Y-TEC Tsumugi Drive Operation Manual

日本語 | English

- **Target version:** 1.0.0-internal-beta
- **Document status:** Source republication edition; isolated development evaluation only
- **Reference specification:** DiskClone_Development_Spec.md v2.0
- **Last updated:** 2026-09-29

This republication covers source code and documentation. General distribution of the product ZIP and EXE is on hold. It is not the stable 1.0.0 release or completion of representative hardware acceptance.

- Product page: https://ytec.cloudfree.jp/forge/projects/tsumugi-drive/
- Public source: https://github.com/ytec-forge-commits/ytec-disk-clone
- Contact: https://ytec.cloudfree.jp/forge/contact/

Old ZIPs, EXEs and PDFs are not reused. Evidence from the 2026-08-28 candidate does not certify this republication candidate.

This manual describes isolated evaluation of development code. Source access does not provide a signed official application, validated rescue media or a hardware guarantee. The pinned source has Japanese UI; English control names below are explanatory translations, not a claim of an English UI in this snapshot. Uncommitted English UI and icon changes are not selected.

> **WARNING** This is not a stable release. Representative hardware acceptance, the final distribution audit, code signing, and acceptance in a clean environment without ADK are incomplete. Do not use it for important data, production or work devices, normal day-to-day work, or as the only backup. Evaluate it only in an isolated test environment using media that may be erased.

1. Before evaluation

Prepare an erasable test-only destination, restore target, or USB drive; a separate, proven-restorable backup; AC power; and a supported x64 test system. Previous Windows 10 22H2 and Windows 11 25H2 VM results are historical evidence, not acceptance of this candidate. No new OS compatibility claim, including Windows 11 24H2, is made by this republication work. Creating rescue media additionally requires properly licensed Windows ADK, WinPE Add-on, and required servicing updates.

Never use the product with irreplaceable, business, or customer data; dynamic disks, LDM, Storage Spaces, Windows software RAID, or an unanalysable layout; a USB flash drive as a clone, restore, or rescue target; GPT-to-MBR conversion; cloud or network image storage; or any attempt to bypass BitLocker, Secure Boot, UAC, or Windows activation.

Verify the Portable ZIP

These steps apply only to a separately authorised evaluation candidate. This source republication does not offer a product ZIP.

Place the Portable ZIP and its external .sha256 file in the same directory. In PowerShell, substitute the actual candidate name and run:

```
$zip = Resolve-Path '.\Y-TEC-Tsumugi-Drive-1.0.0-internal-beta.zip'
$actual = (Get-FileHash -LiteralPath $zip -Algorithm SHA256).Hash
$expected = ((Get-Content -Raw -LiteralPath ($zip.Path + '.sha256')).Trim() -split '\s+')[0]
$actual
$expected
$actual -ceq $expected
```

The last value must be True, and the hash must exactly match the one provided through the authorised delivery channel. Do not extract or run a mismatched archive.

Verify the extracted EXE

Do not run directly from the ZIP. Extract all files into a new ordinary local folder, then compare the EXE with its one matching entry in SHA256SUMS.txt:

```
$exe = Resolve-Path '.\ytec-tsumugi-drive.exe'
$actual = (Get-FileHash -LiteralPath $exe -Algorithm SHA256).Hash
$matchingLines = @(Get-Content -LiteralPath '.\SHA256SUMS.txt' |
  Where-Object { $_ -cmatch ' \*ytec-tsumugi-drive\.exe$' })
if ($matchingLines.Count -ne 1) { throw 'The EXE SHA-256 entry is not unique.' }
$expected = ($matchingLines[0] -split '\s+')[0]
if ($actual -cne $expected) { throw 'EXE SHA-256 mismatch.' }
'EXE_SHA256_OK'
```

The historical 2026-08-28 candidate was unsigned and is not redistributed. This manual makes no current claim about signing-service applications. For any future official direct download, check the actual final EXE's signing method, verification result and SHA-256 at the official distribution source. Unsigned or self-signed files may show publisher or SmartScreen warnings; self-signing is not Microsoft or commercial-CA trust and does not guarantee warning avoidance. Do not disable SmartScreen, UAC, Secure Boot, or anti-malware protection. Only make an individual execution decision after verifying both the ZIP and EXE hash in an authorised isolated evaluation; reject unexpected signer or hash results.

Portable data

Persistent settings, the first-run safety acknowledgement, logs, and resume information are stored only in data beside the EXE. The product does not silently fall back to AppData, cloud storage, or a network location. Preserve the entire data folder when updating. Completed .tsumugi images and their adjacent .partial files are not stored there.

