

Sino Control Hub Admin Manual

Running your organisation's managed vaults from the Control Hub console: first setup, the organisation kits, every policy setting, devices, approvals, recovery, file requests, shared folders, the audit log, routine checks and what to do when something goes wrong

Sino Privacy Vault (<https://sinosecure.app>)

1. About This Manual

This manual is for the people who use the Control Hub console: owners, admins, helpdesk staff and auditors. Installing and running the hub itself (the server, the database, proxies, backups, single sign-on and SIEM connections) is in the **Control Hub Deployment Guide**. The people whose vaults you manage have their own **Sino User Manual**.

What the hub is, in one paragraph: the hub enrolls, configures and audits your organisation's Sino vaults. Files never pass through it. Each device encrypts its files and sends them straight to storage your organisation owns. The hub holds the device list, the policy, the audit events and public keys, and **cannot open a vault**. Only a quorum of your organisation kits can, in the Sino app (section 4). Sensitive actions such as a remote wipe need a quorum of approving admins, each with their own passkey, and devices check those approvals themselves, so even a breached hub cannot wipe a device.

2. Roles

Everyone who signs in to the console has one of four roles. The hub enforces them, and the console hides what a role cannot do.

Role	Can
Owner	Everything, including admins, hub setup and API keys
Admin	Policy, enrollment, devices and commands, people and groups, storage, audit destinations, approvals, file requests, recovery

Helpdesk	Sees devices, people, policy, shared folders and file requests; sends commands that need no approval; asks for (never approves) a wipe
Auditor	Reads the audit log, destinations, devices, approvals, shared folders and file requests

Only owners and admins with a passkey can be **approving admins** (section 7). Every admin signs in with a passkey. An owner can also turn on sign-in with Microsoft Entra ID, Google Workspace or SAML (Deployment Guide, section 11), but **approvals always need the passkey**, and no company sign-in ever opens a vault.

Console sessions end after 30 minutes without activity, and after 12 hours in any case.

3. The First Day

Once the hub runs (Deployment Guide), set it up in this order.

1. **Claim the hub.** Open its address. Enter the setup code from the hub's log (it prints a new one at every start until claimed), the hub's **permanent address**, and your name, then create your passkey. Choose the address carefully: passkeys only work on it, and devices keep it. Changing it later means new passkeys for every admin.
2. **Invite your other admins** under **Admins** (section 15), so they can be approving admins. A quorum of two or more is safer than one: with one approval, a single admin (or a stolen login) can wipe a device alone, after the cooling-off.
3. **Hub setup.** Enter the organisation name (devices show "Managed by ..."), choose the approving admins and how many must approve, and make the setup link.
4. **Run the kit ceremony** by opening that link in the Sino app on your own Windows PC or Android phone (section 4). The app makes the organisation's keys, splits them into kits, and signs the hub's certificate. The page moves on by itself when it is done.
5. **Add organisation storage** under **Storage**, and press **Test** on it. Until you add some, managed vaults sync only to clouds the person connects, and only if the policy allows personal clouds.
6. **Set the policy** under **Policy** (section 6) and publish it.
7. **Add an audit destination** (your SIEM) under **Audit destinations**, and press **Send a test event**.
8. **Turn on e-mail notices** under **Hub setup → E-mail notices**, so approvers hear when something needs them. Each admin sets their own address under **Your account**.

9. **Connect your directory** under **People** (SCIM from Entra ID or Okta, or Google Workspace), or add people by hand. Then choose, under **Hub setup → Retention and the directory**, what happens to a person's devices when the directory removes them.
 10. **Enroll the first vault** under **Enroll a vault** (section 8).
-

4. The Organisation Kits

The kits are the only way to recover a vault, to recover a shared folder whose owners all left, to replace the approving admins without passkeys, or to move the hub. **Nobody, including Sino, can do these without them.**

