Aionda Mail

English edition · 17 November 2026

Aionda Mail Product handbook

For individuals and organizations

Practical workflows, annotated Web screenshots and the boundaries of security, sharing and AI processing.

Contents

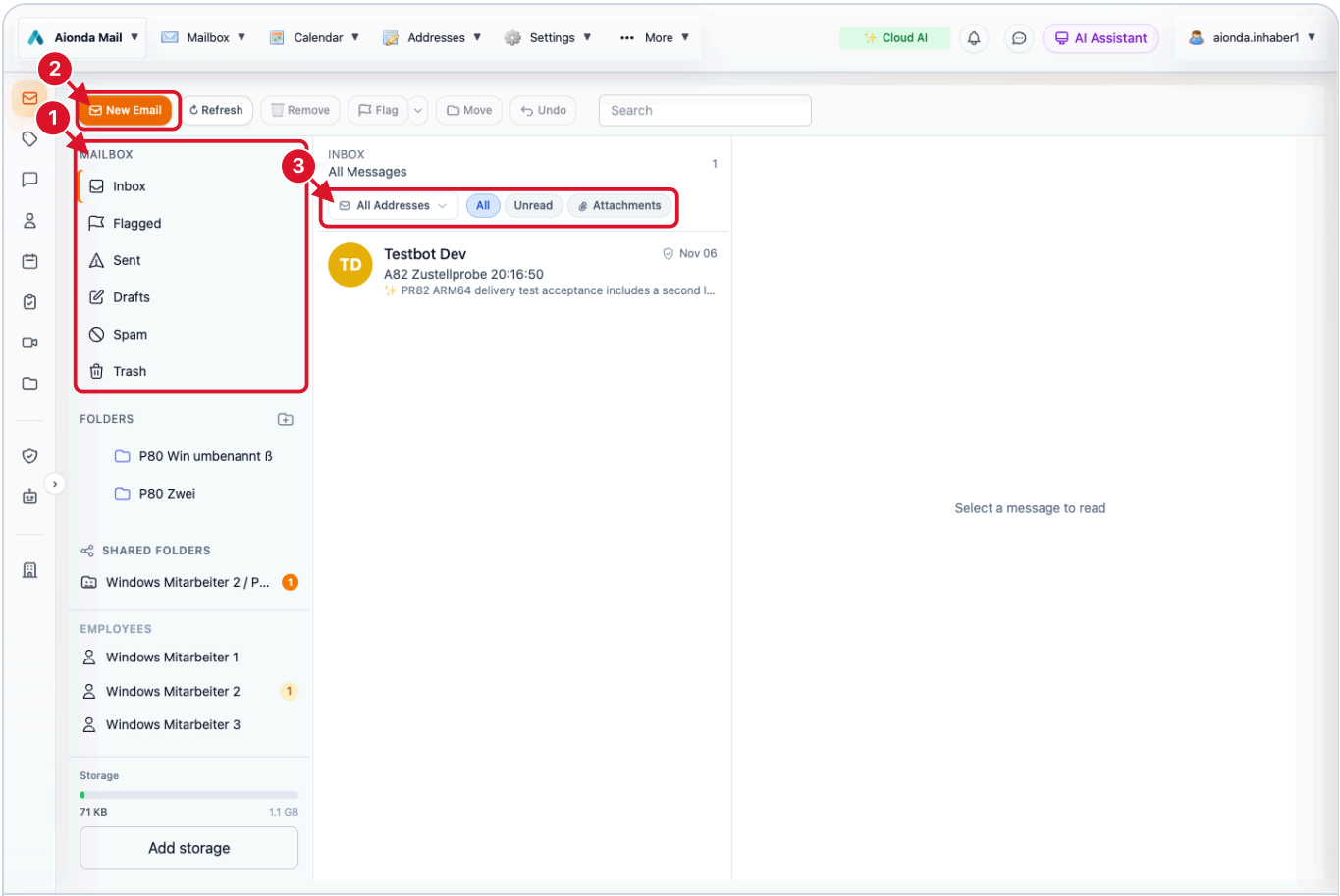
1. Start with Aionda Mail
2. Read, write and organize email
3. Addresses, aliases and forwarding
4. Logging: delivery history and retained email
5. Personal contacts and the company directory
6. Rules and the email processor
7. Import, export and browser integration
8. Drive and file sharing
9. Calendar and invitations
10. Tasks and flagged email
11. Chat and video meetings
12. Set up and manage a company
13. Visibility groups: Company and Private
14. Business archive, integrity and GoBD
15. Spam and phishing protection
16. Security basics: passkeys and post-quantum encryption
17. PGP: encrypted email with external correspondents

18. Choose how AI processes your data
19. AI assistance throughout the workspace
20. AI employees and business responsibilities
21. Connect an external assistant with MCP
22. Troubleshooting and reference

Everyday use · Chapter 1

Start with Aionda Mail

A practical guide to private email, collaboration and AI-assisted work.



1. Mailbox folders.
2. Compose a message.
3. Search and filter the message list.

Select the screenshot to open the full-size image.

Your first session

1. Sign in with your account. Unlock the encrypted mailbox when prompted; signing in and unlocking stored content are separate steps.
2. Open Mailbox, then Inbox. Select a message to read it. On a small screen, use Back to return to the list.

3. Open Addresses to create or review the addresses at which you receive mail. Check whether each address delivers into your mailbox or forwards elsewhere.
4. Open Contacts to find personal contacts and colleagues visible to you. Select the correct sending address before composing your first message.
5. Visit Security and store your recovery information safely. Review Artificial Intelligence before enabling AI processing.

Find your way around

The application menu groups mailbox actions, addresses and settings. The sidebar opens Mailbox, Contacts, Calendar, Tasks, Drive and other workspaces. Enterprise appears for accounts with company functions. A collapsed sidebar still provides icons with labels on hover.

This English edition illustrates the Web client using a dedicated development test company. Sample names and records are test fixtures; some names and browser-native date fields retain their original language. Native apps use the same service but menus and the rollout of individual features differ.

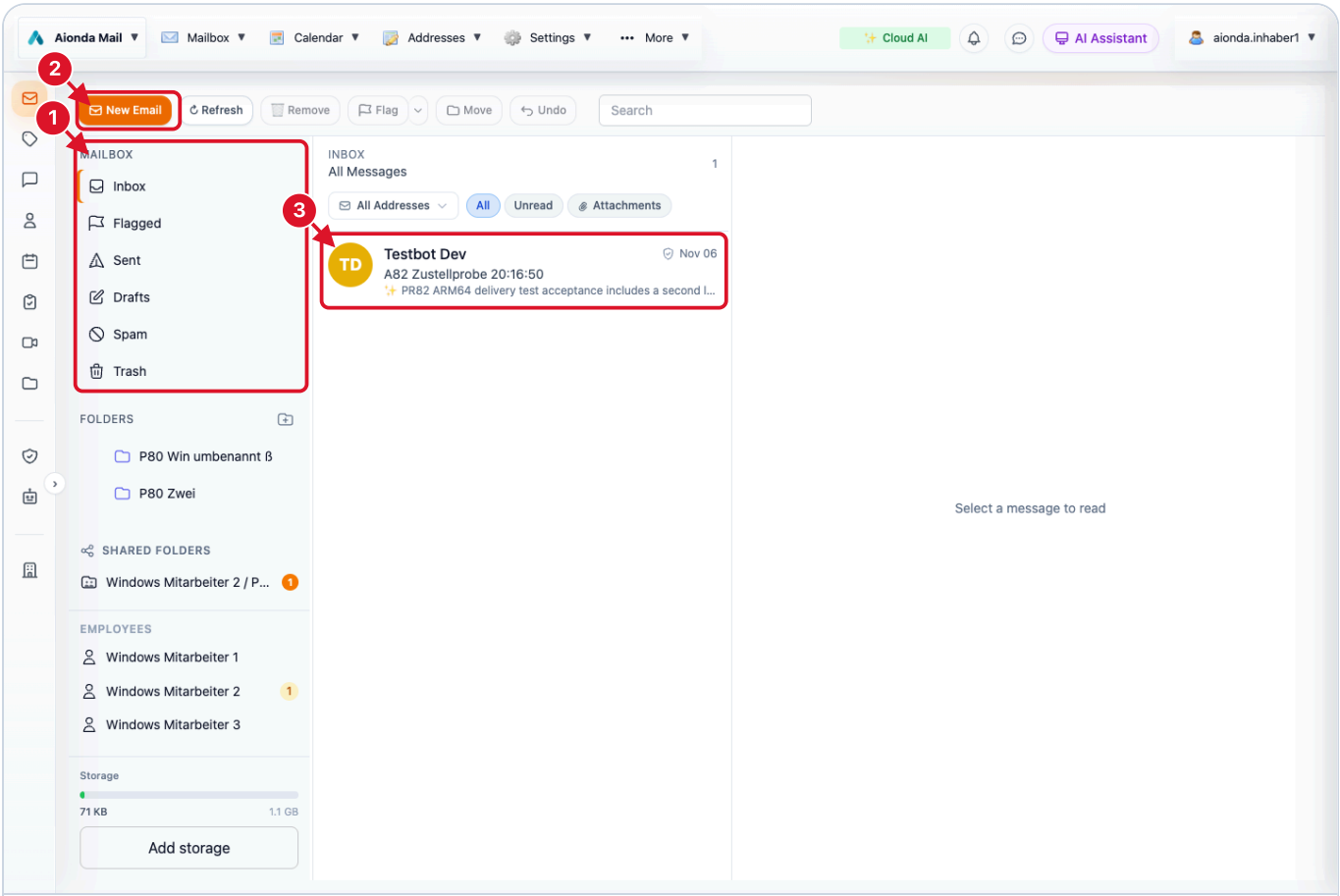
What you need

Use a supported browser or the installed app and a working connection. Sending, storage and business capabilities depend on your account and company plan. The current account screen is authoritative for your quota and entitlement; this handbook does not promise fixed prices or storage allowances.

Everyday use · Chapter 2

Read, write and organize email

Keep the Inbox manageable without losing control of where messages go.



1. Choose a folder before comparing counts or searching.
2. Compose a new message.
3. Select a message to read it.

Select the screenshot to open the full-size image.

Read and inspect

Select a folder, then a message. Expand the header to inspect the sender, To and Cc fields rather than relying only on the display name. Bcc recipients are normally absent from delivered message headers: receiving a message does not guarantee that your address appears in To or Cc. Delivery information and the original headers can help explain which address received it.

Compose and reply

1. Choose New email, Reply, Reply all or Forward.
2. Check the From address and every recipient. Reply all can include people beyond the original sender.
3. Write a subject and message, then add attachments if required. Review AI-generated text before using it.
4. Send and check Sent. If sending fails, keep the draft and inspect the error before retrying to avoid duplicate messages.

Organize

Create folders for projects or topics. Expand or collapse folder branches to reduce clutter. Select messages to move, delete, flag or mark as read. Deleting to Trash differs from permanent deletion. Folder sharing is an explicit permission grant; a colleague appearing in Contacts does not give them access to your mailbox.

Search and flagged mail

Use search and the available filters to narrow the current view. Check the selected folder and search scope before comparing results with Tasks → Flagged email. A folder-specific result is not the same population as all flagged messages. Loading more rows is a presentation detail, not a reliable way to count the entire mailbox.

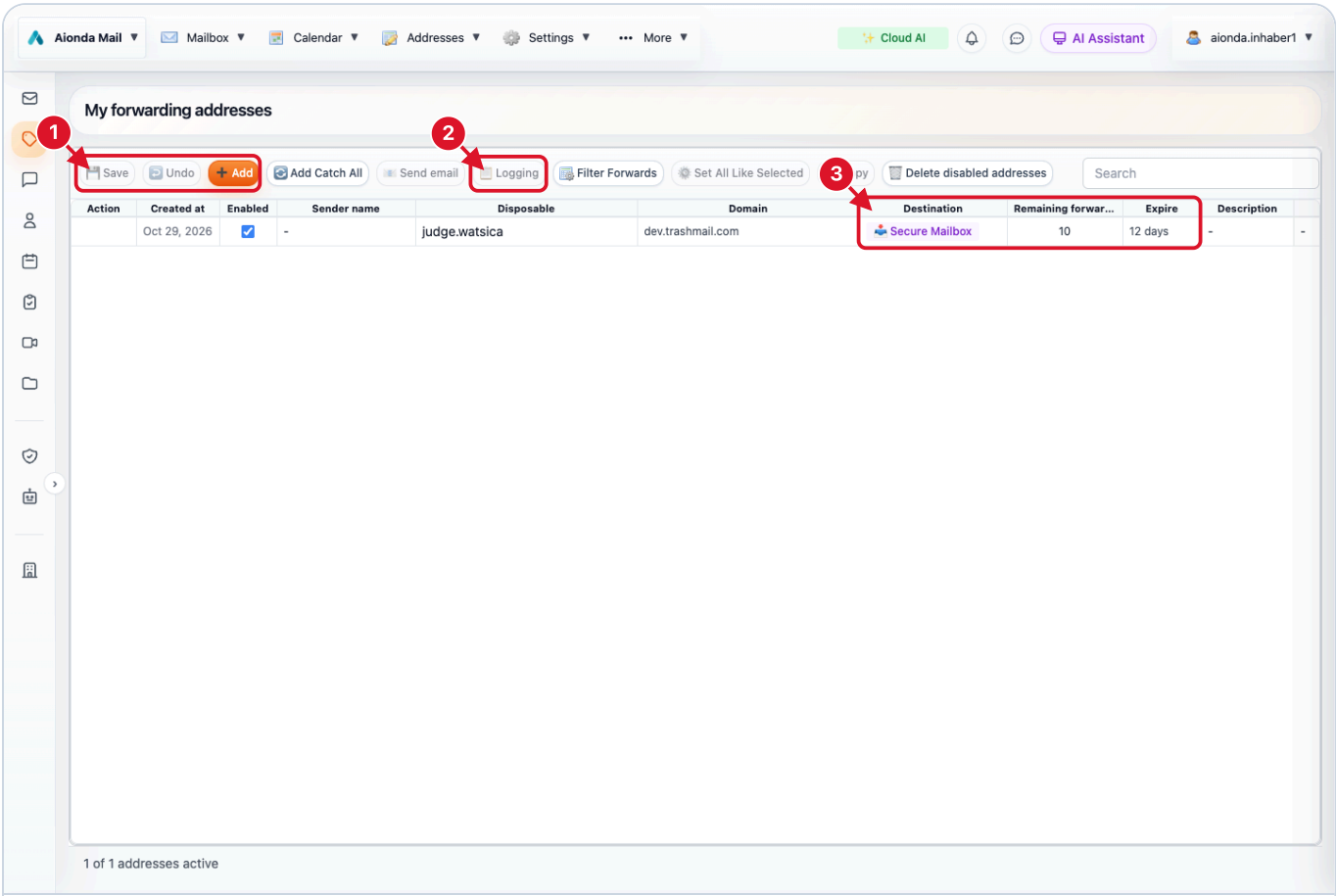
Multiple clients

Connected clients receive change notifications and refresh affected data after new mail, moves or deletions. An offline or suspended app catches up when it reconnects. If another device looks stale, check connectivity and refresh before repeating the action.

