VIPER Q PRO

User Manual

Complete operating guide, function reference, setup instructions, and troubleshooting

Product	Viper Q Pro
Version	3.7.1
Document type	User Manual
Release status	Customer release documentation
Purpose	Clear, readable, operational documentation for installation, use, troubleshooting, and security review.

Read this before deployment or customer release. This document is written for real customers, not internal developers.

1. Read This First

This manual explains how to install, open, use, back up, restore, and troubleshoot Viper Q Pro. It is written for real customers. Follow it in order the first time. Most installation problems happen when users run the app from inside the ZIP, move the EXE away from its folder, or create a shortcut pointing to the wrong location.

Golden rule: Extract the whole VQPro_Setup.zip first. Keep the VQPro folder together. Run VQPro.exe from inside that extracted folder. Create the desktop shortcut only with Windows: right-click VQPro.exe -> Show more options -> Send to -> Desktop (create shortcut).

2. Package Contents

- VQPro.exe - the Windows application.
- Desktop shortcut - create manually from VQPro.exe using Windows Send to -> Desktop (create shortcut).
- README_FIRST.txt - short install instructions.
- docs folder - user manual, security whitepaper, troubleshooting, and setup material where included.

3. Correct Installation

1. Download VQPro_Setup.zip from the official Viper Q Pro payment/download page.

2. Right-click the ZIP and choose Extract All. Do not open the ZIP and run the EXE from the preview window.

3. Extract to a simple location such as Desktop or Documents.

4. Open the extracted VQPro folder.

5. Read README_FIRST.txt if present.

6. Double-click VQPro.exe - the application with the VQPro logo/icon - from inside the extracted VQPro folder.

If Windows shows SmartScreen, only continue if you downloaded VQPro from the official viperqpro.com purchase/download page. Click More info, then Run anyway.

8. After the app launches correctly, create the desktop shortcut manually: right-click VQPro.exe -> Show more options -> Send to -> Desktop (create shortcut).

4. First Launch Setup

On first launch, VQPro may initialise vault folders, create security metadata, build initial keys, and ask for owner configuration. Do not interrupt first launch. Do not close the window while the vault is creating its first files.

1. Choose a strong master password. Use a long phrase you will remember.

2. Write recovery notes and store them offline, away from the computer.

3. Configure optional 2FA only when you have saved recovery codes.

4. Create a first test vault or test chamber before adding critical data.

5. Import one non-critical file and confirm you can preview/export it.

6. Create your first backup before adding large amounts of sensitive material.

5. Complete Function Reference

This section explains each major VQPro function in operational language: what it does, when to use it, how to use it safely, what can go wrong, and how to recover. Some advanced controls may appear only when enabled, licensed, or supported by the machine hardware.

First Launch / Gate I

What it does: The first screen protects access to the vault. The user enters the master password, optional panic phrase, or approved alternate authentication. The vault should be opened only after the package is extracted, not from inside the ZIP preview.

When to use it: every normal session starts here. Treat this area as the front door of the vault. Do not rush through warnings, alerts, or failed-login messages because they often explain the exact problem.

1. Open VQPro from the extracted folder or correct desktop shortcut.

2. Enter the required password or authentication factor.

3. Read any warning, lockout, health, or tamper message before continuing.

4. If the vault opens, check the dashboard before importing, exporting, or changing settings.

Common mistakes: running from inside the ZIP, using a broken shortcut, forgetting that Caps Lock is on, assuming a wrong password is an app fault, or ignoring a dashboard warning after repeated failed access attempts.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Master Password

What it does: The master password is the primary secret. It must be long, memorable, and unique. If it is forgotten there is no ordinary password reset because the system is designed so the developer, hosting provider, and payment processor cannot decrypt the vault.

When to use it: every normal session starts here. Treat this area as the front door of the vault. Do not rush through warnings, alerts, or failed-login messages because they often explain the exact problem.

1. Open VQPro from the extracted folder or correct desktop shortcut.

2. Enter the required password or authentication factor.

3. Read any warning, lockout, health, or tamper message before continuing.

4. If the vault opens, check the dashboard before importing, exporting, or changing settings.

Common mistakes: running from inside the ZIP, using a broken shortcut, forgetting that Caps Lock is on, assuming a wrong password is an app fault, or ignoring a dashboard warning after repeated failed access attempts.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Dashboard

What it does: The dashboard gives the owner a security summary: vault state, health score, chamber status, alerts, backup age, authentication status, and recent security events.

