ZINĀŠANU BĀZES RAKSTS

Password Vault: kas var redzēt jūsu paroles

2026 © Vitextra SIA. Visas tiesības paturētas.

Atruna

Šīs atrunas izpratnē:

- **Uzņēmums** (šajā Atrunā – "Uzņēmums", "Mēs", "Mums" vai "Mūsu") ir SIA Vitextra, LV-1009, Rīga, Matīsa iela 61 – 25;
- **Dokuments** attiecas uz zināšanu bāzes rakstu;
- **Jūs** nozīmē fizisku personu, kura piekļūst Dokumentam, vai uzņēmumu, vai citu juridisku personu, kuras vārdā šī fiziskā persona piekļūst Dokumentam vai izmanto to, atkarībā no situācijas;
- **Tīmekļvietne** attiecas uz Vitextra un ir pieejama https://vitextra.com.

Atruna

Dokumentā iekļautā informācija ir paredzēta tikai vispārējai zināšanai.

Uzņēmums neuzņemas atbildību par kļūdām vai izlaidumiem Dokumenta saturā.

Uzņēmums nekādā gadījumā nav atbildīgs par īpašiem, tiešiem, netiešiem, izrietošiem vai nejaušiem zaudējumiem vai jebkādiem citiem zaudējumiem, neatkarīgi no tā, vai tie izriet no līgumā paredzētas darbības, radušies nolaidības vai citu neatļautu darbību dēļ, kas ir radušās no Dokumenta satura izmantošanas vai saistībā ar to. Uzņēmums patur tiesības jebkurā laikā un bez iepriekšēja brīdinājuma papildināt, svītrot vai grozīt Dokumenta saturu.

Atruna par kļūdām un izlaidumiem

Dokumentā sniegtā informācija ir tikai vispārīgas norādes par interešu jautājumiem. Tāpēc kļūdas var rasties pat tad, ja Uzņēmums veic visus piesardzības pasākumus, lai nodrošinātu, ka Dokumenta saturs ir aktuāls un precīzs. Turklāt, ņemot vērā likumu un noteikumu mainīgo dabu, dokumentā iekļautajā informācijā var būt kavējumi, izlaidumi vai neprecizitātes.

Uzņēmums nav atbildīgs par kļūdām vai izlaidumiem, kā arī par rezultātiem, kas ir iegūti, izmantojot šo informāciju.

Atruna par godprātīgu izmantošanu

Uzņēmums var izmantot ar autortiesībām aizsargātu materiālu, ko autortiesību īpašnieks nav skaidri atļāvis. Uzņēmums nodrošina šāda materiāla pieejamību kritikas, komentāru, jaunumu izziņošanas, mācību, zinātniskā darba vai pētniecības nolūkos.

Uzņēmums uzskata, ka tas ir "godprātīgs" šāda ar autortiesībām aizsargāta materiāla izmantojums, kā ir noteikts ASV Autortiesību likuma 107. pantā.

Ja vēlaties izmantot ar autortiesībām aizsargātu materiālu no Dokumenta saviem mērķiem, kas pārsniedz godprātīgu izmantošanu, ir jāsaņem atļauja no autortiesību īpašnieka.

Atruna "Lietošana uz savu risku"

Visa informācija dokumentā tiek sniegta "tāda, kāda tā ir", bez jebkādām pilnīguma, precizitātes, savlaicīguma vai šīs informācijas izmantošanas rezultātā iegūto rezultātu garantijām, kā arī bez jebkādām garantijām, skaidri izteiktām vai netiešām, tostarp, bet ne tikai, bez garantijām par veiktspēju, komerciālo izmantojamību un piemērotību konkrētam mērķim.

Uzņēmums neuzņemas atbildību attiecībā pret Jums vai kādu citu par pieņemto lēmumu vai rīcību, kas pamatojas uz Pakalpojumā sniegto informāciju, vai par izrietošiem, īpašiem vai līdzīgiem zaudējumiem, pat ja Jums ir paziņots par šādu zaudējumu iespējamību.

Sazinieties ar mums

Ja par šo atrunu rodas jautājumi, sazinieties ar Mums pa e-pastu support@vitextra.com.

Satura rādītājs

Pārskats 4

Vai kolēģi, kuri atver to pašu lapu, var redzēt manas paroles? 4

Vai Teams kanāla dalībnieki var redzēt manas paroles? 4

Vai lapu īpašnieki vai vietņu administratori var redzēt manas paroles? 5

Vai Microsoft 365 vai OneDrive administratori var redzēt manas paroles? 5

Vai citas lietotnes manā organizācijā var piekļūt glabātuves failam? 5

Vai Vitextra var redzēt manas paroles? 6

Ko var redzēt persona pie mana nebloķētā datora? 6

Vai varu apzināti kopīgot ierakstu ar kolēģi? 7

Saistītie raksti 7

Pārskats

Password Vault glabā katra lietotāja ierakstus vienā šifrētā failā, *vitextra-password-vault.json*, šī lietotāja paša OneDrive lietotnes mapē. Tāpēc tas, kas var redzēt jūsu ierakstus, ir atkarīgs no tā, kam ir piekļuve jūsu OneDrive un kas var izmantot jūsu datoru, kurā esat pierakstījies, — nevis no tā, kas var atvērt lapu. Tālāk aplūkoti tipiskie gadījumi.

