ZINĀŠANU BĀZES RAKSTS

Kā Password Vault aizsargā jūsu datus: šifrēšana, PIN kods un glabāšana

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

Kopsavilkums 4

1. līmenis: pierakstīšanās Microsoft 365 un OneDrive piekļuves kontrole 5

2. līmenis: ierakstu šifrēšana pārlūkprogrammā 5

Kas tiek un kas netiek šifrēts 6

Esošās glabātuves tiek jauninātas automātiski 7

3. līmenis: PIN kods un bloķētā glabātuve 7

Automātiskā bloķēšana 8

Neveiksmīgo mēģinājumu ierobežojums 9

Vitextra nav jūsu datu 9

Kam Password Vault ir paredzēts 9

Ieteikumi 10

Pārskats

Password Vault ir personisks paroļu pārvaldnieks SharePoint Online lapām un Microsoft Teams. Katrs lietotājs glabā savus akreditācijas datus vienā šifrētā failā savā OneDrive. Šajā rakstā pa līmeņiem paskaidrots, kā dati tiek aizsargāti, ko PIN kods dara un ko nedara, kuras glabātuves daļas tiek šifrētas un kādiem akreditācijas datiem Password Vault ir paredzēts. Raksts ir paredzēts gan galalietotājiem, kuri vēlas izprast produktu, gan administratoriem un drošības speciālistiem, kuri to pārbauda.

Kopsavilkums

Jautājums	Atbilde
Kur tiek glabāta glabātuve?	Vienā failā, *vitextra-password-vault.json*, lietotāja paša OneDrive lietotnes mapē
Kas var atvērt failu?	Ikviens, kam saskaņā ar Microsoft 365 atļaujām ir piekļuve lietotāja OneDrive, — pēc noklusējuma tikai pats lietotājs
Kura identitāte tiek izmantota?	Pierakstījies Microsoft 365 lietotājs, izmantojot Microsoft Graph ar deleģēto atļauju *Files.ReadWrite.AppFolder*
Kas tiek šifrēts?	Katra ieraksta teksta lauki: nosaukums, lietotājvārds, parole, URL, piezīmes, mape un atzīmes (AES, pārlūkprogrammā, ar atslēgu, kas atvasināta no PIN koda)
Ko dara PIN kods?	Šifrēšanas atslēga tiek atvasināta no 4 ciparu PIN koda; kamēr PIN kods nav ievadīts, tīmekļa daļa nerāda nevienu ierakstu
Kad PIN kods tiek prasīts atkārtoti?	Pēc 5 minūtēm bez darbībām tīmekļa daļā un pēc lapas atkārtotas ielādes
Kas notiek pēc nepareiziem PIN kodiem?	Pēc 5 nepareiziem PIN kodiem pēc kārtas glabātuve tiek bloķēta, un to var tikai atiestatīt, kas izdzēš visus ierakstus
Kas tiek nosūtīts uzņēmumam Vitextra?	Nekādi glabātuves dati; tikai licences

Jautājums	Atbilde
	pārbaudes un lietošanas telemetrijas tehniskie identifikatori

1. līmenis: pierakstīšanās Microsoft 365 un OneDrive piekļuves kontrole

Password Vault nav savu kontu, serveru vai datu bāzu. Tīmekļa daļa darbojas pierakstījušā lietotāja pārlūkprogrammā un lasa un raksta glabātuvi, izmantojot Microsoft Graph ar šī lietotāja identitāti. Fails tiek glabāts lietotāja paša OneDrive, tāpēc to aizsargā tie paši mehānismi, kas jebkuru citu tur esošu failu: pierakstīšanās Microsoft 365 (tostarp daudzfaktoru autentifikācija un nosacījumpiekļuve, ja jūsu organizācija tās izmanto), OneDrive atļaujas un jūsu organizācijas Microsoft 365 politikas.

Tīmekļa daļa izmanto vienu deleģēto atļauju, *Files.ReadWrite.AppFolder*, kas ļauj tai strādāt tikai pierakstījušā lietotāja OneDrive lietotnes mapē. Tā nevar atvērt citus lietotāja failus un nevar atvērt cita lietotāja OneDrive. Plašāku informāciju skatiet rakstā KB10454. Microsoft Graph atļauja Files.ReadWrite.AppFolder: kāpēc tā nepieciešama Password Vault un kā to apstiprināt.