When to use it: every normal session starts here. Treat this area as the front door of the vault. Do not rush through warnings, alerts, or failed-login messages because they often explain the exact problem.

1. Open VQPro from the extracted folder or correct desktop shortcut.

2. Enter the required password or authentication factor.

3. Read any warning, lockout, health, or tamper message before continuing.

4. If the vault opens, check the dashboard before importing, exporting, or changing settings.

Common mistakes: running from inside the ZIP, using a broken shortcut, forgetting that Caps Lock is on, assuming a wrong password is an app fault, or ignoring a dashboard warning after repeated failed access attempts.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Add / Import Files

What it does: Files should be added from trusted local folders. VQPro encrypts protected material before storage. Users should verify the file appears inside the vault before deleting the original outside copy.

When to use it: use these functions whenever you move sensitive files into or out of the encrypted vault. Import protects data; preview minimises exposure; export creates a normal decrypted file and must be treated carefully.

1. Select the correct chamber before adding or retrieving material.

2. Import one file or one small batch first if the material is important.

3. Confirm the item appears in the vault list.

4. Preview or export a test item to confirm it opens correctly.

5. Only then remove the unencrypted original if that is your intention.

Common mistakes: deleting originals before confirming import, exporting to Downloads and forgetting the decrypted copy, importing from unsafe browser download folders, or storing the same file in several chambers with no naming discipline.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Open / Preview Files

What it does: Preview should be used for quick viewing. For sensitive files, avoid exporting unless needed. Close previews before stepping away from the machine.

When to use it: use these functions whenever you move sensitive files into or out of the encrypted vault. Import protects data; preview minimises exposure; export creates a normal decrypted file and must be treated carefully.

1. Select the correct chamber before adding or retrieving material.

2. Import one file or one small batch first if the material is important.

3. Confirm the item appears in the vault list.

4. Preview or export a test item to confirm it opens correctly.

5. Only then remove the unencrypted original if that is your intention.

Common mistakes: deleting originals before confirming import, exporting to Downloads and forgetting the decrypted copy, importing from unsafe browser download folders, or storing the same file in several chambers with no naming discipline.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Export / Retrieve Files

What it does: Export decrypts a protected file back to a normal Windows file. Export only to a safe folder and remove temporary copies when finished.

When to use it: use these functions whenever you move sensitive files into or out of the encrypted vault. Import protects data; preview minimises exposure; export creates a normal decrypted file and must be treated carefully.

1. Select the correct chamber before adding or retrieving material.

2. Import one file or one small batch first if the material is important.

3. Confirm the item appears in the vault list.

4. Preview or export a test item to confirm it opens correctly.

5. Only then remove the unencrypted original if that is your intention.

Common mistakes: deleting originals before confirming import, exporting to Downloads and forgetting the decrypted copy, importing from unsafe browser download folders, or storing the same file in several chambers with no naming discipline.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Chambers

What it does: Chambers separate categories of sensitive material. Use separate chambers for legal files, financial files, identity documents, keys, personal records, and high-risk material.

When to use it: use compartment features when different data sets have different risk levels. Normal documents, financial records, legal documents, seed material, decoy content, and travel-sensitive data should not all sit in one undifferentiated pile.

1. Decide the purpose of the chamber or volume before creating it.

2. Use clear names that do not reveal sensitive secrets.

3. Place a small test file first.

4. Confirm the chamber opens and locks as expected.

5. Create a backup after major chamber changes.

Common mistakes: making the decoy vault empty or unrealistic, forgetting which chamber holds which material, using Travel Mode without recording how to reverse it, or writing hidden-volume hints in plain text outside the vault.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Hidden Volume

What it does: Use hidden volume only when plausible deniability is genuinely required. Keep the outer vault believable and avoid storing references to the hidden vault outside VQPro.

When to use it: use compartment features when different data sets have different risk levels. Normal documents, financial records, legal documents, seed material, decoy content, and travel-sensitive data should not all sit in one undifferentiated pile.

1. Decide the purpose of the chamber or volume before creating it.

2. Use clear names that do not reveal sensitive secrets.

3. Place a small test file first.

4. Confirm the chamber opens and locks as expected.

5. Create a backup after major chamber changes.

Common mistakes: making the decoy vault empty or unrealistic, forgetting which chamber holds which material, using Travel Mode without recording how to reverse it, or writing hidden-volume hints in plain text outside the vault.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Warning: This is a high-impact feature. Test only with disposable data until you understand the behaviour. Destructive or restrictive settings can cause permanent data loss or lockout.