Everyday use · Chapter 3

Addresses, aliases and forwarding

Use separate receiving addresses for different purposes without publishing your underlying account address.



1. Add an alias and save your changes.
2. Select an address, then open Logging.
3. Check its destination and independent forwarding and expiry limits.

Select the screenshot to open the full-size image.

What is an Aionda address?

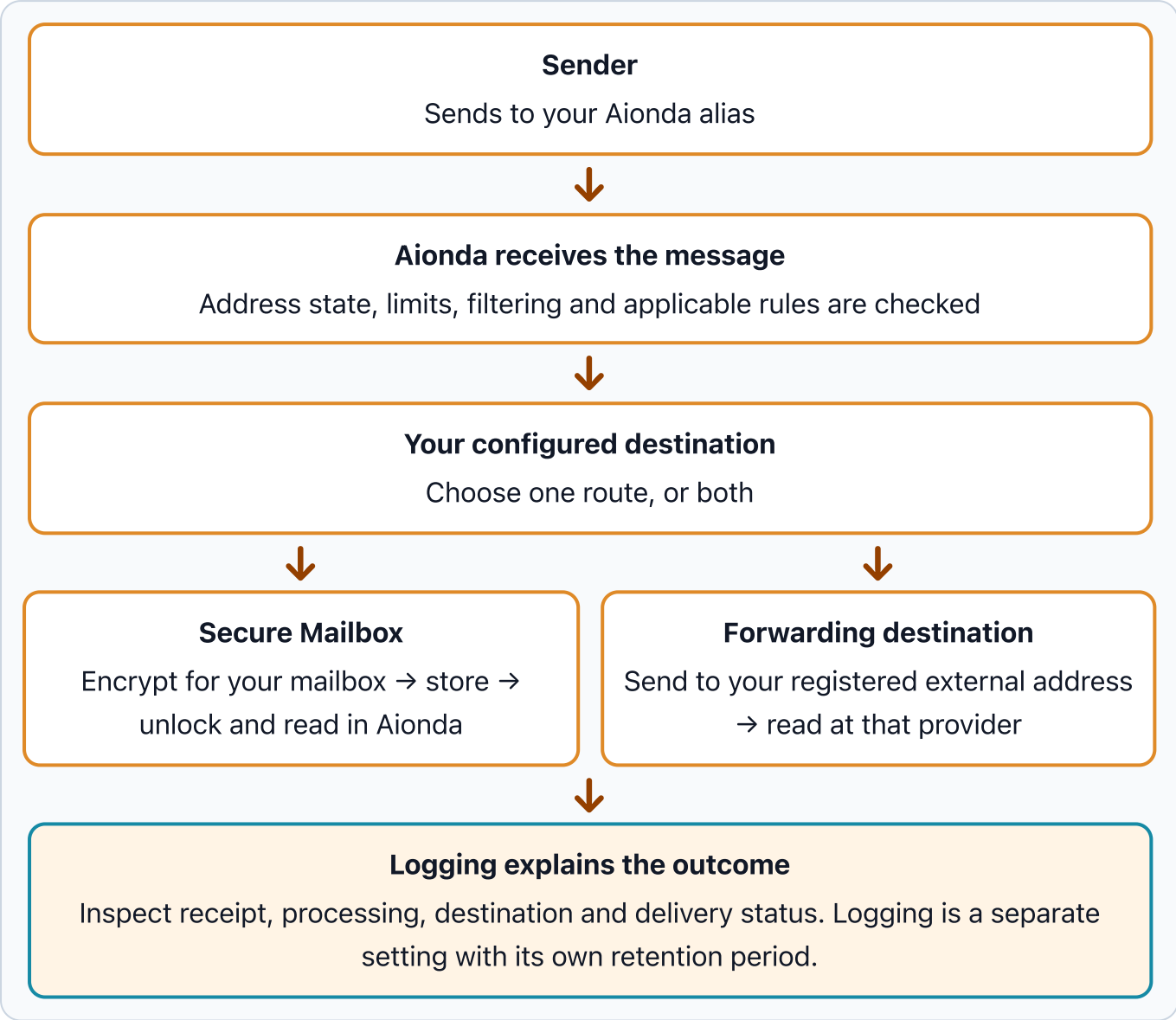
A disposable email address (DEA) is a real receiving address, such as an alias you give to a shop, a project or a mailing list. It hides your underlying destination address from the sender. You can keep it permanently or give it a limited lifetime. A separate alias for each purpose makes unwanted mail easier to trace and stop.

The address is the entrance; its **Destination** decides where the message goes. Receiving into the Secure Mailbox and forwarding to another provider are different choices. They can also be combined.

Create and save an address

1. Open **Addresses** and choose **Add**.
2. Choose the address name and an available domain. Use a description to remember what you created it for.
3. Choose the destination: **Secure Mailbox**, a registered real email address, or the combination offered in the destination picker.
4. Review **Enabled**, **Remaining forwards** and **Expire**. A time limit and a forwarding limit are independent.
5. Choose **Save**. Unsaved grid changes are not a finished configuration.
6. Send a harmless test message, then select the address and open **Logging** to verify its actual delivery path.

Where incoming mail goes



This diagram shows delivery choices, not a guarantee that every sender used end-to-end encryption. With ordinary SMTP mail, Aionda receives readable content before encrypting the stored mailbox copy. If the sender encrypted the message with your PGP public key, its protected content already arrives encrypted. A copy forwarded to another provider is subject to that provider's storage and access rules.

Choose the right destination

Choice	Typical use	What to check
Secure Mailbox only	Read and organize mail in Aionda Web, macOS or iOS.	Mailbox activated and unlock methods available.

Choice	Typical use	What to check
External address	Keep using an existing inbox at another provider.	The destination is registered and verified; check its spam folder if delivery is accepted but the mail is missing.
Secure Mailbox and forwarding	Keep a mailbox copy and deliver another copy externally.	Both destinations are selected. Organizing one copy does not automatically move or delete the other.

Add and verify a real destination through **Settings → Add Real Email**. A fail-over address, where configured, is a fallback for delivery problems; it is not the same as always delivering two copies.

Understand the address list

Control or column	How to use it
Enabled	Temporarily stop the address without treating it as a permanent business identity.
Disposable and Domain	Together form the email address you give to others.
Destination	Review every recipient of incoming mail, including the Secure Mailbox.
Remaining forwards and Expire	Check both limits before using the address for long-term correspondence or account recovery.
Description and Website	Record the purpose or service associated with the alias.
Last Received and Forwarding errors	Identify recently used aliases and investigate delivery problems.

Control or column	How to use it
Columns, Search and Filter Forwards	Expose additional fields and narrow the list. A hidden column does not mean the setting is absent.

Logging: follow a message from receipt to delivery

Select an address row, then choose **Logging**. Select a message and open **Events** for the sequence of processing steps. The summary distinguishes an encrypted mailbox delivery from external forwarding, queued attempts and errors. A destination server accepting a message does not prove that it placed the message in its Inbox.

Email content and **Source** can show retained original mail where logging and retained data are available. **Send again** can deliver a retained message again, or store it in the unlocked Secure Mailbox. **Extend** changes the log's retention; it does not extend the alias's lifetime. See the dedicated Logging chapter for each action, statuses and privacy implications.

Disable, extend or delete an alias

Use the Enabled control for a temporary stop, edit expiry or forwarding limits when the address should remain usable, and save the change. Deletion or expiry can prevent future password-reset and verification messages from arriving. It does not erase messages already delivered or copied elsewhere. Before deleting an alias, replace it at any services that still use it.

Catch-all addresses and your own domains

Add Catch All supports the catch-all workflow offered by your account: incoming names can be handled without creating every alias manually. Review that scope carefully because a catch-all can also attract unwanted traffic. Manage custom domains under Settings and complete the DNS setup shown there. Domain ownership alone does not route mail; the receiving records must point to the intended service.

Replying and PGP

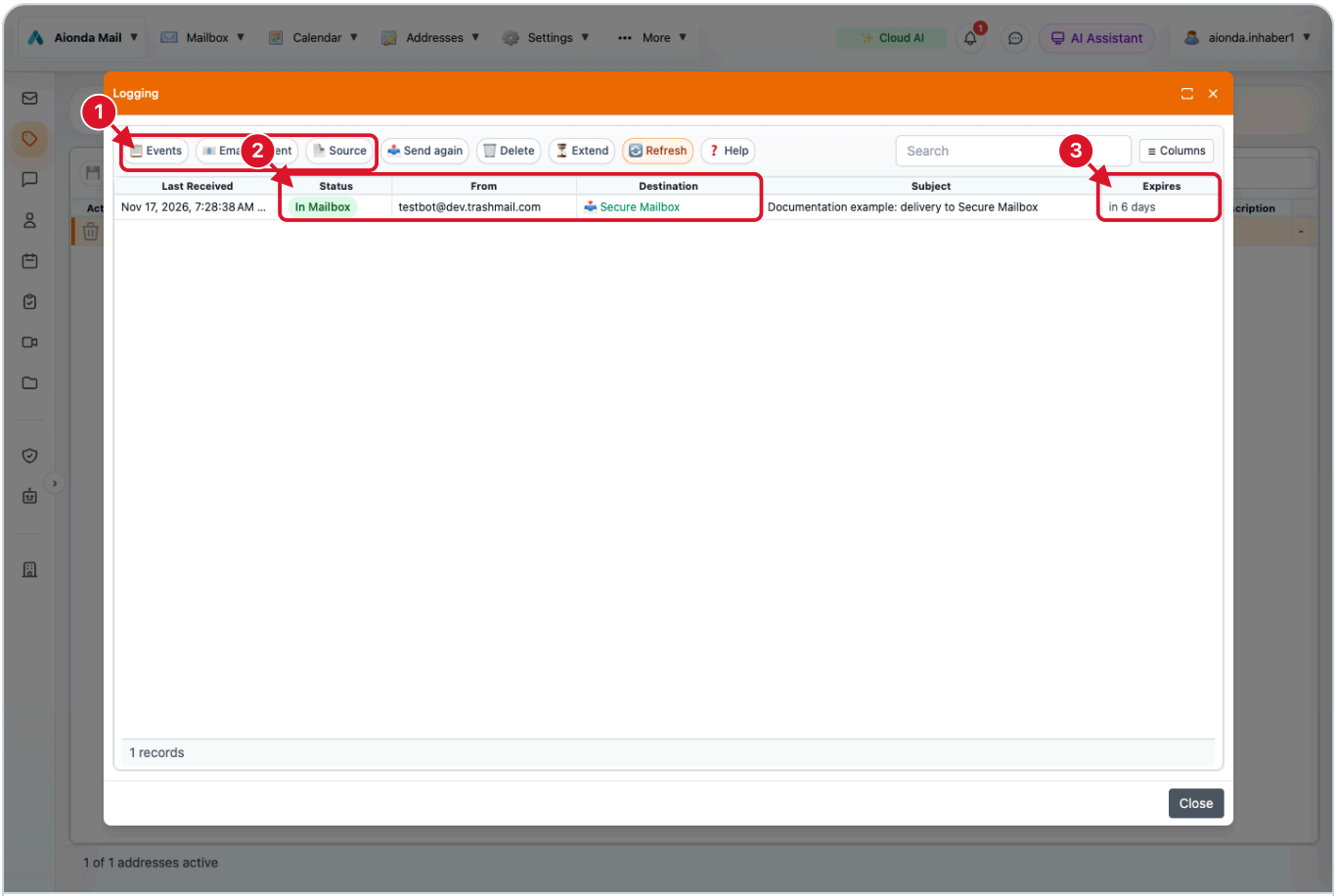
When composing, check the From alias. Reply masking and header rewriting are forwarding options; they are not encryption. For eligible Secure-Mailbox-only aliases, Aionda manages PGP keys and publishes public keys through WKD so compatible senders can discover them. Read PGP email before relying on end-to-end protection for external correspondence.

