VunFisher controlled beta - complete tester walkthrough

Version 1.4.0 | Build 2026102653 | Windows x64

Follow the numbered path from free-access request through credential validation, authorized assessment, retest and feedback. Keep target passwords inside the installed Windows app only.

01

Purpose and authorization

VunFisher is ready for controlled testing. Use it only on computers, accounts and networks you own or have explicit permission to assess. Start with a noncritical Windows test computer. A completed scan covers only the selected checks; it is not a guarantee that a system is secure.

Know the two computers and two accounts:

- SCANNER: the Windows computer where VunFisher is installed. It opens locally at http://127.0.0.1:8787. Its local administrator account protects scans, saved credential references, evidence and reports on that computer.
- TARGET: the authorized Windows computer being assessed. It may be the scanner for a local assessment or a different computer for a remote assessment.
- HOSTED PORTAL: https://txvf.tinkextra.com. Its account is separate. It reviews uploaded results, manages agents and accepts license requests. It does not run a scan directly and does not receive target passwords.

Before you start

1. Use 64-bit Windows 10 or 11 and an email address you can access.
2. Install Microsoft Authenticator or another time-based authenticator on a phone.
3. For a remote Windows test, record the authorized target hostname and fixed private IPv4 address. Obtain an approved scan account and its current password.
4. Identify whether the target is workgroup, Active Directory domain joined or Intune managed. Ask IT before changing Group Policy, Intune or shared settings.
5. Do not use a domain controller, public-network profile or production-critical computer for the first test.

Part 1: Request access, download and install

1. Open https://txvf.tinkextra.com/overview/downloads.html.
2. Choose Get free access. Submit your name, email, package and requested term. No card is required. The activation code is sent to the supplied email address.
3. Download VunFisher-Windows.zip from the official page.
4. Verify the complete SHA-256 value shown on that page: Get-FileHash .\VunFisher-Windows.zip -Algorithm SHA256
5. Extract every file into a new folder. Do not run setup inside the ZIP.
6. Open INSTALL.vbs and choose Install VunFisher. Do not bypass organizational policy if unsigned scripts are blocked; ask IT to approve the package.
7. Open the TX VunFisher Desktop shortcut. The browser should open the local app at http://127.0.0.1:8787.

Part 2: Create the local scanner account, activate and enable MFA

8 Create the local scanner administrator account. This account stays on this Windows computer. It is different from a hosted txvf.tinkextra.com account. Use a password of at least 8 characters that is not a common or easily guessed password.

9 Enter the activation code from the approval email. An unused code must be redeemed within 30 days and binds to one installation. Keep it private.

10 Open account security and set up MFA. Scan the QR code with Microsoft Authenticator, enter the displayed six-digit setup code and save the recovery codes privately.

11 After setup succeeds, wait for the authenticator to display the NEXT six-digit code before signing in. The setup code is single use and cannot be reused.

12 Close VunFisher, reopen the Desktop shortcut and sign in again. Confirm the account, active license, MFA and settings persist before scanning.

Part 3: Choose the test path

13 Local assessment: use the installed app to assess the scanner itself. A remote credential profile is not required.

14 Credentialed remote Windows assessment: continue with Parts 4 through 6. The scanner and target must be able to reach each other over the approved private LAN or VPN path.

Part 4: Prepare the authorized Windows target

15 In the local VunFisher app, open Platform > License and download the licensed Target Setup Assistant 0.2.2.

16 Copy and run the assistant on the TARGET. Enter the SCANNER'S fixed private IPv4 address. Enter the existing scan account identity as DOMAIN\scanuser or TARGETCOMPUTER\scanuser. Do not enter any password in the assistant.

17 Select Audit this target. Review the numbered Credential scan setup plan.

18 Resolve every STOP item before continuing. Public networks, domain controllers and centrally managed settings require the appropriate IT, Group Policy or Intune path. Do not override those controls locally.

19 Use Preview changes before Apply approved plan. Apply only after authorization and only when the assistant has created a checkpoint. The Apply action can restart or configure WinRM and interrupt remote-management sessions.

20 Confirm the target is on a trusted private network, WinRM is available, the approved account has the required rights, and firewall scope permits only the scanner's approved address. The detailed route is in the Remote Scan Setup Guide linked from the download page.

