Security Option for NW3 Document's Protection

GianPaolo Poletti
November 2025

Foreword

In an era where digitalization permeates every aspect of our daily lives, cybersecurity is no longer optional, but an essential necessity. This document aims to analyze and describe the security measures implemented within the program, with the aim of ensuring data protection, resilience against external threats, and compliance with current regulations.

Protecting sensitive documents is essential to ensure the confidentiality of information. A password-based protection system offers a simple and effective method for controlling access to contenti.

The NWWin3 program has implemented a Security option that allows you to protect documents using a master access password and allows sharing using a sharing password. The system is designed to be reasonably effective without being an obstacle to the program's daily use.

The NWWin3 document format

The basic version of NWWin3 does not include any document protection features. The document format is the SQLite database, and where possible, the information is stored in XML format.
The XML (eXtensible Markup Language) format is widely used for storing and exchanging data due to its flexibility and readability.

The main advantages of XML are:

- XML files are textual and structured with tags, so they are easily readable by both humans and software.
- You can open an XML file with a simple text editor and understand the content without any special tools.
- XML allows you to define your **own data structure**, adapting to different needs.
- It's easy to add new elements or change the structure without compromising compatibility.

SQLite is a lightweight, integrated relational database engine that operates without a dedicated server process. All data, tables, and indexes are contained in a single file on the filesystem, making it easy to manage within various applications.

Since SQLite is a public format, you can find several applications that are able to view its contents.

While this is not a problem for most customers, and can even be seen as a positive feature, it can be a problem for customers who have data protection and privacy needs.

For those who have data protection needs, the Security option has been added.

This option consists of three features:

- A **Master Password** that is defined when Security is activated and prevent unauthorized people from opening and modifying your documents.
- A **Sharing Password** that you can optionally define for each document and that allows you to share a document with other colleagues outside your organization, allowing them to view the document but preventing them from modifying it.
- **Encrypting** sensitive data within the document to prevent access to it by using applications that can open and view the contents of SQLite databases.

The option has been structured to allow control by the IT manager, leaving the organization's employees free to use the program and its documents without knowing the passwords and security details.

Setting the Security Option

The setup phase is reserved for the office responsible for internal security.

At this stage, you must define the **Master Password** and a confidential email address to use for two-factor authentication. These two elements are always required for setting up each PC in your organization where the NWWin3 program will be installed and used.

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.

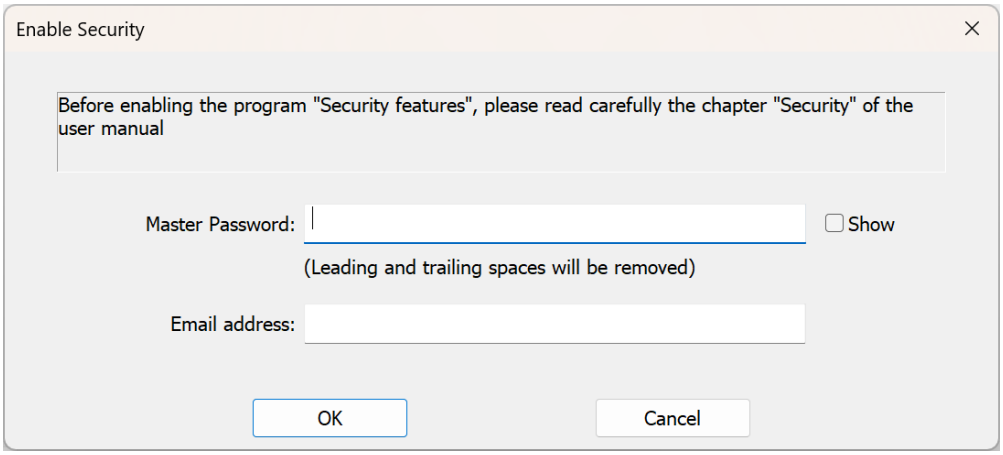


Figure 1 - First Security option use

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 security enablement on each PC where the program is installed must be performed by the security manager so that the Master Password remains confidential.

Important notice

NEVER SHARE YOUR MASTER PASSWORD WITH ANYONE!

