Opzione Sicurezza per la protezione dei documenti NW3

GianPaolo Poletti
Settembre 2025

Premessa

In un'epoca in cui la digitalizzazione permea ogni aspetto della nostra vita quotidiana, la sicurezza informatica non è più un optional, ma una necessità imprescindibile. Questo documento si propone di analizzare e descrivere le misure di sicurezza implementate all'interno del programma, con l'obiettivo di garantire la protezione dei dati, la resilienza contro le minacce esterne e la conformità alle normative vigenti.

La protezione dei documenti sensibili è fondamentale per garantire la riservatezza delle informazioni. Un sistema di protezione basato su password offre un metodo semplice ed efficace per controllare l'accesso ai contenuti.

Nel programma NWWin3 è stata implementata un'opzione Sicurezza che permette la protezione dei documenti utilizzando una password di accesso principale e consente la condivisione tramite una password di condivisione. Il sistema è stato pensato per avere un'efficacia ragionevole senza essere un ostacolo nell'uso quotidiano del programma.

Il formato dei documenti di NWWin3

Il programma NWWin3 nella sua versione base non prevede nessuna caratteristica per la protezione dei documenti. Il formato dei documenti è il database di SQLite, e dove possibile le informazioni sono memorizzate al suo interno in formato XML.
Il formato XML (eXtensible Markup Language) è ampiamente utilizzato per la memorizzazione e lo scambio di dati grazie alla sua flessibilità e leggibilità.

I principali vantaggi di XML sono:

- I file XML sono **testuali** e strutturati con tag, quindi facilmente leggibili sia da persone che da software.
- Puoi aprire un file XML con un semplice editor di testo e comprendere il contenuto senza strumenti speciali.
- XML consente di **definire la propria struttura** dei dati, adattandosi a esigenze diverse.
- È facile **aggiungere nuovi elementi** o modificare la struttura senza compromettere la compatibilità.

SQLite è un motore di database relazionale leggero e integrato che opera senza un processo server dedicato. Tutti i dati, le tabelle e gli indici sono contenuti in un singolo file sul filesystem, il che semplifica la gestione all'interno di applicazioni di vario tipo.

Essendo SQLite un formato pubblico, si possono trovare diverse applicazioni che sono in grado di visualizzarne il contenuto.

Se per la maggior parte dei clienti questo fatto non è un problema, anzi può essere visto come una caratteristica favorevole, per i clienti che hanno esigenze di protezione e di riservatezza dei dati può costituire un problema.

Per coloro che hanno quindi esigenze di protezione dei dati è stata aggiunta l'opzione Sicurezza.
Questa opzione è composta da tre caratteristiche:

- Una **Password Principale** che viene definita al momento dell'attivazione della Sicurezza e serve per impedire l'apertura e la modifica dei vostri documenti alle persone non autorizzate.
- Una **Password di Condivisione** che è possibile definire opzionalmente per ciascun documento e che permette di condividere un documento con altri colleghi al di fuori della vostra organizzazione, permettendo la visualizzazione del documento ma impedendone la modifica.
- La **crittografazione** dei dati sensibili all'interno del documento in modo da impedirne l'accesso tramite l'uso delle applicazioni che sono in grado di aprire e visualizzare il contenuto dei database di SQLite.

L'opzione è stata strutturata per consentire un controllo da parte del responsabile della gestione informatica, lasciando i dipendenti dell'organizzazione liberi di usare il programma e i suoi documenti senza essere alla conoscenza delle password e dei dettagli di protezione.

Impostazione dell'opzione Sicurezza

La fase di impostazione è riservata al principale responsabile dell'organizzazione o all'ufficio responsabile della sicurezza interna.

In questa fase si deve definire la Password Principale e un indirizzo e-mail riservato da usare per l'autenticazione a due fattori. Questi due elementi sono sempre necessari per

l'impostazione di ogni PC della vostra organizzazione, dove sarà installato e usato il programma NWWin3.

Defining a secure password is left to security managers. The program's only requirement is that it be between 10 and 64 characters long. Regardless of the password's complexity (uppercase, lowercase, numbers, or unusual characters, which are good for preventing human attacks), its length is a key characteristic, making it difficult for other programs to attack.

The first time you enable the Security option, a window will appear where you are asked to enter the Master Password and the reference email address that will be used to confirm the activation and will then be used for all subsequent changes via two-factor authentication.

