

Key2Pass Win - användarmanual

Syfte

Syftet med Key2Pass är att ge användare av Windows och iOS enheter stöd i inloggnings-situationer. Användaren kan skapa och använda mycket starka lösenord utan att dessa lagras någonstans eller behöver minnas. Användaren anger istället ett logiskt, skiftlägeskänsligt **alias** som är enklare att komma ihåg, för att med Key2Pass generera korrekt lösenord, vid inloggningen.

Introduktion

Key2Pass består av en Windows-applikation där du, förutom att få inloggningsstöd, också kan skapa alias och generera en krypterad databas [**kräver Premium**]. Dessutom finns en tillhörande iOS-app som kan importera denna databas för att generera identiska lösenord, associerat till ett alias. Du exporterar databasen från Windows-versionen till en fil [**kräver Premium**] som du själv överför till din iOS-enhet och importerar i appen. Överföringen sker manuellt – Key2Pass samlar inte in några personuppgifter och skickar ingen information till externa servrar.

Säkerhetsprinciper

Key2Pass är ett verktyg för att skapa och återskapa starka lösenord baserat på ett godtyckligt valt **alias**, en tillhörande **4-siffrig PIN-kod** och ditt unika **userId**. Allt arbete görs via programikonen i systemfältet och globala snabbkommandon. Programmet genererar lösenord i realtid lokalt på din dator och sparar inga hemliga nycklar eller lösenord i klartext. Lösenorden skapas reproducerbart från alias, dess PIN-kod och ditt userId – de kan återskapas när du behöver dem men är mycket svåra att gissa för andra. Ingen datakommunikation sker och inga lösenord lagras, vare sig i klartext eller krypterat. För hög säkerhet bör du välja originella aliasnamn och PIN-koder, undvika att dela dem med andra och göra regelbundna säkerhetskopior av aliasdatabasen.

Installation och start

Key2Pass levereras som en MSIX-installatör, via MS Store. Följ instruktionerna för att utan kostnad få tillgång till Key2Pass Basic. Programfilerna installeras och en genväg läggs till i Start-menyn.

Första gången efter ny installation kan du behöva starta programmet manuellt via Start-menyn. Du måste också ange en passfras för databasen. Denna passfras är din unika nyckel till databasen (valvet), utan den kommer valvet inte kunna öppnas. Passfrasen sparas automatiskt i din Windows nyckel kedja och används för att öppna valvet automatiskt varje gång du loggar in i Windows. Du måste dock själv kunna ange korrekt passfras om du manuellt behöver öppna valvet (efter att manuellt ha stängt det) eller om du vill byta passfras eller rotera valvets krypteringsnycklar. **DET FINNS INGET SÄTT ATT ÅTERVINNA VALVETS PASSFRAS OM DU SKULLE TAPPA BORT DEN, FÖRVARA DEN DÄRFÖR PÅ ETT SÄKERT SÄTT.**

Fortsatt startar programmet automatiskt varje gång du loggar in i Windows. Du kan också välja att förhindra den automatiska starten (under Windows Inställningar) och istället starta Key2Pass via Start-menyn.

Programmet körs helt i bakgrunden och visar endast en nyckelikon i systemfältet. Det finns inget fönster som öppnas automatiskt; all interaktion sker via ikonens snabbmeny och via snabbtangenter.

Key2Pass (huvudfönster)

Högerklicka på Key2Pass-ikonen och välj **Öppna Key2Pass** för att öppna huvudfönstret. Här ser du information om din databas och licensnivå. Du kan också öppna en dialog för att skapa/redigera dina olika login-ID (max 5 st olika), se nedan.

I huvudfönstret kan du också stänga och öppna (kräver korrekt passfras) valvet (databasen) samt exportera och importera databasen för backup och/eller import till Key2Pass iOS.

Slutligen kan du från huvudfönstret också skapa och redigera alias samt generera lösenord, se nedan.