- **What they are.** The kit ceremony makes two keys: the **recovery key**, to which every managed vault seals a copy of its keys, and the **root key**, which vouches for the hub. Both are split so that a quorum of kits is needed (2 of 3 by default), one kit per holder, printed or saved. The ceremony runs only in the Sino app, never in the console, so a breached hub cannot capture the kits. The keys never reach the hub.
 - **Keep each kit apart.** One holder per kit, each stored somewhere different (a safe, a sealed envelope with a second person). A kit alone opens nothing.
 - **A single admin** can choose 1 of 1. Losing that kit then makes recovery impossible, and it is also that admin's only way back in after losing their passkey.
 - **When a holder leaves, or a kit may be lost,** replace the kits: **Hub setup → Organisation keys**, tick **Replace the kits**, and make the link. Holders bring enough of the current kits to the Sino app, which makes the new kits. Every device takes the new key at its next check-in, and each vault re-seals its recovery copy at its next unlock. **Vaults and recovery** shows which have not yet. Until a vault re-seals, the old kits still open its old copy, so ask people to unlock soon after a rotation.
 - **The recovery key in an HSM.** At the ceremony you can give the public key of an RSA key kept in an HSM or a cloud key service (Azure Key Vault, AWS KMS, Google Cloud KMS, PKCS#11). Every recovery then needs both the kits and the HSM.
-

5. The Console at a Glance

Page	What it is for
------	----------------

Overview	Devices enrolled, devices not seen for 3 days, devices with audit gaps or breaks, failing destinations
Devices	Every enrolled vault and device; open one to send commands and read its events (section 9)
Vaults and recovery	Each vault's recovery copy; recovering a vault; asking for a cloud wipe (section 11)
Approvals	Actions waiting for the approving admins, and earlier ones (section 7)
People	The directory: people, groups, SCIM and Google Workspace sync (section 14)
Shared folders	Folders, members and roles (never names or files), people from outside the company, share links (section 13)
File requests	Requests to take files out of a vault, when the policy says an admin approves (section 12)
Enroll a vault	Enrollment links for one person, and enrollment profiles for your MDM (section 8)
Policy	The default policy, and policies for groups (section 6)
Audit log	Every device and hub event, as your SIEM receives it (section 16)
Audit destinations	Microsoft Sentinel, Splunk, syslog over TLS, HTTPS webhooks
Storage	Organisation storage targets and their tests
Admins	Who can sign in, their roles, the approving admins, invitations, lost passkeys (section 15)
API keys	Keys and OAuth clients for your own scripts and tools (owners only)
Hub setup	Organisation name, kits and certificate, retention and archive, what a directory removal does, e-mail, company sign-in (owners only)
Your account	Your company sign-in links and your address for notices

6. The Policy, Setting by Setting

The policy is what every managed vault follows. The hub signs it; devices take a new version at their next check-in and refuse anything older or unsigned. Every change publishes a new version.

Some rules are not settings, so no policy can change them: **duress (the decoy vault) is always off** in a managed vault, the person can always wipe their own device, and only the hub (with approval) can delete a vault's data from your storage.

Group policies. Under **Policy → Which policy**, give a group its own policy and put the groups in order: a person's vaults follow the first of their groups that has one, otherwise the default. The cooling-off, file names in audit and shared folders always come from the default.

Changes that need the approving admins (section 7): turning on **file names in audit events** (it tells you more about people), and shortening or narrowing the **cooling-off**. The button then reads **Ask the approving admins**, and the policy is published once they approve. Every other change publishes at once.

Unlocking

Setting	Default	What it does, and what to weigh
Lock after this many idle minutes	The person's choice	Locks an open vault after this long without input. A short time stops an unattended PC staying open.
Allow fingerprint, face and Windows Hello unlock	On	Off makes everyone type their password.
Wrong passwords in a row before the device wipes itself	Off	Wipes Sino from that device after this many (3 to 100). Local only: the vault stays in your organisation's storage.
Alert on wrong passwords	On	The person's other devices are told of repeated wrong passwords on one of them.
Lock after this many hours without reaching the hub	336 (14 days)	A device kept offline, stolen or taken by someone leaving locks, an open vault too, and unlocks only after reaching the hub again. 0 turns it off. At least twice the check-in interval.

