

NextGen Widget Encrypt3

Table of contents

Introduction	3
Welcome	4
What's new	4
Getting Started	5
Install and start	7
Create your account	9
Meet the key store	10
Add a key	11
Encrypt a test file	12
Decrypt the same file	13
Optional but useful	14
If something fails	15
License and machine code	16
Using the program	17
Two passwords	19
Create your first key	20
Import a key	22
Bulk import and the CSV template	23
File Task	24
Text Task	26
Revoke, trash, and restore	27
Trust, fingerprint, and QR	28
Vault and settings	29
Backup the vault	31
Move the vault	32
Watch folder	33
Recipient groups and the grid filter	34
Explorer Encrypt and Decrypt	35
Updates	36
Keys and operations	37
Keyserver and WKD lookup	39
Expiration dashboard	40
Key ceremony sheet	40
Audit log	41
Product	42
Licensing	44
Policy notes	46
Menu map	47
System requirements	49
Keyboard and windows	50
Uninstall	51
Glossary	51
Disclaimer	52
System requirements	53
Getting help	54
No refund policy	55

Introduction

[BACK TO HOME](#)



NEXTGEN Widget Encrypt3 — when OpenPGP security matters.

by NextGen Widget Software

Introduction

NEXTGEN Widget Encrypt3 is a Windows OpenPGP workstation for people who need to manage keys and protect files, folders, and text without living in a command line.

Keys, logins, and settings are stored in an encrypted vault (.ngw3). The program is meant for daily work: compose and import keys, encrypt and sign for real recipients, watch a folder, keep an audit trail, and recover from mistakes without guessing.

It is not a mail server, not a web app, and not a replacement for every other OpenPGP program on the market. It is a desktop tool that speaks standard OpenPGP so you can interchange keys and messages with common OpenPGP applications when you use compatible algorithms and ASCII armor.

Use this help file to learn how each area works and where to find it in the menus.

Welcome

Welcome

Welcome to NEXTGEN Widget Encrypt3.

If this is your first run, you will create an account. That username and password protect the vault on this PC. They are not your OpenPGP key passphrase. You will set key passphrases when you compose or import secret keys.

After you sign in you will see the key store. That grid is the center of the product. From here you compose keys, import public or secret material (files or armored blocks), encrypt and decrypt files, folders, and text, and open Settings for the vault path, idle lock, Explorer verbs, and update checks.

Three habits will save you time:

1. Treat the vault file as the source of truth. Know where it lives and keep a tested backup.
2. Distinguish **login password** (vault) from **key passphrase** (OpenPGP secret key).
3. Do not encrypt to expired or revoked keys. The program blocks that on purpose.

Evaluation copies may limit how long a newly composed key can remain valid (30 days). A licensed copy does not apply that cap. Use Help → About for version, build date, and machine code if you are activating a license.

If you are converting from another OpenPGP program, start with **Keys → Import** or **Import from clipboard**, confirm the fingerprint, then run one file encrypt/decrypt round trip before you rely on it for real mail.

What's new

What's New

This release is NEXTGEN Widget Encrypt3 **1.0.0.1**, the first public build of this workstation.

Vault and sign-in

- Encrypted vault for keys, users, and settings
- Login with lockout after three failures; failed attempts shown after a good sign-in
- Optional second administrator
- Idle lock with a configurable timeout
- Change login password and change key passphrase

Keys

- Compose RSA, DSA+ElGamal, ECDSA+ECDH, Ed25519+X25519 with hash, cipher, compression, and expiry
- Password generator and strength meter; mark as verified
- Import and export public, secret, or pair (.asc / .pgp)
- Import armored blocks and clipboard
- Bulk import (CSV template, .asc / .pgp / .gpg, ZIP) with dry-run and checks for duplicates, expiry, revocation, and weak algorithms
- Groups and notes
- Revoke, trash, properties, QR of the public key
- Extend expiration (secret key required)

- Policy blocks obsolete 1024-bit keys for new compose and encrypt
- Evaluation copies cap newly composed keys at 30 days

Files, folders, and text

- Encrypt, decrypt, sign and encrypt, decrypt and verify
- Optional ASCII armor and armor comment; Version header uses this product name
- Encrypt-to-self (recovery recipient you choose)
- Folder encrypt and decrypt, with optional subfolders
- Text: encrypt, decrypt, sign and encrypt, decrypt/verify, clear-sign and verify
- Empty text is not encrypted

Operations

- Watch folder (files, chosen recipient key)
- Recipient groups and grid group filter
- Explorer Encrypt / Decrypt (sign-in if the workstation is locked)
- Keyserver / WKD lookup with several servers and an online check
- Expiration dashboard
- Key ceremony sheet (print; groups)
- Audit log
- Command line and Explorer integration
- Backup and restore of the vault

Help and product

- Help file, Support site, About (version, build date, copyright 2026)
- Optional check for updates every 30 days, plus a manual check
- Evaluation and license dialog; machine code on About

Not in this build

- Hardware tokens
- OpenPGP v6, AEAD, and post-quantum algorithms
- Full mail-client authoring (EML helpers only)

After install, confirm the vault path under **Settings** → **Key store**. When you copy the program to another PC, keep NextGenWidgetEncrypt3.exe.config next to the executable.

Getting Started

[BACK TO HOME](#)

The trial is the evaluation period; purchases are final after the license key is emailed. See No refund policy.

Getting started

This walkthrough takes you from the first launch to one successful encrypt and decrypt. Do that before you

use the program with real files.

1. [Install and start](#)

Copy the program files into a folder you control. You need at least:

- NextGenWidgetEncrypt3.exe
- NextGenWidgetEncrypt3.exe.config

Double-click the executable. If a license or evaluation window appears, continue or enter a license code. If the configuration file is missing, the program cannot run reliably—put the .config back next to the exe.

2. [Create your account](#)

On first run there is no vault yet. Choose **Create account**.

- Pick a username and a strong login password. Confirm the password.
- This password opens the **vault**. It is not the passphrase of an OpenPGP key.
- The vault file (.ngw3) is created in the default location. You can move it later under **Settings** → **Key store**.

Sign in with the same username and password.

3. [Meet the key store](#)

After sign-in you see the key grid. That is home. Menus along the top open compose, import, file/folder/text tasks, settings, and help.

If the welcome line reports failed sign-in attempts, someone (or you) typed the login wrong since the last successful sign-in.

4. [Add a key](#)

You need at least one key that can encrypt, and a secret key if you will decrypt.

Compose a new pair

Keys → **Compose key**. Enter name and optional email, choose the algorithm (Ed25519+X25519 is a good default), set expiry or never expire (evaluation copies cannot use “never” and cap new keys at 30 days), set a key passphrase, then create. Optionally mark it verified.

Import a key you already have

Keys → **Import**, or import from clipboard if you have an armored block (BEGIN PGP PUBLIC KEY / PRIVATE KEY). Confirm the fingerprint before you trust it.

5. [Encrypt a test file](#)

1. Open **File Task**.
2. Choose **Encrypt file**.
3. Select a small test file (not your only copy of anything important).
4. Choose the recipient key (the public key of who should open it).
5. Optionally turn on ASCII armor and **Also encrypt to me** if you want a recovery copy for a second key **you** select.
6. Encrypt. Note where the output file is saved.

6. Decrypt the same file

1. Stay on **File Task** → **Decrypt file**.
2. Select the file you just created.
3. Choose the secret key that should open it and enter that key's passphrase.
4. Confirm the restored file matches the original.

If decrypt asks for a passphrase, that is the **key** password, not the vault login.

7. Optional but useful

- **Settings** → **Security**: idle lock minutes; Explorer right-click Encrypt/Decrypt.
- **Settings** → **Software update**: optional check every 30 days, or **Check for update** now.
- **Help** → **About**: version, build date, machine code (needed if you buy a license).
- Back up the vault from the backup command after you have keys you care about. Test that the backup opens before you need it.

If something fails

- Wrong login three times: the program exits. Start it again and use the vault password.
- "Policy" or weak key: 1024-bit and similar obsolete keys cannot be used to compose or encrypt. Import may warn; use a stronger key.
- Expired or revoked key: decrypt with a secret key may still work; encrypt and sign will not.
- Explorer encrypt while the app is locked: sign in on that prompt, or unlock the running session first.

When this loop works (account → key → encrypt → decrypt), you are ready for folder, text, watch folder, and bulk import. Those are covered in their own topics

Install and start

Getting started — Install and start

What you need

- Windows 10 or 11 (64-bit)
- .NET Framework 4.8 or later (Windows 10/11 usually already have it)
- The download zip for NEXTGEN Widget Encrypt3

The zip contains NextGenWigetEncrypt3.exe and NextGenWigetEncrypt3.exe.config. Keep both in the same folder after you extract.

Install

1. Download the zip and extract it to a folder you will keep, for example C:\Program Files\NEXTGEN Widget Encrypt3\ or a folder under Documents.
2. Open the extracted folder and confirm both files are there:
 - NextGenWigetEncrypt3.exe

- NextGenWidgetEncrypt3.exe.config
and the Help folder if it was included.
- 3. Do not separate the exe from the .config file. Do not copy only the exe to the Desktop.
- 4. Optional: create a shortcut to the exe on the Desktop or Start menu.
- 5. If Windows marks the files as blocked (downloaded from the web), right-click each file → Properties → **Unblock** → OK.

You do not need Administrator rights to run the program. Per-user Explorer integration is turned on later from **Settings**.

A purchased license is locked to one PC. After you start the program, Help → About shows the machine code for that computer. If you replace the PC, send the new machine code with your purchase email so a replacement license can be issued. **Only one replacement is included per purchase.**

First start

1. Double-click NextGenWidgetEncrypt3.exe in the extracted folder (or use your shortcut).
2. If this is an evaluation copy, the license / evaluation window appears first. Choose **Continue Evaluation** or enter a license code. Closing an **expired** evaluation exits the program.
3. The **sign-in** window opens.

No vault yet

1. Choose **Create account**.
2. Enter a username and a login password (and confirm it). This password protects the vault, not an OpenPGP key.
3. Complete creation, then sign in with the same username and password.

Vault already exists

1. Enter your username and password.
2. After three wrong passwords the program exits.
3. On a successful sign-in you should see the key store (empty until you compose or import keys).

After sign-in (once)

1. Open **Settings** → **Key store** and note the vault path (.ngw3). That file is your key database.
2. Optional: **Settings** → **Security** — set idle lock and, if you want, Explorer Encrypt/Decrypt for this user.
3. Optional: **Settings** → **Software update & license** — allow a check every 30 days.
4. Open **Help** → **About** to confirm version, build date, and machine code.

