

Nuoro, 13 Dicembre 2022

COME GESTIRE AL MEGLIO LE NOSTRE PASSWORD

(Manuale Operativo)

Sempre con più frequenza, in un periodo dove ogni applicativo necessita di proprie Password e/o credenziali, e dove ogni accesso a Internet richiede accessi controllati con Login proprie e Password personalizzate, si pone il problema di conservarle e gestirle al meglio.

Abbiamo un centinaio di password da ricordare tutte a memoria?

L'errore più comune in questi scenari è utilizzare una password generica (tipo 12345) per effettuare l'accesso su più siti, così da non sforzare troppo la memoria. Come risultato otterremo che, se uno dei servizi su cui abbiamo utilizzato una password generica viene violato, questa può essere recuperata da gente malintenzionata, pronta ad entrare in tutti i servizi dove essa è stata utilizzata.

Per evitare questo tipo di problemi possiamo utilizzare **KeePass**, un programma multi-piattaforma per salvare le nostre password in un comodo database, accessibile tramite una "Master password".

Invece di ricordare 100 password, basterà ricordarne una (ma buona!)

KeePass ci permette di gestire, conservare, richiamare e tenere aggiornate tutte le Password di cui abbiamo bisogno nel nostro lavoro.

Il presente manuale, elaborato con la versione 2.52 di **KeePass**, vuole essere uno strumento operativo in grado di supportarci durante l'installazione e la gestione.

Come accennato nell'introduzione, **KeePass** è un gestore password multi-piattaforma: il programma è disponibile per Windows, Mac e GNU/Linux.

KeePass ci permette velocemente di operare in piena sicurezza, lontano da sguardi indiscreti e soprattutto non permetterà ad altri di vederne il contenuto in chiaro.

KeePass è indubbiamente il più popolare gestore di password del momento, anche grazie a una miriade di opzioni che garantiscono una sicurezza affidabile e fuori dal comune.

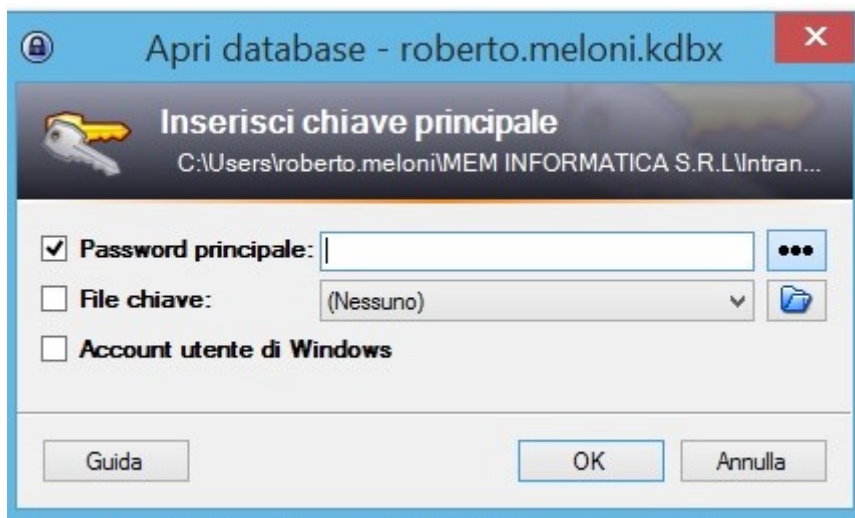
Rilasciato sotto la licenza GPL v2, **KeePass** è gratuito e tale resterà in futuro. Il suo codice sorgente è disponibile per programmatori e sviluppatori del mondo intero che assicurano a **KeePass** tutti gli aggiornamenti e le principali evoluzioni delle sue versioni.

Per questo programma è prevista anche una versione "**portable**" da installare su chiavetta USB e da portare sempre dietro con tutte le password memorizzate.

Un gestore di password semplice e gratuito

Il suo principio base è molto semplice: **KeePass** salva tutte le tue password in un database a lui associato che in realtà è un file cifrato (“crittografato”).

Questo database è accessibile solo grazie alla tua password principale, **l'unica che devi ricordare**



La sicurezza di accesso a questo database può essere ulteriormente migliorata, associando “un file chiave” di tipo .key.

In questo manuale non verrà trattato l'argomento legato alla gestione del **file chiave**.

Un gestore di password per MacOS, Linux, FreeBSD e Windows

Chi produce un Software Operativo, con un monopolio destinato al grande pubblico, in realtà produce un software aperto agli attacchi degli hacker che sfruttano le carenze del suddetto S.O. per accedere alle informazioni sensibili.

Senza puntare il dito contro nessun S.O., **KeePass** è stato pensato per la protezione delle password di tutti i tuoi computer, qualunque sia la piattaforma che utilizzi con qualsiasi S.O. installato. Ad esempio, in una giornata puoi lavorare su una postazione Windows in ufficio per continuare ad utilizzare **KeePass** sul tuo computer personale MacOS o Linux a casa.

Su Windows, l'installazione di **KeePass** è nativa.

Su MacOS, Linux e FreeBSD, l'installazione nativa può operare grazie alla piattaforma Mono (una piattaforma di sviluppo Microsoft.NET basata sulla CLI che proponiamo in download).

