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 PwdGen 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. 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 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 Windows **inloggnings-ID**. 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 inloggnings-ID – 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 MSI-installatör. Kör installationsfilen och följ guiden; du behöver godkänna licensavtalet för att få tillgång till Key2Pass. Programfilerna installeras under `Program Files\Key2Pass` och en genväg läggs till i Start-menyn.

Efter installationen 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. Första gången efter ny installation behöver du starta programmet manuellt via Start-menyn. Programmet körs helt i bakgrunden och visar endast en nyckelikon i systemfältet. Det finns inget fönster som öppnas; all interaktion sker via ikonens snabbmeny och via snabbtangenter.

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), och definiera upp till fem **Användarnamn (ID)** som kan kopieras med snabbtangenter. Du kan också härifrån **Exportera** eller **Importera** databasen med Alias och Användarnamn, se detaljerad beskrivning nedan.
- I inställningsdialogen kan du också ändra Export-algoritm. Denna inställning är för framtida bruk. Om du ändrar den idag kommer du inte längre kunna importera krypterade filer till iOS-plattformen
- När du har gjort dina justeringar klickar du på **Spara**. Vissa ändringar kan kräva att programmet startas om; i så fall visas ett meddelande.

Skapa nya alias

Ett alias fungerar som en etikett som tillsammans med en 4-siffrig PIN-kod och ditt unika inloggnings-ID genererar ett starkt lösenord, enligt den av dig valda policyn (dvs. regler för lösenordets längd och vilka tecken som får användas). Så här skapar du ett nytt alias:

1. Placera markören i ett inmatningsfält

2. Tryck på det globala snabbkommandot **Ctrl+Alt+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 och används endast om du vill att lösenordet ska skilja sig åt mellan olika tjänster trots samma alias). 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.

Redigera befintliga alias

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

1. Placera markören i ett inmatningsfält
2. Öppna aliasfönstret med **Ctrl+Alt+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.

Användning av lagrade användarnamn

Du kan lagra upp till fem **Användarnamn** i inställningarna (Användare1–Användare5). Dessa kopieras enkelt till urklippet med snabbtangenter. Syftet är att underlätta inloggningen 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 sifferraden) 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.

Om Användarnamn-fältet som du försöker hämta från är tomt visas en notifikation om att värdet saknas.

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+Alt+P**, skriv aliaset i fönstret och tryck **Enter** eller
- 1b) Tryck **Ctrl+Alt+P**, skriv aliaset i fönstret, **Högerklicka** i fönstret och välj **Generera lösenord**

Du återvänder nu till inloggningsdialogen 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. Under tiden kan en notifikation visas för att informera dig; du kan avbryta rensningen via notifikationen om du behöver behålla lösenordet längre.

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 alla 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 GLÖMT DET.

- **Exportera:** Öppna inställningsdialogen och välj knappen **Exportera portabel fil...** Du väljer filplats (förslaget är *pwdgen-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.

- **Importera:** För att återställa från en backup, eller läsa in databasen till en ny plattform, väljer du **Importera portabel fil...** i inställningsdialogen och anger JSON-filen du vill läsa in. Befintliga alias kommer att ersättas av de i backupfilen så se till att du verkligen vill skriva över dina nuvarande alias innan du importerar. Du kommer också att få en varning som behöver bekräftas för att importen skall genomföras.

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 måste Key2Pass startas manuellt via Start-menyn innan programikonen dyker upp i systemfältet och snabbkommandot Ctrl+Alt+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-meny. 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 ändra 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 obevakad 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 nås via systemfältet och snabbkommandon, vilket gör verktyget diskret och effektivt.