If the program does not start

- Extract the zip again and confirm the .config file sits next to the exe.
- Run the exe from that folder, not a lone copy of the exe.
- Evaluation expired: start again only with a valid license or a new evaluation, per the license window.

Next

Go to **Getting started** → **Create your first key** (or Import a key) after the key store is on screen.

Create your account

Getting started — Create your account

The account protects the **vault** on this PC. It is not an OpenPGP key and it is not a license.

When you need this

- First run, when sign-in says there is no vault
- You have not created a username for this copy of the program yet
- The login password must be at least eight characters. Longer is better.
- Watch the strength meter. Weak (red) is a poor choice for a vault.

If the vault file already exists, use **Sign in**, not Create account. Creating a second vault is a different Settings / file-location task.

Before you start

- Choose a username you will remember.
- Choose a login password at least as strong as the meter allows (long and not a single dictionary word).
- This password unlocks every key in the vault file. If you lose it, the vault cannot be opened.

Steps

1. On the sign-in window, choose **Create account**.
2. Enter a **username**.
3. Enter a **password**, then enter it again to confirm.
4. The password must be at least eight characters. Watch the strength meter. Prefer medium or strong.
5. Complete creation.
6. You are returned to sign-in. Enter the same username and password and sign in.

After a successful sign-in the key store opens. It is empty until you compose or import a key.

What was created

- A vault file (.ngw3) in the location shown later under **Settings** → **Key store**
- Your administrator login inside that vault

OpenPGP key passphrases are set later, when you compose or import a secret key. They can be different from the login password.

If creation fails

- Passwords do not match: enter both again.
- Password too short: use at least eight characters (longer is better).
- Vault already exists: sign in instead, or move/rename the old vault only if you intend to start over (that hides the old keys).

Next

Getting started → **Create your first key** or **Import a key**.

Meet the key store

Getting started — Meet the key store

After you sign in, the main window is the **key store**. Every key in the vault appears here. Tasks (file, folder, text, compose, import) start from this window.

What you are looking at

- **Title bar** — product name, version, and build date
- **Welcome bar** — your username, last successful sign-in, and failed sign-in attempts since that login
- **Menu** — Keys, File, Folder, Text, Tools / professional items (bulk import, groups, watch folder, lookup, ceremony, backup), Settings, Help
- **Group filter** — limit the grid to a group (or All / Ungrouped)
- **Find** — search box; **Find** sits next to the box; **Cancel search** clears it
- **Grid** — one row per key

Grid columns (typical)

Line number, Key ID, Key ID (hex), username, email, algorithm, size, public/private, created, valid until, trust, group, and related status fields.

Colors

- **Revoked** — red
- **Expired** — purple (not the same as revoked)
- Other rows use the normal text color

A revoked or expired key must not be used to encrypt or sign. Decrypt with a secret key may still be allowed when the policy permits.

Selection and right-click

Click a row to select it. Right-click for shortcuts, including:

- Copy the selected public key
- Set trust (verified)
- Encrypt or decrypt the clipboard (decrypt asks for that key's passphrase; the text must be a proper OpenPGP message)

Double-click or use the Keys menu for **Properties** and **QR** (full public key).

Empty store

A new account shows no rows. That is normal. Compose a key or import one before you encrypt.

What this window is not

It does not encrypt a file by itself. Select a key, then open **File Task**, **Folder Task**, or **Text Task**, or use Explorer after you enable it in Settings.

Next

Getting started → **Create your first key** or **Import a key**

Add a key

Getting started — Add a key

The key store is empty until you add at least one key. You can **compose** a new pair or **import** a key you already have.

Compose a new key

1. Open **Keys** → **Compose key** (or the equivalent Compose command).
2. Enter a **name**. Email is optional but recommended.
3. Choose algorithm (for a first key, **Ed25519+X25519** or **RSA 3072**).
4. Set hash, cipher, and compression if you do not want the defaults (SHA512, AES256, ZIP are the usual defaults).
5. Set **Valid until**, or Never expire if the license allows it.
Evaluation copies cannot use Never expire; new keys must expire within **30 days**.
6. Enter a **key passphrase**, confirm it (minimum eight characters). Optional: generate a password and use Show password.
7. Optional: **Mark as verified** if this is your own key.
8. Choose **Create**. Large RSA (4096) can take a while; stay on the window.
9. The new row appears in the key store.

1024-bit RSA is blocked for new keys.

Import a key you already have

Use this for a public key someone sent you, or a secret key you exported from another program.

- **File:** Keys → Import, and choose .asc, .pgp, or .gpg.
- **Armored block:** paste a BEGIN PGP PUBLIC KEY BLOCK or PRIVATE KEY BLOCK into **Import key block** / clipboard import.
- **Several files:** **Bulk import** (CSV template, folder, or ZIP). Use dry-run first if you want to see duplicates, expiry, and revocation before anything is saved.

If the key is already in the store, expired, revoked, or too weak (for example 1024-bit for encrypt), you get a message and the key may be skipped.

After the key is in the grid

1. Select the row.
2. Open **Properties** and check fingerprint, user ID, created, valid until, public vs secret.
3. For a key you will encrypt to in person, compare the fingerprint (or QR) with the owner. Then set trust to **Verified**.

Imported public keys are not automatically “verified.”

Public vs secret

- **Public only** — you can encrypt to it and verify signatures. You cannot decrypt or sign.
- **Public + secret** — you can decrypt and sign, after you enter that key’s passphrase.

Next

Encrypt a **test file** to your own key and decrypt it before you use the key for real data. See **Getting started** → **Encrypt a test file**.

Encrypt a test file

Getting started — Encrypt a test file

Do this once after you add a key. Use a throwaway text file, not important data.

What you need

- A key in the store that can encrypt (not expired, not revoked; not a blocked 1024-bit key)
- If you will decrypt on this PC, that key must include the **secret** part
- A small test file, for example test.txt on the Desktop

Encrypt

1. Open **File Task**.
2. Open the **Encrypt file** tab.
3. Choose the **input file**.
4. Choose the **recipient** (the key you are encrypting to). For this test, choose your own key.
5. Optional: check **ASCII armor** if you want a text .asc-style file.
6. Optional: enter an **armor comment** only if armor is on and you want a Comment header.
7. Optional: **Also encrypt to me (recovery copy)** adds a **second** recipient you select. Leave it off for the first test so only one key can decrypt.
8. Choose **Encrypt**.
9. Pick where to save the output. Encrypted names use a generated name (not the original filename).

The Version header on armored output uses this product name.

Decrypt

1. Stay on **File Task** and open the **Decrypt file** tab (next to Encrypt file).

2. Choose the encrypted file you just created.
3. When asked, enter the **key passphrase** for the secret key that can open it (not the vault login, unless you used the same password).
4. Save the output. Decrypt restores the **original file name and extension**.
5. Open the result and confirm it matches test.txt.

If it fails

- **Policy / weak key** — that key cannot be used to encrypt. Use a stronger key.
- **Expired / revoked** — choose another recipient.
- **Wrong passphrase** — the secret key password is incorrect.
- **Cannot decrypt** — the file was not encrypted to a secret key in this vault (recovery copy off and recipient was someone else).

Next

Use **File Task** for real files the same way. For many files in a folder, see Folder Task. For messages, see Text Task

Decrypt the same file

Sign and encrypt

If you used **Sign and encrypt** instead of Encrypt only, use **Decrypt and verify** (or the decrypt tab that verifies). You should see that the signature is valid and which key signed, if the signer is in the store and not revoked.

If it fails

- **Wrong passphrase** — try again; three failures here are not the same as vault lockout, but you still cannot open the file.
- **No secret key** — the file was encrypted only to a public key you do not have.
- **Not an OpenPGP file** — you selected the wrong input.
- **Expired key** — encrypt is blocked; decrypt with a secret key may still work.
- **Revoked key** — do not use it to sign; decrypt may still be possible if the secret material is in the vault.

Clipboard

You can also right-click a key in the store and decrypt OpenPGP text on the clipboard. The clipboard must contain a proper BEGIN PGP MESSAGE (or equivalent) block.

Next

When this round trip works, the vault and that key are usable. Continue with Folder Task, Text Task, or import the people you will encrypt to.

Optional but useful

Getting started — Optional but useful

None of these are required for the first encrypt/decrypt test. Turn them on when you start using the program every day.

Settings → Security

- **Idle lock** — lock the workstation after a set number of minutes with no keyboard or mouse in this program. The lock screen is not a full Windows lock.
- **Explorer** — add Encrypt / Decrypt to the right-click menu for this user. If Encrypt3 is running but locked, Explorer asks you to sign in.

Settings → Key store

- Note the .ngw3 path.
- Change location only when you intend to move the vault; the program copies the file and remembers the new path.

Settings → Software update & license

- Check **Authorize checking for an update every 30 days** if you want a notice after sign-in when that interval has passed.
- **Check for update** runs the same check immediately (needs Internet).
- **License / About** — machine code for a per-PC license; one replacement per purchase.

Keys and the grid

- Set **Verified** on keys whose fingerprint you have checked.
- Use **Groups** so the grid filter can show Financial, Technical, Sales, and similar labels (group names are not case-sensitive).
- **QR** on a key shows the public key for comparison.
- **Backup** the vault after you have keys you care about; test a restore before you need it.

Automation and lookup

- **Watch folder** — drop files in an inbox folder; they encrypt to the key you select (files only).
- **Keyserver / WKD lookup** — find public keys on the network (the program checks for Internet first).
- **Bulk import** — many keys at once; use dry-run first.
- **Expiration dashboard** — see what is expiring, including keys with no name (Key ID hex) and revoked keys.

Help

- **Help** opens the help file in the program folder.
- **Support** opens the help desk site.

When these are set the way you want, daily work is: select recipients, File / Folder / Text Task, and keep a current vault backup.

If something fails

Getting started — If something fails

The program does not start

- Extract the zip again. NextGenWidgetEncrypt3.exe and NextGenWidgetEncrypt3.exe.config must be in the **same** folder.
- Do not run a copy of the exe alone on the Desktop.
- If Windows blocked a downloaded file: right-click → Properties → Unblock.
- Evaluation expired: the license window will not let you continue until you have a valid license or a current evaluation.

Cannot create an account

- Passwords must match.
- Login password must be at least **eight** characters.
- If a vault already exists at the configured path, sign in instead of creating a second account in the same file.

Cannot sign in

- Username and password are for the **vault**, not the OpenPGP key.
- Three wrong passwords and the program exits. After a good sign-in, the welcome bar shows whether there were failed attempts.
- Confirm **Settings** → **Key store** path on a machine where you can already open the vault; you may be pointing at a different .ngw3.