Your standard company address

The company directory publishes one eligible DEA, not every alias or a private account address. You or the owner can choose it on the contact card. If no choice exists, the service prefers an eligible non-expiring address and otherwise uses its fallback order. Deleting or disabling the chosen address can select a replacement; if none is eligible, no usable address remains. Choose a stable non-expiring address for a published business identity.

Logging: delivery history and retained email

Find out what happened to a message, inspect its processing events and recover retained mail before it expires.



1. Open Events, Email content or Source for the selected message.
2. Review status and destination.
3. Check expiry before extending retention or recovering a message.

Select the screenshot to open the full-size image.

Open the right log

1. Open **Addresses** and select the alias that received the message.

2. Choose **Logging**. Check the time, sender and subject; use Search when there are many entries.
3. Select the relevant message and choose **Events**.
4. Read the individual receipt, processing and delivery events, not just the summary status.

The log answers “what happened to this delivery?” It is different from the current folder of a message in your mailbox, and different from the long-term enterprise archive.

Enable logging deliberately

The email processor includes **Log email requests**. In the Web menu, open **More → Email processor** to inspect this option. Enabling it affects new processing; it does not recreate content from messages that were never retained.

Logging can retain the complete original message, not just technical events. This separate server-side copy supports viewing and resending. For ordinary unencrypted incoming mail, do not treat that retained original as zero-knowledge vault content. PGP-protected content remains encrypted in its original message form. Choose logging and retention according to the confidentiality of your correspondence.

Read the status correctly

Status	Meaning and next step
In Mailbox	A copy was stored in the Secure Mailbox. Open the mailbox and check its current folder.
Forwarded	The destination server accepted the mail. If it is not visible, check that provider’s spam, rules and mailbox.
Queue or delayed	A delivery is pending or a temporary rejection requires retrying. Read the server response before sending another copy.
Waiting for confirmation	A configured sender confirmation step has not yet completed.

Status	Meaning and next step
Fail-over	A fallback destination was used. Inspect which destination received the message.
Error or rejected	Read Events for the actual rejection or failure, such as a recipient issue, address limit or destination refusal.

Inspect Events, Email content and Source

Events provides timestamps and the processing history. It can explain whether the alias was enabled, which rule or filter intervened and whether delivery succeeded. The events dialog includes a support-text copy action; inspect that text for personal details before sharing it.

Email content opens the retained message when available. **Source** helps inspect the original mail, including headers and MIME structure. These actions depend on retained data; an entry or error notification is not a promise that full content will remain available forever.

Retention: save the evidence you need

Inspect the **Expires** column. The standard log retention is seven days; the displayed deadline is authoritative for that entry. Select messages and choose **Extend** to use the offered 7-, 14- or 30-day extension. Extending a log is separate from extending the receiving address. Expired records are eligible for cleanup, so do not wait until after the deadline to preserve important evidence.

Resend or store in the Secure Mailbox

1. Correct the original delivery problem and select the retained message.
2. Choose **Send again**.
3. Review the destination. Choose a registered real email address to send another copy, or **Secure Mailbox** when offered after unlocking to store it there.
4. Confirm the action and inspect the new result.

Resending can create a duplicate and is a real delivery action. Do not use it repeatedly while a previous attempt is still queued. Saving in the Secure Mailbox creates a separately retained mailbox copy; it does not turn the log itself into an enterprise archive.

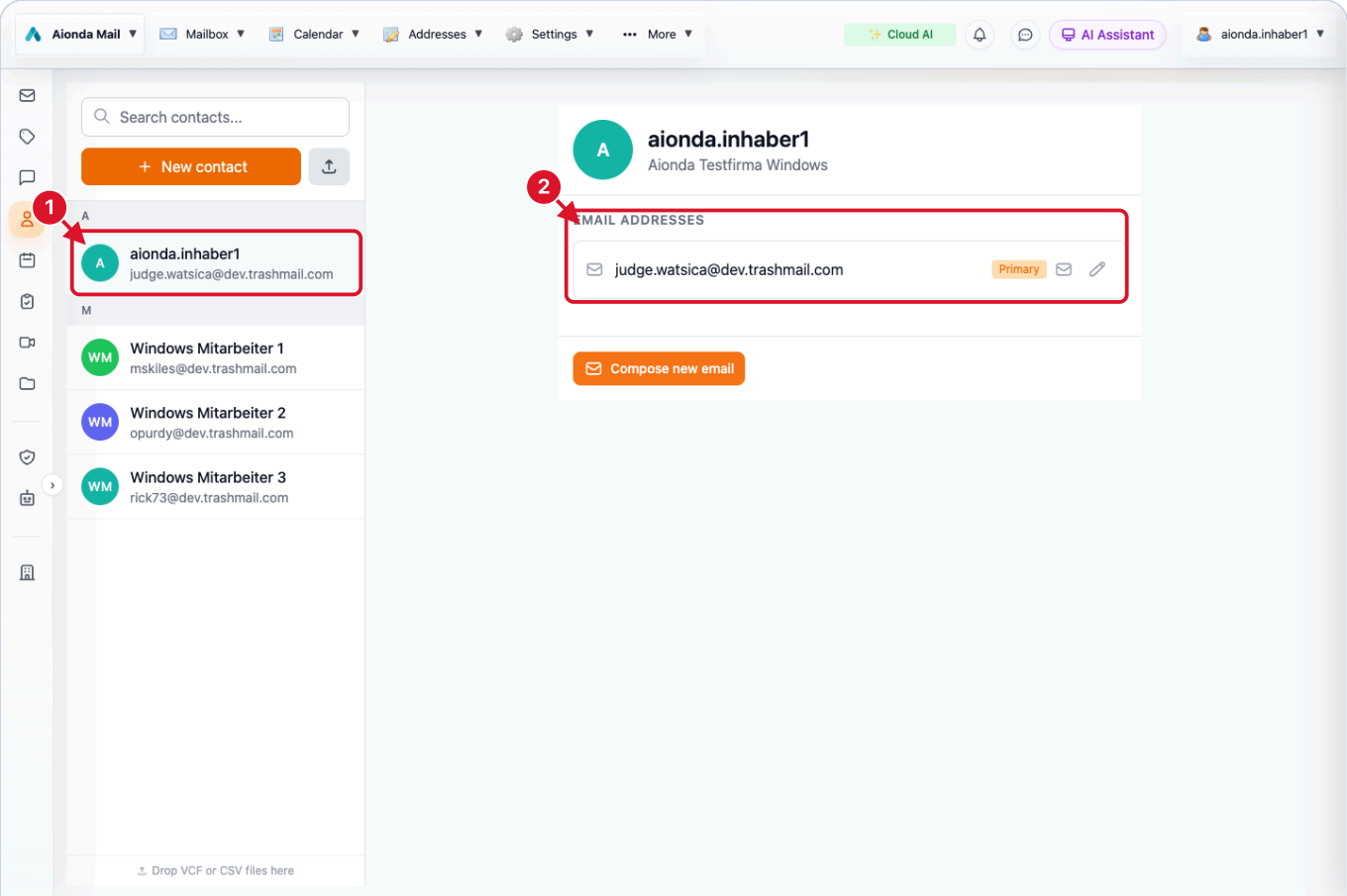
Example diagnosis

A shop says it sent an invoice, but your external Inbox is empty. Find the alias, open Logging and inspect Events. If the external server accepted it, check that provider's folders. If it returned a temporary error, examine the queue state. If the selected destination was Secure Mailbox, read it in Aionda instead. This avoids changing an alias or sending duplicates before identifying the actual route.

Everyday use · Chapter 5

Personal contacts and the company directory

One place to find your own contacts and the colleagues you are allowed to see.



1. Select a directory entry.
2. Review the contact card and its published email address.

Select the screenshot to open the full-size image.

Two kinds of contact

Personal contacts belong to your encrypted address book. Create them with New contact or import supported VCF/CSV files. Review imported names and addresses before saving; an import can contain duplicates or outdated details.

Company contacts are supplied by the organization. They appear automatically according to your membership and visibility permissions. They are not editable copies in every employee's personal address book. Ordinary colleagues see directory records as read-only; the owner manages company profile information.

Choose the published address

1. Open Contacts and select your own directory entry, or an employee entry you are authorized to manage.
2. Use the edit action beside Email addresses.
3. Choose the standard DEA from the eligible addresses and save.
4. Check the address now displayed on the contact card.

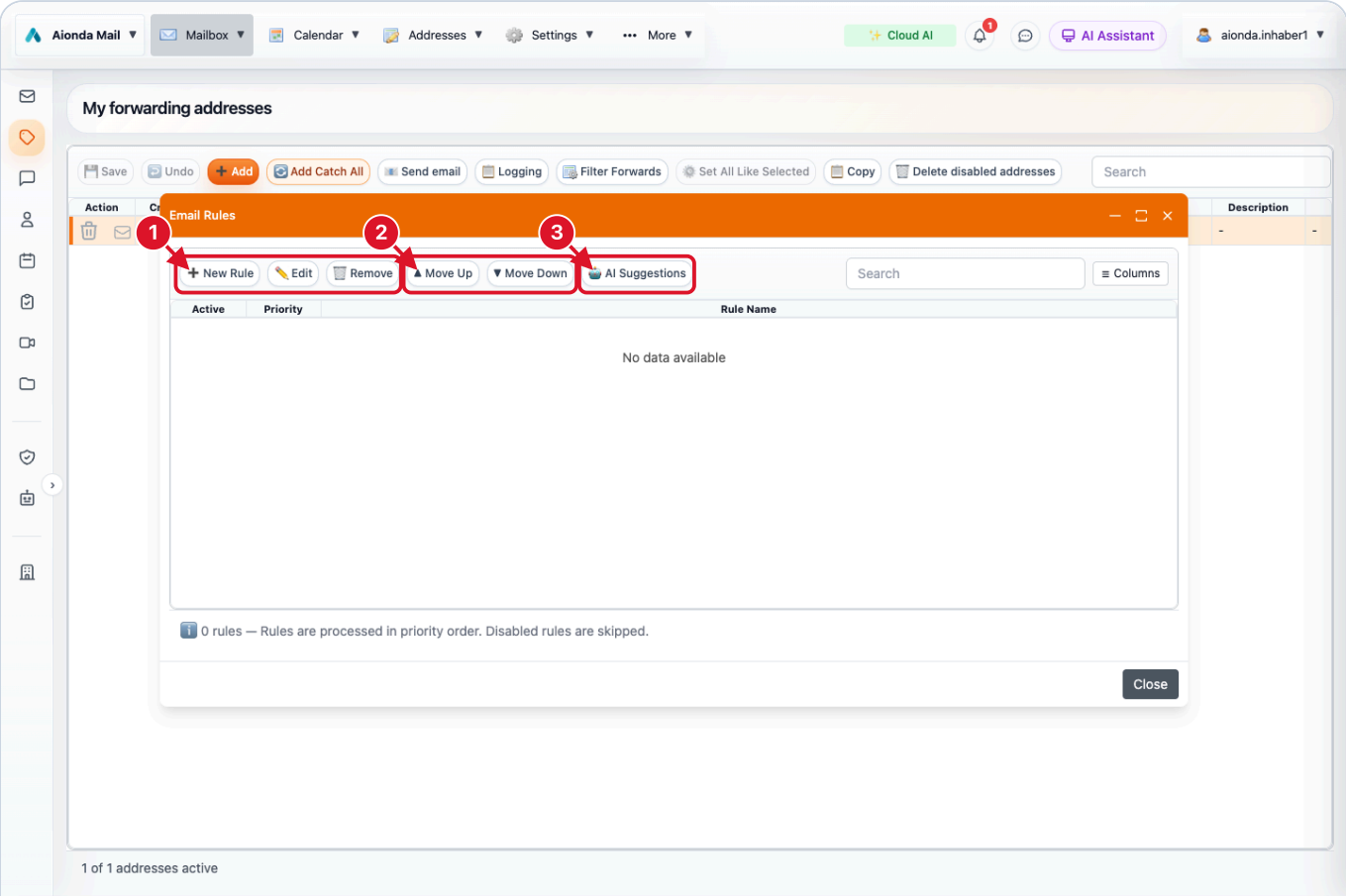
An employee can choose their own standard address; the owner can manage it too. If no first and last name are stored, the username is displayed. Address autocomplete uses eligible directory contacts alongside personal contacts. Check the chosen address before sending to similarly named people.

Privacy boundaries

Directory visibility does not automatically share the contents of personal contacts, mailboxes, files or calendars. A personal contact you created is not removed merely because a company visibility group changes. Publishing personal contacts to an entire visibility group is not part of this first directory version.

Rules and the email processor

Make repeatable decisions explicit and keep exceptions easy to audit.



1. Create a rule or edit a selected rule.
2. Adjust processing priority.
3. Ask AI for a rule suggestion, then review it.

Select the screenshot to open the full-size image.

Create a rule

1. Open Rules from the Mailbox menu.
2. Give the rule a descriptive name and choose whether all or any conditions must match.
3. Select a field such as sender, recipient or subject, then a comparison and value.