Unlock only while the hub can be reached	Off	Every unlock checks in first, so a device you removed or wiped never opens again, even offline. While the hub is down, or a device has no network, nobody can unlock.
Minutes between check-ins with the hub	60	How soon a phone gets a command (15 at the soonest). A Windows PC with Sino open gets commands within seconds.
Keep Sino running on Windows PCs	Off	Closing Sino hides it to the tray, the tray has no Exit, and Sino starts at sign-in, so commands reach PCs within seconds (section 10).

Storage and sharing

Setting	Default	What it does, and what to weigh
Allow personal clouds	Off	People may add their own MEGA, Google Drive or OneDrive alongside your storage. Those copies are outside your control.
Allow legacy beneficiaries and the dead man's switch	Off	The consumer handover feature. Usually left off at work.
Devices per vault	2	How many devices one vault may run on (1 to 10). A recovery needs room for one more (section 11).
Allow shared folders between colleagues	On	Off stops new folders and every member's access to existing ones (section 13).
Let owners invite people outside the company	Off	A client or accountant joins a folder with their own Sino app. Anything they can read, they can keep.
Allow share links to a file	Off	A link opens one file in a browser, for people without Sino, for up to the days set below (1 to 90, 7 by default).

Screen

Setting	Default	What it does
---------	---------	--------------

Always block screenshots and screen recording of Sino	On	People cannot turn the protection off. It hides Sino's windows from capture tools, screen sharing and Android's recent apps, but not a photo of the screen, nor files another app opened.
---	----	---

Taking files out of the vault

Four actions leave a decrypted copy outside Sino: **restoring files to the device**, **saving Local Vault files outside Sino**, **copying shared folder files out**, and **the Windows drive and other Android apps opening vault files**. Each has one rule:

Rule	Effect
Allowed	Runs without asking.
The hub confirms (default)	Runs only after the hub says yes, just before. The hub records it, and refuses it when the device cannot reach the hub, its storage access is stopped, or the daily limit is reached.
An admin approves each time	The request goes to File requests first (section 12).
Off	Not offered in the app at all.

- **Files a vault may take out in 24 hours** (no limit by default) caps what the hub confirms. What an admin approved is not held back by it.
- **Apps trusted to open vault files** open files through the Windows drive or Android's file picker without asking, whatever the rule says, and each device records the files they open. Apps that devices saw trying are listed under **Seen trying to open vault files** with a **Trust** button. A Windows program is its file name and publisher, an Android app its package and signing certificate, so a renamed or unsigned copy is not trusted. On Windows only programs signed by their publisher can be listed. **Trusting an app trusts what it does with a file**: Word can save a copy to OneDrive or attach it to an e-mail.

None of this stops someone photographing the screen, retyping what they see, or using a file once another app has opened it.

Audit

Setting	Default	What it does
An event for every added or changed file	Off	Off sends one summary per sync. Deletes, restores, exports and shares are always sent per file.
People see the events about their own device	On	The person can read their device's activity in Sino.
File names in audit events	Off	Off sends file ids only. Needs the approving admins to turn on , and devices tell the person when it applies.

Updates and approvals

Setting	Default	What it does
Minimum Sino version	None	Older apps sync nothing until they are updated.
Cooling-off before an approved wipe, unenroll or change of approvers runs	6 hours	Gives every admin time to cancel. Shortening it needs the approving admins.
Apply it whatever the quorum	Off	Without it, the cooling-off applies only with a single approving admin, where it is always at least an hour.

7. Approvals, Quorum and Cooling-Off

These need a quorum of the **approving admins**, each approving with their own passkey:

- a **remote wipe** or **unenroll** of a device;
- a **cloud wipe** (deleting a vault's data from your storage);
- taking a vault's **recovery file** or making a **recovery link**;
- deleting a **shared folder**, or taking its recovery file;
- **new approving admins** without the kits;
- a **policy** that lowers privacy or weakens the cooling-off.

How it runs.

1. Someone asks (an admin, a helpdesk member, an API key, or the directory removing a person). It appears under **Approvals → Waiting**, and the approvers are e-mailed.
2. Approvers press **Approve with my passkey** within 24 hours of the request.
3. Once the quorum is met, a wipe, unenroll, cloud wipe, change of approvers or policy waits for the **cooling-off**. **Any admin can cancel it until it runs**, and every owner and admin is e-mailed when it is approved, with when it runs.
4. An approved command waits up to 7 days for its device. An approved recovery file or link must be taken within a day.