No keys in the grid

- A new account is empty until you compose or import.
- Group filter may be hiding rows — set it to **All groups**.
- Clear the Find box.

Cannot compose or import

- Evaluation copy: new keys must expire within 30 days; Never expire is disabled.

- 1024-bit keys are blocked for compose and for encrypt.
- Import messages: duplicate (already in the store), expired, revoked, malformed, or missing encrypt/sign capability.

Encrypt fails

- Recipient expired or revoked.
- Recipient is public-only in a situation that requires something else (signing needs a secret key).
- Policy rejected a weak algorithm or size.
- No text in Text Task — empty boxes are not encrypted.

Decrypt fails

- Wrong **key passphrase** (not the vault password).
- File was not encrypted to any secret key in this vault.
- Input is not a valid OpenPGP message (clipboard decrypt says so if the block is wrong).
- Clear-sign verify needs the signed message **and** the signature section together.

Explorer encrypt/decrypt

- If the workstation is locked or the program is not running, you will be asked to sign in. That is expected.
- The Explorer window should appear in front; if you do not see it, use the taskbar.

Updates

- Manual or 30-day check needs Internet. If the check cannot reach the network, you are told there is no connection.

Still stuck

1. Note the exact message text.
2. Help → About: version, build date, machine code.
3. Settings → Key store: vault path.
4. Use **Support** (help desk site) or the Help file topic for that window.

License and machine code

Getting started → License and machine code

The first time you run NEXTGEN Widget Encrypt3 you may see an evaluation window. A paid license is locked to this computer with a machine code.

Where to find the machine code

- Help → About, then Copy
- %AppData%\NEXTGEN Widget Encrypt3\MachineCode.txt (same folder as the default vault)
- The short window that appears if the trial has ended (Copy machine code)

What it is

The machine code identifies this PC. It is not a password. You send it when you buy so the license will only run here.

During the trial

Copy the code from About or from MachineCode.txt. If the evaluation window has a Pay button, that only opens the purchase page. It does not show the machine code. Checkout asks for a machine-code, so please paste the code from About or the text file exactly as it is. If not done exactly as it is the license code will not work.

After the trial ends

A message appears and closes by itself. Click Copy machine code before it closes. If you miss that, open MachineCode.txt. The file is written every time the program starts, including after expiry. Open the Buy page, paste that code into the required box, and complete payment. You do not change the web address.

Important

The code in About and in MachineCode.txt may include + and =. Leave those characters in. Do not use anything from the Pay link.

Folder

%AppData%\NEXTGEN Widget Encrypt3\

Contains vault.ngw3 and MachineCode.txt unless you moved the vault in Settings.

What the license covers

A paid license is for **one computer**. It stays valid on that machine for as long as you keep using the software there. It is not a subscription. It does not move to a second PC while the first one is still in use.

Replacement license

If that Windows PC is lost, stolen, or replaced because of hardware failure, you may request **one replacement license** for a new machine.

- Ask within **12 months** of the original purchase.
- Send the **Stripe receipt** (order / payment email or Dashboard receipt) and the **machine code** from the new PC (Help → About or MachineCode.txt).
- The old license for the failed PC is retired. The new code is bound to the new machine only.

After 12 months, a new PC needs a new purchase. Reinstalling on the **same** machine (Windows reset, same hardware) does not use up the replacement; use the same machine code.

What we do not replace for free

A second household PC, a work laptop plus a home PC, or an upgrade you chose after the year is up. Those are additional licenses.

Using the program

[BACK TO HOME](#)



NEXTGEN Widget Encrypt3 — when OpenPGP security matters.

by NextGen Widget Software

Using the program

Sign in first. These topics are the work you do with keys and with files or text. The vault password and a key passphrase are not the same thing — start there.

1. [Two passwords](#)

The login password opens the vault. It is created on the login screen and is never stored as an OpenPGP secret.

Each secret key has its own passphrase, set when you compose or import that key. Decrypt, sign, revoke, and change-key-password all ask for the key passphrase.

The program cannot recover either password. A backup of the vault does not help if you have forgotten the login password that wraps it.

2. [Create your first key](#)

Keys → Compose key. Name is required; email is optional. Ed25519+X25519 is a sound default. Set the key passphrase and confirm it.

On a full license you may choose Never expire. On an evaluation license, Never expire is unavailable and Valid until cannot be more than 30 days from today.

If you created the key on this PC, you may mark it verified before you leave the form.

3. [Import a key](#)

Keys → Import. Yes opens a file (.asc, .pgp, or .gpg). No, or Import pasted key block, takes a full BEGIN PGP PUBLIC KEY BLOCK and/or BEGIN PGP PRIVATE KEY BLOCK. Both blocks in one paste become one key pair.

The program tells you if the key is already in the store, revoked, expired, or under 2048 bits. Weak keys are not imported. Check the fingerprint before you mark the key verified.

4. [Bulk import and the CSV template](#)

Keys → Bulk import / dry-run. You can add files, drop a folder, open a ZIP, or import a CSV. Run the dry-run and read the list before you write anything into the vault.

Keys → Save CSV import template writes the matching CSV. The armored column is the key block itself. Group and notes are stored on the key and show up in the grid.

5. [File Task](#)

File → File tasks.

- Encrypt file — pick the recipient. Output is a new file with a random name. The original stays where it is.
- Decrypt file — the next tab. Uses the secret key's passphrase and restores the original file name when the packet has it.
- Sign and encrypt — recipient plus signer.
- Decrypt and verify — says whether the signature is valid and which key signed.
An armor comment is optional. "Also encrypt to me" adds a second recipient you choose, on that same file, not a second file.

6. [Text Task](#)

Text → Text tasks. Tabs: Encrypt text, Decrypt text, Sign and encrypt, Decrypt / verify, Clear-text sign, Clear-text verify.

A blank box is not encrypted. Result boxes are yellow. Clear-text verify needs the whole block from BEGIN PGP SIGNED MESSAGE through END PGP SIGNATURE.

7. [Revoke, trash, and restore](#)

Keys → Revoke key needs the key passphrase and turns the row red immediately. A revoked or expired key cannot encrypt or sign. A secret key may still decrypt older files.

Create, export, or apply a revocation certificate when you need a certificate file instead of an immediate revoke.

Send to trash only hides the row. Open trash bucket to restore it. Trash is not revocation.

8. [Trust, fingerprint, and QR](#)

"Verified" means you checked the fingerprint. It is not set automatically on import.

Keys → Properties (or double-click) shows the full fingerprint. Keys → QR code shows the full public key so another person can compare it. Keys → Toggle trusted, or the grid right-click, sets or clears verified after that check.

Two passwords

Using the program — Two passwords

Encrypt3 never uses a single password for everything. Mixing them up is the usual reason decrypt or sign-in fails.

Vault login

- Created with **Create account**.
- Changed with **Change login password**.
- Unlocks the .ngw3 vault: every key row, settings, groups, audit.
- Used on the **sign-in** window and the **idle lock** screen.
- Minimum **eight** characters; confirm when you set it.
- Three wrong entries at sign-in and the program exits.

If you forget this password, the vault file cannot be opened. A backup of the .ngw3 without the login is not usable.

Key passphrase

- Set when you **Compose** a key or when you **Change key password**.
- Unlocks **one** secret key: decrypt and sign.
- Asked for in File Task, Folder Task, Text Task, clipboard decrypt, and some key operations (extend expiry, revoke, export secret).
- Each secret key can have a different passphrase.
- Public-only keys have no passphrase prompt for decrypt/sign because they cannot do those jobs.

Same characters, two locks

You may type the same string for both. The program still stores them separately. Changing the login does **not** change key passphrases. Changing a key passphrase does **not** change the login.

What to type where

Window	Password to use
Sign-in / lock	Vault login
Create account	New vault login
Change login password	Old vault login, then new vault login
Compose key	New key passphrase
Change key password	Old key passphrase, then new key passphrase
Decrypt / sign / sign-and-encrypt / clear-sign	That key's passphrase

Typical mistakes

- Decrypt dialog: typed the vault login.
- Sign-in: typed a key passphrase.
- Imported a **public** key and expected a passphrase prompt to decrypt.
- Two secret keys: used key A's password on a file encrypted to key B.

After a good first test

Write down (offline) that there are two secrets, and which one opens the vault. Do not store either in the audit log or in a screenshot of the welcome bar.

Create your first key

Using the program — Create your first key

Where: Keys → **Compose key**.

This builds a new OpenPGP key and stores it in the vault. It is not the vault login.

Before you start

- You are signed in.

- Evaluation copy: the key **must expire within 30 days**. Never expire is off.
- Licensed copy: Never expire is allowed.
- RSA **1024** is blocked.

Steps

1. Open **Compose key**.
2. **Name** — required (this becomes the user ID).
3. **Email** — optional; use it if you will look the key up by address.
4. **Algorithm** — for a first key use **Ed25519+X25519** or **RSA 3072**.
Also available: RSA other allowed sizes, DSA+ElGamal, ECDSA+ECDH (including NIST / Brainpool curves the form lists).
5. **Key size** — only where the algorithm needs it (RSA). Prefer 3072 or 4096, not 1024.
6. **Hash, cipher, compression** — defaults are appropriate (typically SHA512, AES-256, ZIP). Change them only if you must match someone else.
7. **Valid until** — pick a date, or Never expire if the license allows it.
8. **Passphrase** — at least eight characters, then confirm.
Optional: **Generate password**, set length, use the strength meter.
Optional: **Show password / Show generated password**.
9. Optional: **Mark as verified** if this is your own key and you accept the fingerprint you are about to create.
10. Choose **Create**. Large RSA can take a long time; leave the window open.
11. Close Compose. The key store shows a new row (public and secret).

After Create

1. Select the row → **Properties**. Check name, email, Key ID hex, fingerprint, algorithm, size, created, valid until, public/secret.
2. Optional: **QR** (full public key) or **ceremony sheet** if someone else must confirm the fingerprint.
3. Run **Encrypt a test file** to this key and decrypt it on the same PC.

If Create fails

- Name empty.
- Passwords do not match or shorter than eight characters.
- Evaluation: date beyond 30 days or Never expire still selected.
- 1024 or another blocked size.
- You walked away and idle lock closed the window — sign in and compose again (unfinished compose is discarded).

Next

Export the **public** key if others will encrypt to you. Keep the secret key in the vault; export secret only to a safe backup you control.

Import a key

Using the program — Import a key

Where: Keys → Import, Import key block / clipboard, or Bulk import (separate topic).

Use import when the key already exists (yours from another program, or someone else's public key).