4. Choose an action such as moving to a folder or marking as read. Use only the actions offered for that processing path.
5. Save and test with a message that should match and one that should not.

For example, match an exact newsletter sender and move new messages into Newsletters. A broad “contains” condition can match more senders than intended. Check rule ordering and overlapping conditions when the result is unexpected.

Sender exceptions are rules

Not spam creates a sender-trust rule in the ordinary rules collection. Keep it visible and editable there rather than maintaining a separate, hidden whitelist. Removing the rule removes that exception for future classification; it does not delete old mail.

Email processor

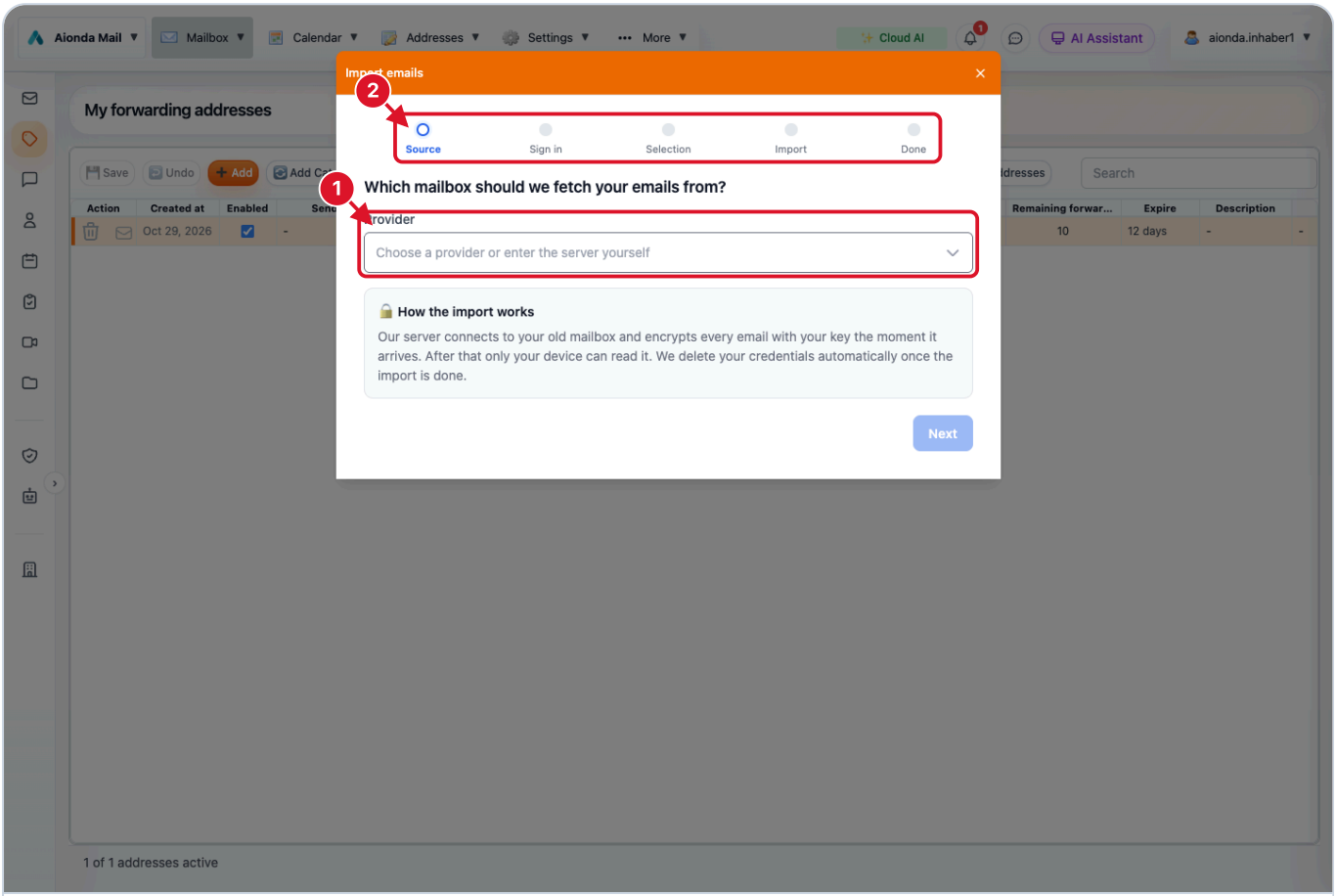
The email processor controls incoming and forwarding behavior, including filtering and header rewriting. It is separate from the low-priority client AI queue. Server rules cannot freely inspect content that exists only encrypted in a user’s mailbox; supported conditions depend on the processing stage.

AI assistance

Describe a rule in natural language if the AI rule assistant is available. Inspect the generated conditions, destination and actions before saving. Test the narrowest useful condition before applying destructive or broad rules.

Import, export and browser integration

Move data deliberately and verify that the destination contains what you expected.



1. Choose the source provider.
2. Follow the sign-in, selection and import steps. No source credentials are shown in this example.

Select the screenshot to open the full-size image.

Import existing information

Use the import workflow for the supported source type. Contacts accepts supported VCF/CSV input; other workspaces expose their own import options. Start with a small representative sample and inspect names, addresses, dates and attachments before importing a large collection.

An import may create duplicates. Keep the original export until the imported records have been verified. Source credentials used for a migration should not be reused as general-purpose sharing credentials.

Export and portability

Use the relevant workspace’s export or download action. Check the resulting file format and open it in an appropriate reader. A PDF is useful for reading but is not automatically a complete machine-readable export with attachments and metadata. An archive forensic export is evidence about integrity, not necessarily a full mailbox backup.

Browser extension

The browser extension can help create and insert disposable addresses in forms. Use the installed extension’s account settings and review the chosen lifetime before submitting a form. An alias that expires too soon can prevent later password-reset messages from reaching you.

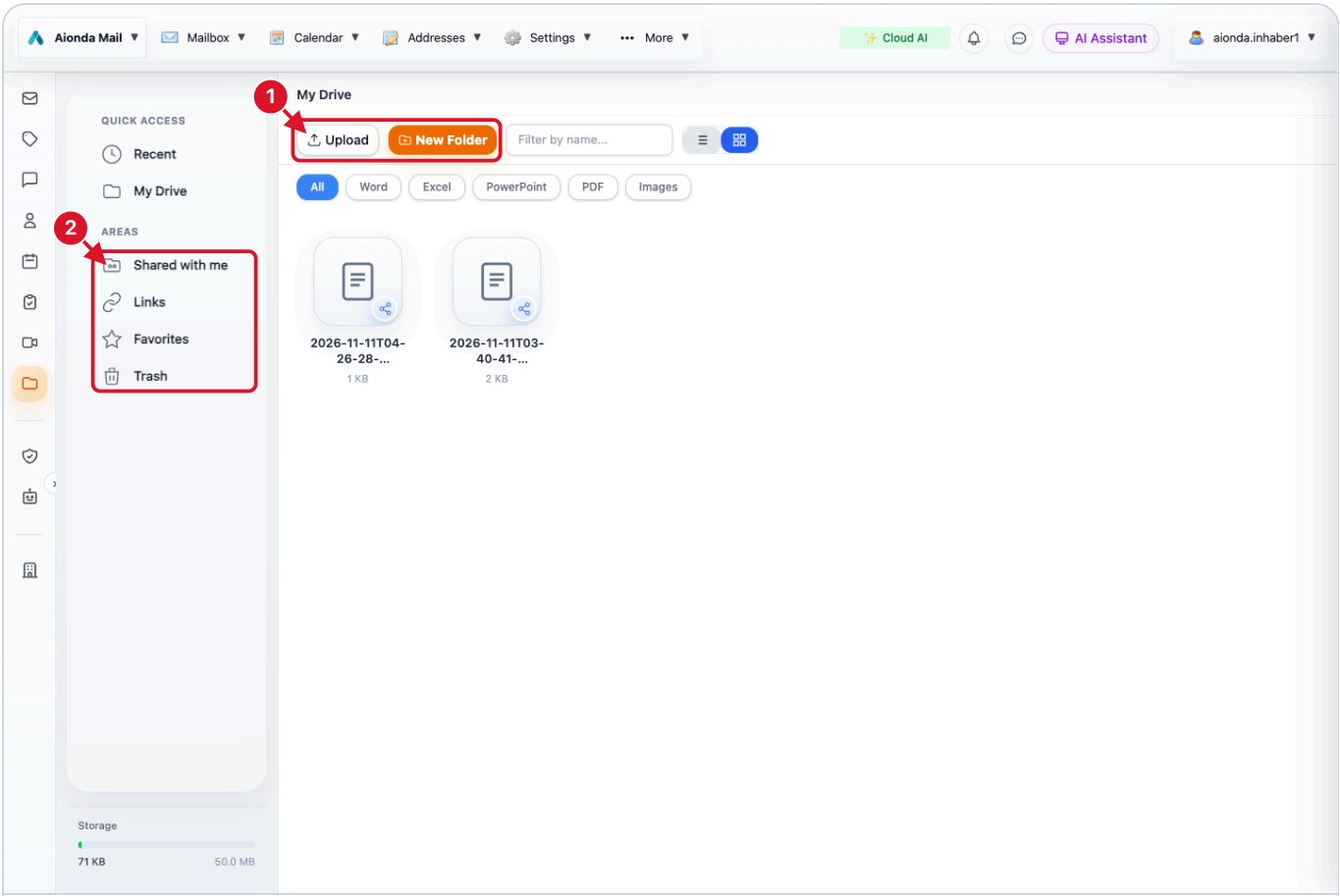
Before changing systems

Check address continuity, exported content, folder structure and recovery methods on the new device. Keep access to the old environment until you have confirmed that important records and authentication methods work in the new one.

Collaboration · Chapter 8

Drive and file sharing

Store files in encrypted storage and grant access deliberately.



1. Upload files or create a folder.
2. Switch between your files, incoming shares and links.

Select the screenshot to open the full-size image.

Upload and organize

1. Unlock your mailbox and open Drive.
2. Choose Upload or drop files into the workspace.
3. Create folders for projects and use search or favorites to find frequent items.
4. Preview or download a file to confirm that the upload completed correctly.

Drive encrypts file content in the client before upload. File keys enable sharing without publishing the rest of your storage. Mail and Drive storage contribute to the quota shown in your account; deleting a local original does not increase the server quota.

Share with an Aionda user

Open the item’s sharing action, choose an eligible recipient and select the permission level. Read access allows viewing or downloading. Full access permits additional changes offered by that share, such as uploading or renaming. Review Shared with me for items received from others. Visibility groups restrict eligible company recipients but do not themselves grant file access.

Share with an external link

Where link sharing is offered, create a link and review its access options, including password or expiry when available. Send the link only to the intended recipient. Anyone who obtains the required link and credentials may be able to use it. Revoke links when access is no longer needed.

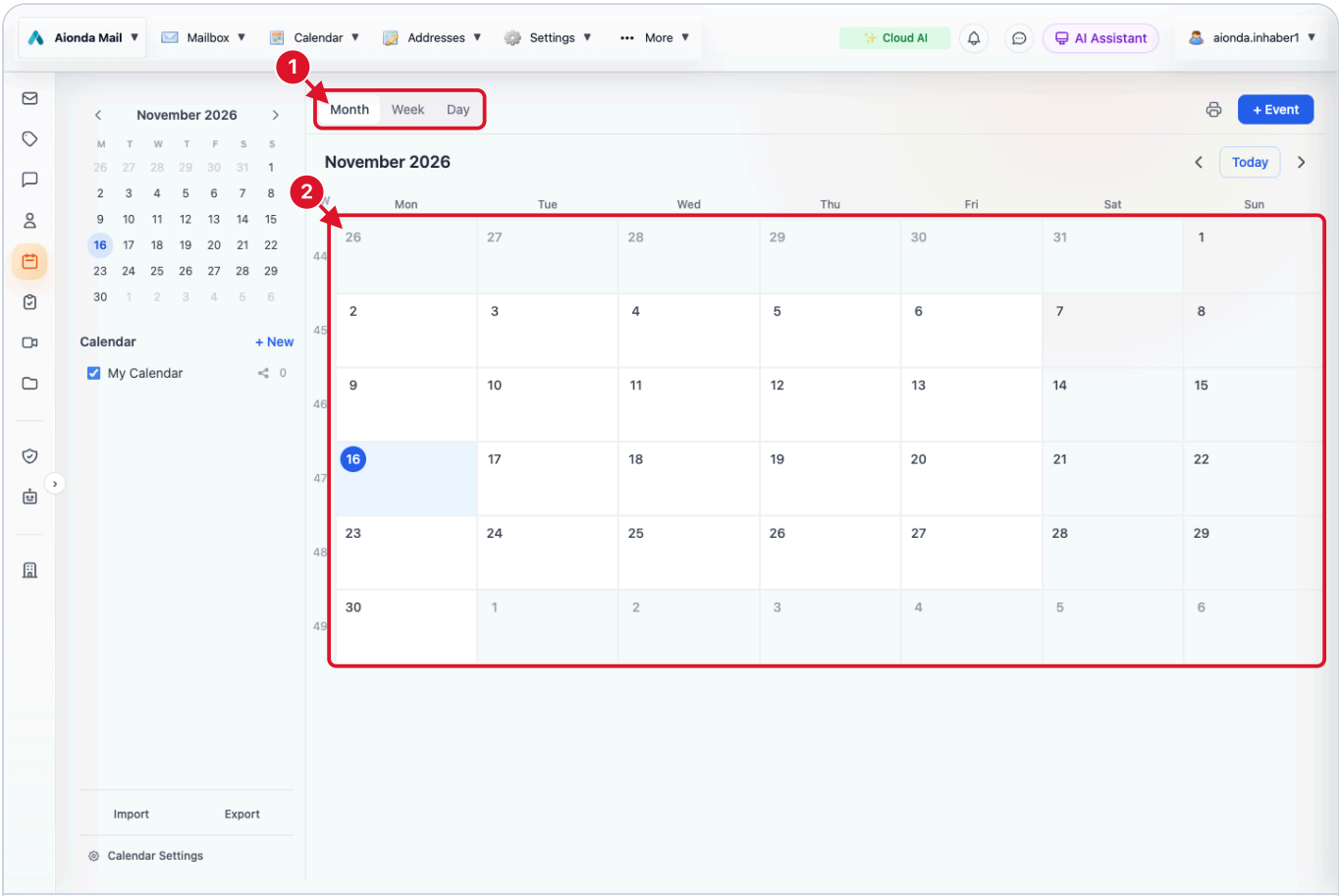
Change or revoke access

Review the item’s sharing settings and remove obsolete recipients or links. Revocation stops subsequent authorized access through the service; it cannot recall copies already downloaded. Moving a file to Trash is different from permanently removing it. Confirm the selected item and ownership before permanent deletion.

