NorthLock Chat — User Manual

Software revision B · October 2026

NorthLock Chat is private, on-premises AI software for a law firm or legal team. It runs a legal-research model and the NorthLock Chat interface on a compatible machine in your office. All inference, indexing, and retrieval happen on that machine. It does not need the internet to answer questions, and your firm's documents never leave the office by default. The internet is used only for optional web search and for downloading software updates.

This manual is the single source of truth for setting up, using, and maintaining NorthLock Chat. It is published at https://northlock.ca/docs. A PDF is available for download. **NorthLock Help**, the built-in assistant, answers from the manual installed with your build, which covers the same software-only setup described here.

At a glance

NorthLock Chat runs on a compatible machine that your firm provides and owns. After setup, open **NorthLock Chat** in a browser at `https://northlock-one.local` and sign in. (If your network blocks that name, use the machine's numeric address instead: `https://<machine-address>`.) Everything runs on that machine; there is no software for your team to install. Your administrator may apply signed operating-system security updates during a scheduled maintenance window (see **Keeping the software current**).

> NorthLock Chat is served over **HTTPS by default**, with a certificate from the machine's own local CA; plain `http://` addresses redirect to it. Install the certificate once on each workstation (see **HTTPS and the certificate**). Keep the machine on your internal network behind the firewall and never expose it to the internet.

Your machine

NorthLock Chat runs on a compatible PC that your firm provides and owns. Use any PC that meets the minimum specs, bought in your firm's name from the seller of your choice. The maker's warranty and support terms apply to the hardware. NorthLock does not sell, ship, or warrant hardware. NorthLock does not recommend a particular make or model either; any PC that meets the minimum specs is supported.

Minimum specs

Any PC that meets all of these is supported:

- Graphics: NVIDIA GeForce RTX 5070 Ti 16 GB or better (at least 15 GB of graphics memory)
- Memory: 32 GB or more
- Storage: 1 TB NVMe SSD or larger
- Network: wired Ethernet port
- Security: TPM 2.0 and UEFI Secure Boot (standard on current PCs)

The NorthLock installer checks the hardware before it installs anything and refuses any machine below these specs.

Have an Ethernet cable (Cat6) long enough to reach your router or network switch. A wired connection is required. NorthLock does not include an Ethernet cable, a UPS, or a second backup drive.

What you use to install

Self-install uses an installer file written to a USB stick you provide. NorthLock does not mail a USB stick. After your setup and licence is paid, this site offers a signed installer from your order when NorthLock has published a verified release.

Writing the installer replaces everything on the USB stick you select. The installer image is written with Rufus in DD mode, balenaEtcher, or dd on Linux. Back up that stick first, and select the stick rather than another drive. Check the file's SHA-256 against the checksum NorthLock publishes with that file before you write it.

The computer needs UEFI with Secure Boot on. The installer names the one internal drive and waits until you type YES. Typing YES erases Windows and the other data on that drive. Back up anything you still need before you confirm. If the computer has more than one internal drive, the installer stops and changes nothing. The USB stick is not written during the install.

If setup asks for a code, read it on a display connected to the machine. It is not printed on a card. Create the administrator account and save the recovery key. NorthLock does not keep a copy.

This manual does not include an installer file.

Installing from Windows (new Windows 11 PC)

If your order page shows **Install from Windows (recommended)**, download **NorthLock Chat Setup** and double-click it on the new PC. It checks the PC, downloads the same signed installer image the USB stick uses, and asks you to type `ERASE WINDOWS`. Plan for one restart. Windows and every file on that PC are erased, so copy anything you want to keep to another drive first.

Setup checks the download and the PC without asking you anything. If the PC cannot run NorthLock Chat, or Secure Boot is missing the Microsoft third-party certificate, it stops before it changes anything and explains what to do. It turns Fast Startup, hibernation and BitLocker protection off by itself; you do not need a BitLocker recovery key. Enter your licence key on the first NorthLock screen, as with the USB route. The download resumes if it is interrupted.

Both routes install the same NorthLock Chat and use the same recovery tool: the USB stick of the same release. Use the USB stick for any other PC, or if the Windows program stops before it changes the disk.

Installing with the USB stick

These are the same three steps as https://northlock.ca/docs/setup/.

1. On another computer, write the installer to a USB stick you provide. You can do this before the computer is ready. Back up that stick first. Writing the installer replaces everything on the stick you select.