Decoy Vault

What it does: The decoy vault is for duress. It should contain realistic but non-sensitive material so an attacker believes access has been surrendered.

When to use it: use compartment features when different data sets have different risk levels. Normal documents, financial records, legal documents, seed material, decoy content, and travel-sensitive data should not all sit in one undifferentiated pile.

1. Decide the purpose of the chamber or volume before creating it.

2. Use clear names that do not reveal sensitive secrets.

3. Place a small test file first.

4. Confirm the chamber opens and locks as expected.

5. Create a backup after major chamber changes.

Common mistakes: making the decoy vault empty or unrealistic, forgetting which chamber holds which material, using Travel Mode without recording how to reverse it, or writing hidden-volume hints in plain text outside the vault.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Public Drop Slot

What it does: The drop slot allows incoming encrypted deposits without exposing the real vault. Share only the public deposit material, never the master password or private vault files.

When to use it: use the drop slot when someone must send you material without seeing your real vault. It is for incoming deposits, not for giving another person full vault access.

1. Generate or locate the public deposit material.

2. Share only the public deposit instructions.

3. Tell the sender not to email passwords or private keys.

4. Open VQPro later and check the deposits area.

5. Move verified deposits into the correct chamber.

Common mistakes: sharing private vault files instead of public deposit material, assuming deposit equals trust, or leaving new deposits unreviewed.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Password Records

What it does: Use records for login credentials, recovery codes, API keys, seed notes, licence keys, and sensitive text. Keep entries named clearly and avoid duplicate stale passwords.

When to use it: use these tools for credentials, recovery codes, API keys, licence keys, passphrases, and sensitive notes. The clipboard is one of the easiest places to leak secrets, so copying should be brief and deliberate.

1. Open the record only when needed.

2. Copy the username, password, or key using the app button where possible.

3. Paste into the intended destination only.

4. Wait for clipboard wipe or clear it manually.

5. Lock the vault when finished.

Common mistakes: pasting a secret into the wrong chat/browser/app, taking screenshots of passwords, keeping duplicate stale records, or disabling clipboard wipe for convenience.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Clipboard Wipe

What it does: When copying usernames, passwords, or keys, the clipboard should clear automatically after the configured delay. Do not paste sensitive content into chat windows, browsers, or unknown apps.

When to use it: use these tools for credentials, recovery codes, API keys, licence keys, passphrases, and sensitive notes. The clipboard is one of the easiest places to leak secrets, so copying should be brief and deliberate.

1. Open the record only when needed.

2. Copy the username, password, or key using the app button where possible.

3. Paste into the intended destination only.

4. Wait for clipboard wipe or clear it manually.

5. Lock the vault when finished.

Common mistakes: pasting a secret into the wrong chat/browser/app, taking screenshots of passwords, keeping duplicate stale records, or disabling clipboard wipe for convenience.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Audit Log

What it does: The audit log is the evidence trail. It records important actions, successful access, failed access, changes, exports, deletes, alerts, and tamper events. Do not manually edit audit files.

When to use it: use monitoring and evidence functions whenever something unusual happens: failed logins, tamper warnings, unexpected exports, integrity changes, or security-score drops.

1. Open the relevant audit, health, SIEM, or alert screen.

2. Read the newest critical events first.

3. Do not delete or edit audit files.

4. Take screenshots if the event may matter later.

5. Resolve the underlying issue, then create a backup once the vault is stable.

Common mistakes: ignoring repeated failed logins, treating integrity warnings as cosmetic, deleting evidence during panic, or continuing normal work after a tripwire fires.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Access Certificate

What it does: Generate an access certificate when you need a dated proof of access or a record for review. Store the certificate outside the vault only when it is safe to do so.

When to use it: use monitoring and evidence functions whenever something unusual happens: failed logins, tamper warnings, unexpected exports, integrity changes, or security-score drops.

1. Open the relevant audit, health, SIEM, or alert screen.

2. Read the newest critical events first.

3. Do not delete or edit audit files.

4. Take screenshots if the event may matter later.

5. Resolve the underlying issue, then create a backup once the vault is stable.

Common mistakes: ignoring repeated failed logins, treating integrity warnings as cosmetic, deleting evidence during panic, or continuing normal work after a tripwire fires.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Vault Health Score

What it does: Health score highlights weak configuration: missing backup, old backup, 2FA not enabled, weak password, disabled hardware binding, unresolved alerts, or missing recovery notes.