Collaboration · Chapter 9

Calendar and invitations

Plan appointments and check the recipient list before inviting others.



1. Choose the calendar view.
2. Select a day or appointment in the calendar workspace.

Select the screenshot to open the full-size image.

Create an event

1. Open Calendar and choose the date or New event.
2. Enter a title, start and end time, and the correct calendar.
3. Check the time zone, all-day setting and recurrence if applicable.
4. Add participants and review the details before saving or sending invitations.

A recurring event represents a series. When editing, pay attention to whether the action affects one occurrence or the series. Browser locale can change the appearance of dates even when the application language is English.

Invitations and shared calendars

Accept, decline or tentatively respond to invitations as appropriate. External recipients receive ordinary calendar invitations through email. Share calendars explicitly with eligible users and the appropriate permission; being visible in the directory does not automatically reveal all calendar details.

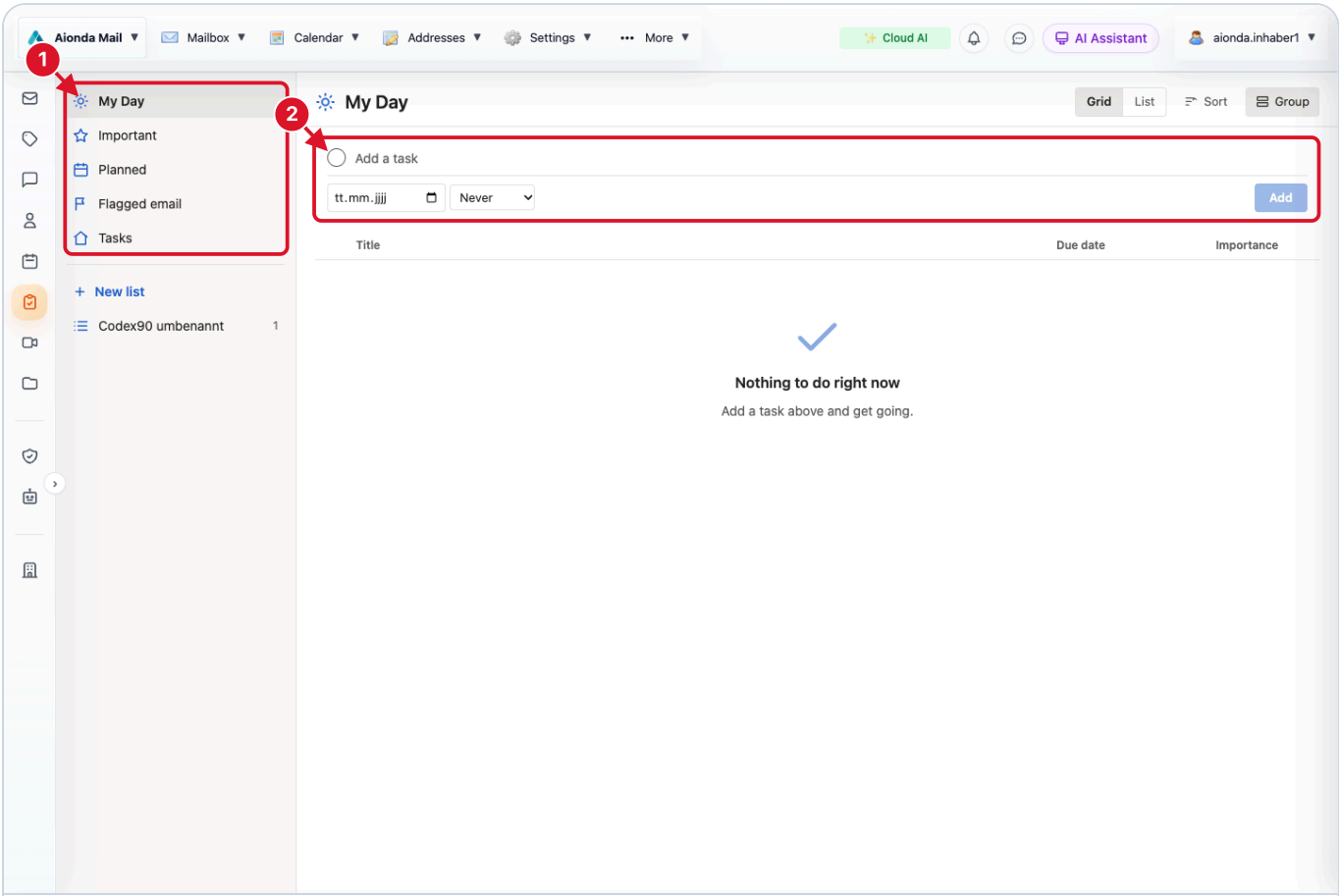
AI scheduling

The assistant can retrieve events and prepare new ones through supported tools. Check dates, time zones and participants in the resulting event, especially when the request uses phrases such as “next Friday”. Use an exact date when ambiguity would matter.

Collaboration · Chapter 10

Tasks and flagged email

Turn follow-up work into a list that you can review independently of the mailbox.



1. My Day, Important, Planned and Flagged email are different views.
2. Enter a task and optional due date.

Select the screenshot to open the full-size image.

Capture and organize

Open Tasks and enter a task title. Add a due date, importance or recurrence when needed. Create lists for separate projects. My Day is a focused daily view; Planned and Important help you find work across lists.

1. Create a task in the intended list.
2. Add a clear action and a useful due date.

3. Mark it complete when done; reopen it if further work is required.

Flagged email

Flag a message in Mailbox to make it available in the flagged-email task view. Opening the task takes you back to the associated mail. Flagged email across the account can differ from a filter on one folder. Counts should describe the actual matching set rather than only the rows currently loaded on screen.

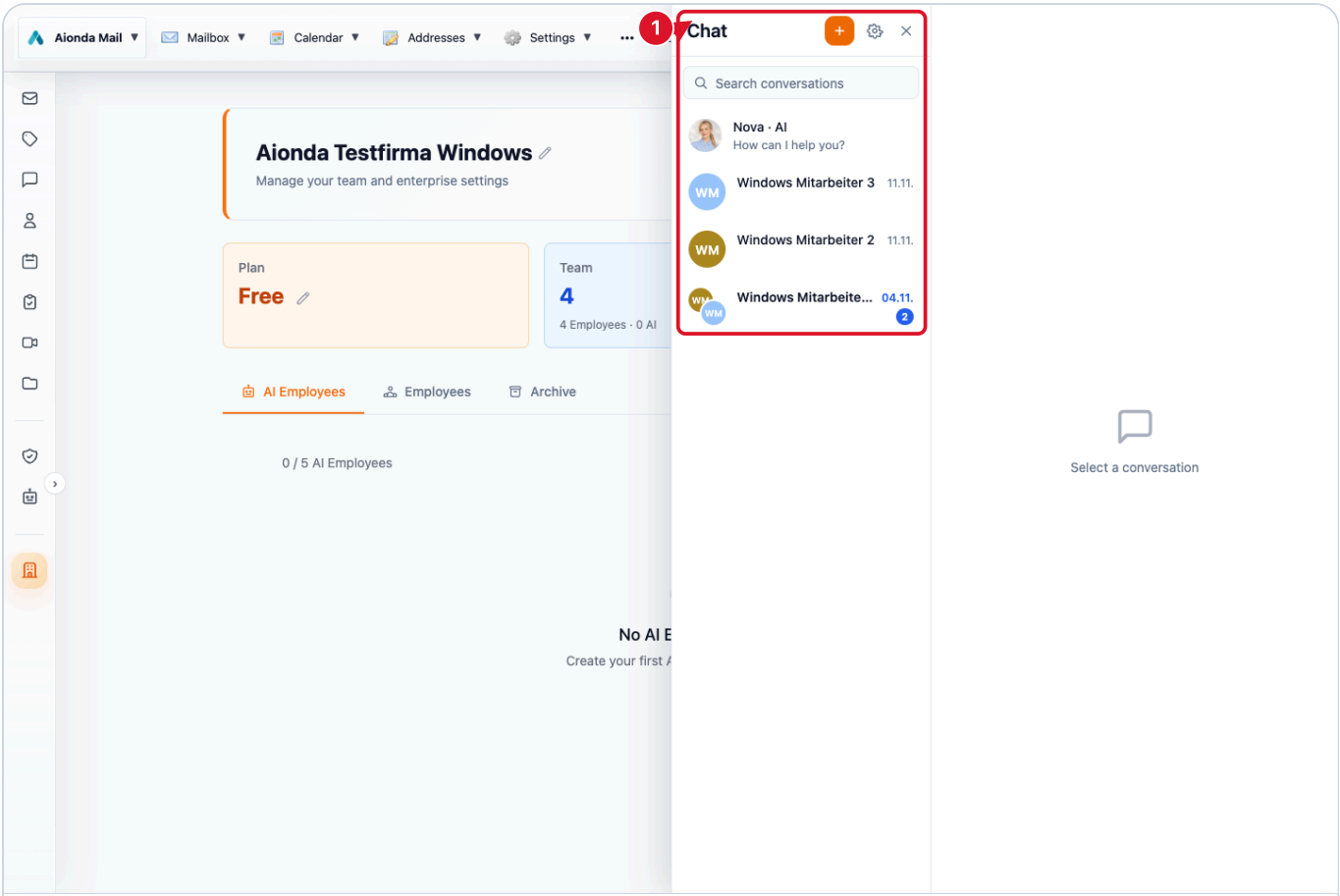
Ask the assistant

The AI task tools support listing, creating, updating, completing, reopening and deleting tasks, as well as working with task lists. Check the selected list and due date after an AI action. A deleted task is not the same as a completed task.

Collaboration · Chapter 11

Chat and video meetings

Discuss work with eligible contacts and keep meeting invitations under control.



1. Open Chat to find conversations and start a new one. Company visibility and conversation access remain separate from mailbox sharing.

Select the screenshot to open the full-size image.

Start a conversation

Open Chat, choose the action to start a chat and select an available contact. Visibility groups influence which company colleagues can be discovered and selected. Existing chat history and separately created personal contacts are not automatically erased when group membership changes.

Check whether you are talking to a human or an AI employee. An AI employee’s response is generated output and may require verification, even when the account has a familiar name

and avatar.

Join a video meeting

1. Open Video meeting and create or join the intended meeting.
2. Allow microphone and camera access when the browser asks, then check the selected devices.
3. Share the invitation only with intended participants.
4. Review which screen or window is selected before screen sharing.

A denied browser or operating-system permission can prevent audio, video or screen sharing even when the meeting itself opens. Check device permissions and another application using the camera before assuming the invitation is invalid.