2. Put the computer where it will stay, on a hard, level surface in a dry, well-ventilated room. Plug in power. Plug your own Ethernet cable (Cat6) into the computer and your router or switch. The installer needs wired Ethernet. Wi-Fi is not used during install. A UPS is not included. You may use your own. Insert the USB stick you wrote. Open the computer's firmware boot menu and choose that stick.
3. Read the drive the installer names. Type YES only if that is the drive you mean to erase. Then open **NorthLock Chat** from any computer on your office network.

Setting up for the first time

When the install finishes, open **NorthLock Chat** in a browser at `http://northlock-one.local` and sign in. (If your network blocks that name, use the machine's numeric address instead: `http://<machine-address>`.)

If the first-boot screen asks for a setup code, read it on a display connected to the machine. It is not printed on a card. Enter your firm name, create the administrator account, and save the recovery key somewhere safe away from the machine. NorthLock can help by phone or video. The same three steps are at https://northlock.ca/docs/setup/.

> Keep the machine on your internal network behind the office firewall. Do not port-forward any port to it from the internet.

Networking

NorthLock Chat runs headless on your machine. Connect it to your office network with an Ethernet cable. It gets an address by DHCP, and you reach it from any browser on the same network. No monitor or keyboard is needed for daily use.

Wired Ethernet is required for the installer. After setup, an administrator can turn Wi-Fi on or off under **Admin** → **Networking** in NorthLock Chat, if the machine offers Wi-Fi. Do not use Wi-Fi for the install.

Using NorthLock Chat

- **New Session** starts a fresh chat. **Search Chats** finds earlier ones.
- **Projects** group related chats, for example around a matter.
- Ask a question in plain language. Answers cite the documents and sections they drew from, so a lawyer can verify before relying on them.
- The **Cited Sources** panel lists the documents behind an answer.
- **Deep Research** runs a longer, multi-step investigation across large document sets.
- **NorthLock Help** (the built-in assistant) answers questions about NorthLock Chat itself, grounded in this manual.

Working with documents

- Administrators add document sources in the admin area. Files can be uploaded directly or synced from connectors.
- Indexing happens on the machine. Large sets take longer to index the first time; the index is reused after that.
- When connector sync is enabled, permissions follow the source system, so users only see what they already have access to.

iManage Work documents (preview)

NorthLock Chat can read documents, versions, and workspace security from iManage Work and keep them alongside your matters. The connector is read-only: it never uploads, edits, checks out, or deletes anything in iManage. Documents are indexed on the machine, and a user only sees a document when both the iManage security and the matter's ethical wall allow it.

> **Vendor approval is required for a real tenant.** iManage must approve the NorthLock Chat application for your tenant before the connector can reach a real iManage Work server. Until that approval is in place, only a NorthLock test environment (a local mock of the iManage API) is supported. Do not enter a production client secret before iManage has approved the application.

Your iManage administrator does the vendor-side setup:

1. Register the NorthLock Chat application in iManage Control Center, turn on refresh tokens for unattended sync, and note the server URL, customer id, library id, client id, and client secret. iManage Cloud hosts are specific to your tenant; use the host iManage gives you, not a generic one.
2. Give the client secret to your NorthLock Chat administrator through a password manager or another secure channel, not email or chat.

Your NorthLock Chat administrator then:

1. Open **Admin** → **Matters** → **iManage Work sync**. Enter the server URL, customer id, client id, client secret, and library ids. If the NorthLock Chat machine's outbound switch is off, tick **Allow this host while outbound is off** so the one saved iManage host can be reached; nothing else is opened.
2. Choose **Save and test**. The test signs in, lists the libraries, and reads one workspace's security. If security cannot be read, the connector stays off rather than indexing documents without permissions.
3. Create one connector per workspace under **Admin** → **Connectors** (source iManage Work, with that library id and workspace id). One workspace per connector keeps each matter's wall exact: a wall on one matter cannot hide or expose another matter's documents.
4. Return to **Admin** → **Matters** → **iManage Work sync**, enter the connector pair id, and choose **Test mapping**. The report lists workspaces that match a matter number and those that do not. A workspace is never turned into a matter automatically; add the matter first, then map again.
5. Choose **Map workspaces** to create the private document set for each workspace and attach it to the matter team.

Ethical walls. Map each iManage wall group to a NorthLock group in the wall group field as `imanageGroupId=localGroupId`. A wall reported by iManage is always added to the matter, because adding a wall only narrows access. A wall that iManage removed is kept unless an administrator ticks **Also remove walls that iManage removed**; removing a wall widens access and should be a deliberate decision. If a wall group has no mapping, that workspace is not indexed and the report says so.