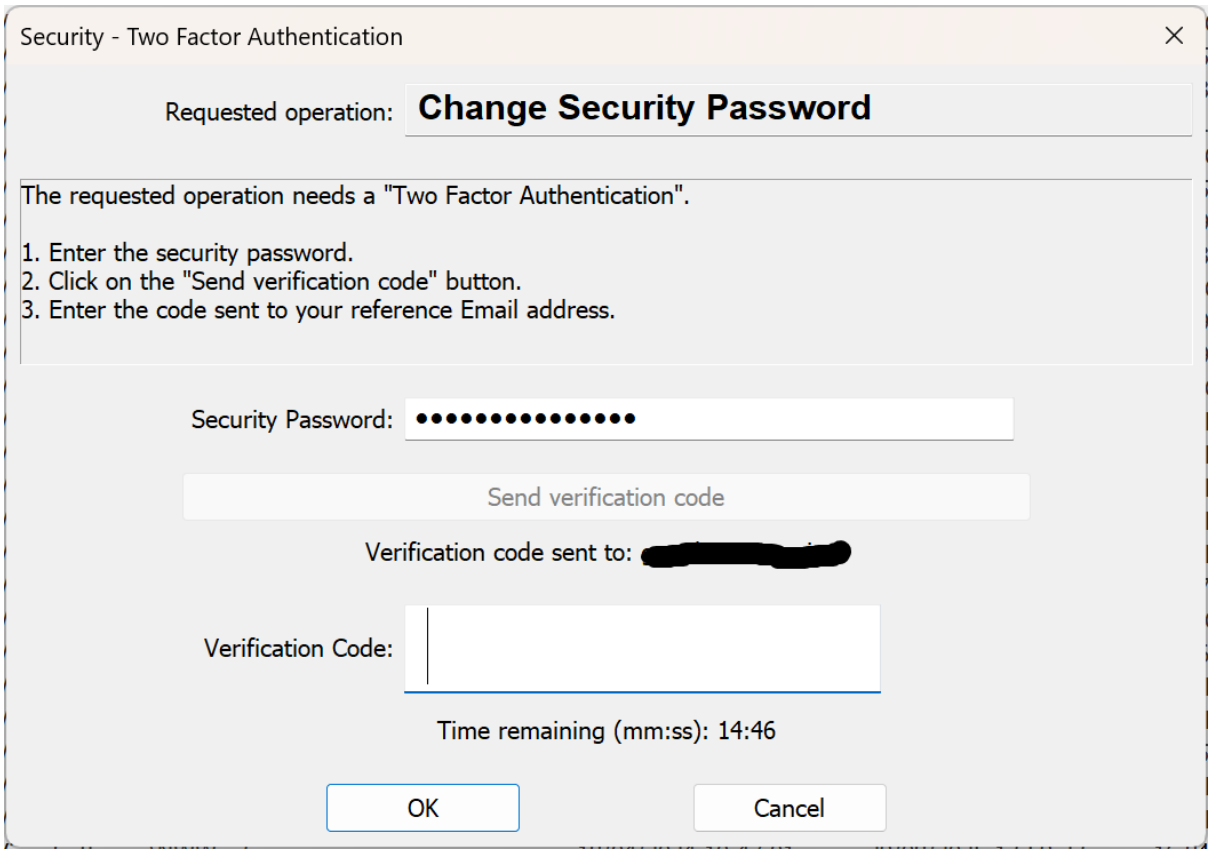
The Master Password and the reference email are saved by the program on each PC where the enabling procedure was executed, in an encrypted and secure manner.

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

All subsequent changes and management of the Security Option require the use of two-factor authentication. One is the Master Password and the other is the sending of a code to the reference email address.

The window that manages Two-Factor Authentication is displayed in the following image.



First, you must enter your Master Security Password. When the password is correct, the "Send Verification Code" button will be enabled.

When you click the “Send Verification Code” button, the program sends an email to your address containing a six-digit code.

Check the contents of your mailbox and when you receive the email, enter the code received in the "Verification Code" field.

Click OK. If the verification code you entered matches, authentication is successful.

For obvious security reasons, the verification codes sent by email are valid for 15 minutes. If you don't receive the email with the code in time, you'll have to start the process again.

The Sharing Password

When a document is protected by your Master Password, it cannot be opened on any PC other than those you have authorized. But what if you need to share the document with someone outside your organization?

There are two options. The first is to remove the Master Password from the document. This way, it becomes a normal document that can be opened and modified by anyone who gains access to it.

The second option is to set a **Sharing Password** for that document. This way, the document can be shared with others as if it were read-only.

A document opened with the Sharing Password has the following restrictions:

1. It is not possible to save the document, not even with commands that involve copying the document such as “Save As…” or “Save Copy As…”.
2. You cannot import measurements from that document into another. The recipient of the document cannot use the measurements in your protected document by importing them into their own document.
3. It's not possible to print or export the document or parts of it if changes have been made. This allows printing or exporting, but only in the state in which you saved it. This should allow the documents to be used in read-only mode, as was done in the previous version with the NWReader application.

When defining the Sharing Password, you must also define its duration in days, after which the password expires automatically.

Encryption

As written above, SQLite is a public format, and you can find several applications that are able to view its contents.

So even if a document is protected by the Master Password and other instances of NWWin3 cannot open it, it is possible to browse its contents using one of the utilities available on the Internet.

For this reason, the program has been added with the option to encrypt document content. Encryption is only possible if the document is already protected by the Master Password. Unprotected documents cannot be encrypted.

Existing protected documents can be encrypted or decrypted from the Archive window's context menu. Additionally, when the Security option is active, you can create a new encrypted document.

Encryption is performed using the Windows “Cryptography API,” with the AES (Advanced Encryption Standard) symmetric encryption algorithm. Standard: FIPS 197. The symmetric key is generated from the Master Password using the 512-bit SHA algorithm. Standards: FIPS 180-2, FIPS 198.