When to use it: use monitoring and evidence functions whenever something unusual happens: failed logins, tamper warnings, unexpected exports, integrity changes, or security-score drops.

1. Open the relevant audit, health, SIEM, or alert screen.

2. Read the newest critical events first.

3. Do not delete or edit audit files.

4. Take screenshots if the event may matter later.

5. Resolve the underlying issue, then create a backup once the vault is stable.

Common mistakes: ignoring repeated failed logins, treating integrity warnings as cosmetic, deleting evidence during panic, or continuing normal work after a tripwire fires.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Backup

What it does: Backups should be created after important changes. Store backups on an external drive or separate encrypted location. A backup is useless if the password and recovery notes are lost.

When to use it: use continuity functions before and after important changes, before hardware replacement, before Windows reset, and before any migration. Strong security without recovery planning can become self-inflicted lockout.

1. Create a current backup before changing security settings.

2. Store the backup away from the main computer.

3. Record the backup date and location.

4. Test restore with care before deleting originals.

5. For new hardware, follow rebind or migration instructions rather than copying random files.

Common mistakes: relying on one copy, backing up to a sync folder without understanding exposure, forgetting machine binding, or deleting the old vault before the restored one opens.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Restore

What it does: Restore should be tested with care. Confirm the restored vault opens before deleting the original. If hardware binding is active, restoration to a new machine may require a rebind procedure.

When to use it: use continuity functions before and after important changes, before hardware replacement, before Windows reset, and before any migration. Strong security without recovery planning can become self-inflicted lockout.

1. Create a current backup before changing security settings.

2. Store the backup away from the main computer.

3. Record the backup date and location.

4. Test restore with care before deleting originals.

5. For new hardware, follow rebind or migration instructions rather than copying random files.

Common mistakes: relying on one copy, backing up to a sync folder without understanding exposure, forgetting machine binding, or deleting the old vault before the restored one opens.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Cloud Sync

What it does: Zero-knowledge cloud sync means the cloud provider receives encrypted data only. Do not upload unencrypted exports to cloud storage by mistake.

When to use it: use continuity functions before and after important changes, before hardware replacement, before Windows reset, and before any migration. Strong security without recovery planning can become self-inflicted lockout.

1. Create a current backup before changing security settings.

2. Store the backup away from the main computer.

3. Record the backup date and location.

4. Test restore with care before deleting originals.

5. For new hardware, follow rebind or migration instructions rather than copying random files.

Common mistakes: relying on one copy, backing up to a sync folder without understanding exposure, forgetting machine binding, or deleting the old vault before the restored one opens.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Machine Binding

What it does: Machine binding ties the vault or licence to hardware identity. It protects against stolen vault copies but can complicate motherboard replacement, Windows reset, or migration.

When to use it: use continuity functions before and after important changes, before hardware replacement, before Windows reset, and before any migration. Strong security without recovery planning can become self-inflicted lockout.

1. Create a current backup before changing security settings.

2. Store the backup away from the main computer.

3. Record the backup date and location.

4. Test restore with care before deleting originals.

5. For new hardware, follow rebind or migration instructions rather than copying random files.

Common mistakes: relying on one copy, backing up to a sync folder without understanding exposure, forgetting machine binding, or deleting the old vault before the restored one opens.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Windows Hello

What it does: Windows Hello can improve convenience, but it should not replace a strong master password and recovery discipline.

When to use it: use additional authentication when the vault holds material that would cause serious damage if exposed. Convenience factors are useful, but recovery codes and spare devices matter.

1. Enable the factor from settings.

2. Save recovery codes or configure a spare device where supported.

3. Lock the vault and test unlock.

4. Document the recovery process offline.

5. Do not enable a factor minutes before travel or emergency work without testing it.

Common mistakes: losing the only phone or hardware key, failing to save recovery codes, assuming biometrics replace the master password, or testing new factors on live data without backup.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

YubiKey

What it does: YubiKey support adds a physical possession factor. Keep a spare key where possible. Losing the only configured key may lock you out depending on policy.

When to use it: use additional authentication when the vault holds material that would cause serious damage if exposed. Convenience factors are useful, but recovery codes and spare devices matter.

1. Enable the factor from settings.

2. Save recovery codes or configure a spare device where supported.

3. Lock the vault and test unlock.

4. Document the recovery process offline.

5. Do not enable a factor minutes before travel or emergency work without testing it.

Common mistakes: losing the only phone or hardware key, failing to save recovery codes, assuming biometrics replace the master password, or testing new factors on live data without backup.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

TOTP 2FA

What it does: TOTP uses an authenticator app. Save recovery codes offline. If the phone is lost and recovery codes are missing, access may be blocked.