Per gli utenti Windows esiste una seconda versione di **KeePass** che permette sia di collegare il database a un utente Windows sia di autorizzare l'inclusione di allegati negli ingressi (per le versioni 2.x).

Un gestore di password certificato ANSSI

Nel quadro delle sue missioni per la difesa e la sicurezza nazionale l'ANSSI (l'Agenzia Nazionale della Sicurezza dei Sistemi d'Informazione) prova i software utilizzati nelle amministrazioni pubbliche francesi.

Dal 2012, la Fondazione Interministeriale che si occupa di Software Liberi definisce un elenco di software a codice sorgente aperto che devono essere utilizzati nelle amministrazioni francesi, software liberi che l'ANSSI testa rispetto alla sicurezza. È dal 2010 che l'ANSSI certifica **KeePass** nella versione 2.10. La sua distribuzione avviene a livello nazionale in tutte le amministrazioni francesi dal 2012.

Un gestore di password raccomandato per la sua sicurezza

Oltre all'ANSSI, anche l'Ufficio Federale della Sicurezza Tecnologica in Germania nel 2018 emanò una nota per i PME al fine di raccomandare loro l'utilizzo di **KeePass**.

La Commissione europea ordinò un audit di sicurezza in occasione del primo EU-FOSSA (Audit europeo Software Codice Sorgente Libero e Gratuito) del 2016, poi lo ripeté nel 2019 nella cornice del terzo "bug bounty" di **KeePass** che ricompensa i generosi tester di sicurezza che riportano i bug e le carenze di sicurezza agli sviluppatori.

In breve, con **KeePass** raggiungi i vertici in materia di sicurezza, e non siamo noi che lo diciamo!

Gestisci le tue password anche su mobile

Il database che contiene le tue password crittografate (o cifrate, se si vuole utilizzare il termine corretto) può essere sincronizzato a distanza. Con l'applicazione **KeePass** installata sul tuo smartphone puoi sincronizzarti da un sito distante via FTP col tuo BlackBerry, Pocket PC, iPhone, Windows Phone 7, e naturalmente anche con Android.

Esistono delle soluzioni di sincronizzazione più semplici grazie al cloud su altri software di gestione di password, tuttavia il grado di sicurezza della trasmissione dati è più problematico e un buon numero di utenti diffidano di soluzioni cloud come Dashlane o Lastpass.

KeePass è quindi un'eccellente alternativa ai gestori di password per cloud.

Una funzionalità drag and drop facilmente utilizzabile

Per quanto riguarda i dati in entrata del tuo file (il tuo database) avrai la possibilità di trascinarli semplicemente e di rilasciare le informazioni necessarie, per introdurre in seguito il nome utente e la password associata. Tutte le voci del database possono essere inserite con la funzionalità drag and drop.

Ancora più semplice con l'inserimento automatico di password

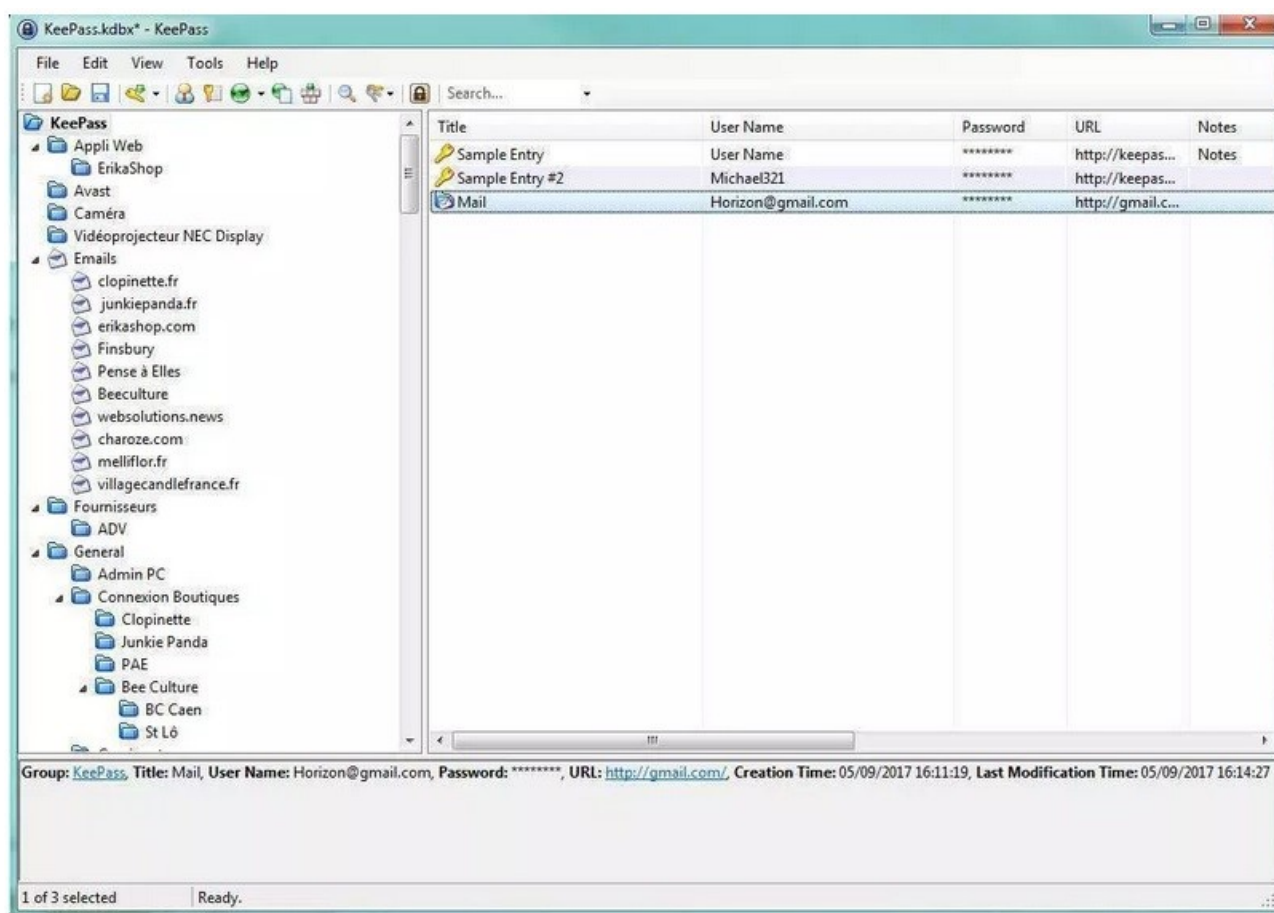
Se desideri guadagnare ancora più tempo, in **KeePass** puoi controllare il codice identificativo e le password da utilizzare per un'applicazione o per un sito, grazie al loro URL, affinché siano inserite automaticamente a ogni lancio dell'applicazione o del sito internet. Ti basterà aprire il contestuale menu nel database delle tue password, cliccando col tasto destro su una voce per selezionare "eseguire inserimento automatico."