Inställningar

Inställningarna nås via tray-ikonen:

- Högerklicka på Key2Pass-ikonen och välj **Inställningar** för att öppna inställningsdialogen.

- I dialogen kan du ställa in hur länge ett kopierat lösenord ska ligga kvar i urklipp (kopieringstid), välja krypteringsalgoritm och språk samt visuellt tema.
- I inställningsdialogen kan du också se och uppgradera programlicens, från Basic till Premium.
- Du kan byta lösenfras för valvet (databasen), efter att först ange den nuvarande lösenfrasen
- Du kan, av säkerhetsskäl, också byta krypteringsnycklar för valvet, utan att de genererade lösenorden kommer att påverkas.

Skapa nya alias

Ett alias fungerar som en etikett som tillsammans med en 4-siffrig PIN-kod och ditt unika userId genererar ett starkt lösenord, enligt den av dig valda policyn (dvs. regler för lösenordets längd och vilka tecken som får användas). Med licens **Basic** kan du maximalt ha 10 st alias, med licens **Premium** finns ingen begränsning. Du kan skapa nytt alias från aliasfönstret eller från huvudfönstret:

1. Placera markören i ett inmatningsfält
2. Tryck på det globala snabbkommandot **Ctrl+Shift+P** för att öppna aliasfönstret.
3. Skriv in aliasnamnet (case sensitive). När du har skrivit namnet använder du högerklicksmenyn för att fortsätta.
4. Högerklicka i fönstret och välj **Nytt alias**. Ett dialogfönster öppnas där du får ange aliasets policy (t.ex. lösenordslängd, teckenklasser) och en 4-siffrig PIN-kod. Du kan också ange ett domännamn (valfritt). PIN-koden och ev domännamn används tillsammans med aliaset för att, på kommando, generera ett unikt lösenord enligt bestämd policy.
5. När du sparar aliaset genererar programmet automatiskt lösenordet enligt policyn och kopierar det till urklippet. Lösenordet är bara synligt via urklippet under den tid du har ställt in; därefter rensas urklippet.

Du kan också skapa ett nytt alias från huvudfönstret. Klicka på knappen **Nytt alias** för att öppna dialogfönstret för att skapa alias enligt 4. ovan.

Redigera befintliga alias

Ett befintligt alias kan redigeras eller raderas i redigeringsfönstret som kan öppnas från aliasfönstret eller huvudfönstret.

1. Placera markören i ett inmatningsfält
2. Öppna aliasfönstret med **Ctrl+Shift+P** och skriv namnet på det befintliga aliaset (case sensitive).
3. Högerklicka i aliasfönstret och välj **Redigera alias**. Ett dialogfönster visas där du kan ändra aliasets policy (t.ex. lösenordslängd, teckenklasser) och/eller byta eller behålla 4-siffrig PIN-kod.
4. När du sparar ändringarna uppdateras aliaset. Varje alias använder sin egen PIN-kod. Om du inte anger ny PIN-kod återanvänds den tidigare PIN-koden för aliaset. Det finns inget sätt att i efterhand se vilken PIN-kod som valts för ett visst alias men koden behöver inte kommas ihåg och matas aldrig in vid användning.

Du kan också redigera ett alias från huvudfönstret. Välj ett alias från listan, klicka på knappen **Redigera alias** för att öppna dialogfönstret för att redigera alias enligt 3. ovan.

Användning av lagrade användarnamn (login-ID)

Du kan lagra upp till fem **login-ID** i dialogen som du når från huvudfönstret (Användare1–Användare5). Dessa kopieras enkelt till urklippet med snabbtangenter. Syftet är att underlätta dina inloggningar genom snabbare inmatning. Användare får själv hålla reda på vilka Användarnamn som skall användas för olika inloggningar och bakom vilka snabb-kommandon dessa ligger:

- **Ctrl+Shift+1** till **Ctrl+Shift+5** (1–5 från den övre siffraden) kopierar Användarnamnen.
- **Ctrl+Alt+NumPad1** till **Ctrl+Alt+NumPad5** gör samma sak via det numeriska tangentbordet.
- Efter snabbkommandot använder du **Ctrl+V** för att klistra in Användarnamnet i tillhörande fält i inloggningsdialogen.