What you can import

- .asc, .pgp, .gpg files
- ASCII blocks:

text

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
-----BEGIN PGP PRIVATE KEY BLOCK-----
```

Public and secret may be in one paste; the store accepts what is valid. RSA **1024** is not imported for encrypt use; you are told it is obsolete.

Import from a file

1. Keys → Import (or Import file).
2. Choose the key file.
3. Read the result: how many keys imported, or why a key was skipped.
4. Find the new row; open **Properties** and check the fingerprint.

Import from a block or clipboard

1. Copy the **entire** block, including BEGIN and END lines.
2. Open **Import key block** (or Import from clipboard).
3. Paste and import.
4. "Zero key(s) imported" means the paste was incomplete, already in the store, or not OpenPGP key material.

Do not put a BEGIN PGP MESSAGE here. That is ciphertext; use File Task or Text Task.

What the program checks

- **Duplicate fingerprint** — already in the store; you are told it is a duplicate.
- **Expired** — imported or skipped per the message; do not encrypt to it.
- **Revoked** — same; row will be red if it is stored.
- **Weak / 1024** — blocked for encryption use; you get a policy message.
- **Malformed user ID** — warning.
- **Public only vs secret** — Properties and the grid show whether private material is present.

After import

1. Compare the **fingerprint** with the owner (Properties or QR).

2. Set **Verified** only after that check. Import does not mean verified.
3. If you imported **your** secret key, test decrypt of a file encrypted to it.
4. Assign a **group** if you use groups.

If it fails

- Wrong file (a message file, not a key).
- Only the public half when you needed the secret.
- Key already in the store under a user ID you did not recognize (read the message; the “name” may be the user ID string).
- Idle lock closed the import window — paste again after sign-in.

Bulk import and the CSV template

Using the program — Bulk import and the CSV template

Where: Keys → **Bulk import** (or Tools, same window).

Use this when you have many keys. Use single **Import a key** when you have one file or one paste.

What you can feed it

- One or more .asc, .pgp, .gpg files
- A folder (scan; drag-and-drop onto the bulk window if enabled)
- A **ZIP** of those files (the zip is checked before keys are stored)
- A **CSV** that matches the template

CSV template

The template ships in the Help folder:

Help\ngwe3-bulk-import-template.csv

Copy it, keep the header row, add one key per line.

Typical columns:

- **name** — label in the sheet (does not replace the user ID inside the key)
- **email** — optional
- **file path** — full path to an .asc / .pgp / .gpg on disk
- **armored** — the full BEGIN PGP ... KEY BLOCK text when you are not using a file path
- **group** — stored on the key if import applies groups (e.g. Financial)
- **notes** — stored as notes when the importer supports notes
- **armored (flag)** — whether the armored column is used

Use **either** a file path **or** an armored block. A path with no file fails that row. An armored column must include the complete block, not a truncated line. Group and notes are extra data in the vault; they are not written into the OpenPGP key itself.

Dry-run

1. Add files, folder, zip, or CSV.
2. Run **dry-run** (preview) **before** import.
3. Read each row: import, skip duplicate, expired, revoked, weak algorithm, missing encrypt or sign capability, public-only vs secret, malformed.
4. Only then run the real import.

Dry-run does not change the key store.

After import

- Duplicates stay skipped.
- Open the grid, filter by group if you set one.
- Verify fingerprints before **Verified**.
- Weak/1024 keys are not used for encrypt even if a row appears.

If it fails

- CSV: armored text not recognized — put the whole block in the armored column, or use a file path instead.
- Many skipped, one duplicate — those keys are already in the store or failed a check; read the status column.
- ZIP invalid — use a clean zip of key files only.
- IO error on a path — the file moved or the path in the CSV is wrong.

Next

Recipient groups if you used the group column. **Encrypt a test file** to one imported public key only after you check the fingerprint.

File Task

Using the program — File Task

Where: File → File Task.

Work on **one file** at a time. Folders are Folder Task. Explorer right-click is separate.

Tabs

Use them in this order on the window: **Encrypt file**, **Decrypt file**, then **Sign and encrypt**, **Decrypt and verify**.

Encrypt file

1. Choose the **input file**.
2. Choose the **recipient** (public key, not expired, not revoked, not a blocked 1024-bit key).

3. Optional: **ASCII armor** for a text-style OpenPGP file.
4. Optional: **Armor comment** — only used when armor is on; leave blank to omit the Comment header.
5. Optional: **Also encrypt to me (recovery copy)** — turn it on and pick the **second** key (your recovery key). Both keys can decrypt the **same** output file. It is not a second file on disk. If you leave it off, only the recipient can decrypt.
6. Encrypt. Save the output. The name is a **generated** name (not the original filename).

The armored Version header is this product name.

Decrypt file

1. Open **Decrypt file** (next to Encrypt file).
2. Choose the ciphertext.
3. Enter the **key passphrase** for a secret key that is a recipient of that file.
4. Save. The program restores the **original file name and extension**.

Sign and encrypt

Same as encrypt, plus a **signer** (secret key, not revoked). Enter the signer's passphrase. Armor comment and recovery copy work as on Encrypt. Output name is generated.

Decrypt and verify

Opens a signed-and-encrypted file. Enter the recipient passphrase. You get the file back and a signature result: valid or not, which key signed, expired/revoked/altered if the program can tell.

Recovery copy

- Recipient = who you send the file to (their public key).
- Recovery = a second public key **you** choose, usually one of your secret keys in this vault.
- Preview must list **two different** keys when recovery is on. If both lines show the same key, pick a different recovery key.
- To open the file later without the recipient's secret key, decrypt with **your** recovery secret key and its passphrase.

If it fails

- Policy / 1024 — choose another key.
- Expired or revoked recipient or signer.
- Wrong passphrase (key, not vault).
- Decrypt of a file encrypted only to someone else, with recovery off.
- Armor comment sitting under another control — still type in the comment box if it is on the Encrypt or Sign-and-encrypt tab.

Next

Folder Task for directories. **Explorer Encrypt and Decrypt** for right-click. Always test decrypt once when you first use recovery.

Text Task

Using the program — Text Task

Where: Text → Text Task.

OpenPGP for **text in boxes**, not files. Yellow boxes are output.

Tabs

Encrypt text | Decrypt text | Sign and encrypt text | Decrypt/verify text | Clear-sign | Verify clear-sign

Rules for every tab

- Do not encrypt an empty box; you get a notice and nothing is produced.
 - Recipients and signers must not be expired or revoked.
 - Signing needs a **secret** key and that key's passphrase.
 - Optional armor comment: used when the tab builds a BEGIN PGP MESSAGE (or signed message). Blank = no Comment header. Version is this product name.
-

Encrypt text

1. Paste or type plaintext.
2. Choose recipient.
3. Optional comment.
4. Encrypt.
5. Copy the yellow BEGIN PGP MESSAGE block.

Decrypt text

1. Open **Decrypt text** (beside Encrypt text).
2. Paste output from **Encrypt text** only (not sign-and-encrypt).
3. Enter the secret-key passphrase.
4. Decrypt and read the yellow plaintext.

Sign and encrypt text

1. Plaintext.
2. Recipient + signer (signer has secret material, not revoked).
3. Signer passphrase.
4. Optional comment.
5. Copy the resulting message.

Decrypt/verify text

1. Paste the sign-and-encrypt block.
2. Recipient secret passphrase.

3. Decrypt/verify.

Read both the text and the signature line (valid, signer, expired/revoked/changed).

Clear-sign

1. Type the readable text.
2. Signer + passphrase.
3. Generate. Copy **from** BEGIN PGP SIGNED MESSAGE **through** END PGP SIGNATURE, including the text in the middle.

Verify clear-sign

1. Paste that **entire** signed message.
2. Verify.

If you paste only the signature, verify reports no signature or invalid.

Grid shortcut

Right-click a key → encrypt or decrypt **clipboard**. Decrypt checks for a real OpenPGP block. Use Text Task when you need tabs or a comment.

If it fails

Wrong tab, truncated paste, vault password typed instead of key passphrase, revoked signer, or empty source.

Revoke, trash, and restore

Using the program — Revoke, trash, and restore

Where: key store selection, then **Keys** → **Revoke**, **Trash**, or **Trash** window.

Revoke and trash are different. Revoke is a cryptographic “do not use this key.” Trash hides a row in the vault until you restore or delete it.

Revoke

Use revoke when **your** secret key must never sign or be used as a recipient again (lost passphrase policy, key replaced, compromise).

1. Select the key (it must include secret material for a self-revocation).
2. Keys → **Revoke**.
3. Enter that key's passphrase if asked.
4. Confirm. The row turns **red**.

A revoked key must not be chosen as signer or encrypt recipient. Decrypt with the secret may still be possible so old files can be opened.

Revocation certificate

If you saved a revocation certificate when the key was created:

1. Keep that certificate offline.
2. When you need it, use the command to **apply the revocation certificate** to that key (Keys menu on the selected key).
3. The store should then show the key as revoked (red).

Applying a certificate you did not create for that fingerprint will fail.

Trash

1. Select a key you want off the live grid but not destroyed.
2. Send it to **Trash**.
3. Open the **Trash** window to see those keys.
4. **Restore** puts the row back in the key store.
5. Permanent delete from Trash cannot be undone from the grid.

Trash is not a revocation. A trashed key that was valid is still valid if restored.

Colors on the live grid

- **Red** — revoked
- **Purple** — expired
- **Normal** — in date and not revoked

Expired and revoked are not the same color and not the same action.

If it fails

- No secret key — you cannot self-revoke someone else's public key.
- Revoked key still offered as signer in Text Task — do not use it; pick another signer.
- You revoked by mistake — you cannot “un-revoke.” Compose or import a new key and tell people the new fingerprint.

Next

Export a fresh **public** key for the replacement. Update recipient groups so they do not point at the revoked row.

Trust, fingerprint, and QR

Using the program — Trust, fingerprint, and QR

Where: select a key → **Properties**, **QR**, right-click **Verified**, or **Keys** menu.

Import only means “this key is in the vault.” **Verified** means you compared the fingerprint with the owner.

Fingerprint

1. Select the key.
2. Open **Properties**.
3. Read the full fingerprint (long hex), user IDs, created, valid until, algorithm, size, public vs secret, capabilities, revoked/expired.

Compare that fingerprint with what the owner shows you (in person, known-good channel, or their ceremony sheet). Do not trust a fingerprint that arrived in the same email as the key file alone.

Mark Verified

1. After the fingerprints match, right-click the row → set **Verified** (or use the trust command on the form).
2. The grid trust column should show verified, not only “imported.”

Clear or leave unverified if you have not checked. Group filters do not change trust.

QR

1. Keys → **QR** (or the QR command on the selected key).
2. The code contains the **full public key**, not only a short ID.
3. The other person scans or compares; they still should read the fingerprint in Properties.

QR is for public material. Do not put a secret key in a QR you will display.

Ceremony sheet