Risulta incredibilmente efficace e molto semplice per completare le informazioni di connessione a un sito o a un software che richiedono l'autenticazione. Come sempre, l'inserimento automatico è cifrato e di conseguenza è protetto nell'ambito stesso di **KeePass**, perciò l'utilizzazione di questa opzione non crea alcuna preoccupazione in materia di sicurezza.

Cambi spesso password?

Bisognerebbe avere una memoria fenomenale per ricordare la quantità di password importanti che supportano la nostra vita di utenti. Evidentemente è assolutamente sconsigliato utilizzare sempre la stessa password e lo stesso nome utente, ma per fortuna c'è **KeePass** che gestisce tutto per conto nostro.

Per ciò che riguarda i siti o i software dove è necessario cambiare regolarmente le password, **Keepass** è in grado di tenere traccia delle vecchie password, grazie a uno storico dei dati d'ingresso del database.



Parli l'estone, il croato oppure il gallego?

KeePass è originariamente disponibile in inglese, ma puoi aggiungere numerose traduzioni ufficiali (grazie all'abile lavoro di generosi volontari) in più di 50 lingue e dialetti. Questi file, di traduzione, sono disponibili nel formato.lng e.lngx, a seconda della tua versione di **KeePass**.

Installazione di KeePass e traduzione

Non c'è alcuna difficoltà nell'installazione su Windows, poiché l'Installer è molto semplice e comune. Tuttavia, **KeePass** viene installato per impostazione predefinita in lingua inglese e sarà necessario scaricare il pacchetto di traduzione in italiano.

Possiamo scaricare gratuitamente KeePass per PC direttamente dal sito ufficiale di **KeePass** (<https://keepass.info/download.html>): si consiglia di puntare subito sulla Professional Edition, disponibile anch'essa gratuitamente. Dal sito ufficiale di **KeePass** sarà anche possibile scaricare e/o installare la versione Portable, utile per chi vuole portarsi sempre dietro il software su chiavetta USB o su hard disk esterno.

In alternativa, la versione installante di **KeePass** potrà essere scaricata dal sito:

www.meminformatica.it accedendo alla scelta SUPPORTO / AREA DOWNLOAD



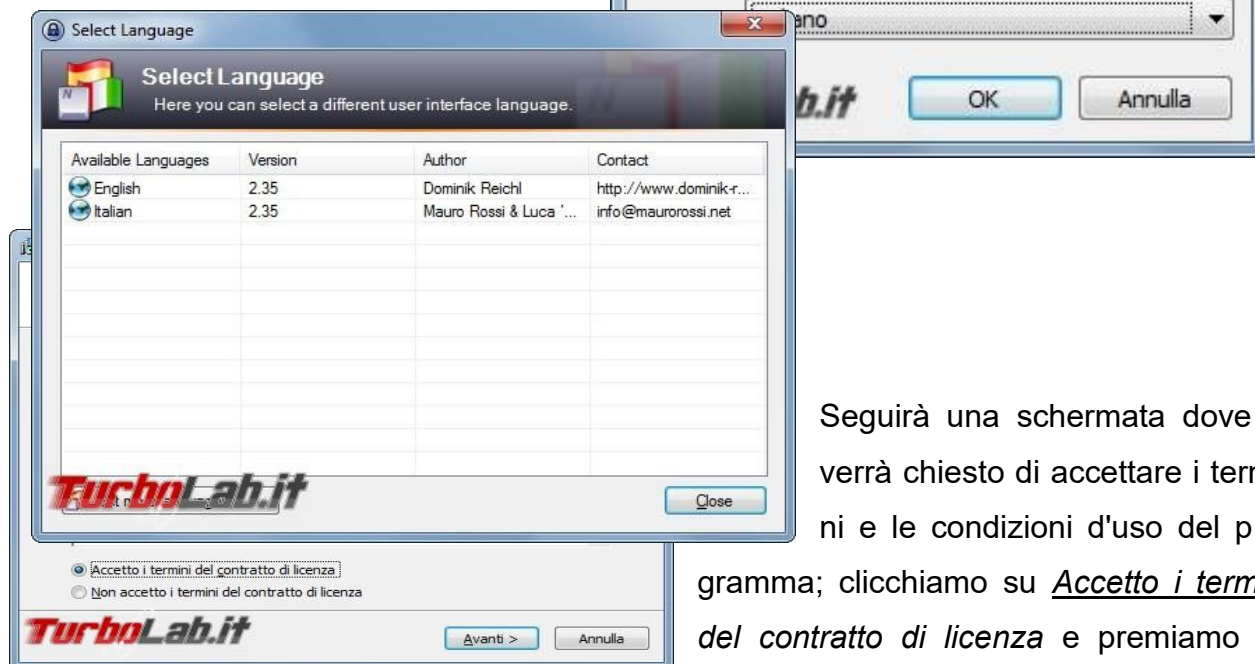
.. e successivamente, nella sezione Programmi di utilità accedere ad Altro.

Nella cartella contenente il file di installazione, viene scaricato anche il file della traduzione in "italiano".

Questo file, in formato .Ignx, una volta installata la procedura, dovrà essere copiato nella cartella di installazione che potrebbe essere: "Program Files\ KeePass Password Safe 2\ Languages". A questo punto sarà possibile selezionare la lingua installata dal menu "Visualizza ➔ Cambia lingua".

N.B.: Su Windows l'unico prerequisito è la presenza nel sistema del Microsoft.NET Framework 2.0 o superiore (se abbiamo Windows 7 o superiore non dovremo fare altro), mentre su Mac e GNU/Linux sarà necessario procurarci le librerie Mono.

Una volta scaricato e avviato l'installer, ci verrà chiesta la lingua per la procedura d'installazione. Scegliamo ovviamente l'italiano come lingua.



Seguirà una schermata dove ci verrà chiesto di accettare i termini e le condizioni d'uso del programma; clicchiamo su Accetto i termini del contratto di licenza e premiamo su

Avanti.

Nella successiva schermata confermiamo su **Avanti** per mantenere il percorso d'installazione predefinito.

Ci ritroveremo ora davanti alla schermata dove scegliere quali componenti installare sul sistema insieme al programma principale.

Se cerchiamo un'installazione pulita, scegliamo **Installazione compatta** per installare il minimo indispensabile; se abbiamo un

database del vecchio **Keepass 2.x** o necessitiamo di tutte le componenti del programma scegliamo invece Installazione completa o Personalizzata. Premiamo su Avanti quando pronti.



Purtroppo il programma, pur essendo stato installato nella versione in italiano si presenterà in lingua inglese e, per un programma del genere, non è consigliabile andare a "tentativi", meglio tradurre subito il programma nella lingua di Dante!

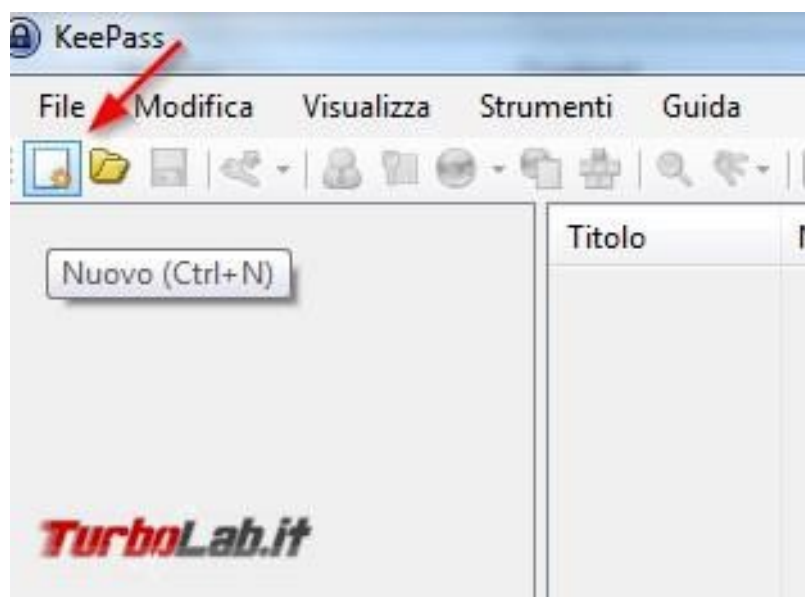
Il file della lingua italiana è presente sul sito della MEM Informatica srl (all'interno dell'applicazione, troverete la cartella con la lingua italiana) insieme al file del programma oppure potrà essere scaricato dal sito ufficiale di **KeePass** al seguente indirizzo: <https://keepass.info/translations.html>

Una volta scaricato il file (=Italian.Ingx) copiarlo nella cartella di origine del programma, scelta all'inizio dell'installazione, all'interno della cartella Languages.