Before write-capable operations, the product verifies that data is an ordinary non-reparse directory and that it can safely write, flush, read back, and remove a test file. If this cannot be proven, the application stays in diagnostic-only mode. If the data backing disk cannot be kept separate from the source or destination, logs can be isolated to bounded RAM for that session; the product still does not fall back to AppData.

2. Safety checks for every operation

1. Do not identify a disk by number or letter alone. Compare model, capacity, connection type, GPT/MBR state, serial-number suffix, partition map, and Windows/data/USB designation.
2. Confirm that source and destination are different physical disks.
3. Read the displayed overwrite scope, storage location, operation mode, and verification mode.
4. For destructive work, tick the confirmation and enter uppercase ASCII OK. ok, full-width characters, and surrounding spaces do not start an action.
5. If final re-identification fails, reconnecting does not resume work. Start selection again.

6 Do not remove a target or force-close the application before its final result is shown.

Failure, cancellation, missing data, and incomplete verification are never reported as success. A stopped destination or restore target can remain incomplete or offline. Do not online, format, or retry it before determining the reason.

The Windows application itself does not write to the source disk, but the running operating system and VSS can perform their normal writes. Use WinPE when an OS-level read-only source is required. The operation fails closed when stable identity, read-only state, or Snapshot-to-physical-range mapping cannot be established.

3. Windows application

The Japanese left navigation contains ドライブをクローン (**Clone Drive**), イメージを作成 (**Create Image**), イメージを復元 (**Restore Image**), 起動を修復 (**Repair Boot**), レスキューメディア (**Rescue Media**), and ログ・診断 (**Logs & Diagnostics**). Initial inventory is read-only. An unknown selection, unhealthy disk, USB flash drive, or unsupported layout cannot proceed to safety confirmation.

Clone Drive

Select an erasable destination and a source, then choose one mode:

- **Normal (exact clone):** clones the whole disk to a same-or-larger target with the same logical-sector arrangement and preserves partition style.
- **Shrink migration:** reconstructs a smaller layout only on the destination; it does not shrink the source.
- **Rescue (data disk):** Windows accepts only an already read-only or offline, non-system data disk with 512-byte logical sectors and a same-or-larger destination. It neither shrinks nor converts partition style.

For shrink migration, select preserved partition style or eligible system-disk MBR-to-GPT conversion, then review partition and spare-capacity placement. Required Windows boot partitions cannot be removed. Select **Continue to Safety Review**, review the read-only analysis, power warning, and target summary, then enter uppercase OK on the final screen. Wait for progress, VSS, read-back, and final-verification results.

Normal and shrink system clones reflect the VSS start point. A result of “verification complete, ready to swap” proves write and read-back completion, not successful boot after hardware replacement; the destination remains offline. A rescue result remains “possible partial loss” even when no unread range was found.

Create Image

Select a source and one mode: **Normal** writes a whole disk to a single .tsumugi; **Shrink migration** captures NTFS through VSS while preserving static system areas as exact RAW; **Rescue** stages an already protected non-system data disk once into owned temporary storage before making the image.

Choose **Full (recommended)** for every write read-back, authentication/hash, metadata verification, and an additional final scan, or **Fast** to omit only that additional pre-completion scan. Choose a new NTFS or exFAT filename on a physical disk separate from the source. Completed images are never overwritten. If encryption is selected, no recovery key exists: losing the password makes the image unrecoverable.

Creation writes to an adjacent .partial; the final .tsumugi name is used only after verification, VSS cleanup, and destination re-identification all succeed. The current Windows image UI operates on a whole disk only and rejects BitLocker, exFAT, and FAT32 content areas for shrink creation.

Restore Image

Choose a .tsumugi image, enter its password when encrypted, and wait for full validation using the same read handle. This is mandatory even for an image created with Fast verification. Then choose whole-disk or individual-partition restore where supported, select the destination, review the overwrite scope, and enter uppercase OK.

The running Windows system disk cannot be restored from Windows; select the image and target again in WinPE. No hidden scheduled job is created. Shrink whole-image restore starts only when WIM staging, checkpoint, and logs can be placed on a third safe local disk distinct from both image storage and restore target. Boot repair, if needed, is a separate WinPE operation.

Repair Boot

Windows **Repair Boot** does not write boot repairs directly to the running Windows disk. It opens the path to create rescue media. Perform actual repair in WinPE after selecting the target again.

4. WinPE application

WinPE uses no scheduled jobs. In one booted session, select source, destination, or image; confirm; execute; and verify.