What the sync does. The latest version of each document is indexed, with version metadata retained. Deleted documents are removed by the normal index prune pass; closed or archived matters are skipped, and a matter closed in NorthLock Chat is never reopened by the sync. A permission change in iManage reaches NorthLock Chat on the next permission sync.

Limits. This preview supports one workspace per connector and matches by the `matter_number` custom field (or an exact matter-number workspace name). It does not read iManage Security Policy Manager policies, so a firm that enforces walls only in SPM must confirm that Work's workspace security reflects them before relying on this connector.

Users, roles, and access

- Administrators invite users and assign access to matters, document sets, and agents.
- Each user can turn on two-factor authentication in their own settings (Settings → Security).
- Support access for troubleshooting is available to NorthLock staff only, and only with the firm's consent.
- The first account created is the administrator. Add further administrators deliberately.
- Your firm can let people sign in with their Microsoft 365 account instead of a separate NorthLock password. Your administrator sets this up; when it is on, the sign-in page shows a Microsoft 365 button. Two-factor protection then comes from Microsoft 365, and the firm's local administrator account stays available as a fallback.

Retention and legal hold

- Configure retention and legal hold per matter in the admin area.
- Retention purge and legal hold are enforced by NorthLock Chat, not by the client application, so a hold cannot be bypassed from a chat.

Privacy and security

- All inference is local. NorthLock Chat sends no telemetry and never sends client documents, queries or answers anywhere. Its only outbound connections are checking for and downloading software updates, renewing its service-plan licence when your administrator starts it (using the machine's device token), and optional web search if your firm turns it on. NorthLock keeps only what it needs to register your installation, renew your service plan and invoice you.
- Your documents, indexes, and matter data stay on hardware you own. Keep the machine behind your firewall; never expose it to the internet.

- Accounts are provisioned by your firm admin; each user can turn on two-factor authentication in their own settings (Settings → Security).
- Web-search features are optional and can be left unconfigured to keep the machine fully offline.
- Client and matter documents are confidential and are never used to train, fine-tune, or improve any model.
- Never paste client or matter documents into the NorthLock Help chat.

For the Privacy Policy, Data Processing Agreement (DPA), or current sub-processor list, contact info@northlock.ca.

Keeping the software current

When an update is available, the admin page shows it. Nothing changes until an administrator installs it. Open **NorthLock Chat** → **Admin** → **Software Updates**: it shows whether a newer version is available, the last check, the last backup time, and whether a rollback is available.

Routine updates replace **only the changed containers** — the machine is not reimaged. Each update is signature-checked, takes a backup first, runs a health check, and rolls back automatically if the check fails. Updates require an active service plan; if the plan lapses, the installed version keeps running, but new updates and legal-content refreshes stop (the admin page shows "Renew to update"). Software updates and security fixes are provided only while the service plan is active, and no particular number, frequency, or schedule of updates is promised.

Updates are installed from **NorthLock Chat** → **Admin** → **Software Updates**. For offline firms, use the offline-update link in your NorthLock order e-mail to get the signed offline package for your installation, then:

1. Format a USB stick as exFAT (use FAT32 only when no file is larger than 4 GB).
2. Unzip the download and copy the `northlock-one-<version>` folder to the root of the stick. Keep the file names exactly as they are.
3. Insert the stick into the NorthLock Chat computer.
4. Open **Admin** → **Software Updates** and choose **Apply from USB**. The computer checks the signature, takes a backup, applies the update and checks its health. Leave the stick in place until the page says the update finished.

The download page lists each package's version, release notes, size and SHA-256, and requires an active service plan. The browser uploads nothing. If the signature or a checksum does not match, the update is refused and the installed version keeps running.

Major operating-system or driver upgrades, and recovery, are handled by NorthLock support.

If an update cannot be applied, contact NorthLock support.

Disk encryption and your data

The firm's data volume (databases, the search index, uploaded documents, and the firm's settings and credentials) is encrypted with LUKS2, separate from the operating system, so reinstalling or reimaging the operating system never wipes firm data. Backups are encrypted like the data volume and are written separately from the live data.

The data volume unlocks automatically at boot using the machine's TPM. Each installation is created with its own recovery key; if the machine cannot use the TPM, or the TPM is reset, NorthLock support can help you unlock it with your recovery key. On a machine without a TPM, the volume unlocks from a key stored on the machine instead (this is weaker, because that key is not itself protected by the TPM).