Key ceremony sheet prints user ID, key ID, fingerprint, algorithm, and dates with two operator sign-off lines. Use it when two people confirm a fingerprint. Print one key or print a **group**.

If it fails

- QR too dense on a small screen — use Properties fingerprint instead.
- Two keys with similar names — match **Key ID hex** and fingerprint, not the display name only.
- “Unverified” cut off on the grid — widen the column; the value is still stored.

Next

Encrypt only to keys you have verified when the data matters. Unverified public keys are fine for a first connectivity test, not for secrets.

Vault and settings

[BACK TO HOME](#)



NEXTGEN Widget Encrypt3 — when OpenPGP security matters.

by NextGen Widget Software

Vault and settings

One encrypted .ngw3 file holds the accounts, the keys, the settings, and the audit log. These topics are where that file lives, how you copy it, and the options that sit next to the grid.

1. [Backup the vault](#)

Key store → Backup vault. A backup is a copy of vault.ngw3. The same username and login password open it.

Copy vault backup writes one file where you choose. Keep a second copy that is not on the same disk.

Restore test only checks that the file has a valid vault header. It does not replace the live vault. To restore, close the program and put that file in place, or point Settings at it.

Scheduled backup runs only while you are signed in. If the program is closed or locked at the scheduled time, that slot waits until the next time you are signed in.

2. [Move the vault](#)

Settings → Key store shows the current path. The default is %AppData%\NEXTGEN Widget Encrypt3\vault.ngw3.

Browse to a new location and save. The new path is stored for the next start. Sign in against that file with the same login password. MachineCode.txt stays in the default folder even if you move the vault.

3. [Watch folder](#)

Operations → Watch folder. Choose the inbox, the output folder, and the private key that will encrypt. An optional recipient group adds those members as extra recipients. Turn it on and save.

Only files are encrypted. A folder dropped in the inbox is ignored. Stay signed in. Finished originals move to Processed. A file that cannot be encrypted moves to Failed with a short error note. The audit log records which key was used.

4. [Recipient groups and the grid filter](#)

Operations → Recipient groups. Type a name (financial, technical, sales), check the member keys, and save. The name box clears after a successful add, and you are told the members were saved. The filter above the grid lists those names. Matching is by keyword and is not case-sensitive. The same group can be selected in Watch folder.

5. [Explorer encrypt and decrypt](#)

Operations → Windows Explorer integration registers Encrypt and Decrypt on the Windows right-click menu.

If this program is already signed in, Explorer uses that session. You are not asked to log in again. The task window is brought to the front. Armor is on that encrypt dialog. Decrypt keeps the original file name when the packet contains it.

6. [Update](#)

Settings → Software update and license.

Authorize checking every 30 days, and you get a confirmation that the choice was saved. Check for update runs now. If there is no internet connection, you are told. If the version on the server is newer, you are notified at the next login. If it is not newer, nothing is shown.

Backup the vault

Vault and settings — Backup the vault

Where: **Key store** → **Backup vault**. The live file path is shown there and under **Settings** → **Key store**.

The vault file (.ngw3) is the database: keys, logins, groups, settings, audit. Exporting one public key is not a vault backup.

Find the file

1. Settings → Key store, or the “Current vault” box on Backup vault.
2. Read the path (default %AppData%\NEXTGEN Widget Encrypt3\vault.ngw3).
3. That is the file you must copy.

Make a backup (manual)

1. Key store → Backup vault → **Copy vault backup**. Choose where to save the .ngw3.
2. Or exit or lock Encrypt3, then copy the .ngw3 in Explorer.
3. Store the copy offline (other disk or USB, not only the same PC).
4. The copy is still encrypted. You need the vault login from the day you made the copy.

Back up after you compose, import, revoke, or add an administrator.

Scheduled (automatic) backup

Same page: **Scheduled backup**. Off until you turn it on.

1. Check **Create automatic backups while signed in**.
2. Browse to a folder that is not only the AppData vault folder.
3. Choose **Daily**, **Weekly** (weekday list appears), or **Monthly** (day 1–28 appears).
4. Set the time (24-hour).
5. **Keep last N** files. Names look like vault-20260920-1800.ngw3. Older copies in that folder are removed.
6. Click **Save schedule**.

The copy runs only while Encrypt3 is **signed in**. If the day and time pass while the program is closed or locked, that slot is skipped until you sign in after that time; then one copy is made. Failures go to the audit log. This is still a file copy of the encrypted vault — it does not store the login password next to the backup.

Restore test

On Backup vault, **Restore test** only checks that the file has a valid vault header. It does not replace the live vault.

Restore

1. Close Encrypt3.
2. Replace the current vault file with the backup, **or** in Settings → Key store point the path at the backup .ngw3.
3. Start Encrypt3 and sign in with the username and password that were in force when that backup was made.
4. Confirm Settings → Key store still points at the file you meant.
5. Open the grid and check key count and a known fingerprint.

Test restore before a disaster, using a spare copy, not your only backup.

Move vs backup

Change location copies the live vault to a new path and remembers it. That is not a dated backup. Keep a separate dated copy anyway. Scheduled backups are dated copies; moving the vault is not.

If it fails

- Restored an old .ngw2 or a key .asc by mistake — those are not this vault format.
- Wrong password on a good backup — that is the vault login from the day you made the copy.
- Copied the exe but not the .ngw3 — the program on another PC starts empty or points at a different path.
- Expected Friday's automatic copy but the program was not signed in at that time — sign in and wait for the next check, or use **Copy vault backup** once.

Next

Move the vault if you only want a new working path. Two passwords if you are unsure which password opens a backup.

Move the vault

Vault and settings — Move the vault

Where: Settings → Key store → Change location.

Use this when the working .ngw3 should live on another drive or folder. This is not a dated backup.

Steps

1. Sign in.
2. Settings → **Key store**.
3. Note the current path.
4. Choose **Change location**.
5. Pick the new folder and file name. The filter is *.ngw3.
6. The program **copies** the vault to that path and saves the path in the application config.
7. Confirm the text box shows the new path.
8. You should see a success notice.

After a move

- Sign out and sign in once to be sure the new file opens.

- Keep the old file only until you have confirmed the new one. Then you may delete or archive the old copy.
- Explorer shortcuts and Watch folder paths do not move by themselves.

Do not

- Edit the path box by hand and expect the file to follow. Use **Change location**.
- Store the only copy on a USB stick you will misplace.
- Point two PCs at the same file on a share unless you know only one person will write it at a time (this vault is not a multi-writer server).

If it fails

- No write permission on the destination.
- Disk full.
- You cancelled the save dialog — the old path remains in use.

Next

Backup the vault for a dated extra copy after the move.

Watch folder

Vault and settings — Watch folder

Where: Tools or Settings → **Watch folder**.

Drop **files** into an inbox folder. Encrypt3 encrypts them to a key **you select** and writes the ciphertext to an output folder. It does not encrypt folders you drop in.

Set it up

1. Open **Watch folder**.
2. Choose the **inbox** folder (example: Watch folder In).
3. Choose the **output** folder (example: Watch folder Out).
4. Select the **key used to encrypt**. Pick a key you can decrypt later (it should have secret material in this vault), not a random grid row.
5. Optional: recipient **group** name.
6. Save. You should see that settings were stored.

Leave Encrypt3 running (or at least signed in, not locked) so the watcher can work.

What happens

- You copy a finished file into the inbox.
- The watcher waits until the file is done growing, then encrypts to the selected key.
- Success: ciphertext in the **output** folder.
- The original is moved to **Processed** under the inbox.

- Failure: file goes to **Failed** under the inbox.

Decrypt

Use **File Task** → **Decrypt file** on the output file. Enter the passphrase for the secret key you chose in Watch folder.

Do not expect

- Subfolders dropped in the inbox to be packed as a tree (files only).
- Encryption if the program is closed or the session is locked.
- A mystery recipient — if you did not pick a key, you will not know what opens the files. Always set the key.

If it fails

- First file worked, later files went to Failed — the file was still being written, or the key/policy rejected it. Leave the file alone until the copy finishes.
- No key selected — set one and Save.
- Inbox and output are the same folder — use two different folders.
- Idle lock — unlock, then drop the file again.

Next

File Task for one-off files. **Recipient groups** if you filter by group instead of one key.

Recipient groups and the grid filter

Vault and settings — Recipient groups and the grid filter

Where: **Tools** → **Recipient groups**, and the **group** list above the key store grid.

Groups are labels in the vault (Financial, Technical, Sales). They are not OpenPGP user IDs.

Create a group

1. Open **Recipient groups**.
2. Type a group name.
3. Choose **Add**. The name box should **clear**.
4. Select the group.
5. Check the keys that belong in it.
6. Choose **Save members**. You should see a notice that members were saved.
7. Repeat for more groups.

Names are **not** case-sensitive (sales and Sales are the same idea). Use plain words you will recognize in the filter.

Filter the grid

On the key store:

- **All groups** — every key
- **Ungrouped** — keys with no group
- A named group — only members

Find / Cancel search is separate. Search looks at text in the grid; the group list limits which rows are candidates.

Both groups can exist on the groups page even if only one showed in the filter until you saved members and reopened the filter — Save members, then look at the filter list again.

CSV import

Bulk import can set a **group** column. That is the same kind of label as here.

If it fails

- Added a group but it is missing from the filter — Save members and reopen the key store or the filter list.
- Name still in the add box — Add should clear it; delete leftover text before Add again.
- Expected grouping by algorithm — groups are only the names you create, not automatic keywords inside the key.

Next

Meet the **key store** for colors and Find. **Watch folder** if you also set an optional group there.

Explorer Encrypt and Decrypt

Vault and settings — Explorer Encrypt and Decrypt

Where: Settings → Security → Windows Explorer, then right-click in File Explorer.

Turn it on

1. Settings → **Security**.
2. In **Windows Explorer**, check **Add Encrypt / Decrypt to the right-click menu (this user)**.
3. That writes verbs for your Windows account only.

Uncheck the box to remove the verbs.

Encrypt from Explorer

1. Right-click a file.
2. Choose Encrypt with NEXTGEN Widget Encrypt3.
3. If Encrypt3 is not running or the workstation is **locked**, sign in. If you are already signed in and unlocked, you should not have to sign in again.

4. The encrypt window should appear **in front**. Pick recipient, optional **armor**, optional comment if shown.
5. Finish. Output uses a generated name. Armor on or off follows that prompt.

Decrypt from Explorer

1. Right-click the ciphertext.
2. Choose Decrypt.
3. Sign in if locked.