Clone, image, and restore

For a clone, select source and destination, choose exactly one of Normal, Rescue, MBR-to-GPT (other disk), or Shrink migration (WinPE/GPT/512B), then run read-only review. WinPE fixes the source read-only and checks stable identity, capacity, sectors, and that the booted rescue USB is excluded. Review the layout and overwrite scope, enter uppercase OK, and start. Rescue reads forward and backward in small blocks with finite retries and zero-fills any remaining unread regions; it does not combine shrinking, conversion, or boot repair.

To create an image, choose source and a new .tsumugi path on another physical disk, Full or Fast validation, Rescue only for suspected failure, optional encryption, then review and enter uppercase OK. Current WinPE UI creates Normal exact or Rescue images; it does not expose shrink-image or arbitrary partition-only creation. Rescue creation needs enough separate space for both RAW staging and the largest image.

To restore, choose an image, password if needed, full validation, whole disk or eligible individual partition, and a destination. Review that target, image media, and work area are separated, then enter uppercase OK. Rescue missing ranges remain zero-filled and reported as partial loss. A shrink image with no missing range and 512-byte logical sectors restores only as a whole disk.

Repair Boot

Choose one repair target, run automatic analysis, and review Windows, GPT/MBR, ESP/Active partition, WinRE, and third-party EFI loaders. Preserve third-party EFI by default; removal needs its own explicit confirmation. Current-PC UEFI NVRAM repair is planned only after explicitly selecting that the disk is for this PC. If a required ESP or BIOS system area can safely be created through NTFS shrinking, the product requires another uppercase OK, reanalyses, and asks for review again.

Repair rebuilds BCD with Microsoft-signed BCDBoot and handles boot files, required attributes, UEFI fallback, and identifiable WinRE. An ambiguous WinRE is reported as partial repair. Completion does not guarantee a successful physical boot.

5. Pause, resume, cancellation, and one persistent slot

Pause for clone, image creation, and restore becomes available only at a verified safe boundary. It takes effect after the current safe unit, and the same button resumes. **Cancel safely** waits for a cancellable boundary; short final-metadata phases cannot be cancelled. Do not substitute force-close or power loss for cancellation.

There is at most one persistent record at data\active.checkpoint. A new write-capable operation does not start while that slot is occupied. There is no job list, scheduled execution, or automatic run. Product UI can currently resume only a WinPE Normal exact/Rescue whole-disk image restore, and only when image, destination, output, work area, and restore plan exactly match. Unknown, corrupt, orphaned, replaced, or identity-mismatched state is not resumed or automatically deleted. The Windows backend does not currently resume a persistent checkpoint.

Discard removes only a re-identified active.checkpoint and explicitly bound, application-owned incomplete output. It never removes completed .tsumugi files, destination disks, legacy jobs, user files, or other history, and it refuses discard when identity changed after display.

6. Completion power action

Only after full success evidence exists and automatic sleep prevention has been released, the product offers an action after completion. Windows can offer Do nothing (default), Sleep, Restart, or Shut down; WinPE offers Do nothing, Restart, or Shut down. Selection and final confirmation are separate. A failed power request does not invalidate a verified operation result, and no power action is offered for failure, cancellation, or partial loss.

7. ADK, rescue ISO, and rescue USB

The Portable ZIP contains no Windows ADK, WinPE, WIM, ISO, CAB, or Microsoft EXE/DLL payload. Rescue media are created only from verified local ADK/WinPE installed under the user's own licence; this product does not grant or transfer Microsoft licences.

Rescue Media checks the environment. The UI can show official Microsoft install, verified offline-layout install, create official offline layout, and remove only Tsumugi-managed ADK. In this 1.0.0-internal-beta candidate, the ADK safety gate is closed: these choices only display the stop reason and do not start network access, browsing, EULA retrieval, UAC, installer execution, layout creation, or removal. A user-selected official Microsoft guidance link can open in the default browser, but packages are not automatically acquired or installed.

When a validated installed ADK, WinPE Add-on, and required update are present, you may create a new ISO: select ISO, 2011 CA (compatibility) or 2023 CA (newer PCs), choose a new location, review content and administrator requirements, and wait for WIM, fonts, Y-TEC payload, manifest, per-file hash, and full ISO hash verification. A completed ISO is not proof that it boots on physical hardware.

For USB, use an erasable test USB of at least 8 GiB (16 GiB preferred), verify model/capacity/connection/serial suffix, choose initialisation or an eligible owned-media refresh, choose NTFS (default) or exFAT for data, review the erase scope, enter uppercase OK, and wait for all-file SHA-256 verification. The physical disk of the USB from which WinPE is booted is excluded from clone, restore, and rescue write targets.