Ora per ottenere la lingua italiana su KeePass basterà aprire il programma, portarsi nel menu View->Language e selezionare la lingua **Italian**.

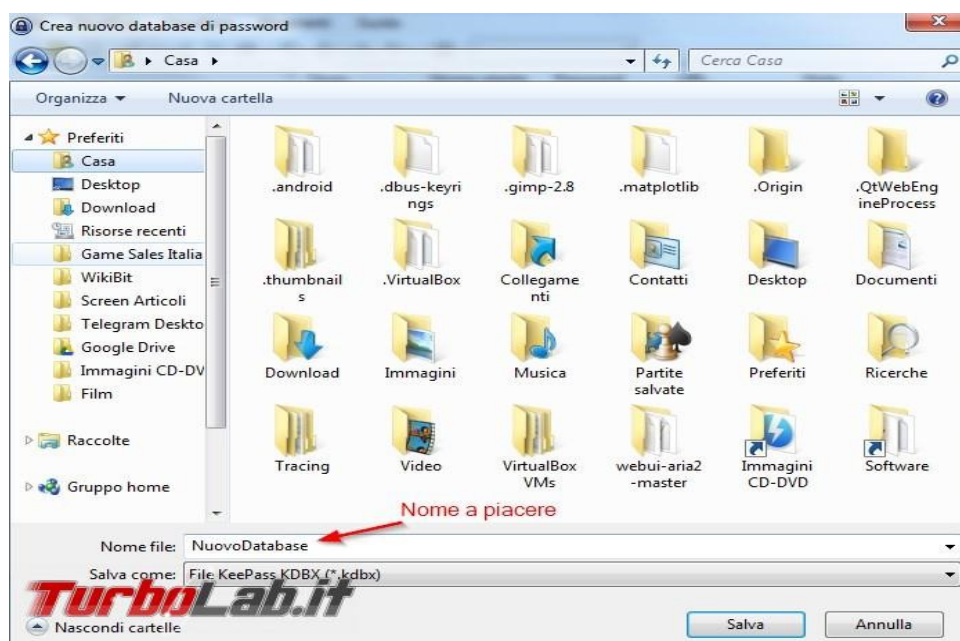
Una schermata ci chiederà il riavvio del programma per rendere effettive le modifiche; eseguiamo senza troppi pensieri.

KEEPASS: COME CREARE UN DATABASE



Per salvare le password dovremo prima di tutto creare un nuovo database, il "contenitore" che le custodirà. Apriamo **KeePass** e premiamo sulla tastiera CTRL+N o portiamoci sulla voce **Nuovo**.

Ci verrà chiesto subito dove salvare il database; possiamo scegliere un percorso e un nome a piacere per il file.



Confermiamo premendo il tasto Salva.

Nella successiva schermata dovremo scegliere la Master Password, la password che proteggerà il database.

Scegliamone una abbastanza robusta da non essere indovinata da nessuno. Evitiamo le date di nascita, ricorrenze e compleanni e concentriamoci su qualcosa che possiamo indovinare (o ricordare!) solo noi. Consiglio una password da almeno 20 caratteri con lettere, numeri e maiuscole.

Per i più pignoli possiamo aggiungere anche i caratteri speciali per rendere la password davvero difficile.

In alternativa, e tale alterna-

tiva è consigliata solamente ai più esperti, possiamo utilizzare anche il file chiave come metodo d'accesso al database.

In cosa consiste il file chiave? Con quest'ultimo possiamo accedere al database indicando un qualsiasi file presente nel sistema, con qualsiasi estensione. Può essere utilizzato da solo o insieme ad una password.