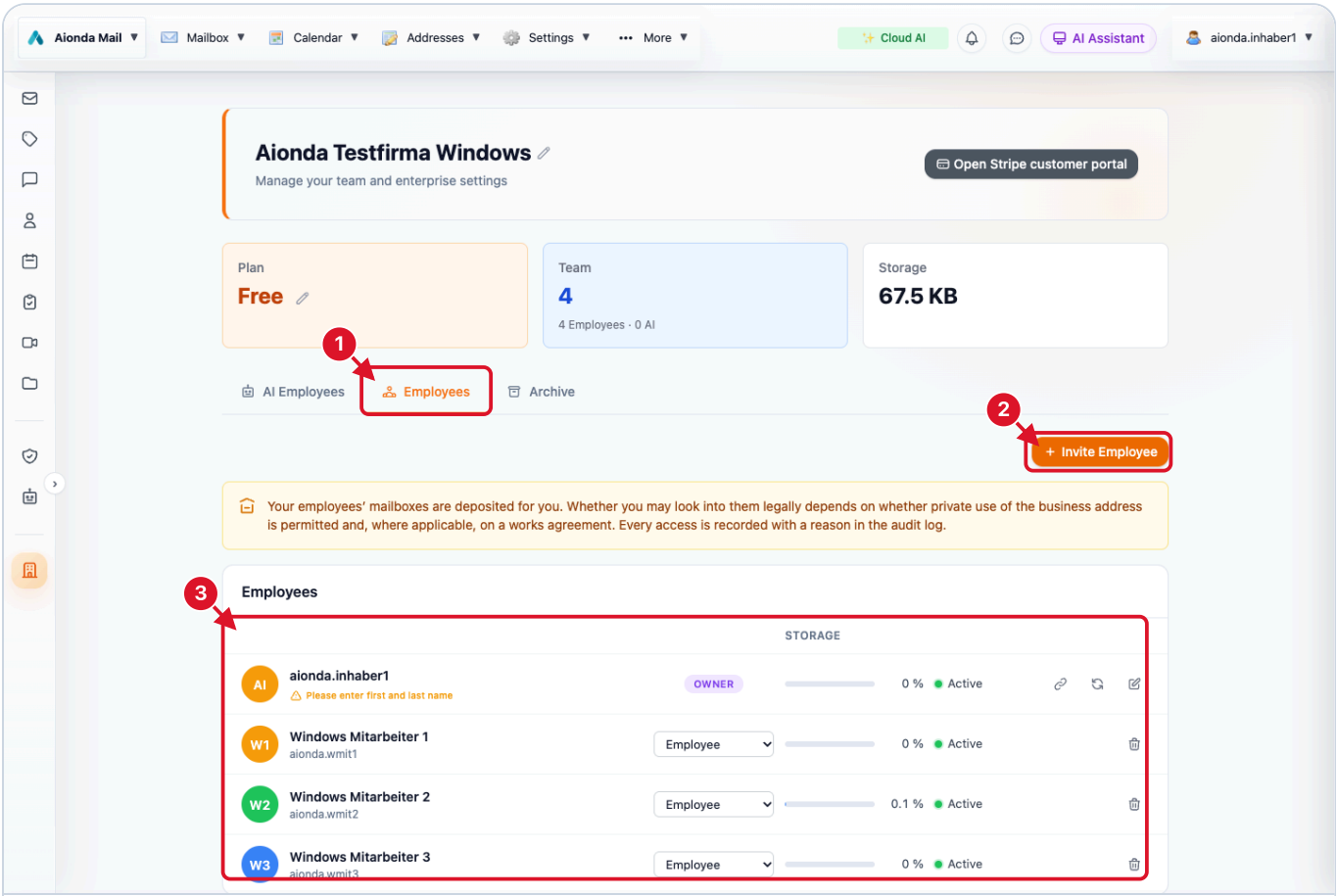
Keep boundaries clear

A chat membership is not a blanket grant to a mailbox, file store or archive. Share the relevant resource explicitly. Do not send recovery words, passwords or MCP credentials in a conversation.

Business · Chapter 12

Set up and manage a company

Give people and AI employees the access they need, with clear ownership and oversight.



1. Open Employees.
2. Invite a colleague.
3. Review membership and roles.

Select the screenshot to open the full-size image.

Company administration

Open Enterprise to see company settings, the employee roster, AI Employees and Archive. The owner manages the organization and employee profiles. Roles such as administrator, compliance officer, manager and employee represent different responsibilities; choose the least access needed for the job.

1. Review the company name and owner profile.
2. Invite employees using Invite Employee.
3. Check the resulting membership and role after the invitation is accepted.
4. Review each employee’s published contact address and visibility membership.
5. Configure archive and AI access separately from ordinary directory membership.

Names and directory identities

Store a first and last name for a readable directory. If these are absent, the username is used. Human employees and AI employees have distinct identities. Do not classify people automatically by surname: a family member can also be a genuine employee with different access needs.

Owner access and key deposit

Enterprise mailbox access can use deposited key material for authorized owner access. Review deposit status before assuming a mailbox can be opened. Access is recorded with a reason in the audit trail. The technical ability to open a mailbox does not decide whether doing so is legally appropriate for a particular employment or private-use arrangement.

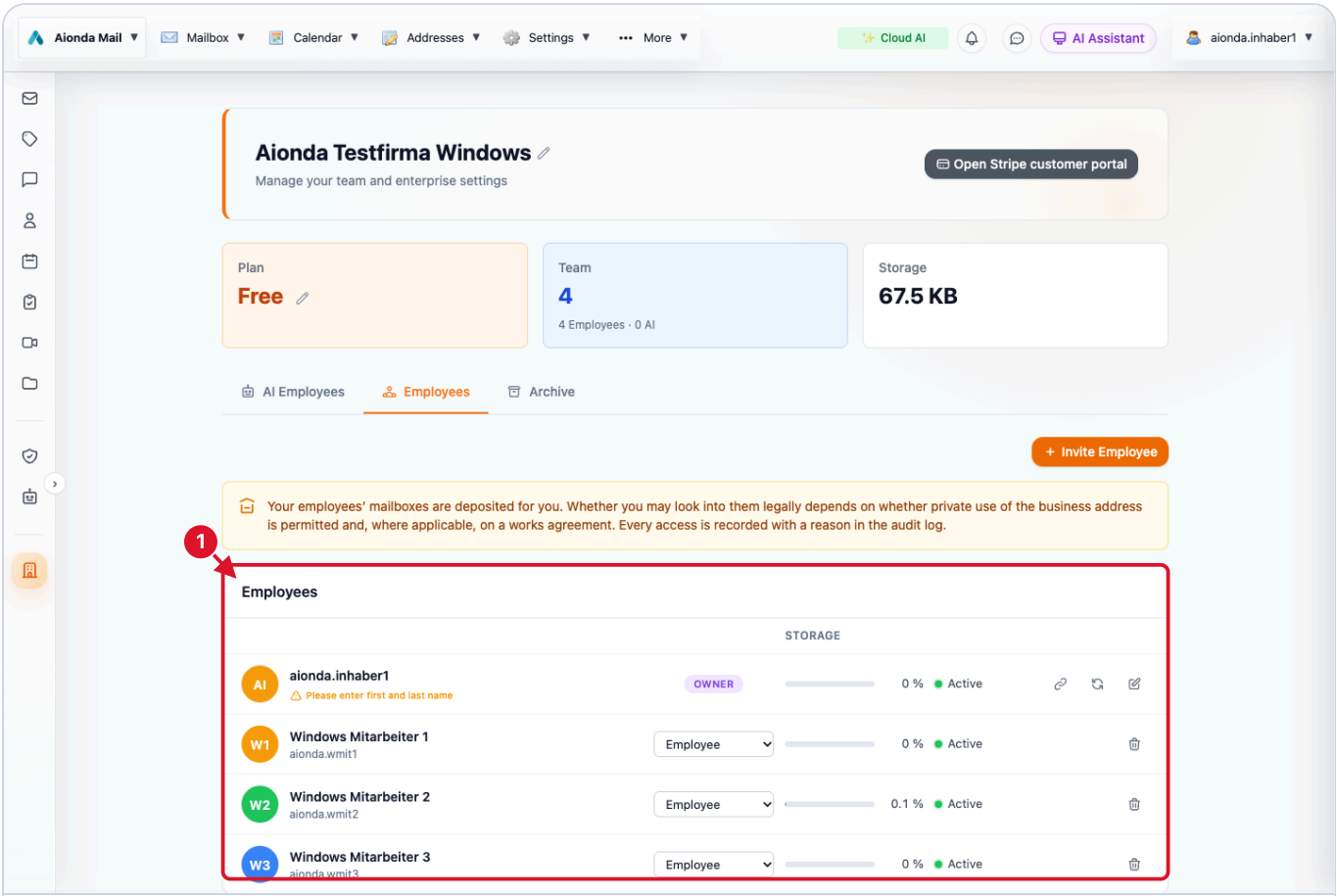
Offboarding

Before removing a member, review their shared resources, responsibilities, aliases and records that must remain available. Retained archive records and exported copies are separate from the employee’s current directory visibility. Test access from the affected role after changes.

Business · Chapter 13

Visibility groups: Company and Private

Control who can discover whom without confusing visibility with access to content.



1. The Web employee roster shows company membership and roles. Group administration is currently in macOS; this is not a screenshot of the group editor.

Select the screenshot to open the full-size image.

How groups work

When the company enables visibility groups, company-directory and recipient discovery use shared membership. For example, people in Private can see one another, while colleagues who belong only to Company do not discover those private members through the company directory. The owner retains an administrative view across the organization.

Membership is explicit. A surname, family relationship or job title does not decide the group. A person who works in the business and participates privately can belong to more than one group. A human member must retain a group; an AI employee belongs to exactly one.

Example

Member	Membership	Directory scope
Owner	Company and Private	Administrative view
Office colleague	Company	Company colleagues
Private member	Private	Private members
Private AI assistant	Private	Authorized private context

This is a conceptual example, not a screenshot or a statement about actual employee memberships.

Administration and client availability

In the Web app, open Enterprise → Employees → Visibility groups as the owner. The macOS app offers the equivalent group administration. Enable groups deliberately and review the initial memberships. Choose Edit to add or rename groups and select human and AI memberships. Review the preview before saving; Cancel discards the changes. In Chat, members of multiple groups can filter people by group. Other native clients may not yet offer the same administration screen.

AI employees already in use cannot simply be moved to another group in this first version. Create a separate AI identity for the new scope instead of carrying existing context across that boundary. Group deletion is not offered in the initial administration flow.

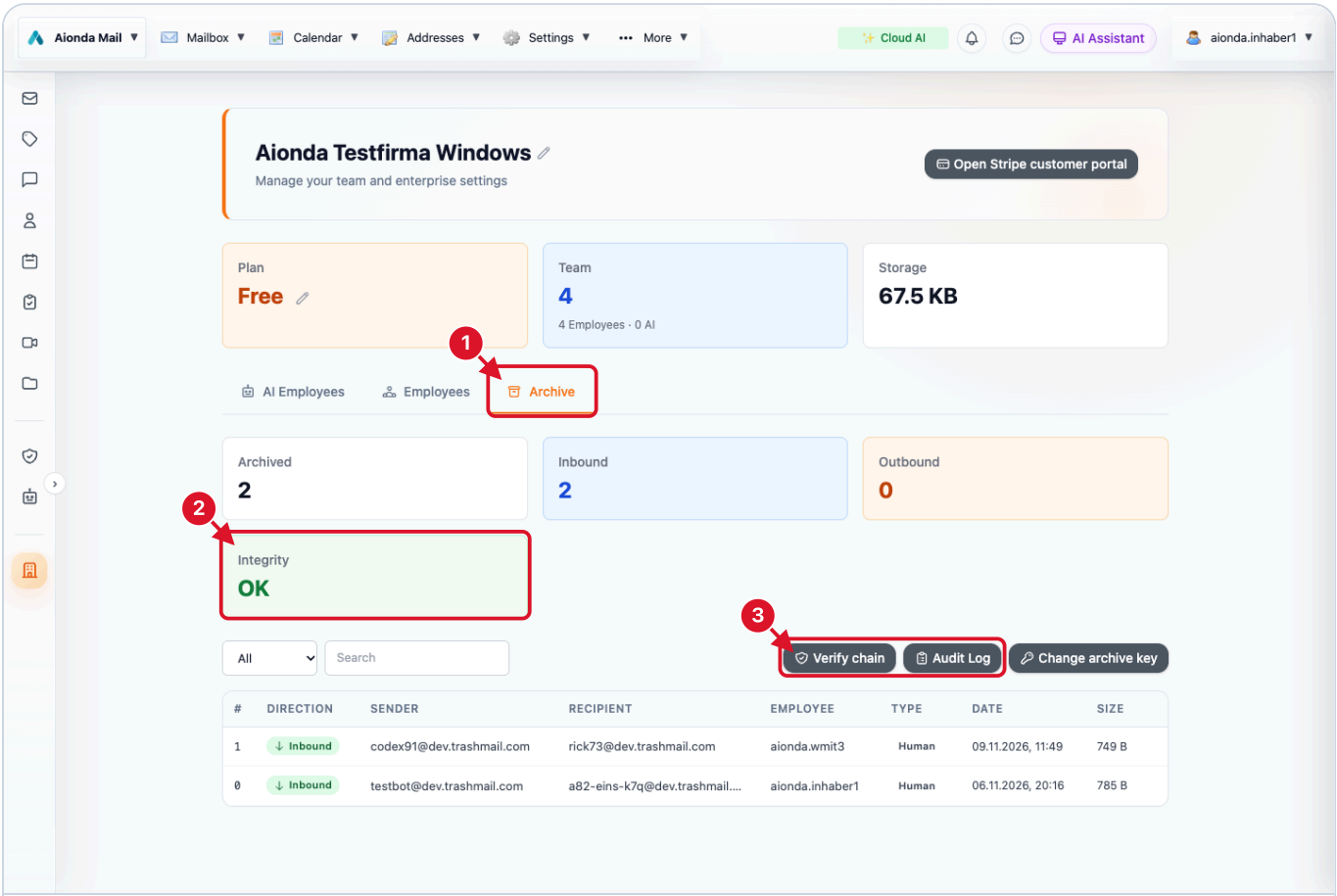
What groups do not do

Groups do not grant file or mailbox access by themselves. They do not erase existing chat history, personal contacts or previously downloaded copies, and they do not hide members from authorized owner administration. Grant and revoke resource shares separately.

Business · Chapter 14

Business archive, integrity and GoBD

Preserve business records and understand exactly what the archive's hash chain proves.



1. Open Archive.
2. Read the integrity status.
3. Verify the chain and inspect the audit log.

Select the screenshot to open the full-size image.