Generering av lösenord

Du kan generera lösenord på följande två sätt, båda via aliasfönstret. I båda fallen är utgångsläget att du placerar markören i det inmatningsfält där lösenordet skall skrivas. Aliasfönstret öppnas alltid tomt — skriv aliaset du vill använda. Om aliaset inte finns visas ett felmeddelande. Tänk då på att aliaset är skiftlägeskänsligt.

- 1a) Tryck **Ctrl+Shift+P**, skriv aliaset i fönstret och tryck **Enter** eller

- 1b) Tryck **Ctrl+Shift+P**, skriv aliaset i fönstret, **Högerklicka** i fönstret och välj **Generera lösenord**

Du kan också generera lösenord från huvudfönstret genom att välja aktuellt alias från listan och därefter klicka på knappen **Generera lösenord**

Efter att lösenordet genererats återvänder du nu till inloggningsdialogens lösenordsfält och trycker **Ctrl+V** varpå lösenordet kopieras till inmatningsfältet.

Programmet använder aliasets policy och PIN-kod för att skapa lösenordet och kopierar det till urklippet. Urklippet rensas automatiskt efter den tid du har ställt in.

Om Key2Pass

Högerklicka på Key2Pass-ikonen och välj **Om Key2Pass** för att öppna informationsfönstret. Här ser du information om appen, såsom version och aktuell licensnivå. Du kan härifrån också initiera köp av uppgradering av licensen. Här finns även en länk till Key2Pass supportsida där du hittar mer information och kan rapportera felaktigheter.

Avsluta

För att tillfälligt avsluta Key2Pass, högerklicka på Key2Pass-ikonen i systemmenyn och välj **Avsluta**. Appen kan återstartas manuellt under samma Windowssession genom att starta det från Startmenyn. Passfrasen till valvet hämtas då från Windows nyckel kedja.

Backup och återställning

För att skydda dina alias bör du regelbundet exportera aliaslistan till en backupfil och kunna importera den senare om det behövs. Backupen innehåller all information som behövs för att du skall kunna använda dina alias till att generera korrekta lösenord, efter att filen har importerats till någon av Key2Pass plattformar. Backupfilen krypteras via ett lösenord som du anger vid exporten. **VAR MYCKET NOGA MED ATT DU KOMMER IHÅG DETTA LÖSENORD. DET FINNS INGET SÄTT ATT KOMMA ÅT INNEHÅLLET I FILEN UTAN TILLGÅNG TILL DETTA LÖSENORD OCH DET FINNS INGET SÄTT ATT ÅTERVINNA LÖSENORDET OM DU FÖRLORAT DET.**