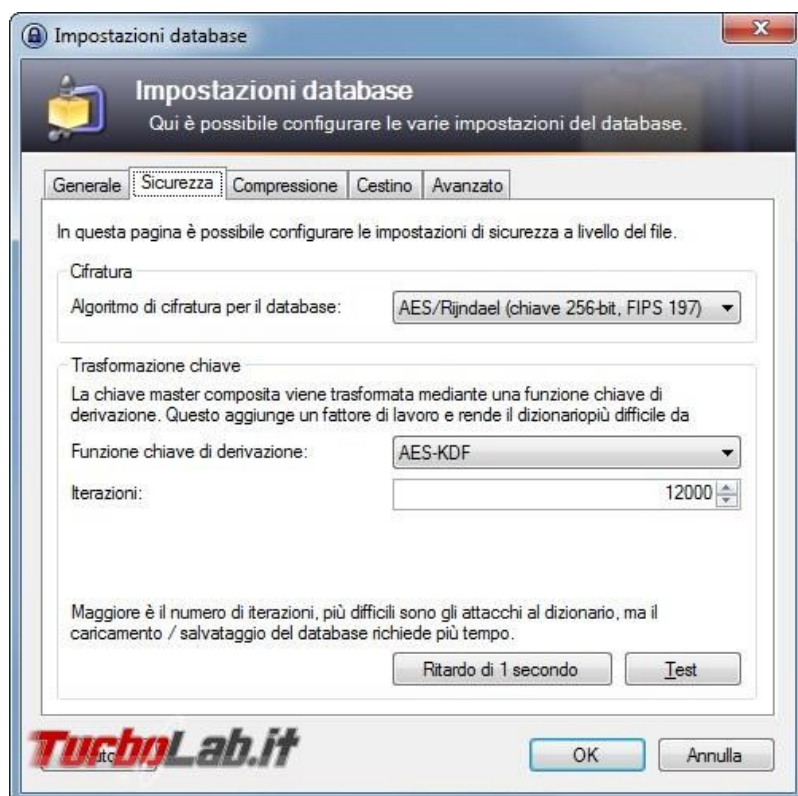


ATTENZIONE

L'integrità del file chiave è fondamentale per l'accesso al database: se perdiamo, modifichiamo o danneggiamo il file chiave non potremo mai più riaccedere al database!

Nella finestra successiva che si aprirà possiamo scegliere il nome da dare al database e fornire una descrizione, scegliere il livello di sicurezza per la crittografia dei contenuti, sce-

gliere il livello di compressione, impostare un cestino per le voci cancellate e accedere ad alcune voci avanzate.



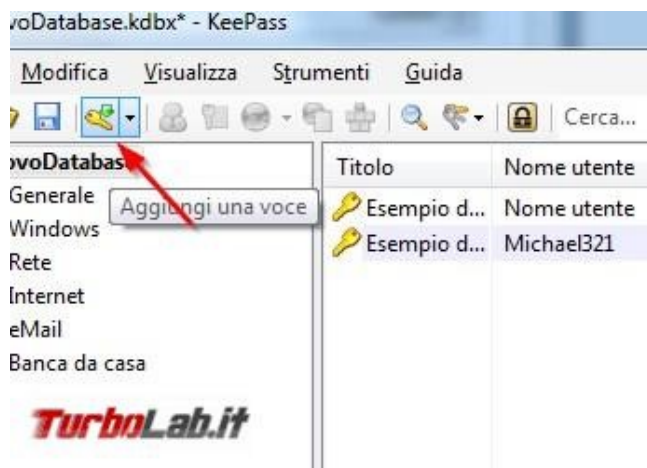
Possiamo tranquillamente ignorare gran parte delle schermate, limitandoci a scegliere un nome per il database e assicurandoci che nel tab Sicurezza sia selezionato:

- AES/Rijndael (chiave 256bit, FIPS 197)
- AES-KDF
- Iterazioni: almeno 12.000

KEEPASS: AGGIUNGERE VOCI AL DATABASE

Dopo aver visto come creare il database, vediamo come aggiungere una voce allo stesso. Nella voce salveremo il nome utente e la password per il sito o il servizio da memorizzare.

Apriamo **KeePass** e inseriamo la password per l'accesso all'ultimo database caricato (selezioniamo anche il file chiave se abbiamo utilizzato questo metodo).



Premiamo sulla barra dei tasti Aggiungi una voce, come indicato nella immagine qui di lato.

Si aprirà una nuova finestra simile a quella visibile qui di lato ...

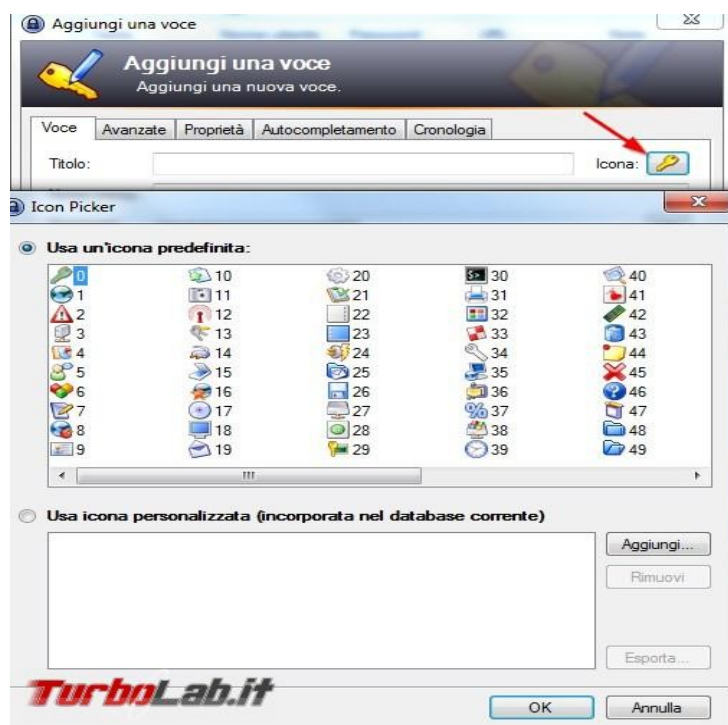
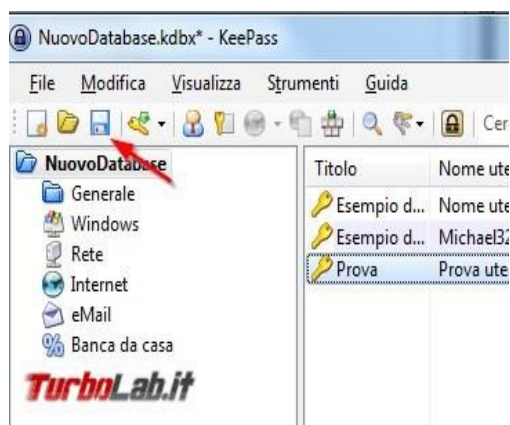
Le voci da compilare sono molte e molte sono le opzioni offerte nelle altre schede, ma per iniziare subito ad utilizzare il programma basterà compilare i seguenti campi:

- Titolo: inseriamo il nome del sito, del servizio o dell'accesso da salvare



- Nome utente: inseriamo qui il nome utente
- Password/Ripeti Password: inseriamo due volte la password da salvare (oscurate)

Appena compilati questi campi premiamo su OK per aggiungere la voce. Per salvare il database con le aggiunte dovremo premere il tasto a forma di floppy nella barra delle icone o utilizzare da tastiera CTRL+S.



Volendo, possiamo personalizzare e riordinare le nostre voci in due modi: aggiungendo un'icona identificativa ad ogni nuova voce...

... oppure creando dei **Gruppi** dove raccogliere le password a tema (per esempio PC, Posta, Banca, Siti, Rete etc.)



KEE PASS: GENERARE UNA PASSWORD SICURA

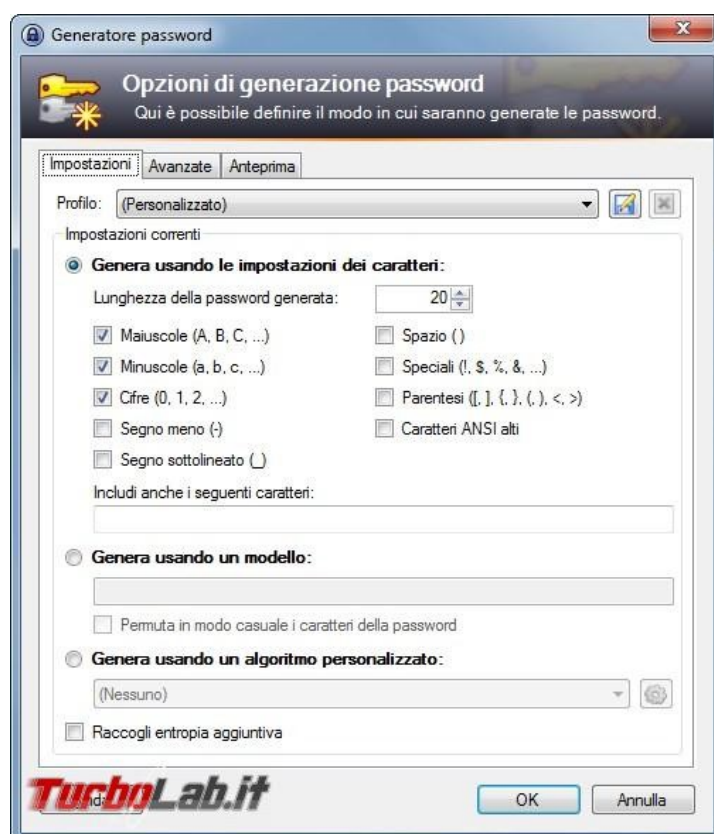
Abbiamo sicuramente solo trattato alcune delle tante funzionalità di **KeePass**, ma sicuramente una delle caratteristiche da sfruttare senza indugi è il generatore di password.

Portiamoci nel menu:

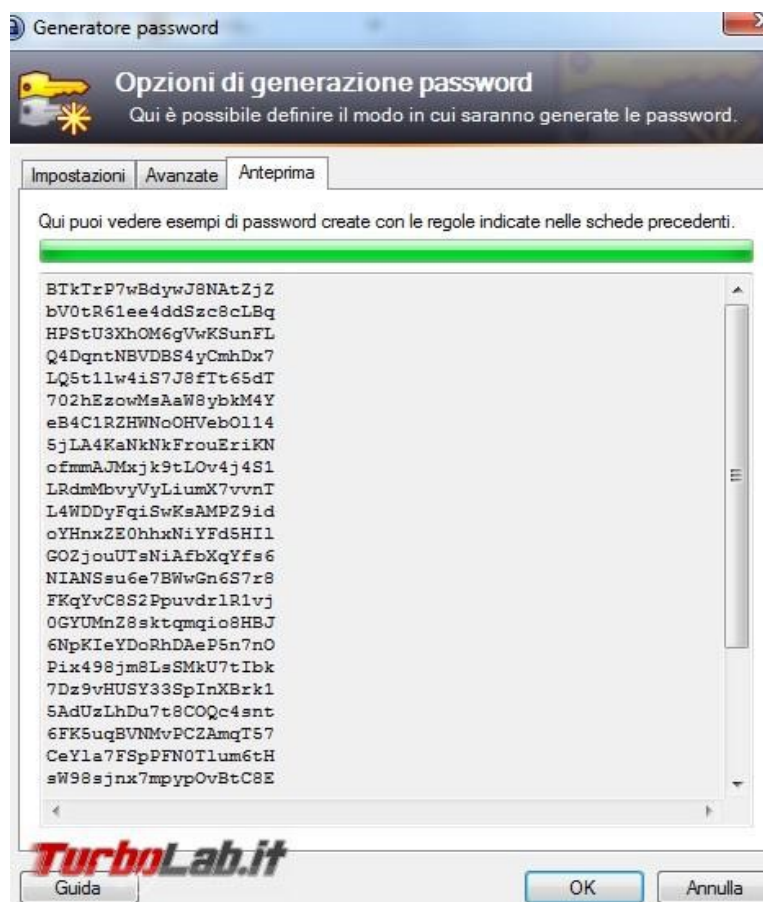
Strumenti-> Genera Password.