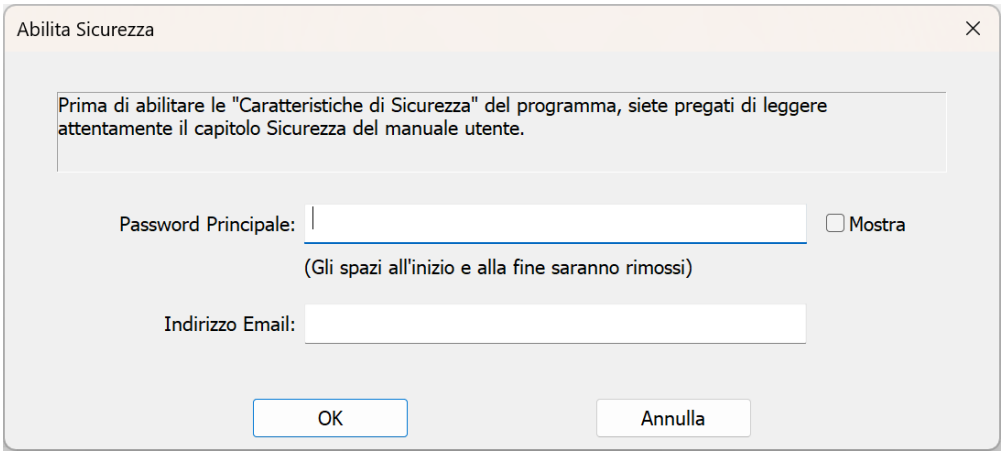


Figura 1 – Enabling Security

After confirming the window with the OK button, the program generates a temporary 6-digit code and sends it to the specified email address. A window will then open where you will need to enter the code to complete the activation process.

The first time the "Securoty" is enabled on a PC with NWWin3 must be performed by the security manager so that the Master Password remains confidential.

Important notice

NEVER SHARE YOUR MASTER PASSWORD WITH ANYONE!

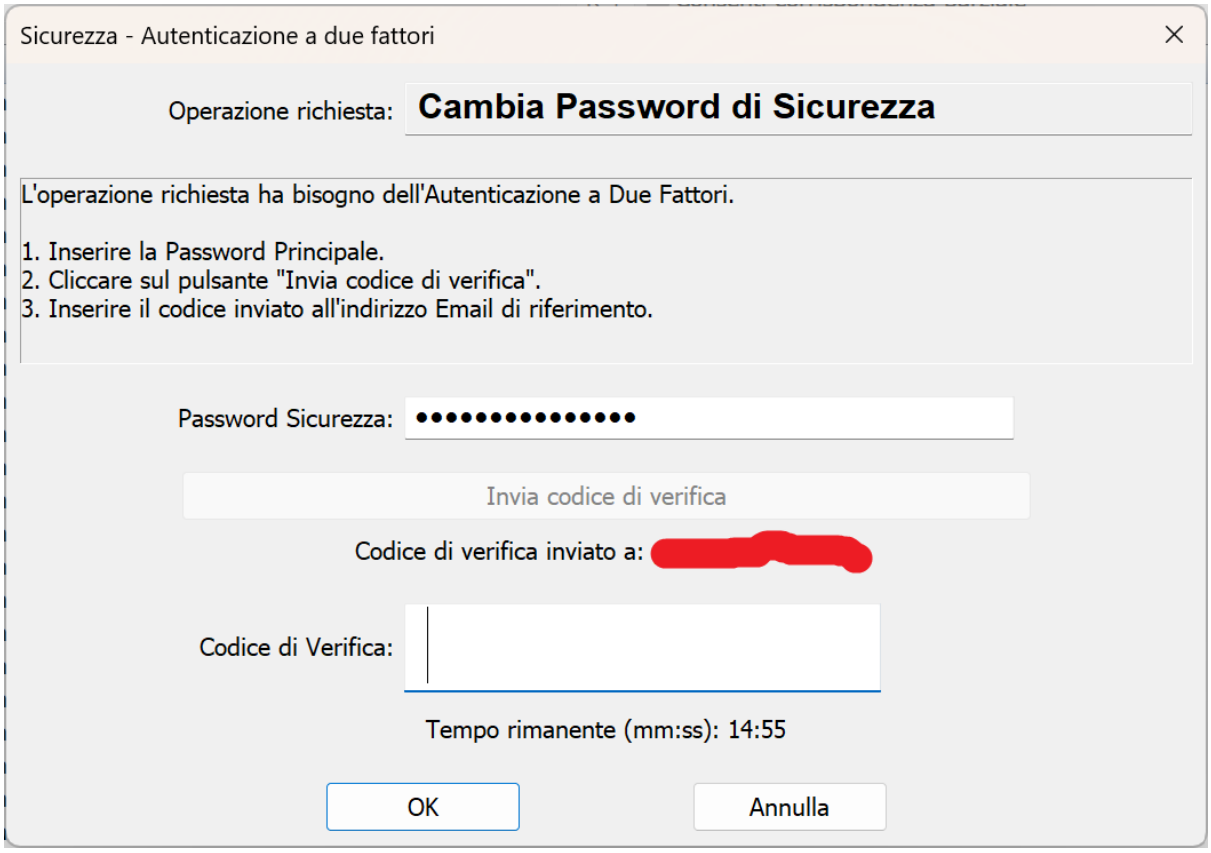
The Master Password and the reference email are saved by the program on each PC where the enabling procedure was performed, in an encrypted and secure manner.