The approving admins and the quorum are part of the hub's certificate. Change them under **Admins → New approving admins** (the current approvers approve) or, if too few approvers are left, by signing a new certificate with the kits under **Hub setup**. **Removing an admin does not take them off the approvers' list**: change the list too.

8. Enrolling Vaults

A vault enrolls into the hub once; it stays your organisation's until it is unenrolled. The person needs **a new, empty vault**, unlocked, and Sino shows them what your organisation can do with it before they confirm.

- **One person:** under **Enroll a vault**, choose the person in the directory (so removing them later acts on this vault), give a label that only admins see, choose how long the link is valid (1 to 24 hours), and create it. Send the link to that person only. On Android they scan it in Sino; on Windows they open it.
- **Through your MDM (Intune and others):** make an **enrollment profile**: one link your MDM gives every device. It lasts up to a year, may be limited to a number of vaults, and can be revoked at any time. Tick **Tie each vault to the person the MDM names** to put each vault with its person.
 - **Android (work profile):** in Sino's managed configuration, set `enrollment_link` to the link, and `user_principal_name` to `{{UserPrincipalName}}`.
 - **Windows:** set the strings `EnrollmentLink` and `UserPrincipalName` under `HKLM\Software\Policies\Sino\Managed` (or the user's `HKCU` key), with a configuration profile or a script.
 - Anyone holding a profile link can enroll a vault of their own until it is revoked or used up, so keep it in your MDM. It never gives access to another person's vault.

- **A second device for the same vault** joins from the person's first device in Sino; it counts towards **Devices per vault**.
-

9. Devices

Devices lists each vault and the devices it runs on: the platform, the Sino version, when it was last seen (marked once it is over 3 days), the policy version it applied, and its audit chain (**intact**, **gap** or **chain broken**). Devices check in at start, at every unlock and on the check-in schedule.

Open a device to see its ids, enrollment date, policy and certificate it applied, whether its organisation storage access is allowed, and its events.

Commands that need no approval (owners, admins and helpdesk):

Command	Effect
Sync now	Starts a sync on the device.
Refresh policy	Makes it fetch the policy at once.
Lock the vault	Locks it; the person needs their password to unlock again.
Stop its storage access	It stops syncing until you press Give it back . Taking files out that the hub confirms is refused too.

Commands that need approval: Ask for a remote wipe (Sino and the vault are removed from the device; the encrypted copy in your storage stays) and **Ask to unenroll** (the vault leaves managed mode and is no longer your organisation's). The device runs these only with the approvers' signatures, which it checks itself.

Remove from the hub refuses the device's calls from now on. **It does not wipe it**, and a removed device gets no more commands, so remove a lost device only after its wipe has run.

When a command arrives. A Windows PC with Sino running holds a live link to the hub and gets commands within seconds. Any other device gets them at its next check-in while it is on and online. There is no push: a closed app runs no code (section 10).

10. Keeping Sino Running on PCs

Commands reach a PC within seconds only while Sino runs there. Tick **Keep Sino running on Windows PCs** in the policy:

- closing Sino's window hides it to the tray, and the tray has no Exit;
- **Launch on System Startup** and **Background Orchestration** show on in Sino's settings, and people cannot turn them off; Sino puts its start-up entry back if someone removes it;
- only one Sino runs per person, however many times it is started.

Someone can still end Sino from Task Manager. When it next starts, it records **Sino not running** (`NOT_RUNNING`) with when it stopped and until when, in the device's events and your SIEM. Signing out, restarting or a power cut is not reported. A PC where Sino never starts again shows as not seen after 3 days.

To stop people removing the start-up, set the machine-wide entry with Intune (a custom OMA-URI or a script) or Group Policy (Preferences, Registry): the string value `SinoPrivacyVault` under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, set to `"C:\Program Files\SinoPrivacyVault\SinoPrivacyVault.exe" --minimized` (where Sino is installed). Sino then adds no start-up entry of its own.

Closing Sino never avoids a wipe: the vault opens only through Sino, which checks in with the hub before any unlock.