Tā kā glabātuve atrodas lietotāja OneDrive, nevis lapā, katrs lietotājs, kurš atver lapu vai Teams cilni ar tīmekļa daļu, redz tikai savu glabātuvi. Tīmekļa daļas ievietošana koplietotā lapā nekoplieto nevienu paroli.

2. līmenis: ierakstu šifrēšana pārlūkprogrammā

Pirms glabātuves saglabāšanas Password Vault šifrē katra ieraksta teksta laukus ar AES. Šifrēšana un atšifrēšana notiek lietotāja pārlūkprogrammā; fails tiek pārsūtīts tikai starp pārlūkprogrammu un lietotāja OneDrive, izmantojot Microsoft Graph. Tādējādi vērtības nekad netiek glabātas vai pārsūtītas kā vienkāršs teksts: persona, kas atver failu, nosaukumu, lietotājvārdu un paroļu vietā redz šifrētas virknes.

Šifrēšanas atslēga tiek atvasināta no PIN koda pārlūkprogrammā ar PBKDF2-SHA256 (Web Crypto), izmantojot nejaušu 16 baitu sāli un 600 000 iterāciju; jauns sāls tiek izveidots ikreiz, kad PIN kods tiek iestatīts vai mainīts. Atslēga netiek nekur glabāta — ne glabātuves failā, ne pārlūkprogrammas krātuvē, ne pie Vitextra. Tā pastāv tikai atvērtās lapas atmiņā, kamēr glabātuve ir atbloķēta. Lai pārbaudītu PIN kodu, tīmekļa daļa atvasina no tā atslēgu un atšifrē pārbaudes vērtību — zināmu tekstu, kas šifrēts ar atslēgu —, ko fails glabā kopā ar sāli un iterāciju skaitu. Netiek glabāts ne PIN kods, ne

PIN koda jaucējvērtība. Tāpēc ar glabātuves failu vien nepietiek, lai izlasītu ierakstus: ir nepieciešams PIN kods.

Brīdinājums!

PIN kodam ir tikai 4 cipari, tas ir, 10 000 iespējamo kombināciju. PBKDF2 apzināti palēnina katru minēšanas mēģinājumu, taču tas, kurš iegūst jūsu glabātuves faila kopiju, joprojām varētu izmēģināt visus PIN kodus bezsaistē, ārpus tīmekļa daļas: piecu mēģinājumu ierobežojums darbojas tikai tīmekļa daļā. Tāpēc piekļuves kontrole jūsu OneDrive joprojām ir pirmā aizsardzības līnija. Rūpējieties par sava Microsoft 365 konta drošību un nekoplietojiet glabātuves failu vai mapi, kurā tas atrodas.

Kas tiek un kas netiek šifrēts

Dati glabātuves failā	Šifrēti
Ieraksta **Nosaukums**	Jā
Lietotājvārds	Jā
Parole	Jā
URL	Jā
Piezīmes	Jā
Mape	Jā
Atzīmes	Jā
Izlases atzīme (zvaigznīte)	Nē
Ierakstu identifikatori, izveides un modificēšanas datumi	Nē
Sāls, iterāciju skaits un pārbaudes vērtība (izmanto PIN koda pārbaudei)	Sāls un iterāciju skaits: nē; pārbaudes vērtība ir zināms teksts, kas šifrēts ar atslēgu. PIN kods, tā jaucējvērtība un atslēga netiek glabāti
Lietotāja Microsoft Entra ID objekta ID	Nē
Neveiksmīgo PIN koda mēģinājumu	Nē

Dati glabātuves failā	Šifrēti
skaitītājs	

Nekas netiek ierakstīts SharePoint sarakstos, tīmekļa daļas rekvizītos vai pārlūkprogrammas krātuvē. Atslēga un atšifrētās vērtības pastāv tikai atvērtās lapas atmiņā, kamēr glabātuve ir atbloķēta.

Esošās glabātuves tiek jauninātas automātiski

Glabātuves, kas izveidotas ar iepriekšējām Password Vault versijām, izmanto iepriekšējo faila formātu, kurā atslēga tika atvasināta no failā glabātas PIN koda SHA-256 jaucējvērtības un lietotāja Microsoft Entra ID objekta ID. Kad jaunajā versijā pirmo reizi ievadāt pareizo PIN kodu, tīmekļa daļa atkārtoti šifrē visus ierakstus ar jaunu atslēgu, kas atvasināta ar PBKDF2, un saglabā glabātuvi jaunajā formātā. Ieraksti un to modificēšanas datumi tiek saglabāti, un neveiksmīgo mēģinājumu skaitītājs tiek atiestatīts. Jums nekas nav jādara. Pēc jaunināšanas failā vairs nav PIN koda jaucējvērtības.