Operate the archive

1. Open Enterprise → Archive with an authorized account and unlock the required keys.
2. Check that archiving is enabled for the intended organization and review retention settings. Draft archiving is a separate option.

3. Use direction filters and search to locate a record.
4. Run Verify chain and inspect the reported result.
5. Review the audit log and export the available forensic evidence when needed.

Archive records are separate from ordinary Inbox organization. Moving an email to another mailbox folder does not mean that the archived business record has been removed. Retention and any legal hold must be handled through the archive workflow, not through ordinary mailbox cleanup.

What “blockchain” means here

The implemented archive maintains a company hash chain using SHA3-256. Each block links to the previous hash and includes the record’s hash, timestamp and metadata. Verification checks the internal continuity and integrity of that chain. The implementation reviewed for this edition does not establish publication to a public blockchain or independent consensus.

This makes the chain useful as tamper-evidence relative to a trusted reference. It is not an absolute guarantee against a privileged party rebuilding an entire chain and replacing the reference. Keep independently retained exports or other trusted evidence as part of your organization’s verification process.

Exports and readable records

A forensic export describes chain evidence and verification data. Do not assume that it is a complete, readable export of every email and attachment. Check the export format, preserve the necessary decryption capability and test that the business records can actually be retrieved and read for the required period.

GoBD responsibilities

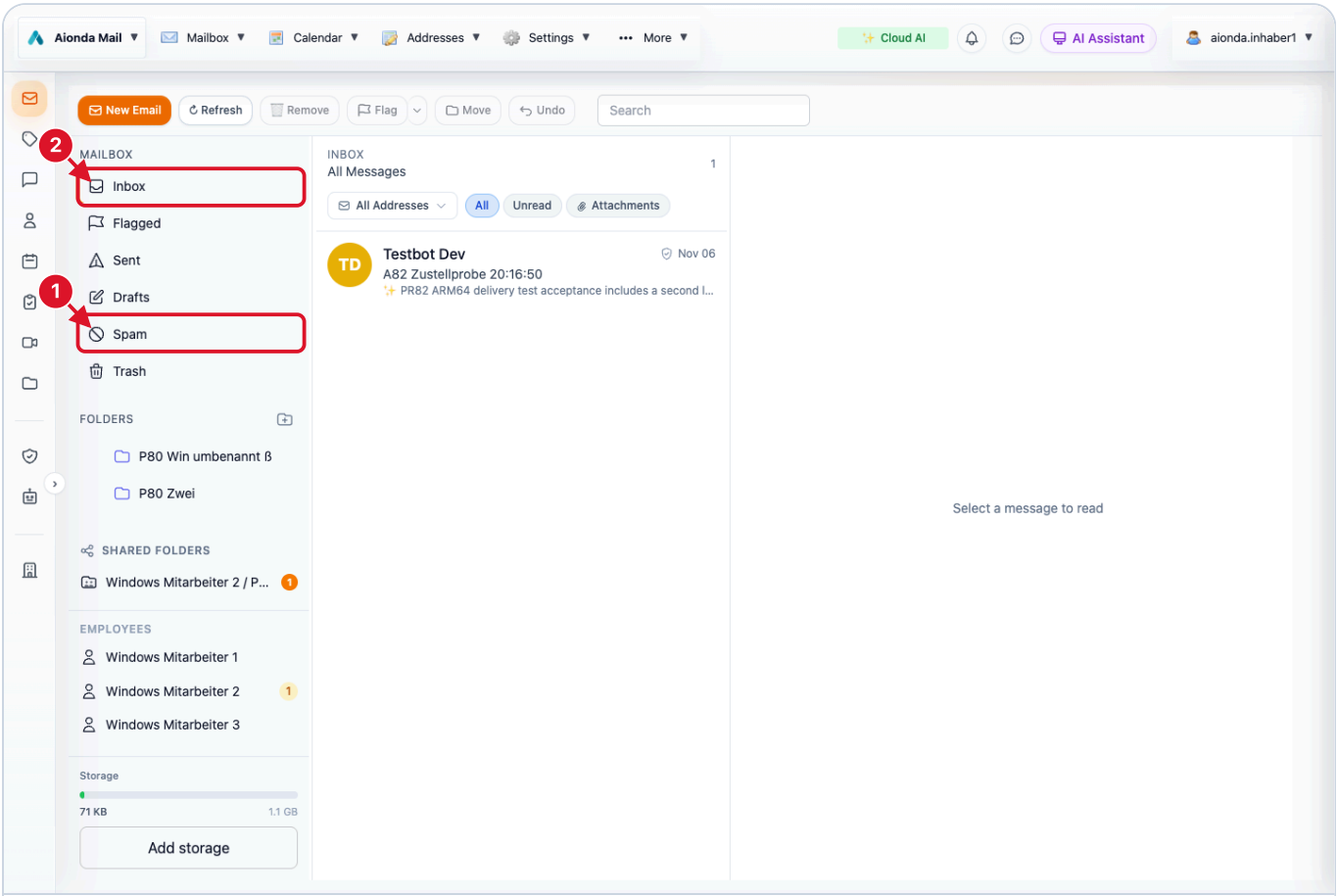
GoBD concerns the overall recordkeeping process, including completeness, traceability, retention, accessibility and procedural documentation. A hash chain alone does not certify a company’s compliance. Define the applicable record categories, retention periods, authorized access and verification procedures with the responsible advisers. The software’s default retention value is not individual tax advice.

Primary reference: German Federal Ministry of Finance: GoBD, including its published amendments. This handbook explains product behavior; it is not a compliance certificate.

Security · Chapter 15

Spam and phishing protection

Understand why a message moves, how to recover a false positive and what trusting a sender actually does.



1. Open Spam to inspect an automatically moved message.
2. Automatic background scanning applies to Inbox, not every folder.

Select the screenshot to open the full-size image.

Two stages of detection

Server-side filtering evaluates incoming mail and technical signals before or during delivery. Client-side AI can analyze readable message content later, after the mailbox is unlocked. These stages can produce a warning banner or a recommendation to move a message to Spam.

Automatic client scanning and automatic Spam moves are restricted to the Inbox. Mail already placed in a custom folder is not swept into Spam by this background workflow. Messages already in Spam are not repeatedly moved there. The UI briefly explains the automatic move so that a message disappearing from the list is understandable.

Background work and priority

While the app is active and the mailbox unlocked, queued Inbox analysis runs at lower priority. Opening a message gives its analysis priority over waiting background work. This is not a promise of continuous AI processing while an iPhone or iPad app is suspended or closed.

Recover a false positive

1. Open the Spam folder and inspect the message and sender.
2. Choose Not spam when you are satisfied it is legitimate.
3. The message returns to Inbox and an exact-sender trust rule is stored among the normal mail rules.
4. Review or remove that exception in Rules if it is no longer appropriate.

A trust rule is not a certificate that every future message is safe. Malware detection and failed sender authentication can still prevent the trust exception from bypassing protection. The warning banner remains available when reading a message in Spam.

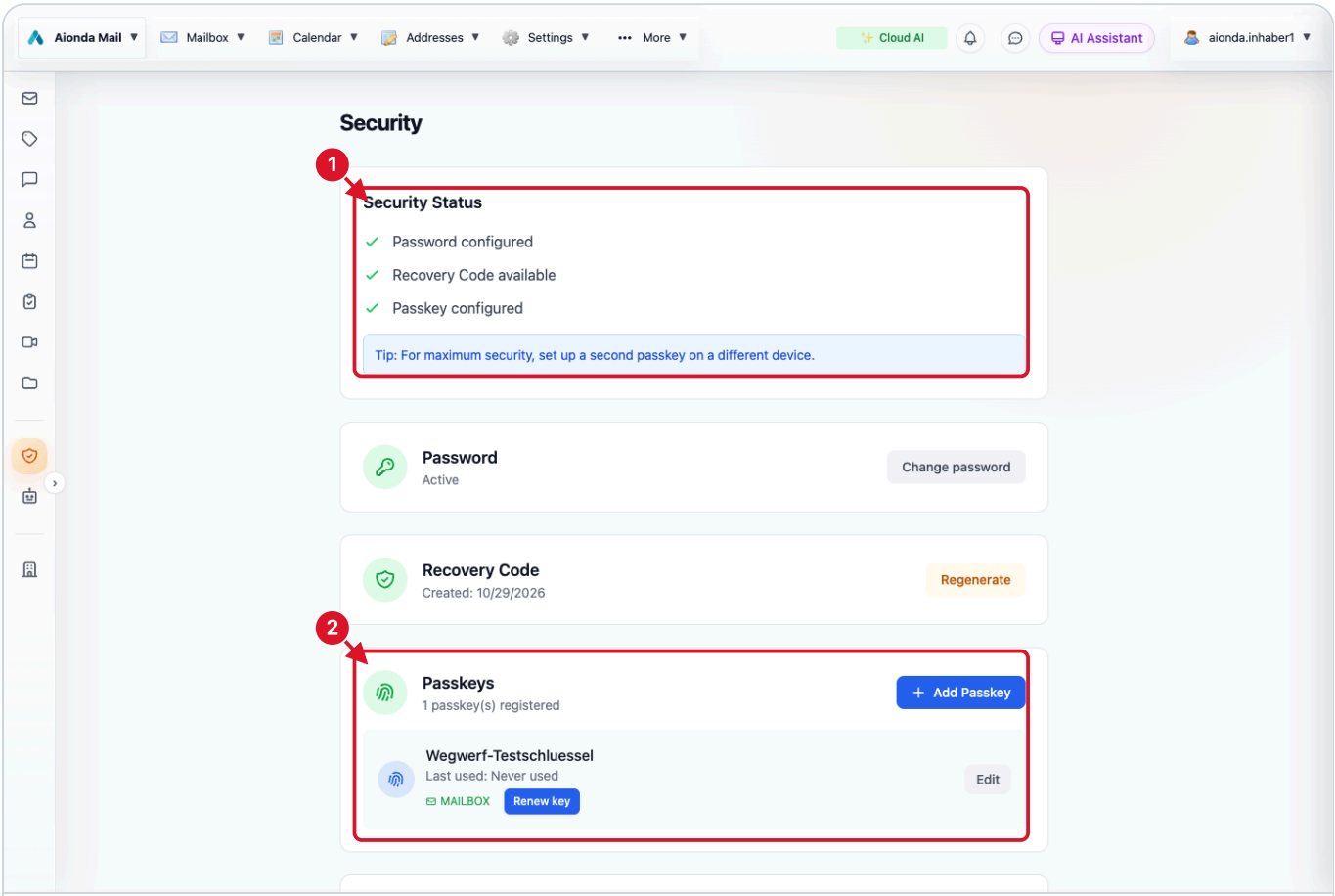
Report a suspicious message

Use Move to spam where offered, including a suspicious-message warning or a message covered by a sender exception. A manual Spam decision removes the sender’s trust exception. Verify unusual payment requests or password requests using an independent contact channel; do not treat an AI verdict or a familiar display name as proof of identity.

Security · Chapter 16

Security basics: passkeys and post-quantum encryption

Understand who can read your data, how you unlock it and why the security of an email depends on its entire route.



1. Review the configured password, recovery and passkey methods.
2. Check the passkey's mailbox capability and manage your authenticators.

Select the screenshot to open the full-size image.

Start with three different questions

Who may sign in? Authentication checks access to the account. **Who can unlock stored content?** Encryption keys protect the mailbox and workspace. **Was the message protected before it reached Aionda?** That depends on the sender and the delivery route. A secure account does not make every ordinary Internet email end-to-end encrypted.

Public and private keys, in plain language

A public key lets someone prepare an encrypted message for you. Your corresponding private key opens it. Publishing the public key is expected; protecting the private key is essential. Aionda encrypts private mailbox key material under a master key that is reconstructed on your device when you unlock the mailbox.

How a passkey helps

A passkey is a cryptographic sign-in credential approved through your device or authenticator, often with a fingerprint, face recognition or a device PIN. You do not type a reusable password into the site for the passkey operation. Whether a passkey can also unlock the mailbox depends on support for the required **WebAuthn PRF** capability.

PRF supplies key-derived material for protecting one part of the vault unlock secret. A passkey that works for sign-in is therefore not automatically sufficient for mailbox unlocking. Review its mailbox status in Security. Biometrics approve the local authenticator operation; Aionda does not need a copy of your fingerprint or face.

Two out of three unlock factors

The vault master key uses a two-of-three sharing scheme. One share is protected through your password, one through a compatible passkey and one through your recovery information. Two different available shares reconstruct the key; this is not the same as merely having two passkeys.

Available factors	Typical purpose
Password + compatible passkey	Normal vault unlock.
Password + recovery information	Recover access when a passkey is unavailable.
Compatible passkey + recovery information	Recover or change access when the password is unavailable, through the supported recovery flow.

Keep recovery words offline and never send them to support. Confirm another usable recovery path before removing a credential. A device’s ability to sign in is not proof that it can reconstruct the mailbox keys.

What “post-quantum” protects

An attacker could collect encrypted traffic today and try to decrypt it later with a powerful quantum computer. Aionda’s mailbox key encapsulation combines **X25519**, a classical method, with **ML-KEM-1024**, a post-quantum method. Message content is protected with **AES-256-GCM**. In everyday terms, the hybrid construction protects the key needed to open the encrypted mailbox copy.