11. Vaults and Recovery

Each managed device seals its vault's keys to your organisation's recovery key whenever it unlocks with new keys or new kits. The hub keeps that **recovery file** but cannot open it.

Vaults and recovery shows, for each vault, whether it is sealed, sealed to old kits (it re-seals at its next unlock), or not sealed yet (it waits for an unlock).

Recovering a vault (a successor takes over someone's vault, or a person lost every device):

1. Make room: the vault needs space for one more device under **Devices per vault**. Remove a lost device first.
2. Under **Vaults and recovery**, **Ask for a recovery link** and **Ask for the recovery file**. The approving admins approve both under **Approvals**, then take them there (within a day).
3. Enroll the device that should receive the vault with the recovery link. It shows a **recovery code**.

4. In the Sino app of an admin, open **Work vault** → **Recovery console**, load the recovery file, and bring enough kits.
5. Paste the device's recovery code, **compare the fingerprint with the person on the phone**, and send them the answer code. The vault opens on the new device.

Ask for a cloud wipe deletes a vault's data from your organisation's storage, once approved and after the cooling-off. It cannot be undone. A remote wipe only removes a device's copy; a cloud wipe removes the backup.

12. File Requests

When the policy says **an admin approves** for an action, a person's Sino asks under **File requests** first, with the reason they typed. You see who, what and how much, **never file names**. Press **Approve** or **Decline**; Sino tells them the answer. Once approved, the same files may go once, within 24 hours. Unanswered requests expire after 7 days.

Admins with a vault of their own: link each one to their person in the directory under **Admins**. Another admin then answers their requests, and the console marks their own requests as theirs.

13. Shared Folders

People share folders with colleagues from their Sino app. Each folder is end-to-end encrypted with keys of its own: the console shows members and their roles (owner, editor, viewer), **never the folder's name or files**. The hub gives each member storage access for that folder alone, read-only for viewers, and stops it when they are removed or leave.

- **Turning it off:** the policy's **Allow shared folders** stops new folders and every member's access.
- **Deleting a folder:** an owner deletes it from the app, or admins **Ask to delete** under **Shared folders** and the approvers approve. Its storage is erased 30 days later.
- **Old keys:** after a member is removed, the folder gets a new key; the page shows how many files are still under an older key, and an owner can **Re-encrypt all files** in the app.
- **A folder whose owners all left:** download its **Recovery file**, then in an admin's Sino app open **Work vault** → **Recovery console** → **Shared folder**, load the file, bring enough kits and choose the new owner. Paste the app's answer back on the page.

- **People outside the company** (when the policy allows it) join with an owner's invitation and their own Sino app. They are listed under **People from outside the company**; **Remove** stops their access at once. What they do in your folders is in your audit log, marked as someone outside the company.
 - **Share links** (when the policy allows it) are listed with who made them, until when they open, and how often they were downloaded. **End** stops one at once. The hub never sees a link's file name or key.
 - **Without Sino**: the open-source Sino Open SDK reads a copy of a folder's storage with the kits, and opens a share link's copy with the link.
-

14. People and Groups

People is your directory: the people your vaults belong to. People come from Entra ID or Okta through SCIM, from Google Workspace (read every hour), or are added here. Setting up SCIM and Google Workspace is in the Deployment Guide, section 12.

- **Removing a person**, here or in your directory, acts on their devices as **Hub setup → Retention and the directory** says: lock them, stop their storage access, ask for a remote wipe (the approvers still decide), or only flag them.
 - **Groups** give people a policy of their own (section 6). Groups from your directory are changed there; only groups made here are changed here.
 - Signing in to a company account never opens a vault: the vault password stays the key.
-

15. Admins and Passkeys

- **Invite an admin** under **Admins → Invite an admin**: a name, an optional e-mail for notices, and a role. Send them the link; it works once, within 24 hours, and they create their passkey with it.
- **Remove** an admin when they leave. If they were an approving admin, also change **New approving admins**, and if they held a kit, replace the kits (section 4).
- **A lost passkey**: another owner or admin presses **Replace a lost passkey** and sends them the link. If they were an approving admin, they come back on the approvers' list once the approvers approve the change. A **single owner**, or admins who all lost their passkeys, use the organisation kits in the Sino app to sign a new admin list.
- **Admins who also have a vault**: link them to their person (section 12).

