuse ja sujuva integreerimise veebisaitide ja rakendustega. See on kasutajasõbralik, toetab mitmefaktorilist autentimist ja sünkroonib seadmete vahel.

Plussid:

- avatud lähtekoodiga ja tasuta
- täiustatud turvafunktsioonidega
- kohandatav andmebaasi formaat
- toetab paroolide automaatset täitmist
- sünkroonimine seadmete vahel (kolmanda osapoole sünkroonimistööriistadega)
- saadaval on nutiseadmete rakendused
- saadaval on Chrome'i, Firefox'i ja Edge'i laiendused

Miinused:

- seadistamine võib olla keerulisem kui teised paroolihaldurid
- seadmete vahel sünkroonimiseks on vaja kolmanda osapoole tööriistu
- Internet Exploreri või Safari ametlik tugi puudub

Kokkuvõte: KeePassXC on kohandatav ja turvaline valik, mis pakub paroolide automaatset täitmist ja sünkroonimist seadmete vahel kolmanda osapoole tööriistadega. See on parim kasutajatele, kes eelistavad turvalisust ja kohandamist, kuid on valmis esialgsesse seadistusse rohkem aega investeerima. Samuti pakub see nutiseadmete rakendusi ja brauseri laiendusi Chrome'i, Firefox'i ja Edge'i jaoks.

Kui vajate tugevamat turvalisust ja soovite oma paroole täielikult kontrollida, on KeePassXC parim valik.

Plussid:

- kasutajasõbralik liides ja lihtne seadistamine
- toetab mitmeastmelist autentimist
- täidab veebilehtedel ja rakendustes paroolid automaatselt
- sünkroonib seadmete vahel
- nutiseadme rakendused saadaval
- Chrome'i, Firefox'i, Edge'i ja Safari laiendused saadaval

Miinused:

- saab kasutada ainult Apple'i seadmetes
- võrguühenduseta kasutamine pole võimalik

Kokkuvõte: Keychain sobib kõige paremini Apple'i ökosüsteemi kasutajatele. Rakendus on eelinstalleeritud igasse Apple seadmesse. Keychain on hõlpsasti kättesaadav Mac'i ja iOS-i seadmetel ning toetab ka mitmefaktorilist autentimist. Keychain sünkroonib automaatselt kõigi Apple'i seadmete vahel ning võimaldab salvestada ja jagada turvaliselt erinevaid autentimisandmeid.

Juhendid

- [Paroolide eksportimine ja importimine](#)
- [Paroolihalduri Bitwarden seadistamine](#)
- [Paroolihalduri LastPass seadistamine](#)
- [Paroolihalduri KeePassXC seadistamine](#)
- [Paroolihalduri Apple iCloud Keychain seadistamine](#)

Küsimuste korral võta ühendust [arvutiabiga](#).

Lisamaterjalid:

- [Mis on paroolihaldur ja miks on see kasulik?](#)

- [Avatud lähtekoodiga tarkvara](#)