When to use it: use additional authentication when the vault holds material that would cause serious damage if exposed. Convenience factors are useful, but recovery codes and spare devices matter.

1. Enable the factor from settings.

2. Save recovery codes or configure a spare device where supported.

3. Lock the vault and test unlock.

4. Document the recovery process offline.

5. Do not enable a factor minutes before travel or emergency work without testing it.

Common mistakes: losing the only phone or hardware key, failing to save recovery codes, assuming biometrics replace the master password, or testing new factors on live data without backup.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Time Lock

What it does: Time Lock prevents access before a configured date/time. Do not enable it casually. Confirm the unlock date before applying it.

When to use it: use high-risk controls only when the risk justifies the restriction. These tools can hide, block, or destroy access. They are powerful because they are dangerous when used carelessly.

1. Create a disposable test vault first.

2. Enable the control with harmless data.

3. Confirm exactly how to reverse it or what destruction will occur.

4. Write down the owner-side recovery notes.

5. Only then consider using it on real vault material.

Common mistakes: testing destructive features on live data, setting a wrong unlock date, storing wipe tokens carelessly, forgetting geofence boundaries, or triggering panic actions without understanding consequences.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Warning: This is a high-impact feature. Test only with disposable data until you understand the behaviour. Destructive or restrictive settings can cause permanent data loss or lockout.

Geofencing

What it does: Geofencing depends on location data and system conditions. Treat it as an additional policy control, not the only security barrier.

When to use it: use high-risk controls only when the risk justifies the restriction. These tools can hide, block, or destroy access. They are powerful because they are dangerous when used carelessly.

1. Create a disposable test vault first.

2. Enable the control with harmless data.

3. Confirm exactly how to reverse it or what destruction will occur.

4. Write down the owner-side recovery notes.

5. Only then consider using it on real vault material.

Common mistakes: testing destructive features on live data, setting a wrong unlock date, storing wipe tokens carelessly, forgetting geofence boundaries, or triggering panic actions without understanding consequences.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Travel Mode

What it does: Use before travel or inspection risk. Confirm which chambers will be hidden. Do not carry written notes that reveal the hidden material.

When to use it: use compartment features when different data sets have different risk levels. Normal documents, financial records, legal documents, seed material, decoy content, and travel-sensitive data should not all sit in one undifferentiated pile.

1. Decide the purpose of the chamber or volume before creating it.

2. Use clear names that do not reveal sensitive secrets.

3. Place a small test file first.

4. Confirm the chamber opens and locks as expected.

5. Create a backup after major chamber changes.

Common mistakes: making the decoy vault empty or unrealistic, forgetting which chamber holds which material, using Travel Mode without recording how to reverse it, or writing hidden-volume hints in plain text outside the vault.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Warning: This is a high-impact feature. Test only with disposable data until you understand the behaviour. Destructive or restrictive settings can cause permanent data loss or lockout.

Stealth Mode

What it does: Stealth Mode hides or disguises the vault interface. It is for shoulder-surfing and casual observation, not a substitute for locking Windows.

When to use it: use high-risk controls only when the risk justifies the restriction. These tools can hide, block, or destroy access. They are powerful because they are dangerous when used carelessly.

1. Create a disposable test vault first.

2. Enable the control with harmless data.

3. Confirm exactly how to reverse it or what destruction will occur.

4. Write down the owner-side recovery notes.

5. Only then consider using it on real vault material.

Common mistakes: testing destructive features on live data, setting a wrong unlock date, storing wipe tokens carelessly, forgetting geofence boundaries, or triggering panic actions without understanding consequences.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Panic Phrase / Kill Switch

What it does: Panic actions are destructive by design. They should be tested only with a disposable test vault, never with live customer data.

When to use it: use high-risk controls only when the risk justifies the restriction. These tools can hide, block, or destroy access. They are powerful because they are dangerous when used carelessly.

1. Create a disposable test vault first.

2. Enable the control with harmless data.

3. Confirm exactly how to reverse it or what destruction will occur.

4. Write down the owner-side recovery notes.

5. Only then consider using it on real vault material.

Common mistakes: testing destructive features on live data, setting a wrong unlock date, storing wipe tokens carelessly, forgetting geofence boundaries, or triggering panic actions without understanding consequences.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Warning: This is a high-impact feature. Test only with disposable data until you understand the behaviour. Destructive or restrictive settings can cause permanent data loss or lockout.