Health checks

NorthLock Chat watches its own health. Open **NorthLock Chat** → **Admin** → **Health** to see the status of the AI engine, the chat service, disk space, and the model files. No setup is required, and nothing leaves the machine.

NorthLock does not monitor your machine remotely and cannot see its health. If the Health page shows a problem, contact NorthLock support; you can share a status report from the software so we can help.

Backups and disaster recovery

NorthLock Chat backs up the firm's data automatically every night, encrypted like the data volume and written separately from the live data. An update always takes a fresh backup first. The admin page shows the last backup time. The software also verifies the backup on its own — it checks the repository and performs a test restore every month — so you can be confident a restore works. Before sending the machine to its maker for service, make sure the last backup succeeded. If a drive fails, the maker replaces the hardware; NorthLock restores your data from the backup under the service plan.

Maintenance and care

- Keep the machine dry and well-ventilated, and follow the maker's care instructions. Use only the power supply supplied with the machine.
- Do not open the case or service the hardware yourself. Contact the machine's maker for hardware service. See **Your computer and the software licence**.
- Apply operating-system security updates during a scheduled maintenance window.

NorthLock supplies the software only. It does not service, repair, or replace the machine.

Troubleshooting

Most issues show up on the **Admin** → **Health** page. If something is not working:

- Ask the built-in **NorthLock Help** assistant in the chat — it answers questions about running NorthLock Chat.

- If a problem persists, contact NorthLock support (info@northlock.ca) and give the machine's serial number.

A detailed technical guide is available to NorthLock and your IT support.

Open-source software

NorthLock Chat includes third-party open-source software, each governed by its own licence rather than the NorthLock software licence. The complete list of components and their licences is available at https://northlock.ca/docs/open-source/.

Your computer and the software licence

Hardware. You buy the machine directly from its maker. The maker's warranty and support terms apply to the hardware. NorthLock gives no hardware warranty and handles no hardware returns. For a hardware fault, contact the maker with the machine's serial number.

Data before hardware service. Before sending a machine to the maker, export the data you still need, then use the NorthLock wipe tool. You are responsible for your own data backups beyond the included local backups.

After a hardware repair. While your service plan is active, NorthLock reinstalls or restores the NorthLock software after a hardware repair or replacement.

Software licence. Your purchase includes a perpetual licence to run NorthLock Chat on one supported machine, identified by its serial number. Software updates and support require an active service plan. If the plan is cancelled or lapses, the installed version keeps running, but new updates and legal-content refreshes stop. The licence is non-exclusive and non-transferable, and is for internal use within your firm on that machine. If the machine is replaced after a hardware failure, the licence transfers to the replacement machine.

Setup and licence refund.

Once you purchase NorthLock's setup and licence, a change of mind is not a ground for a refund. That rule starts at purchase. It does not start when the software is installed, activated, or first used. Waiting to install does not create a refund.

The service plan billed each month is a separate charge from the one-time setup and licence. Cancel any month; no contract or lock-in. Service stops at the end of the paid month. Cancelling that plan does not refund the setup and licence, and the no-change-of-mind rule for the setup and licence does not remove that cancellation.

This policy is shown before you pay, including on the order form before you place the order.

This does not say that NorthLock never provides a remedy, and it is not a certification that the policy meets every law. Rights that cannot be excluded under applicable law still apply.

If NorthLock does not give you access to the installer download for a setup and licence you purchased, contact NorthLock. That is not a change of mind.

If the software has a material defect and NorthLock cannot correct it, contact NorthLock about a remedy. That is not a change of mind.

The computer is a separate purchase from its seller. The seller's return terms apply to the computer. Do not return that computer to NorthLock. A return to the seller does not, by itself, refund the setup and licence, and this policy does not depend on returning the computer.

The $200 CAD/month service starts after setup is complete on your machine. Cancel any month; no contract or lock-in. Service stops at the end of the paid month.

Support: email info@northlock.ca and give the machine's serial number. Replies during business hours, Monday to Friday, 9:00 to 17:00 Eastern.

Disposal and regulatory

- The machine is yours. When you retire it, dispose of it through your local electronic-waste (EPRA) program; do not put it in household waste.
- Before disposal, use the NorthLock wipe tool to erase firm data.
- The machine's own safety and regulatory documents come from its maker.

Contact

NorthLock support: info@northlock.ca. Mailing address: NorthLock AI Inc., PO Box 23527, North York RPO Dexter, ON M2H 3R9. Web: https://northlock.ca