8. Logs, support ZIP, and update check

Windows logs are saved to data\logs. Routine logs are retained for 30 days or 200 MiB total; failure logs for up to 90 days. The product does not log full serials, passwords, derived keys, BitLocker recovery keys, Windows product keys, cookies, credentials, or file contents, and it minimises paths.

To make a support ZIP, open **Logs & Diagnostics**, select a new local save location, review post-masking names, sizes, and exclusions, then create. It is finalised only after complete verification and is never sent automatically. Review it again before sharing and never post unredacted logs, personal or customer data, disk images, recovery keys, passwords, or credentials in a public Issue.

Only an explicit **Check for updates** action contacts the fixed Y-TEC HTTPS URL. There is no startup check, background connection, automatic download, automatic update, or automatic execution. The result shows version, published time, distribution page, and SHA-256; the user chooses whether to open the page. Product networking is limited to this manual update check and a future, release-gated, explicitly consented Microsoft ADK acquisition path. It has no telemetry, advertising, cloud sync, or automatic log upload.

9. Known limitations and stop conditions

Representative hardware acceptance for normal Windows clone, shrink migration to a smaller SSD, WinPE direct clone, data-disk imaging/restore, and physical USB creation/boot remains incomplete. Synthetic tests, VM results, source-code review, or a previous candidate do not guarantee safety for the current build or physical media. The ADK acquisition/EULA/quiet-install/offline-layout/managed-removal gate remains closed.

In the first historical SATA-SSD to USB-enclosed SSD test, copying and booting after replacement succeeded, but the product completion judgment failed with error 1168. Retesting the fixed path on that configuration is still required; this failure is not erased or relabelled as a full pass.

Historical 2026-08-28 Golden corpus, deterministic and coverage-guided fuzzing, regular/static analysis/ASan CTest gates, and Codex Security diff audit are evidence for software paths; they are not a substitute for representative hardware, real USB, 4Kn, or post-swap boot acceptance. The 2026-08-28 local Portable candidate passed its internal/external hash audit and excludes Microsoft payloads, but it is unsigned and unpublished. These are not fresh test results. Legacy VirtualBox procedures must not be applied unchanged to the current VMware lab.

Normal cloning requires equal logical sector sizes. 4Kn and conditional 512-byte/4Kn migration have not passed representative physical acceptance. BitLocker is not guaranteed; the product does not store or transmit recovery keys or passwords or bypass encryption. Windows 7/8 disk compatibility is not guaranteed. Windows 11 26H1 x64, ARM64, 32-bit Windows and Windows Server are outside the declared stable support scope.

The WinPE candidate has no Windows-equivalent Logs & Diagnostics/support-ZIP screen. Completion proves only the reported operation verification, not physical boot, hardware compatibility, data recovery or business continuity.

Do not distribute or describe 1.0.0-internal-beta as stable 1.0.0. If you observe anomalous physical I/O, suspected source writes, target confusion, or unexpected online state, stop new operations immediately. Do not alter the target; retain the minimum evidence excluding secrets and use the private reporting path below.

10. Report a security issue

After republication, use GitHub Private Vulnerability Reporting when enabled:

https://github.com/ytec-forge-commits/ytec-disk-clone/security/advisories/new

Fallback contact: https://ytec.cloudfree.jp/forge/contact/

Do not post vulnerability details, proof of concept, logs, images, full serials, disk images, recovery keys, passwords, credentials, or personal information in a public Issue. If the form is unavailable, consult the current route in SECURITY.md or send only a secret-free summary through the contact page. Do not attach disk images, recovery keys or credentials to that contact form.

11. Licence, terms, and official-build distinction

Y-TEC-owned source, documentation, and build output are under Apache License 2.0. See LICENSE, NOTICE, THIRD-PARTY-NOTICES.txt, licenses, and SBOM.spdx.json. Use, modification, copying, and redistribution are allowed under Apache-2.0 and applicable third-party licences. A third-party build or modified version is not an official Y-TEC build unless Y-TEC expressly says so; clearly distinguish its name, display, distributor, and modifications, and follow TRADEMARKS.md.

Windows, ADK, WinPE, and other Microsoft licences are not included in this product. Review packaging/terms-of-use.txt, packaging/privacy-and-network.txt, and packaging/safety-and-limitations.txt for the pre-release validation terms, privacy/network boundary, and safety limits. These terms do not add restrictions to rights granted by Apache-2.0 or third-party licences.