4. Enter the **key passphrase**.
5. Output should keep a usable original name and extension when the tool can recover them.

If Encrypt3 is already open

One copy of the program should own the session. Explorer forwards the file to that session when it can. If the session is locked, unlock or sign in there first.

If it fails

- No verbs — turn the Settings box on again; use the same Windows user.
- Window behind everything — use the taskbar; current builds keep it topmost.
- Asked to sign in while you are already in the app — the other window is locked or is a second instance.
- .bin output — older behavior; use a current build so decrypt restores the real extension.
- Armor missing on the prompt — use File Task if you need armor on that file.

Next

File Task for sign-and-encrypt and recovery copy. **Idle lock** if Explorer keeps hitting the lock screen.

Updates

Vault and settings — Updates

Where: Settings → Software update & license.

The program compares this build's version to a one-line text file on the update host:

<https://www.ngwidgetsoftware.com/patches/VersionUpdate3.txt>

(or the host you configured for Encrypt3). The file contains only the newest version, for example v1.0.0.2.

Automatic check

1. Check **Authorize checking for an update every 30 days**.
2. You should see a confirmation that automatic checks are **on** (or **off** if you uncheck).
3. After a successful sign-in, when 30 days have passed since the last **successful** check, the main window can notify you.
4. If the server version is newer, you get both version numbers. If you are current, there is no notice.
5. If there is no Internet at that moment, you are told there is no connection.

Opening Settings does not show that confirmation; only changing the box does.

Manual check

1. Choose **Check for update**.
2. The program checks Internet first, then reads the version file.
3. You are told: new version, already current, no Internet, or the file could not be read.

The button does not freeze the window; wait for the message.

License button

License on the same tab is for the license / evaluation dialog, not for downloading a new exe.

If it fails

- No .config next to the exe can break other features; it is not a substitute for this check.
- Firewall or offline PC — use the manual button when you have a network.
- You never see a 30-day balloon — the box is off, or 30 days have not passed since a successful check.

Next

Download a new zip from your product site when a newer version is announced. Keep NextGenWidgetEncrypt3.exe.config beside the new exe. **Licensing** if you also need the machine code from About.

Keys and operations

[BACK TO HOME](#)



NEXTGEN Widget Encrypt3 — when OpenPGP security matters.

by NextGen Widget Software

Keys and operations

These four topics sit on the Operations and Key store menus. They do not create the key. They look one up, watch its dates, print a fingerprint check, or show what the vault has recorded.

1. [Keyserver and WKD lookup](#)

Operations → Keyserver / WKD lookup. Lookup checks for a network connection first. If there is none, it stops and tells you.

Otherwise it searches keys.openpgp.org, keyserver.ubuntu.com, and pgp.mit.edu. If you entered an email address, it also tries WKD. Import only after you have compared the fingerprint.

2. [Expiration dashboard](#)

Operations → Expiration dashboard. Filter by 30, 60, or 90 days, by expired, by never expires, by revoked, or show all. Each row shows the name and the Key ID (hex), so a key with no name is still identifiable.

Extend selected needs the private-key passphrase. A revoked key cannot be extended. Expired rows are purple in the main grid; revoked rows are red.

3. [Key ceremony sheet](#)

Operations → Key ceremony sheet. Print the selected key, or print every key in a group.

The sheet is for two people to compare the fingerprint on paper and tick Match. Printing does not mark the key verified. You set verified yourself after the check, from the grid or from Keys → Toggle trusted.

4. [Audit log](#)

Key store → Audit log. The vault keeps the newest 5,000 events, including failed sign-ins and watch-folder encrypts. Filter by person. Export CSV, JSON, or CEF. Clearing the failed-attempt line on the welcome bar does not remove these rows.

Keyserver and WKD lookup

Keys and operations — Keyserver and WKD lookup

Where: Tools → **Lookup** (keyserver / WKD).

This finds **public** keys on the network. It does not upload your secret key.

Servers

The Lookup window can query:

- **WKD** (Web Key Directory) for an email's domain
- keys.openpgp.org
- keyserver.ubuntu.com
- pgp.mit.edu
- keys.mailvelope.com

One server may miss a key another has. Try a second server if the first returns nothing.

Steps

1. Open **Lookup**.
2. Enter an **email** or key id as the form requires.
3. Choose a server (or WKD).
4. Choose **Lookup**. The program **checks Internet first** (ping to 8.8.8.8 / Google).
5. If there is no network, you are told to connect and try again.
6. If keys are listed, select one, inspect the fingerprint, then import.
7. Compare the fingerprint again in **Properties**. Set **Verified** only after that.

If it fails

- No Internet — connect, then Lookup again.
- No result on keys.openpgp.org — try Ubuntu or MIT.
- WKD empty — that domain does not publish WKD, or the address is wrong.
- Imported a key you have not checked — treat it as unverified.

Next

Trust, fingerprint, and QR. Import a key if you already have a file and do not need a server.

Expiration dashboard

Keys and operations — Expiration dashboard

Where: Tools → Expiration dashboard .

This list is for **lifecycle**: what is expiring, expired, or revoked — including rows with **no username**. Those rows still show **Key ID (hex)** so you can find them on the grid.

What you see

- Keys with an end date (soon or already past)
- **Revoked** keys (red on the main grid)
- Keys that **never** expire, if that group is shown so you can see they have no date

Expired on the grid is **purple**. Revoked is **red**. The dashboard is not only “dates in the next month.”

What to do

1. Open the dashboard.
2. Identify the key by name or Key ID hex.
3. On the key store, select that key.
4. If you still use it and you have the **secret** key, **extend expiration** (Keys menu) and enter the key passphrase.
5. If it should die, stop encrypting to it; revoke it if it is yours.
6. Update recipient groups so jobs and Watch folder do not point at a dead key.

If it fails

- Cannot extend — no secret key, or passphrase wrong.
- Evaluation copy — new/extended dates may still be capped at 30 days from now.
- You only looked at names — use Key ID hex when the user ID is empty.

Next

Revoke, trash, and restore. Policy notes for 1024 and evaluation caps.

Key ceremony sheet

Keys and operations — Key ceremony sheet

Where: Tools → Key ceremony sheet (or Keys, selected key).

A ceremony sheet is a **printable record** so two people can confirm a fingerprint. It is not a CA certificate and not a substitute for Properties.

What is on the sheet

- Product title and copyright line

- User ID
- Key ID
- Fingerprint
- Algorithm and size
- Created / valid until
- Two operator lines: name, date, fingerprint-match checkbox
- A bar at the bottom of the page

QR in the program is separate; print the sheet when you need ink-on-paper sign-off.

Print one key

1. Select the key in the store.
2. Open the ceremony sheet.
3. Confirm the fingerprint matches Properties.
4. Print.

Print many / by group

Use the sheet command that prints **all keys** or only a **group**. That is the right path when you have more than one key to check. Do not print one-at-a-time if you have a full group to inventory.

How to use it

1. Two operators each compare the printed fingerprint to the owner's copy.
2. Tick the match box and sign.
3. File the paper with your key procedures.
4. Only then set **Verified** in the store if your process says so.

If it fails

- Empty user ID on the sheet — use Key ID and fingerprint; the name may be blank.
- Brackets wrapping oddly — use a current build; the footer bar should sit at the bottom.
- Need the public key in a phone — use **QR**, not the ceremony sheet.

Next

Trust, fingerprint, and QR. Recipient groups if you print by group.

Audit log

Keys and operations — Audit log

Where: Tools → Audit log.

The log is a short history stored **in the vault**: sign-in failures and other store events. It is not a Windows Event Log and not a SIEM export.

What you should see

- Failed sign-in attempts (wrong username or password)
- After you sign in correctly, the **welcome bar** also reports failures since the last good login
- Other vault actions the build records (imports, backup, settings), if those lines appear in your version

An authorized user who mistyped the password can still see those failures after a good sign-in so they know someone tried the lock.

What you will not see

- Key passphrases or vault passwords
- Full decrypted message text
- A guaranteed multi-year archive

If the log looks empty after two bad passwords, sign in with the **correct** account and open the log again; older bugs missed the write until that path was fixed.

How long it is kept

Entries live with the vault file. Treat the log as **limited history** on this PC, not a compliance archive. A vault backup includes whatever the log held at backup time. Moving the vault moves the log. Clearing or rotating is only what this build offers in that window (if there is no Clear button, the log just grows with the vault).

If it fails

- No lines for failures — update to a build that writes FailLog into the vault on a bad attempt, then test two wrong passwords and one good one.
- Wrong vault file — Settings → Key store path.

Next

Two passwords. **Licensing** does not use this log. Do not paste log screenshots that include user IDs you do not want in a ticket.

Product

[BACK TO HOME](#)



NEXTGEN Widget Encrypt3 — when OpenPGP security matters.

by NextGen Widget Software

Product

What this build is, what the license allows, and the short reference topics. Step-by-step encrypt and key work stay under Using the program and Keys and operations.

1. [Licensing](#)
The license window runs before the login screen. An evaluation license may continue while days remain. After it expires, the program tells you and exits.
The only feature limit on an evaluation copy is key lifetime: Never expire is off, and a new key cannot be valid more than 30 days. A full license removes that cap.
Help → About shows the machine code for this PC. A paid license is for that machine.
MachineCode.txt in %AppData%\NEXTGEN Widget Encrypt3\ holds the same code.
2. [Policy notes](#)
Keys under 2048 bits are obsolete and are blocked for compose, import, and encrypt.
Revoked keys (red) and expired keys (purple) cannot encrypt or sign. A matching secret key may still decrypt.
Optional policy can also refuse a recipient you have not marked verified.
The trial is the time to decide. After a license key is emailed, the purchase is final. See **No refund policy**.
3. [Menu map](#)

- File — File tasks (encrypt, decrypt, sign and encrypt, decrypt and verify).
 - Folder — Folder tasks.
 - Text — Text tasks.
 - Keys — compose, import, import pasted block, bulk import, CSV template, export, properties, QR, trust, key password, revoke, revocation certificate, trash.
 - Operations — expiration dashboard, recipient groups, watch folder, key ceremony sheet, keyserver / WKD lookup, PGP/MIME email, Windows Explorer.
 - Key store — backup vault, audit log.
 - Lock — lock workstation, clear failed-attempt notice, administrators (maximum 5).
 - Settings — key store path, idle lock, software update.
 - Help — this help file, support (<https://www.ngwidgetsoftware.com/helpdesk/>), About.
4. [System requirements](#)
Windows with .NET Framework 4.8.1. The folder you run must contain NextGenWidgetEncrypt3.exe and NextGenWidgetEncrypt3.exe.config. An internet connection is required only for keyserver lookup, update checks, and the help desk. Encrypt and decrypt work offline.
 5. [Keyboard and windows](#)