Remote Wipe Token

What it does: Store wipe tokens carefully. Anyone who can trigger a valid wipe may permanently destroy the vault.

When to use it: use high-risk controls only when the risk justifies the restriction. These tools can hide, block, or destroy access. They are powerful because they are dangerous when used carelessly.

1. Create a disposable test vault first.

2. Enable the control with harmless data.

3. Confirm exactly how to reverse it or what destruction will occur.

4. Write down the owner-side recovery notes.

5. Only then consider using it on real vault material.

Common mistakes: testing destructive features on live data, setting a wrong unlock date, storing wipe tokens carelessly, forgetting geofence boundaries, or triggering panic actions without understanding consequences.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Warning: This is a high-impact feature. Test only with disposable data until you understand the behaviour.

Destructive or restrictive settings can cause permanent data loss or lockout.

Local SIEM

What it does: Review critical SIEM alerts before continuing normal use. Repeated failed logins, file integrity changes, and tripwire events should be treated seriously.

When to use it: use monitoring and evidence functions whenever something unusual happens: failed logins, tamper warnings, unexpected exports, integrity changes, or security-score drops.

1. Open the relevant audit, health, SIEM, or alert screen.

2. Read the newest critical events first.

3. Do not delete or edit audit files.

4. Take screenshots if the event may matter later.

5. Resolve the underlying issue, then create a backup once the vault is stable.

Common mistakes: ignoring repeated failed logins, treating integrity warnings as cosmetic, deleting evidence during panic, or continuing normal work after a tripwire fires.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Tripwires

What it does: Tripwires detect intrusion indicators. If a tripwire fires, disconnect from networks, preserve evidence if needed, and move to recovery steps.

When to use it: use monitoring and evidence functions whenever something unusual happens: failed logins, tamper warnings, unexpected exports, integrity changes, or security-score drops.

1. Open the relevant audit, health, SIEM, or alert screen.

2. Read the newest critical events first.

3. Do not delete or edit audit files.

4. Take screenshots if the event may matter later.

5. Resolve the underlying issue, then create a backup once the vault is stable.

Common mistakes: ignoring repeated failed logins, treating integrity warnings as cosmetic, deleting evidence during panic, or continuing normal work after a tripwire fires.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Manual / Help Tab

What it does: The manual should be available offline inside the package. Use it first when installing, moving, backing up, restoring, or troubleshooting the vault.

When to use it: use this function when the matching risk exists and the feature has been configured deliberately. Do not enable advanced controls simply because they sound impressive.

1. Read the setting text inside the app.

2. Test with a non-critical example.

3. Confirm the result.

4. Back up after configuration changes.

Common mistakes: enabling features without testing, forgetting recovery notes, and confusing encrypted vault data with exported unencrypted copies.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

Desktop Shortcut

What it does: The correct shortcut must target the launcher or EXE in the extracted VQPro folder and must use that same folder as Start in. Do not create a shortcut from inside the ZIP preview.

When to use it: use this function when the matching risk exists and the feature has been configured deliberately. Do not enable advanced controls simply because they sound impressive.

1. Read the setting text inside the app.

2. Test with a non-critical example.

3. Confirm the result.

4. Back up after configuration changes.

Common mistakes: enabling features without testing, forgetting recovery notes, and confusing encrypted vault data with exported unencrypted copies.

Troubleshooting: if this function does not behave as expected, first confirm you are using the current extracted VQPro folder, not an old deploy folder or temporary ZIP path. Then check dashboard alerts, audit log entries, Windows Security notifications, and backup status before changing more settings.

6. Daily Use Workflow

1. Open VQPro from the desktop shortcut or extracted folder launcher.

2. Unlock using the master password and any configured second factor.

3. Check dashboard alerts before working.

4. Open the correct chamber.

5. Import, preview, edit records, or export files as needed.

6. Avoid leaving decrypted exports on the Desktop or Downloads folder.

7. Lock the vault when finished.

8. Back up after meaningful changes.

7. Adding Files Safely

Before deleting original files, always confirm the imported file exists inside the vault and can be opened or exported. For critical documents, keep the original until at least one backup has been created and verified.

- Use clear file names.
- Place files into the right chamber.
- Add notes when the document needs context.
- Avoid importing temporary browser downloads that you have not checked.
- Do not import malware, cracked tools, or unknown executables.

8. Credentials and Sensitive Notes

Password records and sensitive notes should be treated like high-value files. Name each record clearly, keep old/stale passwords marked or removed, and avoid copying secrets unless needed.