Possiamo generare delle password sicure e difficili da indovinare, anche in caso di attacco!

Di base troviamo selezionate le maiuscole, le minuscole e le cifre ma possiamo aggiungere caratteri speciali e variare la lunghezza della password con un numero di caratteri a noi gradito.



Premendo su OK verrà automaticamente creata una nuova voce nel database contenente la password creata casualmente; in alternativa possiamo controllare le password generate con i parametri impostati nella scheda Anteprima.



KEEPASS: USARE LA COMPILAZIONE AUTOMATICA SU PC

Necessitiamo di recuperare da un PC username e password salvate in una precisa voce di **KeePass**?

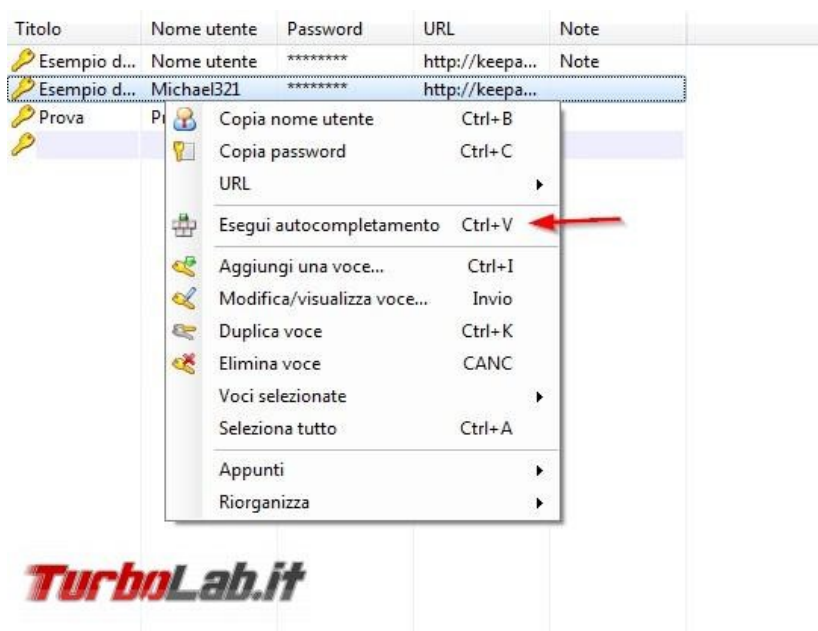
Possiamo utilizzare la compilazione automatica del programma per riempire i campi d'accesso di un sito o di un servizio.

Prima di tutto apriamo il browser web e portiamoci nella pagina d'accesso del sito (o servizio) e selezioniamo i campi di testo da riempire (consiglio di selezionare sempre il campo Username o Nome utente);

senza chiudere il browser apriamo **KeePass**, troviamo la voce desiderata e premiamoci sopra con il tasto destro del mouse.

Utilizziamo la voce indicata dalla freccia rossa (Esegui autocompletamento) per compilare automaticamente i campi selezionati nel browser.

Dopo questa operazione vedremo i campi d'accesso riempirsi automaticamente, con tanto di tasto Invio premuto automaticamente per noi.



CONCLUSIONI

La MEM Informatica S.r.l. non fornirà nessun tipo di assistenza su questa procedura, ma vuole dare un suggerimento per quanto riguarda la gestione/memorizzazione delle password.

KeePass è un programma sicuro, affidabile, molto intuitivo e in italiano. E' lo strumento ideale per la conservazione e la gestione delle password che viene usato su scala mondiale. Permette la creazione di DataBase separati per tipo di password o meglio ancora, creare un solo database dove all'interno catalogo per tipologia le password che inserisco. La password da ricordare sarà solo una mentre, quelle relative ai vari applicativi, verranno scritte su **KeePass** e imputate automaticamente dalla procedura, richiamando la relativa voce.

ATTENZIONE

Si ricorda inoltre che, la MEM Informatica S.r.l. non deve e non può conoscere le Vostre password; ogni richiesta del tipo “ non mi ricordo la password per accedere, l'abbiamo creata mesi fa assieme, ma non la ricordo più ... “relativamente all'accesso sia sul Sistema Operativo, e/o alla rete e/o ai vari applicativi, verrà sistematicamente rigettata in quanto, **per motivi di privacy e di normativa**, le password sono strettamente personali e devono essere conosciute esclusivamente dai diretti interessati.

MEM INFORMATICA S.r.l.

Assistenza Contabile/Fiscale

Roberto Meloni