The main window and the task windows are fixed size. Maximize is off.
Idle lock and Lock workstation close every open task window before the login screen returns, so a compose or encrypt form is not left visible behind the lock.
On the grid, Find is beside the search box. Right-click a key for copy public key, set or clear verified, and encrypt or decrypt the clipboard.
 6. [Uninstall](#)
Remove the program folder you copied the executable into.
That does not delete the vault. Keys and account passwords remain in %AppData%\NEXTGEN Widget Encrypt3\vault.ngw3 until you delete that file yourself. Deleting it is permanent. Export or back up first if you still need the keys.
MachineCode.txt in that same folder can stay or be deleted; it is not the license key.
 7. [Glossary](#)
 - Vault — the .ngw3 file. Login password.
 - Key passphrase — the secret on one OpenPGP key.
 - Key ID (hex) — short id shown in the grid.
 - Fingerprint — the full id you compare before you trust a key.
 - Verified — you checked that fingerprint.
 - Armored — ASCII BEGIN PGP text. Binary export is .pgp.
 - Recovery copy — a second recipient on the same encrypted file, not a second file.
 - Revoked — key must not be used to encrypt or sign. Red in the grid.
 - Expired — past Valid until. Purple in the grid. Decrypt of old files is still allowed with the secret key.
 8. [Disclaimer](#)
This help file describes how NEXTGEN Widget Encrypt3 behaves. It is not legal advice and it is not a promise that a third party's OpenPGP software will accept every option you select.
You are responsible for the login password, each key passphrase, and for checking fingerprints before you mark a key verified. The publisher cannot recover a forgotten vault password or a forgotten key passphrase.
Copyright 2026 NextGen Widget Software. All rights reserved.

Licensing

Product — Licensing

Where: the start-up evaluation / license window, **Help** → **Buy license**, **Help** → **Enter license**, **Settings** → **Software update & license** → **License**, and **Help** → **About**.

Evaluation

On first runs the evaluation window appears. **Continue Evaluation** uses the trial. If the trial is expired, leaving the window ends the program.

Evaluation limits new composed keys to 30 days. **Never expire** is disabled until the copy is licensed.

Closing the window with X while the trial is still valid is the same as **Continue Evaluation**. When the trial is already expired, X does not unlock the program.

Buy license (2Checkout)

Help → **Buy license** opens the 2Checkout order page for this product. The same page opens from **Pay** on the evaluation window.

This PC's machine code is already in the **Machine Code** box on that page. You do not paste it yourself. Do not edit the link. Characters such as + and = are already encoded.

The same link is written at the bottom of MachineCode.txt, in the same folder as the default vault:

%AppData%\NEXTGEN Widget Encrypt3\MachineCode.txt

That file is written every time the program starts, including after the trial has expired. If the program has already closed, open that file and use the buy link at the bottom.

Enter license

When the license email arrives, you do not have to close the program and wait for the start-up window.

1. Open **Help** → **Enter license**. The same window is **Settings** → **Software update & license** → **License**.
2. Paste the code, or click **Load from file**.
3. Click **Apply license**.

The program stores the code in the registry on this PC. A valid full license takes effect immediately. You do not restart.

Help → **Buy license** then disappears. The 30-day limit on new composed keys is removed. **Help** → **Enter license** stays, so a replacement code can still be entered.

You can also enter the code on the start-up evaluation window the next time the program opens.

Purchase

1. Buy a license (United States sales as stated on the product site). Use **Help** → **Buy license**, **Pay** on the evaluation window, or the link in MachineCode.txt.
2. Confirm the **Machine Code** box already shows this PC. If it is empty, copy the code from **Help** → **About**, **Help** → **Enter license**, or MachineCode.txt, and paste it into that box.
3. You receive a license code.
4. Open **Help** → **Enter license**, or the start-up window, and enter the full code.
5. The program stores it for the next start.

Per machine

A paid license is locked to one PC. **Help** → **About** and **Help** → **Enter license** both show the machine code. Each has a copy button.

If you replace the computer, send:

- the new machine code from About on the new PC
- the purchase email

One replacement per purchase. The old PC should not keep using the same paid unlock.

About

About shows the product name, version, build date, copyright, and machine code. It also indicates an evaluation copy when that applies. Use About when you write to support about a license.

If it fails

- "Validation key is invalid/malformed" — the program's built-in validation string is wrong in that build, not your customer code. Use a complete vendor build.
- Code typed with spaces or missing characters — paste the full code, or use **Load from file**.
- The message says the license was saved but it is still an evaluation license — that code is not a full license. **Help** → **Buy license** stays. The 30-day compose limit stays.
- The buy page does not open — check the internet connection, then use the link in MachineCode.txt.
- New PC — you need the replacement license, not the old machine code.

Next

Disclaimer for AS IS, hold harmless, and export. Updates for version checks. System requirements for the PC you are licensing.

Policy notes

Product — Policy notes

Encrypt3 blocks some OpenPGP choices on purpose. The message should say the key is **obsolete and vulnerable**, not only "policy."

Key size

- **1024-bit** (and other blocked weak sizes) cannot be **composed**.
- They cannot be used to **encrypt**.
- Import may refuse them or warn; do not use them as recipients.

Use RSA 3072/4096 or Ed25519+X25519 for new work.

Evaluation

- Newly composed keys must expire within **30 days**.
- Never expire is disabled.
- If you pick a later date, it is snapped back and you are told.
- A full license sets that cap to off.

Expired keys (purple)

- Cannot be used to **encrypt**.
- **Decrypt** with a secret key may still work so you can open old files.
- Extend expiry only if you have the secret key and the license allows the new date.

Revoked keys (red)

- Cannot **sign**.
- Cannot be chosen as an encrypt **recipient**.
- May still **decrypt** old ciphertext if the secret material is in the vault.

Signing

The signer must be a secret key that is not revoked. Text Task and File Task should refuse a revoked signer.

Watch folder and groups

Watch folder encrypts only to the key you selected. If that key later expires or is revoked, files go to **Failed** until you pick a valid key and Save.

Next

Expiration dashboard. **Create your first key**. **Licensing** for the 30-day evaluation cap.

Menu map

Product — Menu map

Use this to find a command. Window titles use two-word capitals (File Task, Text Task).

Keys

Command	What it does
Compose key	Create a new key pair
Import / Import key block / clipboard	One key from file or armored text
Bulk import	Many keys, CSV, ZIP, dry-run
Export	Public, secret, pair; .asc or .pgp
Change key password	Passphrase for one secret key
Revoke	Mark your key revoked (red)
Trash	Remove from the live grid
Properties	Fingerprint and details
QR	Full public key as QR
Extend expiration	New valid-until date (secret key)

File / Folder / Text

Command	What it does
File Task	Encrypt, decrypt, sign and encrypt, decrypt and verify one file
Folder Task	Same idea for a folder, optional subfolders
Text Task	Encrypt/decrypt/sign/verify/clear-sign text

Tools

Command	What it does
Recipient groups	Names and members; grid filter
Watch folder	Inbox → encrypt → output
Lookup	Keyserver and WKD
Expiration dashboard	Expiry, never, revoked, Key ID hex
Key ceremony sheet	Print fingerprint sign-off
Audit log	Vault events and failed sign-ins
Backup / Restore	Copy or replace the .ngw3

Settings

Tab	What it does
Key store	Vault path; Change location
Security	Idle lock minutes; Explorer verbs
Software update & license	30-day check, Check for update, License

Help

Command	What it does
Help	Opens the help file in the program folder
Support	Opens the help desk site
About	Name, version, build date, copyright, machine code

Main grid

Welcome bar, group filter, Find / Cancel search, right-click (copy public key, Verified, clipboard encrypt/decrypt).

Next

Meet the key store for columns and colors. **If something fails** if a command is missing in your build — use the closest name in this table.

System requirements

Product — System requirements

Operating system

- Windows 10 or Windows 11, 64-bit
- .NET Framework **4.8** or later (4.8.1 is fine). Windows 10/11 usually include it.
- Not supported: macOS, Linux, or Windows on ARM as a published configuration

Computer

- Typical 64-bit Windows PC or laptop
- About **50 MB** free for the program folder (exe, .config, Help), plus space for the vault and working files
- Display at least **1280 × 720**. Windows are fixed size (no maximize).

Files that must stay together

- NextGenWidgetEncrypt3.exe
- NextGenWidgetEncrypt3.exe.config

Extract the zip; do not run the exe alone.

Permissions

- Standard user can run the program.
- Administrator is not required to start.
- Explorer verbs are per Windows user, from Settings.

Network (optional)

Only for Check for update, keyserver / WKD, and opening Support in the browser. Encrypt, decrypt, compose, and the vault work offline.

Not required

GnuPG, Kleopatra, a hardware token, a Microsoft account, or always-on Internet.

License

Evaluation uses the same PC requirements. A paid license is for **one PC** (machine code on About).

If this page already exists under Getting started, keep **one** copy here in **Product** and link to it from Install and start.

Keyboard and windows

Product — Keyboard and windows

Window shape

Task windows and Settings use **FixedSingle** borders. The maximize box is **off**. Do not expect the window to fill the screen. If a control is tight, use the form as laid out; scroll only where a list or grid provides a scrollbar.

The key store can grow vertically within a minimum height; it does not stretch wide without limit. Widen columns if **Unverified** or similar text is clipped.

Keyboard

- **Tab** / **Shift+Tab** — next / previous field
- **Enter** — default button when one is set (Sign in, OK)
- **Esc** — often Cancel / close on dialogs
- Password fields: optional **Show password** checkbox; default is hidden

There is no full application hotkey map beyond normal Windows Forms behavior.

Idle lock

Idle lock watches **keyboard and mouse in this application** (main window and tasks). Using File Task or Text Task resets the timer. Switching to another program without input in Encrypt3 can let the timer expire. Lock does not replace the Windows session lock.

When the lock fires, open task windows should close or hide so they are not left readable behind the sign-in box.

High DPI

Use Windows display scaling you already use. If a form was designed at 100%, 150% scaling may crowd labels; that is a layout limit, not a maximize option.

Help

Help opens the help file from the program directory. **Support** opens the help desk in the browser. Neither is a keyboard-only wizard.

Next

Meet the **key store** for the grid. **Settings** → **Security** for lock minutes.

Uninstall

Product — Uninstall

Encrypt3 is not an installed “Programs and Features” product. You remove a folder.

Before you delete files

1. Settings → **Security** → turn **off** Explorer Encrypt/Decrypt.
2. Finish Watch folder work; move anything still in inbox/output.
3. **Backup the vault** if you still need the keys.
4. Exit Encrypt3.

Remove the program

1. Delete the program folder (NextGenWigetEncrypt3.exe, .exe.config, Help, and any extra DLLs you shipped).
2. Delete Desktop / Start shortcuts.