Piezīme

Jaunināšana maina tikai pašreizējo glabātuves failu. Agrākās faila versijas, ko OneDrive glabā versiju vēsturē vai atkritnē, un kopijas dublējumos paliek iepriekšējā formātā, kurā ierakstus varēja atšifrēt no paša faila, bez PIN koda. To, kas tās var atvērt, nosaka OneDrive piekļuves kontrole un jūsu organizācijas saglabāšanas un dublēšanas iestatījumi.

3. līmenis: PIN kods un bloķētā glabātuve

PIN kods ir 4 ciparu kods, ko lietotājs iestata, kad tiek izveidota glabātuve (skatiet KB10442. Kā iestatīt PIN kodu risinājumā Password Vault). Tas ir nepieciešams vienreiz — lai atvērtu glabātuvi: tīmekļa daļa to pārbauda, tiklīdz ir ievadīts ceturtais cipars. Līdz tam glabātuve ir bloķēta, un tīmekļa daļa nerāda nevienu ierakstu — pat ne to nosaukumus. Saraksta vietā tā rāda uzvedni **Ievadiet PIN kodu** ar tekstu „Ievadiet PIN kodu, lai turpinātu” un četriem ciparu lodziņiem, un rīkjoslā ir pieejama tikai poga **Atsvaidzināt**.

Darbība	Pieejama, kamēr glabātuve ir bloķēta
Saraksta skatīšana ar ierakstu nosaukumu, lietotājvārdu, URL, mapi,	Nē — saraksts ir paslēpts

Darbība	Pieejama, kamēr glabātuve ir bloķēta
atzīmēm un piezīmēm	
Paroles parādīšana (acs poga) vai **Kopēt starpliktuvē** parolei vai lietotājvārdam	Nē
Jauns vienums, **Rediģēt**, **Noņemt**	Nē
Mainīt PIN kodu (zobrats **Konfigurēt**)	Nē
Pievienot izlasei / **Noņemt no izlases**	Nē
Meklēt un filtrs	Nē
Atsvaidzināt	Jā

Pēc pareiza PIN koda glabātuve ir atbloķēta, un visas šīs darbības darbojas tieši, atkārtoti neprasot PIN kodu, līdz glabātuve tiek bloķēta.

Brīdinājums!

Kamēr glabātuve ir atbloķēta, visu tajā esošo — arī paroles — var parādīt un nokopēt ikviens, kurš izmanto jūsu datoru, līdz glabātuve atkal tiek bloķēta. Bloķējiet datoru ikreiz, kad no tā aizejat.

Uzvednē **Ievadiet PIN kodu** cipari ir maskēti, kamēr tos ievadāt. Ekrānos **PIN koda iestatīšana** un **Mainiet PIN kodu** tie ir redzami, tāpēc iestatiet vai mainiet PIN kodu vietā, kur neviens nevar redzēt jūsu ekrānu.

Automātiskā bloķēšana

Pēc lapas ielādes glabātuve ir bloķēta: netiek rādīts neviens ieraksts, tikai uzvedne **Ievadiet PIN kodu**. Pēc pareiza PIN koda glabātuve atveras un paliek atbloķēta, kamēr strādājat. Ja **5 minūtes** tīmekļa daļā nav bijis neviena klikšķa vai taustiņa nospiešanas (tiek ņemtas vērā arī darbības ekrānā **Mainiet PIN kodu**), glabātuve atkal tiek bloķēta: saraksts pazūd, parādītās paroles tiek paslēptas, atslēga tiek noņemta no atmiņas, un katrs atvērtais dialoglodziņš (**Jauns vienums**, **Rediģēt rekvizītus**, noņemšanas apstiprinājums) tiek aizvērts bez saglabāšanas. Lapas atkārtota ielāde arī bloķē glabātuvi, jo atbloķētais stāvoklis pastāv tikai atvērtajā lapā. Skatiet KB10451. Automātiskā bloķēšana: kad Password Vault atkal pieprasa PIN kodu.