Kas	Vai var redzēt jūsu ierakstus?
Kolēģi, kuri atver to pašu lapu	Nē — viņi redz savas glabātuves
Teams kanāla dalībnieki, kuriem ir Password Vault cilne	Nē — katrs dalībnieks redz savu glabātuvi
Lapu īpašnieki un vietņu administratori	Nē — lapā vai vietnē nekas netiek glabāts
Microsoft 365 / OneDrive administratori	Viņi var piekļūt failam tāpat kā jebkuram citam failam jūsu OneDrive, bet bez PIN koda nevar izlasīt ierakstus; ar faila kopiju viņi varētu bezsaistē izmēģināt visus 10 000 PIN kodu
Vitextra	Nē — Vitextra nesaņem glabātuves datus
Persona pie jūsu nebloķētā datora	Bez PIN koda neko — pat ne ierakstu nosaukumus; visu, kamēr glabātuve ir atbloķēta

Vai kolēģi, kuri atver to pašu lapu, var redzēt manas paroles?

Nē. Tīmekļa daļa vienmēr atver tās personas glabātuvi, kura ir pierakstījusies. Ja desmit kolēģi atver vienu un to pašu SharePoint lapu, katrs no viņiem redz tikai savus ierakstus, kas nolasīti no viņa paša OneDrive. Password Vault ievietošana koplietotā lapā nekoplieto nevienu paroli.

Vai Teams kanāla dalībnieki var redzēt manas paroles?

Nē. Password Vault cilne Teams kanālā darbojas tāpat kā tīmekļa daļa lapā: katrs kanāla dalībnieks, kurš atver cilni, redz savu glabātuvi. Tā ir tā pati glabātuve, ko dalībnieks redz SharePoint lapās un personiskajā lietotnē. Skatiet KB10457. Kā

pievienot Password Vault pakalpojumā Microsoft Teams.

Vai lapu īpašnieki vai vietņu administratori var redzēt manas paroles?

Nē. Password Vault neko neglabā SharePoint sarakstos, bibliotēkās vai tīmekļa daļas rekvizītos; lapā ir tikai tīmekļa daļa un tās virsraksts. Lapas vai vietnes īpašumtiesības vai vietņu kolekcijas administratora loma nedod piekļuvi to cilvēku glabātuvju failiem, kuri to izmanto.

Vai Microsoft 365 vai OneDrive administratori var redzēt manas paroles?

Password Vault nav administrēšanas konsoles: administratori nevar ar produkta palīdzību skatīt, pārvaldīt, atbloķēt vai atkopt glabātuves.

Pats glabātuves fails ir parasts fails jūsu OneDrive, un to aizsargā Microsoft 365 un OneDrive piekļuves kontrole. Tāpat kā jebkuram citam failam jūsu OneDrive, tam var piekļūt administratori, kuriem ir piekļuve jūsu OneDrive vai kuri to sev piešķir saskaņā ar jūsu organizācijas politikām, — piemēram, izmeklēšanas laikā, ar atbilstības rīku palīdzību vai tad, kad tiek nodots aizgājuša darbinieka OneDrive. Tā ierakstu lauki ir šifrēti ar atslēgu, kas atvasināta no jūsu PIN koda un netiek glabāta failā, tāpēc piekļuve failam vien neļauj administratoram izlasīt jūsu ierakstus. Tomēr PIN kodam ir tikai 4 cipari: tas, kuram ir piekļuve failam, varētu to nokopēt un bezsaistē izmēģināt visus 10 000 PIN kodu. PBKDF2 palēnina katru minēšanas mēģinājumu, un piecu mēģinājumu ierobežojums darbojas tikai tīmekļa daļā.

Brīdinājums!

Pret personu, kura izmēģina visus PIN kodus faila kopijā, 4 ciparu PIN kods nodrošina tikai ierobežotu aizsardzību, tāpēc OneDrive piekļuves kontrole joprojām ir pirmā aizsardzības līnija. Password Vault ir paredzēts personiskiem, ikdienas akreditācijas datiem. Administratoru kontiem, pakalpojumu kontiem un citiem augstu privilēģiju vai koplietotiem akreditācijas datiem ievērojiet savas organizācijas politiku. Skatiet KB10452. Kā Password Vault aizsargā jūsu datus: šifrēšana, PIN kods un glabāšana.

Vai citas lietotnes manā organizācijā var piekļūt glabātuves failam?