Using the Master Password on all NWWin3 installations where the Security option has been enabled is completely transparent. Every new document will be created protected by the password, and every time you open a protected document, the program will do so without ever asking for the password.

Two-factor authentication

Tutte le successive operazioni di modifica e di gestione dell'Opzione Sicurezza prevedono l'uso dell'Autenticazione a due fattori. Uno è la Password Principale e l'altro è l'invio di un codice all'indirizzo e-mail di riferimento.

La finestra che gestisce l'Autenticazione a Due Fattori è visualizzata nella seguente immagine.



Per prima cosa si deve inserire la Password Principale di sicurezza. Quando la password è corretta si abilita il pulsante “Invia codice di verifica”.

Quando si clicca sul pulsante “Invia codice di verifica”, il programma invia una mail al vostro indirizzo con all’interno un codice di sei cifre.

Controllate il contenuto della vostra casella di posta e quando avete ricevuto la mail inserite il codice ricevuto nel campo “Codice di Verifica”.

Eseguire OK. Se il codice di verifica inserito corrisponde, l’autenticazione è conclusa con successo.

Per ovvii motivi di sicurezza i codici di verifica inviati nella mail hanno una durata di 15 minuti. Se non si fa in tempo a ricevere la mail con il codice, si dovrà rifare la procedura da capo.

La Password di Condivisione

Quando un documento è protetto dalla vostra Password Principale, non può essere aperto su nessun PC al di fuori di quelli che voi avete abilitato. Ma cosa fare se avete la necessità di condividere il documento con qualcun altro al di fuori della vostra organizzazione?

Ci sono due possibilità. La prima e quella di eliminare la Password principale dal documento. In questo modo diventa un documento normale che può essere aperto e modificato da chiunque ne venga in possesso.

La seconda possibilità è di definire una **Password di Condivisione** per quel documento. In questo modo il documento può essere condiviso con altri più o meno come se fosse di sola lettura.

Un documento aperto con la Password di Condivisione prevede le seguenti restrizioni:

1. Non è possibile salvare il documento, nemmeno con i comandi che prevedono la copia del documento come “Salva come…” o “Salva Copia come…”.
2. Non è possibile importare misure da quel documento in un altro. La persona che riceve il documento non può usare le misure che stanno nel vostro documento protetto importandole in un proprio documento.
3. Non è possibile stampare o esportare il documento o delle parti di esso se sono state fatte delle modifiche. Questo permette la stampa o l’esportazione, ma solo nello stato in cui lo avete salvato. Questo aspetto dovrebbe consentire l’uso dei documenti in sola lettura come veniva fatto nella versione precedente con l’applicazione NWReader.

Quando si definisce la Password di Condivisione si deve anche definire la sua durata in giorni, oltre la quale la password scade automaticamente.

Crittografazione

Cone scritto sopra, SQLite è un formato pubblico e si possono trovare diverse applicazioni che sono in grado di visualizzarne il contenuto.

Quindi anche se un documento è protetto dalla Password Principale e le altre istanze di NWWin3 non lo possono aprire, è possibile scorrerne il contenuto usando una delle utility disponibili su internet.

Per questo motivo è stata aggiunta al programma la possibilità di crittografare il contenuto di un documento. La crittografazione è possibile solo se il documento è già protetto dalla Password Principale. I documenti non protetti non possono essere crittografati.

I documenti protetti esistenti possono essere criptati o decriptati dal menu contesto della finestra Archivio. Inoltre, quando l’opzione Sicurezza è attiva è possibile creare un nuovo documento criptato.

La crittografazione è eseguita usando la “Cryptography API” di Windows, con l’algoritmo di crittografia simmetrica AES (Advanced Encryption Standard). Standard: FIPS 197. La chiave simmetrica è generata a partire dalla Password Principale usando l’algoritmo SHA 512-bit Standard: FIPS 180-2, FIPS 198