- Use the copy buttons instead of manually selecting text where possible.
- Wait for clipboard wipe after copying.
- Do not paste secrets into chat apps or untrusted websites.
- Keep recovery codes in a separate chamber or offline backup.

9. Chambers and Organisation

Chambers prevent one messy vault from becoming impossible to manage. Use chambers by risk and category. A simple structure works best: Personal, Identity, Finance, Legal, Business, Crypto, Recovery, and Archive.

Crypto users: Do not store seed phrases casually. If you store wallet recovery material, place it in a dedicated high-risk chamber, back it up offline, and avoid copying it to clipboard unless absolutely necessary.

10. Backup and Restore

Backups are part of security, not an afterthought. Encryption protects against outsiders. Backup protects against your own device failure, accidental deletion, Windows corruption, and hardware replacement.

1. Open VQPro and confirm there are no unresolved critical alerts.

2. Choose the backup function.

3. Select an external drive or safe local backup folder.

4. Let the backup finish without closing the app.

5. Write down the backup date and location.

6. Safely eject external drives after backup.

7. Periodically test restore with a non-destructive test.

11. Moving to Another Computer

If machine binding is enabled, copying the folder to another computer is not the same as migration. The vault may refuse to open because that is the intended protection. Use the proper restore or rebind process.

1. Create a fresh backup on the old machine.

2. Confirm you know the master password and have recovery material.

3. Install/extract VQPro on the new machine.

4. Use the documented restore/rebind flow.

5. Open the restored vault and confirm files are visible.

6. Only after confirmation, retire the old copy safely.

12. Owner-Side Payment and Download Checks

This section is for the site owner, not ordinary customers. The Netlify site should preserve the correct payment and download flow.

- The public website must remain the proper Viper Q Pro page, not a stripped placeholder.
- Stripe payment links must be the live links intended for the product.
- Stripe success URL must end with thank-you.html?session_id={CHECKOUT_SESSION_ID}.
- Netlify must have STRIPE_SECRET_KEY set to the live secret key.
- The thank-you page should verify the session before triggering the customer download.
- The customer download should be VQPro_Setup.zip, not loose EXE files.

13. Troubleshooting - Fast Diagnosis

Windows says the file might be corrupted

Most common cause: the app was launched from inside the ZIP, extracted incorrectly, moved away from support files, or a bad shortcut points to the wrong place. Extract the entire ZIP first, keep the VQPro folder together, right-click VQPro.exe, Properties, tick Unblock if visible, then run VQPro.exe from inside the extracted folder.

SmartScreen warning appears

This can happen for unsigned or newly distributed Windows software. Confirm the file came from the official purchase/download flow. Click More info then Run anyway only if you trust the source. A future code-signing certificate is the correct long-term fix.

Shortcut opens the wrong app or old folder

Delete the broken shortcut. Open the extracted VQPro folder. Double-click VQPro.exe directly. If it opens, create a fresh shortcut using right-click VQPro.exe -> Show more options -> Send to -> Desktop (create shortcut).

Double-click does nothing

Run VQPro.exe directly from inside the extracted VQPro folder so any shortcut problem is bypassed. Also check Windows Security, Controlled Folder Access, antivirus quarantine, missing permissions, and whether the file is still blocked.

App opens from folder but not shortcut

Cannot find VQPro.exe

The customer may have uploaded/deployed the wrong ZIP, extracted only part of it, or moved files separately. Re-download VQPro_Setup.zip, extract all, then open the VQPro folder.

Vault will not open after moving computers

Machine binding is doing its job. Use the documented rebind or restore process. Do not copy random vault files between machines and expect them to open.

Forgot master password

There is no normal reset if zero-knowledge encryption is active. Use recovery material only if it was created earlier. Otherwise the vault may be unrecoverable.

TOTP phone lost

Use recovery codes if saved. If none exist, follow the account recovery policy configured before loss. For future use, store recovery codes offline and add a spare authenticator where supported.

YubiKey missing

Use a spare key if configured. If no spare exists and policy requires the YubiKey, access may be blocked. This is why a spare key and recovery plan matter.

Backup will not restore

Check you selected the full backup folder, not a partial file. Confirm the backup was created by the same version or a compatible version. Confirm the password and hardware binding requirements.

Files missing after import

Do not delete originals until the vault confirms import and you can preview or export the file. Check the selected chamber, filters, and audit log.

Antivirus quarantines VQPro

Restore only if you trust the source. Add an exclusion only for the exact extracted folder, not for your whole Downloads folder. Scan the ZIP and verify the source.