16. The Audit Log and Your SIEM

Audit log shows every device and hub event, in OCSF, as your destinations receive it. Search it and filter by severity. Devices send ids, never file names (unless the policy turns them on), paths or content.

- **Retention:** the hub keeps events 90 days by default (**Hub setup → Retention and the directory**). Your SIEM keeps its own copy.
- **Archive:** tick **Archive events to the organisation's storage** to write every finished hour's events to `sino-hub/audit/` in each storage target, as gzipped JSON Lines. Turn on object lock or immutable storage there to keep it unchanged.
- **Destinations** get every event in order. One that is down gets everything it missed once it is back, within the retention. Webhook deliveries are signed (`X-Sino-Signature` , `HMAC-SHA256`).
- **Each device's events form a hash chain.** The hub checks every upload: **gap** means events were lost or withheld before an upload, **chain broken** means some were changed, reordered or rewritten. Both raise an event and show on the overview.

Events worth acting on

Event	Severity	What it means, and what to do
Audit chain broken (<code>AUDIT_BROKEN</code>)	High	A device's events were changed. Treat the device as suspect: lock it, stop its storage access, and investigate.
Audit gap (<code>AUDIT_GAP</code>)	Medium	Events are missing. Often a reinstall or lost storage on the device; check with the person.
Heartbeat missed (<code>HEARTBEAT_MISSED</code>)	Low	Not seen for 3 days: off, offline, wiped by your MDM, or Sino not started.
Sino not running (<code>NOT_RUNNING</code>)	Low	Sino was ended or crashed on a PC kept running by the policy. Repeated ones from one person are worth a conversation.

Repeated wrong passwords (<code>WRONG_PASSWORD_ALERT</code>)	Medium	Someone is guessing, or the person forgot. Check with them; lock the vault if in doubt.
Files out refused (<code>DATA_OUT_REFUSED</code>)	High	The hub refused taking files out: no hub contact, stopped storage access, or the daily limit.
An untrusted app (<code>APP_NOT_TRUSTED</code>)	Low	An app tried to open vault files. Trust it on Policy if it should.
Command refused (<code>COMMAND_REFUSED</code>)	Medium	A device refused a hub command; its details say why.
Approval granted / released (<code>APPROVAL_GRANTED</code> , <code>APPROVAL_RELEASED</code>)	High	A destructive action was approved, or has run. Check you expected it.
Kits rotated, approvers changed, recovery taken (<code>KITS_ROTATED</code> , <code>ADMIN_LIST_CHANGED</code> , <code>RECOVERY_REQUESTED</code>)	High	Changes to who can recover or approve. Check you expected them.
Credentials refused, cloud full (<code>CREDENTIALS_REFUSED</code> , <code>CLOUD_FULL</code>)	Low	A storage target is refusing or full: check Storage .

Device events

Event	Meaning
<code>DEVICE_ENROLLED</code> , <code>DEVICE_JOINED</code> , <code>DEVICE_UNENROLLED</code>	The vault enrolled, a device joined it, the vault left managed mode
<code>POLICY_APPLIED</code> , <code>APP_UPDATED</code> , <code>ROOT_KEY_ROTATED</code>	A new policy, a new Sino version, the organisation's new root key
<code>UNLOCK_SUCCEEDED</code> , <code>UNLOCK_FAILED</code> , <code>WRONG_PASSWORD_ALERT</code>	Unlocks and wrong passwords (count inARow)
<code>AUTO_LOCK</code> , <code>LOCKED_NO_HUB_CONTACT</code>	The vault locked itself; locked after too long without the hub

