

VaultNX

Quick Start Guide

Version 1.1.0 · May 2026

This guide will get you from zero to an encrypted, working vault in under 10 minutes. Follow the four steps in order. Keep this document — you will need it if you ever need to restore access using a recovery key.

1
Install

2
NAS Setup

3
Vault Creation

4
Recovery Key

Support: support@vaultnx.com · Docs: vaultnx.com/docs

1. Install VaultNX

VaultNX is a single self-contained installer (.exe) for Windows 10 and 11 (64-bit). It installs the VaultNX tray application and a background Windows Service that manages the NAS connection.

System Requirements

OS	Windows 10 22H2 or later · Windows 11
Architecture	64-bit (x64) only
RAM	256 MB free (512 MB recommended)
Disk	50 MB for the application + vault space on NAS
Network	TCP port 445 open between this PC and the NAS
Privileges	Local administrator required for install

Installation Steps

- 1 Download **VaultNX-1.1.0-Setup.exe** from vaultnx.com/download.
- 2 Right-click the installer and select **Run as administrator**. If Windows SmartScreen shows a warning, click *More info* → *Run anyway*. (This warning disappears once the installer is code-signed.)
- 3 Follow the installer prompts. VaultNX installs to C:\Program Files\VaultNX\ by default.
- 4 After install, the VaultNX icon appears in your system tray (bottom-right). The Setup Wizard opens automatically on first launch.

■ **Administrator rights are required.** The installer registers a Windows Service (VaultNXService) that starts automatically at login. Standard user accounts cannot complete this step.

✓ The installer does not require an internet connection. Activation of your license key does require connectivity to lic.vaultnx.com (port 443).

2. NAS Connection Setup

VaultNX connects directly to your NAS over SMB2/3 — no drive letters, no Windows share mapping. Your NAS must be reachable over your local network or VPN on TCP port 445.

What You Will Need

NAS Host / IP	The IP address or hostname of your NAS — e.g. 192.168.1.100 or nas.local
---------------	--

Share Name	The name of an SMB share on the NAS — e.g. documents (for \\NAS\documents)
Username	A NAS user account with read/write access to the share
Password	Password for that account. Leave blank for public/guest shares.
Domain	For home NAS devices: WORKGROUP. For Active Directory: your domain name.
Port	Default is 445. Only change this if your NAS uses a custom SMB port.
Vault Folder	A subfolder name on the share — e.g. activevault. Created automatically.

Configuring the Connection

- 1 In the Setup Wizard, select the **Connection** step (or open **Settings** → **NAS Connection** later).
- 2 Enter the Host/IP, Share Name, Username, Password, and Domain. Leave the Vault Folder as `activevault` unless you have a reason to change it.
- 3 Click **Test Connection**. A green "✓ Connected" message confirms VaultNX can reach the share. A red message includes a specific reason — check the table below.
- 4 Click **Save Connection**. Your NAS password is stored encrypted using Windows DPAPI (tied to your Windows login).

Common Connection Errors

3. Creating Your Vault

A vault is an encrypted container on your NAS. Each file you upload is individually encrypted with AES-256-GCM before leaving your PC. The master password never leaves your machine — it is used locally to derive an encryption key using Argon2id.

■ **Critical — read before continuing.** Your master password is the **ONLY** key to your data. VaultNX does not store it, cannot recover it, and has no back-door. If you lose it without a recovery key, your files are permanently inaccessible. **Store your master password in a password manager (Bitwarden, 1Password, KeePass) before you click Create Vault.**

Creating a Vault

- 1 In the Setup Wizard, reach the **Vault** step (after NAS connection is saved).
- 2 Type your master password in the **Master Password** field. The strength bar must reach at least **Moderate** before you can proceed. Aim for **Strong** or better.

- 3 Re-enter the same password in **Confirm Password**.
- 4 Click **Next**. VaultNX creates the vault structure on the NAS and the Setup Wizard moves to the final step.

Password Guidelines

Using the Vault Browser

Once your vault is unlocked, the Vault Browser shows your encrypted files. You can:

- 1 **Upload files** — drag and drop, or click Upload in the toolbar. Files are encrypted before they reach the NAS.
- 2 **Download files** — right-click a file and select Download, or double-click to open directly. VaultNX decrypts the file to a temporary local copy.
- 3 **Create folders** — right-click in the browser and select New Folder.
- 4 **Lock the vault** — right-click the tray icon and select Lock, or it locks automatically after the idle timeout (default: 15 minutes).

4. Recovery Key

A recovery key is an encrypted backup of your master password stored as a `.avr` file. If you forget your master password, you can use this file to regain access — but only if you remember the recovery key password you set when generating it.

- Generate your recovery key **immediately after creating your vault**. Without it, a forgotten master password means **permanent data loss**. Store the `.avr` file on a USB drive, a different cloud account, or printed as a QR code — not on the same NAS as your vault.

Generating the Recovery Key

- 1 Open **Settings** → **Security**.
- 2 Click **Generate Recovery Key**.
- 3 Enter your **current master password** to authorise generation.
- 4 Enter and confirm a **recovery key password**. This can be different from your master password — write it down separately.
- 5 Click **Save Recovery Key** and choose a location **outside your VaultNX NAS share**. A USB drive or separate cloud folder is ideal.

Restoring from a Recovery Key

- 1 On the Login screen, click **Use Recovery Key**.
- 2 Browse to your `.avr` file.
- 3 Enter the **recovery key password** you set during generation.
- 4 VaultNX decrypts the recovery key and unlocks the vault. **Immediately go to Settings → Security and set a new master password.**

■ **What the `.avr` file contains:** Your master password bytes, encrypted with AES-256-GCM using a key derived from your recovery key password via Argon2id. Without the recovery key password, the `.avr` file is useless. Keep both safe.