Part 5: Create the credential profile on the scanner

21 Return to the local app at http://127.0.0.1:8787 and open Assessment > Credentials.

22 Step 1, Create Credential Profile:

- ✓ Profile name: a clear label for this target or account.
- ✓ Type: Windows WinRM.
- ✓ Username: the approved scan account name.
- ✓ Domain / Computer Name: the Active Directory domain or target computer name.
- ✓ Port: 5985 unless IT approved a different WinRM configuration.
- ✓ Password Environment Variable: a unique reference such as TXVF_LAB1_PASSWORD. This is a reference name, not the password.

23 Step 2, Add Windows Password: select the profile and enter the target account's actual password. Do not enter the VunFisher password or a Windows PIN.

- ✓ Leave secure remember unchecked for a one-time test.
- ✓ If approved for repeat scans, Windows DPAPI can protect the secret for this Windows user. Plaintext passwords are not stored in reports or the database.

Part 5B: Validate the credential before scanning

24 Step 3, Test Connection: enter the exact target IPv4 address, select the profile, confirm authorization and run Test Credential.

25 Continue to a full inventory only when Authentication is SUCCESS and the target identity is correct. Full Windows inventory normally requires Privilege ADMINISTRATOR and Evidence SUCCESS. STANDARD or PARTIAL results mean coverage is incomplete and must be investigated.

Part 6: Run, review, retest and report

26 Open Scans > New Scan and choose Credentialed Windows Assessment.

27 Enter only the authorized target, select the validated credential profile, read the scope statement, confirm authorization and start the scan.

28 Watch the scan monitor. Keep the target awake and connected. Cancel the job if the target or authorization changes.

29 When complete, verify Scan status, Connectivity, Authentication, Identity, Privilege, Evidence and plugin coverage. A completed job with failed or blocked checks is not complete coverage. Zero findings does not prove the target secure.

30 Review each finding's observation, evidence, match rationale, confidence, severity, TXVF Plugin ID/version and remediation guidance.

31 Record an owner and action. Use remediation, POA&M, accepted risk or another supported disposition as appropriate. Retest changed systems and compare the new evidence with the original assessment.

32 Export a report and confirm that a security, IT or audit reviewer can understand the scope, authentication result, coverage, evidence, action and retest result.

Part 7: Optional hosted review and feedback

33 If your test includes the Windows agent uploader, register the scanner through the hosted portal and upload only approved completed finding summaries. The uploader is not a remote command channel.

34 Submit feedback at https://txvf.tinkextra.com/overview/beta-feedback.html. Include Windows edition, VunFisher build, assessment ID, exact steps, expected result, actual result and the displayed error. Remove passwords, activation codes, MFA seeds, recovery codes, credentials, private keys, customer data and unredacted scan evidence from screenshots and attachments.

Troubleshooting order

- Website credentials fail locally: use the local account created at 127.0.0.1:8787. Hosted and local accounts are separate.
- MFA fails immediately after enrollment: wait for the next authenticator code or use one unused recovery code.
- Activation email is missing: confirm the address, check junk/spam and contact support. Do not publish or forward an activation code.
- Port 5985 is unreachable: check target address, power, private network profile, WinRM listener, firewall source scope and LAN/VPN isolation.
- Windows rejects authentication: confirm DOMAIN\user or TARGET\user, reload the actual account password, and check whether the account is disabled, locked or expired. A Windows PIN is not a remote account password.
- Authentication succeeds but privilege is STANDARD: verify the approved rights and workgroup remote-token policy. Use the target setup guide and IT policy.
- Evidence is PARTIAL: review the unavailable checks and diagnostic messages. Missing evidence must not be interpreted as a clean result.
- A remembered secret is unavailable after restart: reload it in Credentials or use approved DPAPI persistence. A stored reference does not prove the password is still valid.
- Hosted rerun says to use the Windows app: open the Desktop shortcut and run the assessment at 127.0.0.1:8787. The hosted portal does not execute scans.

Official links

Main website: https://txvf.tinkextra.com/overview/

Downloads, license request and checksum: https://txvf.tinkextra.com/overview/downloads.html

Interactive tester walkthrough: https://txvf.tinkextra.com/overview/downloads/VunFisher-Tester-Walkthrough.html

Detailed remote scan guide: https://txvf.tinkextra.com/overview/downloads/VunFisher-Remote-Scan-Setup-Guide.html

Resources: https://txvf.tinkextra.com/overview/resources.html

Feedback: https://txvf.tinkextra.com/overview/beta-feedback.html