Netlify payment succeeds but download does not trigger

Confirm Stripe success URL includes ?session_id={CHECKOUT_SESSION_ID}. Confirm Netlify has STRIPE_SECRET_KEY set to the live secret key. Redeploy after setting variables. Check the function path /api/verify-download.

Customer sees old website or old docs

Clear browser cache, check Netlify deploy ID, and confirm the uploaded package is the latest final ZIP. Old files can appear if the wrong deploy ZIP was dragged into Netlify.

PDF manuals look unreadable

Replace both VQPro_Security_Whitepaper_v3_7_1.pdf and VQPro_User_Manual_v3_7_1.pdf in the deploy root and in the customer ZIP docs folder. Do not use tiny screenshot-based PDFs.

14. Recovery Playbooks

A. Shortcut/corruption warning recovery

1. Delete old desktop shortcuts.
2. Delete partial or old VQPro folders if you are sure they are not holding live vault data.
3. Re-download the official customer ZIP.
4. Right-click the ZIP and choose Extract All.
5. Open the extracted VQPro folder.
6. Double-click VQPro.exe directly from inside the extracted VQPro folder.
7. If the app opens, create a fresh desktop shortcut: right-click VQPro.exe -> Show more options -> Send to -> Desktop (create shortcut).
8. Test the new shortcut once.

B. Suspected tampering recovery

1. Stop normal use immediately.

2. Disconnect from network if malware or remote access is suspected.

3. Do not delete audit logs.

4. Take screenshots of alerts.

5. Export or preserve access certificates if required.

6. Restore from a known-good backup only after the machine is clean.

7. Change passwords and rotate keys that may have been exposed.

C. Backup failure recovery

1. Check the destination drive has enough space.

2. Avoid OneDrive/Dropbox sync folders for first backup tests.

3. Use a simple local path without unusual characters.

4. Run VQPro as a normal user first; only elevate if documentation requires it.

5. Check antivirus/Controlled Folder Access if write access is blocked.

6. Retry to a different folder or external drive.

15. Best Practice Checklist

- Use a strong master password and do not store it beside the computer.
- Enable second factor only after saving recovery codes.
- Create a backup after every important change.
- Test restore before relying on a backup strategy.
- Never run the EXE from inside a ZIP preview.
- Never move VQPro.exe away from its folder.
- Never keep decrypted exports sitting in Downloads or Desktop longer than needed.
- Review audit logs after failed login attempts or alerts.
- Keep the customer ZIP and documentation together.
- Update only from trusted official packages.

16. What Not To Do

- Do not upload development keys, audit logs, vault config, or test vault material to the public website.
- Do not replace the website with a placeholder deploy package.
- Do not tell customers to drag VQPro.exe onto the Desktop by itself.
- Do not create shortcuts from inside the ZIP file.
- Do not claim recovery is possible if the password and recovery material are lost.
- Do not test kill switch, remote wipe, panic phrase, or self-destruct on real data.

17. Support Information to Collect

When asking for help, collect useful facts without exposing secrets.

- Windows version.
- Where the ZIP was downloaded from.

- Where it was extracted.
- Screenshot of the VQPro folder contents.
- Exact error message.
- Whether SmartScreen, antivirus, or Controlled Folder Access appeared.
- Whether VQPro.exe opens directly from inside the extracted VQPro folder.
- Do not send master passwords, seed phrases, vault keys, or private vault files.

Verified Windows Launch and Shortcut Procedure

This section replaces all older launcher-script instructions. The tested working method is to launch the real VQPro.exe from inside the extracted VQPro folder, then create a normal Windows desktop shortcut from that EXE.

Correct first launch

1. Download VQPro_Setup.zip from the official viperqpro.com purchase/download page.
2. Right-click the ZIP and choose Extract All.
3. Open the extracted VQPro folder.
4. Double-click VQPro.exe - the application with the VQPro logo/icon.
5. Keep VQPro.exe inside the VQPro folder.

Correct desktop shortcut

Right-click VQPro.exe -> Show more options -> Send to -> Desktop (create shortcut). Use the shortcut Windows creates. Do not drag VQPro.exe to the Desktop and do not use a shortcut that fails or points to the wrong location.

SmartScreen and password warning

If Windows SmartScreen appears, only continue if you downloaded VQPro from the official viperqpro.com purchase/download page. Click More info -> Run anyway. Do not forget or lose your master password. VQPro is zero-knowledge - there is no password recovery.