Glabātuve tiek saglabāta, izmantojot Microsoft Graph atļauju *Files.ReadWrite.AppFolder*. Pakalpojumā SharePoint Online šī atļauja tiek piešķirta vienai lietojumprogrammai, ko kopīgi izmanto visi nomnieka SharePoint Framework risinājumi, tāpēc citi jūsu organizācijā izvietotie SPFx risinājumi, kas izmanto to pašu atļauju, pierakstījušā lietotāja vārdā strādā ar to pašu lietotnes mapi. Šāds risinājums varētu nolasīt vai mainīt glabātuves failu; tajā esošie ieraksti ir šifrēti ar atslēgu, kas atvasināta no jūsu PIN koda, ar iepriekšējā sadaļā aprakstīto ierobežojumu. Administratoriem jāizvieto tikai tie SPFx risinājumi, kuriem viņi uzticas. Skatiet KB10454. Microsoft Graph atļauja Files.ReadWrite.AppFolder: kāpēc tā nepieciešama Password Vault un kā to apstiprināt.

Vai Vitextra var redzēt manas paroles?

Nē. Šifrēšana un atšifrēšana notiek jūsu pārlūkprogrammā, un glabātuves fails tiek pārsūtīts tikai starp jūsu pārlūkprogrammu un jūsu OneDrive. Vitextra nesaņem, neglabā un nedublē glabātuves datus, jūsu PIN kodu vai no tā atvasināto atslēgu. Tīmekļa daļa nosūta uzņēmumam Vitextra tikai licences pārbaudes un lietošanas telemetrijas tehniskos identifikatorus; skatiet KB10363. Kur Vitextra produkti glabā jūsu datus: konfidencialitāte, datu atrašanās vieta un VDAR.

Ko var redzēt persona pie mana nebloķētā datora?

Ikviens, kurš var izmantot jūsu pārlūkprogrammu, kamēr esat pierakstījies Microsoft 365, var atvērt lapu ar Password Vault. **Bez PIN koda** šī persona neredz nevienu ierakstu — pat ne to nosaukumus:

- saraksta vietā tīmekļa daļa rāda tikai uzvedni **Ievadiet PIN kodu**, un rīkjoslā ir pieejama tikai poga **Atsvaidzināt**;
- paroles, lietotājvārdi, URL, mapes, atzīmes un piezīmes netiek rādītas, un **Jauns vienums**, **Mainīt PIN kodu**, **Meklēt**, filtrs un izlase nav pieejami;
- persona var ievadīt PIN kodus, un katrs nepareizs PIN kods tiek ieskaitīts piecu mēģinājumu ierobežojumā (skatiet tālāk).

Kad ir ievadīts pareizais PIN kods, katra darbība — paroļu parādīšana un kopēšana, **Jauns vienums**, **Rediģēt**, **Noņemt** un **Mainīt PIN kodu** — darbojas, atkārtoti neprasot PIN kodu.

Pēc PIN koda ievadīšanas glabātuve paliek atbloķēta, kamēr lapa ir atvērta un tiek izmantota: ikviens pie datora var parādīt un kopēt paroles un mainīt ierakstus, līdz pēc **5 minūtēm** bez darbībām stājas spēkā automātiskā bloķēšana (skatiet KB10451. Automātiskā bloķēšana: kad Password Vault atkal pieprasa PIN kodu). Arī jūsu nokopēta parole paliek starpliktuvē, līdz tiek nokopēts kaut kas cits.

Persona, kura nezina PIN kodu, var arī ievadīt nepareizus PIN kodus. Pieci nepareizi

PIN kodi pēc kārtas bloķē glabātuvi, un vienīgā izeja ir atiestatīšana, kas izdzēš visus ierakstus (skatiet KB10455. Password Vault: nepareizi PIN koda mēģinājumi un kas notiek pēc piecām neveiksmīgām reizēm).

Padoms

Bloķējiet datoru ikreiz, kad no tā aizejat, un iestatiet vai mainiet PIN kodu vietā, kur neviens neredz ekrānu: ekrānos **PIN koda iestatīšana** un **Mainiet PIN kodu** cipari ir redzami, kamēr tos ievadāt (uzvednē **Ievadiet PIN kodu** tie ir maskēti).

Vai varu apzināti kopīgot ierakstu ar kolēģi?

Nē. Password Vault ir personiska glabātuve: tajā nav koplietotu ierakstu, koplietotu mapju vai komandas glabātuvju. Akreditācijas datiem, kas komandai jāizmanto kopīgi, ievērojiet savas organizācijas politiku.

Saistītie raksti

- KB10453. Kur Password Vault glabā jūsu paroles: OneDrive lietotnes mape
- KB10452. Kā Password Vault aizsargā jūsu datus: šifrēšana, PIN kods un glabāšana
- KB10439. Password Vault: bieži uzdotie jautājumi