FILE_ADDED , FILE_CHANGED	Per file only with An event for every added or changed file ; otherwise in SYNC_SUMMARY
FILE_DELETED , FILE_RESTORED , FILE_EXPORTED , FILE_SHARED	Always per file: to the trash or deleted for good (permanent), out of the trash, out of the vault in the clear, into a shared folder
SYNC_SUMMARY	A sync pass: files added and changed, bytes, failures
CLOUD_FULL , CREDENTIALS_REFRESHED , CREDENTIALS_REFUSED	Storage
NUCLEAR_WIPE , RECOVERY_PERFORMED	The person wiped the device; the vault was recovered with the kits
COMMAND_RUN , COMMAND_REFUSED	A hub command ran or was refused
SHARE_JOINED , SHARE_LEFT , SHARE_FILE_* , SHARE_KEYS_CHANGED , SHARE_REFUSED , SHARE_REENCRYPTED	Shared folders
APP_OPENED_FILE , APP_NOT_TRUSTED	Another app opened a vault file, or tried to
NOT_RUNNING	Sino was ended or crashed on a PC kept running (stoppedAt , until)

Hub events cover admins, sign-ins, policy, enrollment, commands, approvals, recovery, storage, the directory, shared folders and file requests; each one's description is in the log.

17. Routine Checks

Every day (or let your SIEM alert you):

- **Overview:** anything under **Not seen for 3 days, With audit gaps or breaks**, or a failing destination.
- **Approvals** → **Waiting** and **File requests** → **Waiting**.

Every week:

- **Storage:** each target reads **Working**; press **Test** after changing credentials.
- **Devices:** Sino versions; raise **Minimum Sino version** once people have updated.
- **Vaults and recovery:** any vault **not sealed yet** or **sealed to old kits** (ask the person to unlock).
- **Shared folders:** folders with no owner left, files still under an older key, guests and share links you no longer need.

After a change of people:

- An admin left: remove them, change the approvers' list, replace the kits if they held one.
- Someone left the company: section 18.

Every few months: check that each kit holder still has their kit and knows where it is, and that the hub's backups restore (Deployment Guide, section 8).

18. When Something Happens

A new employee. Add them in your directory (or **People**), then send an enrollment link naming them, or let your MDM's enrollment profile do it.

A lost or stolen device.

1. Open it under **Devices: Lock the vault** at once, and **Ask for a remote wipe**.
2. **Stop its storage access**, so it cannot sync even before the wipe runs.
3. Do not **Remove from the hub** until the wipe has run.
4. A phone that is not checking in can also be wiped from your MDM, which has its own push channel. The hub does not hear of an MDM wipe: remove the device once the MDM reports it.

A device kept offline locks itself after **Lock after this many hours without reaching the hub**.

Someone leaving. Remove them in your directory: their devices are locked, lose storage access, or get a wipe request, as you set. To keep their work, recover their vault to a successor (section 11) before or after. Consider **Unlock only while the hub can be reached** with a short idle lock beforehand, so a removed device never opens again. If they owned

shared folders, name a new owner from the app or recover the folders with the kits (section 13).

An admin lost their passkey. Section 15.

A kit may be lost, or a kit holder left. Replace the kits (section 4).

Sino was ended on a PC. The device's events show **Sino not running** with the times. Talk to the person; set the machine-wide start-up entry if you have not (section 10).

A device's audit chain broke. Lock it, stop its storage access, and look at its events around the break. Do not remove it before you have what you need.

The hub is down. Vaults keep working, and keep syncing to your storage until their storage credentials expire (they last hours), since files never pass through the hub; after that, syncing waits for the hub. What stops at once: commands, policy changes, enrollment, the console, the actions **the hub confirms** (refused while it cannot be reached), and, if you turned it on, **unlocking**. Devices lock after **Lock after this many hours without reaching the hub**. Restart or restore the hub (Deployment Guide, section 8); devices reconnect by themselves.

A storage target fails. **Storage** shows the last error. Devices keep syncing to your other targets. Fix the target and press **Test**.

19. What the Hub Cannot Do

- **Open a vault, or read a file.** Only a quorum of kits can, in the Sino app.
- **Wipe a device without the approvers.** Devices check the approvals themselves.
- **Reach a closed app.** There is no push; use **Keep Sino running** on PCs, and your MDM for phones.
- **Stop someone photographing the screen** or using a file another app opened.
- **Manage iPhone, iPad, Mac or Linux.** Managed vaults are for Android and Windows today. Linux and iOS are planned next.