Neveiksmīgo mēģinājumu ierobežojums

Pēc katra nepareiza PIN koda tiek parādīts ziņojums „PIN kods ir nepareizs" un atlikušo mēģinājumu skaits (**Atlikušie mēģinājumi**). Skaitītājs tiek glabāts glabātuves failā un vienmēr tiek palielināts, balstoties uz jaunāko faila versiju, tāpēc dažādās ierīcēs un lapās veiktie mēģinājumi droši summējas. Rindiņa **Atlikušie mēģinājumi** tiek rādīta uzvednē **Ievadiet PIN kodu** vienmēr, ja iepriekš ir bijuši nepareizi mēģinājumi, — arī pēc lapas atkārtotas ielādes vai citā ierīcē. Laika gaitā skaitītājs netiek atiestatīts — to atiestata tikai pareizs PIN kods. Pēc **5** nepareiziem PIN kodiem pēc kārtas glabātuve tiek bloķēta: tīmekļa daļa rāda tikai ekrānu **Atiestatīt**, un atiestatīšana izdzēš visus ierakstus un PIN kodu. Skatiet KB10455. Password Vault: nepareizi PIN koda mēģinājumi un kas notiek pēc piecām neveiksmīgām reizēm.

Brīdinājums!

Aizmirstu PIN kodu nevar atkopt vai atiestatīt ne jūs, ne jūsu administrators, ne Vitextra. Pierakstiet savu PIN kodu drošā vietā un svarīgus akreditācijas datus glabājiet arī citā vietā, ko apstiprinājusi jūsu organizācija. Skatiet KB10460. Aizmirsāt Password Vault PIN kodu? Kādas ir iespējas.

Vitextra nav jūsu datu

Vitextra nesaņem, neglabā un nedublē glabātuves datus. Vienīgie tīmekļa daļas pieprasījumi Vitextra pakalpojumiem ir licences pārbaude un lietošanas telemetrija ar tehniskiem identifikatoriem. Pilnu sarakstu skatiet rakstā KB10363. Kur Vitextra produkti glabā jūsu datus: konfidencialitāte, datu atrašanās vieta un VDAR.

Kam Password Vault ir paredzēts

Password Vault ir izstrādāts kā ērta, personiska vieta ikdienas akreditācijas datiem — pierakstīšanās datiem tīmekļa portālos, partneru sistēmās, testa kontiem un līdzīgiem ierakstiem, ko lietotājs citādi glabātu piezīmju grāmatiņā vai teksta failā. Tā aizsardzība apvieno Microsoft 365 piekļuves kontroli ar glabāto vērtību šifrēšanu ar atslēgu, kas atvasināta no 4 ciparu PIN koda.

Tā nav priviliģētās piekļuves pārvaldības sistēma: tajā nav koplietošanas starp lietotājiem, administratora veiktas atkopšanas, sava audita žurnāla un augstas stiprības galvenās paroles. Administratoru kontiem, pakalpojumu kontiem, komandas koplietotiem akreditācijas datiem un citiem augstu privilēģiju noslēpumiem ievērojiet savas organizācijas politiku un izmantojiet tās noteiktos rīkus. Salīdzinājumu ar citām

pieejām skatiet rakstā KB10440. Password Vault, pārlūkprogrammu paroļu pārvaldnieki un uzņēmumu paroļu pārvaldnieki: ko izvēlēties.

Ieteikumi

- Aizsargājiet savu Microsoft 365 kontu: glabātuve ir tikai tik droša, cik drošs ir konts, kuram pieder OneDrive.
- Izvēlieties PIN kodu, ko nav viegli uzminēt (izvairieties no *0000*, *1234* vai sava dzimšanas gada), un glabājiet to drošā vietā.
- Nekoplietojiet un nekopējiet glabātuves failu: tas, kuram ir tā kopija, varētu bezsaistē izmēģināt visus 10 000 PIN kodu.
- Bloķējiet datoru, kad no tā aizejat, pat uz īsu brīdi.
- Nokopēta parole paliek starpliktuvē, līdz nokopējat kaut ko citu; koplietotos datoros pēc lietošanas notīriet starpliktuvi.
- Ja izmantojat glabātuvi vairākās ierīcēs vai cilnēs, izmaiņas tiek apvienotas automātiski; nospiediet **Atsvaidzināt**, lai redzētu citur veiktās izmaiņas (skatiet KB10453. Kur Password Vault glabā jūsu paroles: OneDrive lietotnes mape).
- Glabājiet tikai tos akreditācijas datus, kurus jūsu organizācija atļauj glabāt personiskā paroļu pārvaldniekā.

Padoms

Lai precīzi uzzinātu, kas var un kas nevar redzēt jūsu ierakstus, skatiet KB10456. Password Vault: kas var redzēt jūsu paroles.