- **Exportera portabel fil [Premium och Basic]:** För backup och eller överföring till annan Windows installation. Öppna huvudfönstret och välj knappen **Exportera portabel fil** Du väljer plats och filnamn (förslaget är *backup.portable.json*) och anger ett fillösenord två gånger. Filen blir krypterad och kan öppnas på andra Key2Pass plattformar med fillösenordet. Förvara fillösenordet säkert – det kan inte återställas och filen kan inte öppnas utan detta lösenord.
- **Synk-export [Premium]:** För export till annan plattform, inklusive iOS med kryptering AES-CBC + HMAC. Öppna huvudfönstret och välj knappen **Synk-export**. Du väljer filplats och namn (förslaget är *sync.k2s*) och anger ett fillösenord två gånger. Du väljer dessutom krypteringsmetod (AES-CBC + HMAC för iOS). Filen blir krypterad och kan öppnas på andra Key2Pass plattformar med fillösenordet. Förvara fillösenordet säkert – det kan inte återställas och filen kan inte öppnas utan detta lösenord.
- **Importera portabel fil [Premium och Basic]:** För att återställa hela databasen från en backup, eller läsa in databasen till en ny enhet, väljer du **Importera portabel fil** i huvudfönstret och väljer JSON-filen du vill läsa in. Importen skall göras till en nyinstallerat version av Key2Pass med en tom databas. Import till en befintlig databas kommer att misslyckas om alias från backupen redan finns i databasen. Om backupen enbart innehåller nya alias som inte redan finns i databasen kommer importen att genomföras. Dock kommer sannolikt de nya aliasen att generera andra lösenord än vad de gjorde tidigare.
- **Synk-import [Premium och Basic]:** För att uppdatera databasen från en backup eller läsa in databasen till en ny enhet klickar du **Synk-import** i huvudfönstret och väljer synk-filen du vill läsa in. Vid befintliga alias kommer senaste version att behållas i databasen efter importen. Vill du läsa in en äldre aliasversion från backup måste du därför först radera det senare alias från databasen.

Installation av ny Key2Pass version

En ny större programversion kan installeras utan att den tidigare versionen tas bort, detta görs då, efter ditt godkännande, automatiskt av installeraren. Med större programversion avses en ändring av någon av de tre första versionssiffrorna (t ex från version 1.0.1 till version 1.0.2).

Observera att vid installation av ny större version utan att den tidigare versionen först avinstalleras så återanvänds befintlig databas! Som extra säkerhet rekommenderas du ändå ALLTID att TA EN AKTUELL BACKUP via export-kommandot INNAN INSTALLATIONEN PÅBÖRJAS!

Om du väljer att först avinstallera Key2Pass via Start-menyns Inställningar så kommer även databasen att raderas. För att då kunna återinstallera Key2Pass och återställa dina alias-data krävs att du har tillgång till en backupfil och dess fillösenord.

Tagna backuper skall förvaras på säker plats och lösenorden till backupfilerna skall bevaras på säkert sätt.

Efter ny installation kan Key2Pass behöva startas manuellt via Start-menyn innan programikonen dyker upp i systemfältet och snabbkommandot Ctrl+Shift+P åter fungerar.

Fullständig avinstallation av Key2Pass

Om du inte längre vill använda Key2Pass eller av andra skäl helt vill avinstallera Key2Pass så gör du detta via Start-menyn. Öppna Inställningar - Appar - Key2Pass och välj Avinstallera. Alla delar av Key2Pass, utom de backup-filer som du själv skapat och sparat på säker plats, kommer då att raderas från datorn.

Tips för säkerhet och användning

- Genom att kunna associera ett visst, skiftlägeskänsligt alias med en viss tjänsteinloggning så slipper du komma ihåg säkra, krångliga lösenord, de genereras istället åt dig vid behov
- Välj alltid **unika aliasnamn** och **starka 4-siffriga PIN-koder**. Dela inte dina alias eller PIN-koder med andra.
- För att byta genererat lösenordet, om detta krävs av säkerhetsskäl, så räcker det att ändra PIN-koden. Ett helt nytt lösenord genereras då, associerat med samma alias som tidigare och med bibehållen policy.
- Byt aliaspolicys (t.ex. längd eller teckenklasser) enkelt om säkerhetskraven ändras, samma alias kan behållas.
- Var försiktig med globala snabbtangenter om du delar dator; lösenord kopieras till urklippet och rensas efter en tidsgräns, men lämna inte datorn oövakad under denna period.
- Förvara dina backupfiler på en säker plats och kom ihåg fillösenorden
- Kontrollera regelbundet att du har den senaste versionen av programmet för att få säkerhetsuppdateringar och nya funktioner.

Detta avslutar manualen för Key2Pass Windowsversion. Alla funktioner kan nås via systemfältet och snabbkommandon, vilket gör verktyget diskret och effektivt.