3. Do **not** delete the .ngw3 vault unless you intend to destroy the keys.

Vault

The vault path is under Settings → Key store. That file can live outside the program folder. Uninstalling the exe does not always delete it. Delete the .ngw3 only when you mean to.

License

A license stored for this PC may remain in the registry until you or the license tool clears it. That does not keep the program running after the folder is gone. A new install on the **same** PC may still see the old license.

Explorer leftovers

If right-click verbs remain, start the program from a leftover copy, open Settings, uncheck Explorer, then delete that copy. Or ignore the verbs after the exe is gone; they will fail until removed.

Next

Backup the vault before you uninstall if the keys matter. **Licensing** if you will install on a replacement PC (one replacement per purchase).

Glossary

Product — Glossary

1. **Armor (ASCII armor)** — Text form of OpenPGP data, with BEGIN / END lines. Optional comment and Version headers sit under the begin line.

2. **Audit log** — Short event list inside the vault (including failed sign-ins).
3. **Bulk import** — Import many keys from files, a folder, a ZIP, or a CSV, with an optional dry-run.
4. **Clear-sign** — Readable text plus a signature in one signed-message block.
5. **Dry-run** — Preview of a bulk import that does not change the store.
6. **Evaluation** — Time-limited license. New keys must expire within 30 days.
7. **Fingerprint** — Long hex identity of a key. Compare it before Verified.
8. **Group** — Label you assign (Financial, Technical). Not part of the OpenPGP packet. Filter is not case-sensitive.
9. **Key ID / Key ID hex** — Short and hex identifiers on the grid. Use hex when the name is empty.
10. **Key passphrase** — Secret that unlocks one OpenPGP secret key.
11. **Machine code** — PC identity on About; used for a per-machine license.
12. **Public key** — Encrypt to this key and verify signatures. Cannot decrypt or sign.
13. **Recipient** — Public key a message or file is encrypted to.
14. **Recovery copy** — Extra recipient on the same ciphertext so you can decrypt too.
15. **Revoked** — Key marked unusable for sign/encrypt; grid row red.
16. **Secret (private) key** — Decrypt and sign, after the key passphrase.
17. **Sign and encrypt** — Signature plus encryption in one output.
18. **Trash** — Hidden in the vault until restore or permanent delete; not the same as revoke.
19. **Trust / Verified** — You compared the fingerprint. Import is not Verified.
20. **Vault** — Encrypted .ngw3 file: keys, logins, settings, log.
21. **Vault login** — Password that opens the vault (sign-in and idle lock).
22. **Watch folder** — Inbox files encrypted to a key you choose; output folder holds ciphertext.
23. **WKD** — Web Key Directory; lookup by email domain.
24. **.asc / .pgp / .gpg** — Common OpenPGP file extensions (text armor vs binary).
25. **.ngw3** — This product's vault file. Not an OpenPGP message.
26. **.exe.config** — Must sit next to the exe. Required on .NET Framework for this build.

Disclaimer

License and disclaimer

(for Help and for the license / evaluation text)

NEXTGEN Widget Encrypt3

Software by NextGen Widget Software.

Not a product of a company, employer, or other organization.

License. A purchased license is granted to you for use of the software on **one computer**, identified by the machine code shown under Help → About. Evaluation use is allowed only as shown in the evaluation

window. Newly composed keys on an evaluation copy may be limited to a 30-day lifetime. **One replacement license per purchase** is available if that computer is replaced; you must provide the new machine code and the original purchase email. The license is not a sale of the software. You may not rent, sublicense, or share the license code to unlock additional machines.

AS IS. The software and documentation are provided AS IS, without warranty of any kind, express or implied, including merchantability, fitness for a particular purpose, title, and non-infringement.

No liability. To the maximum extent permitted by law, NextGen Widget Software shall not be liable for any claim, damage, or loss arising from install, use, inability to use, or results of use of the software or help file, including lost data, lost keys, failed encryption or decryption, incompatibility with other OpenPGP programs, or business interruption. You use the software at your own risk.

Hold harmless. You agree to hold NextGen Widget Software harmless from claims by you or third parties arising out of your use of the software, including misuse, unlawful use, or failure to safeguard passwords, keys, and vault backups.

Your duties. You must choose suitable algorithms and key sizes, verify fingerprints before trusting a key, protect vault and key passphrases, back up the vault and test restore, and comply with applicable law, including export rules for cryptography.

OpenPGP. The software is intended to interchange with other OpenPGP programs when both sides use compatible algorithms and formats. There is no guarantee that every third-party key or message will work.

Acceptance. Installing or running the software constitutes acceptance of these terms. If you do not accept them, do not install or run the program.

Export. This software uses encryption and is subject to the US Export Administration Regulations (EAR) and other US law. You may not export, re-export, download, or transfer the software, a license code, or a vault backup to a country, region, or person prohibited by the United States, including destinations and parties on the current lists maintained by the Bureau of Industry and Security (BIS) and the Office of Foreign Assets Control (OFAC).

A license is not valid for use in a prohibited destination. Obtaining a copy from a US website or email does not authorize use or further export where US law forbids it.

For the current rules and lists, see:

- BIS: <https://www.bis.gov/>
- EAR encryption / License Exception ENC: 15 CFR 740.17 and 15 CFR 742.15
- OFAC sanctions: <https://ofac.treasury.gov/>

You are responsible for complying with these rules. This notice is not a government license and is not legal advice.

System requirements

[BACK TO HOME](#)

System requirements

Operating system

- Windows 10 or Windows 11, 64-bit
- .NET Framework **4.8** or later (4.8.1 is fine). Windows 10/11 usually already include it.
- Not for macOS, Linux, or Windows on ARM as a supported configuration

Computer

- A normal PC or laptop that can run 64-bit Windows
- About **50 MB** free disk for the program folder (exe, .config, Help), plus space for the vault and encrypted files
- Display at least **1280 × 720**; the windows are fixed size and do not maximize

Files you must keep together

- NextGenWigetEncrypt3.exe
- NextGenWigetEncrypt3.exe.config

Extract the download zip and leave both in the same folder. The program does not install into the Windows “Programs and Features” list.

Permissions

- A standard user account can run the program.
- Administrator is not required to start Encrypt3.
- Explorer Encrypt/Decrypt for **this user** is registered from Settings without an all-users install.

Network (optional)

Needed only for:

- Check for update
- Keyserver / WKD lookup
- Support / Help desk link in the browser

Encrypt, decrypt, compose keys, and the vault work offline.

Not required

- GnuPG or Kleopatra
- A hardware token
- A Microsoft account
- Always-on Internet

License

- Evaluation runs on the same requirements.
- A purchased license is valid for **one PC** (machine code under Help → About).

Getting help

[BACK TO HOME](#)

Product — Getting help

In the program

- **Help** → **Help** opens NextGen Widget Encrypt3.chm in the **same folder** as the exe.
- **Help** → **Support** opens the help desk in your browser.
- **Help** → **About** shows version, build date, and machine code (needed for license tickets).

If Help says the file was not found, put NextGen Widget Encrypt3.chm next to NextGenWigetEncrypt3.exe and start Help again.

On the web

The same manual can be published as HTML when that site is ready. The support desk is:

<https://www.ngwe3.com/helpdesk/>

That page is a **ticket system**. Create an account if the desk asks for one, then open a ticket.

What to include in a ticket

1. What you were doing (window name, Encrypt / Import / sign-in).
2. The exact message text.
3. **Help** → **About**: version, build date, machine code.
4. Windows version (10 or 11).
5. Whether this is evaluation or a paid license (do not paste the full license code in public).

Do not put vault passwords, key passphrases, or secret key blocks in a ticket.

What Help and Support are not

- Help does not reset a lost vault password.
- Support does not replace a backup of the .ngw3 file.
- Licensing replacement (one per purchase) is a ticket plus the **new** machine code and purchase email.

No refund policy

[BACK TO HOME](#)



NEXTGEN Widget Encrypt3 — when OpenPGP security matters.

by NextGen Widget Software

No refund policy

Last updated 24 September 2026.

NEXTGEN Widget Software has a **no-refund** policy on a **try-before-you-buy** basis. Evaluate the software with the trial **before** you purchase.

What you are buying

You are buying a **license** — a right to use NEXTGEN Widget Encrypt3 on **one PC** — not ownership of the program and not a boxed product that can be shipped back. After payment is approved, we email a **per-PC activation key**. Digital delivery is complete when that key is sent to the order email.

No refunds after the key is emailed

Once the key is emailed, **there are no refunds**. A license key is intangible digital content. After we send it, you have received the product. It is not possible to return a registered copy.

This is enforced to protect the integrity of the software. Completing checkout, installing a paid key, or continuing past the in-app license constitutes acceptance of these terms, together with the website terms of use.

Try the trial first

Download, install, and test the trial on the same kind of PC and workflow you intend to license. Confirm encryption, decryption, the vault, and any feature you rely on. If the trial does not fit, do not purchase. We do not refund after a key has been delivered because you later decide you do not need the product, you bought the wrong edition, you changed PCs, or you did not read this topic.

Replacement keys (not refunds)

- A paid key is for one PC, identified by that PC's machine code. It may be used indefinitely on that computer. It is not a license for a second computer.
- If that computer crashes, is replaced, or is rebuilt with a new operating system, and the machine code changes, the existing key will not move to the new computer. Within one year of the original purchase date, you may buy one replacement key for that mishap at 50% of the current license price. Send the original purchase receipt and the machine code from the replacement computer through the help desk. That replacement is a new per-PC key for one replacement computer. It is not a free reissue, and it is not permission to run the software on two computers at the same time.
- After that one-year date, or if you want the software on an additional computer, a full new license is required.
- A replacement key is not a refund of the original purchase. Once an activation key has been emailed, the original purchase is not refundable.

If something went wrong with delivery

If we sent the wrong product through our error, or the key never arrived and we cannot resend it, contact the help desk promptly with the order email. That is a delivery problem, not a change-of-mind refund.

Unjustified payment disputes or chargebacks after the key is emailed may be contested with the payment processor, with this policy, the order record, and the delivery email as evidence.

Where this also appears

The same policy is on the website at the No refunds page and in the software license presented in the program.

For questions: Help → Getting help, or <https://www.ngwidgetsoftware.com/helpdesk/>