This protection is about the implemented encryption path. It does not make a compromised device safe, hide all delivery metadata, or automatically upgrade an external provider, a traditional PGP key or the sender’s original connection. The **PQ** indicator describes the mailbox protection; inspect the other security information to understand the whole route.

Read the security indicators

Protection	What it tells you
TLS transport	A connection between systems was encrypted. The participating mail servers can still process ordinary mail.
Vault / PQ encryption	The stored mailbox copy uses Aionda’s encrypted mailbox scheme. This alone does not say that the sender encrypted the original.
PGP encryption	The sender encrypted protected message content for the recipient before delivery. See the PGP chapter.
Signature	A signature can support authenticity and integrity relative to a trusted key. Signing is different from keeping content confidential.

The boundaries of end-to-end protection

Drive uploads and supported encrypted workspace records are encrypted on the client. Ordinary external SMTP mail can arrive readable and is then encrypted for mailbox storage. For external end-to-end email, use a compatible content-encryption mechanism such as PGP at the sender and recipient.

Explicit shares give recipients access to the selected data. Enterprise key deposit can authorize organizational access. Cloud AI receives the readable context sent for processing, and an external MCP assistant receives its tool results. Optional email logging can retain a separate original message. Review these boundaries instead of interpreting “encrypted mailbox” as “no other copy or authorized reader exists”.

Keep access recoverable

1. Open Security and review password, recovery and passkey status.
2. Add a compatible second authenticator when appropriate and verify that the required unlock workflow works.
3. Keep recovery information securely offline, separate from the device.
4. Inspect key-renewal prompts and their sharing implications before proceeding.
5. Lock or sign out on shared devices. Report unexpected key changes through a separate trusted channel.

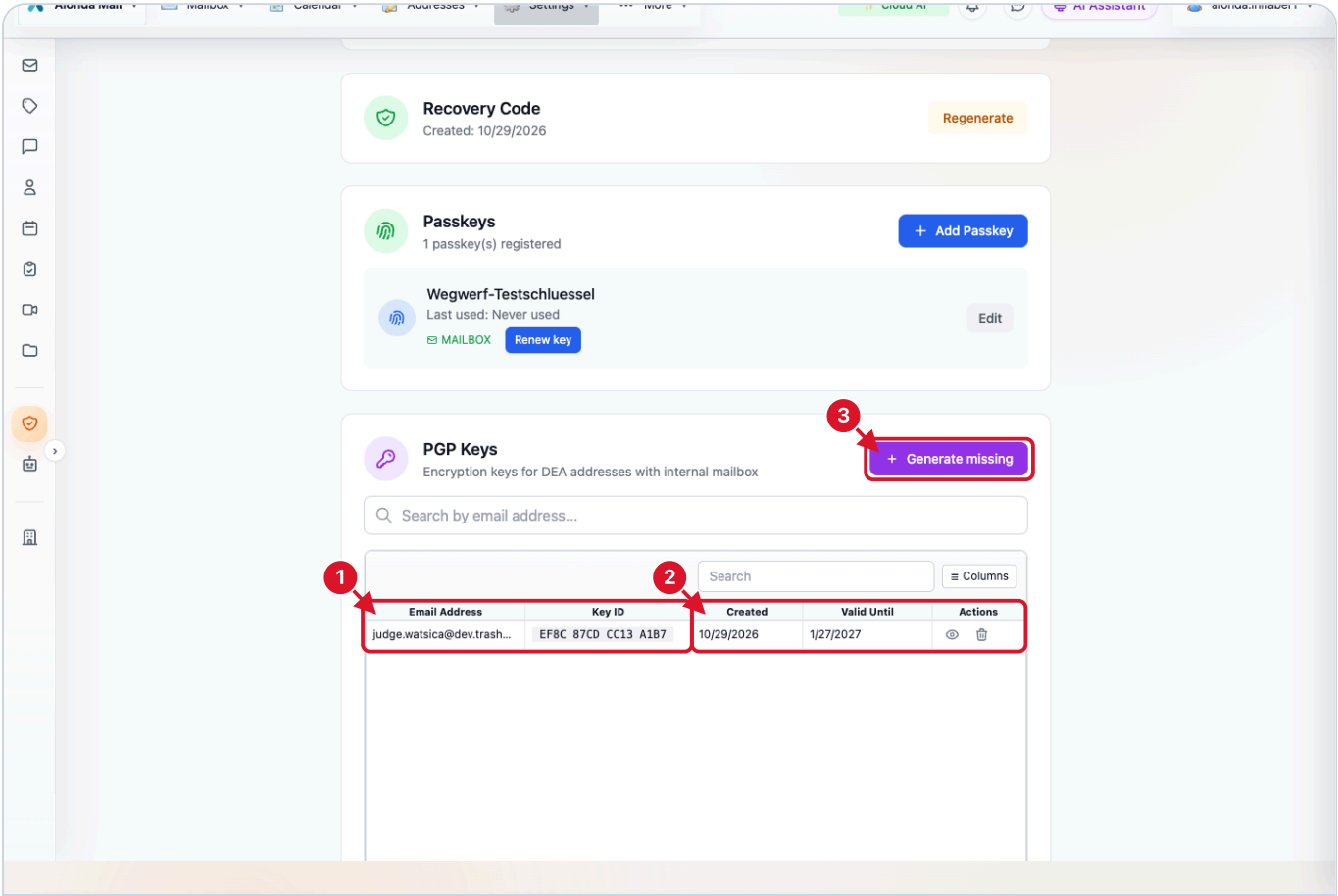
Background standards

For the underlying standards, see NIST FIPS 203: ML-KEM and the W3C Web Authentication specification. These describe cryptographic and authentication building blocks; the product-specific boundaries above explain how they apply to Aionda Mail.

Security · Chapter 17

PGP: encrypted email with external correspondents

Protect message content before it reaches a mail server, and distinguish encryption from signing and post-quantum mailbox storage.



1. Find the PGP key for your Secure Mailbox address.
2. Check validity and open Details.
3. Generate missing keys only for eligible addresses.

Select the screenshot to open the full-size image.

What PGP adds

OpenPGP encrypts content for a recipient’s public key so that the corresponding private key is needed to read it. If the sender encrypts before sending, the protected body and

attachments can cross mail servers as ciphertext. This is different from encrypting an ordinary message only after it arrives in the Secure Mailbox.

A signature serves another purpose: it helps verify integrity and the signing key. A signed but unencrypted email remains readable. Trust in the key's owner must still be established; a familiar display name alone is not enough.

Your address keys

1. Open **Security** and scroll to **PGP Keys**.
2. Locate the Secure-Mailbox-only alias you want to use. Check its Key ID and Valid Until date.
3. Open **Details** to inspect the public-key information. Share public information, never private key material.
4. If an eligible alias has no key, use the offered **Generate missing** workflow after unlocking.

Public keys for eligible aliases are published through **WKD (Web Key Directory)**, allowing compatible senders to discover them. Automatic key management is designed for eligible Secure-Mailbox-only addresses; an alias that also forwards externally is a different delivery arrangement. Verify the destination and available key before promising a correspondent that you can decrypt their mail.

Send an encrypted message

1. Select the intended From address and enter every To, Cc and Bcc recipient.
2. Allow key discovery, or use an appropriate recipient public key stored with the contact. The Web composer can look up keys through WKD and the supported key service.
3. Inspect the PGP state. All recipients need usable keys for an encrypted send; a key for only one recipient is not sufficient.
4. Check fingerprints with the recipient through another trusted channel when identity matters.
5. Confirm that encryption is enabled, review attachments and send. Resolve a missing, expired or revoked key instead of assuming that the message remained encrypted.

The composer encrypts the supported body and attachments in the client using PGP/MIME. Delivery metadata, such as routing addresses, is still needed by mail systems. Do not assume that the ordinary Subject header is hidden.

Read, renew and preserve keys

Unlock the mailbox to use the protected private keys needed for decryption. If an old message cannot be opened, check whether the matching historical key is available. Rotating a key for new mail does not make an old message readable with the new key alone. Avoid deleting key material needed by existing correspondence.

PGP and post-quantum are not interchangeable

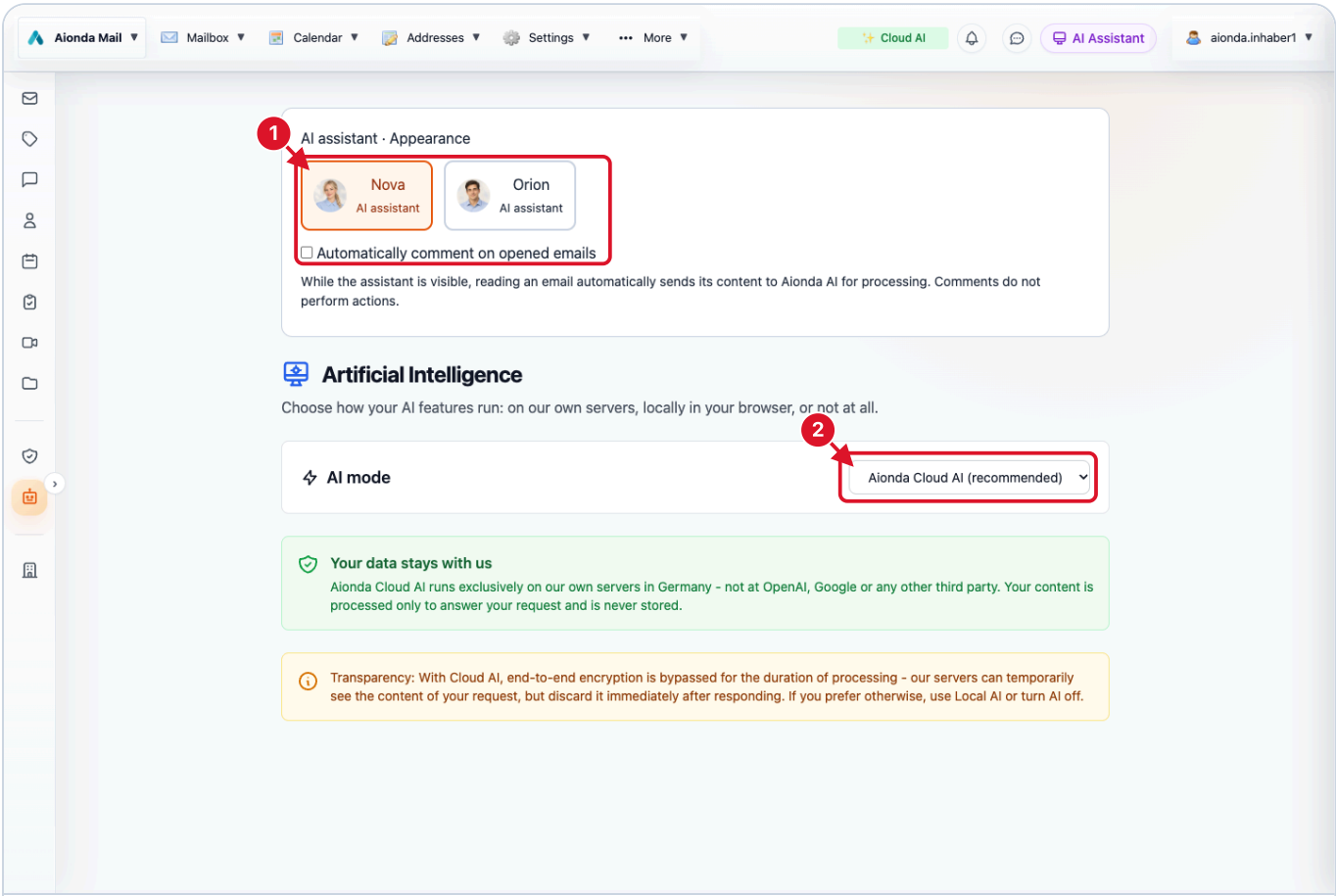
The PGP key generation reviewed for this Web version uses classical Ed25519/X25519 keys. Aionda's mailbox storage separately uses hybrid X25519 + ML-KEM-1024 key encapsulation. Therefore a PQ badge on the stored mailbox copy must not be read as proof that the external PGP exchange itself used a post-quantum algorithm.

A practical check

Exchange a harmless test message with your correspondent, inspect the encryption and signature information, and confirm that both sides can read the reply. Repeat the check after changing addresses or keys. For messages received without PGP, the Security information can still explain the transport and encrypted-storage protection that did apply.

Choose how AI processes your data

Local text processing, cloud processing and external assistants have different data boundaries.



1. Choose the assistant presentation and reading behavior.
2. Review the processing mode and data information.

Select the screenshot to open the full-size image.

Select a mode

Open Artificial Intelligence and review the available mode before enabling features. Cloud AI processes the supplied readable context on Aionda's AI infrastructure. Local AI runs supported text inference on the device using a downloaded model and compatible browser hardware. Off disables the corresponding AI assistance.

Mode or capability	Where to pay attention
Local text AI	Model download, device memory and supported browser GPU capabilities.
Cloud AI	Readable prompts and selected context are sent for server processing.
Speech, image or PDF analysis	These features can use separate cloud endpoints; local text mode is not a blanket offline guarantee.
External MCP assistant	The connected assistant receives the content returned by its authorized tools.

Control context

The assistant can comment on the currently opened message when that option is enabled. Turn it off if you prefer to initiate analysis yourself. Check the AI indicator and settings rather than assuming that the persona name, such as Nova or Orion, determines the processing location.

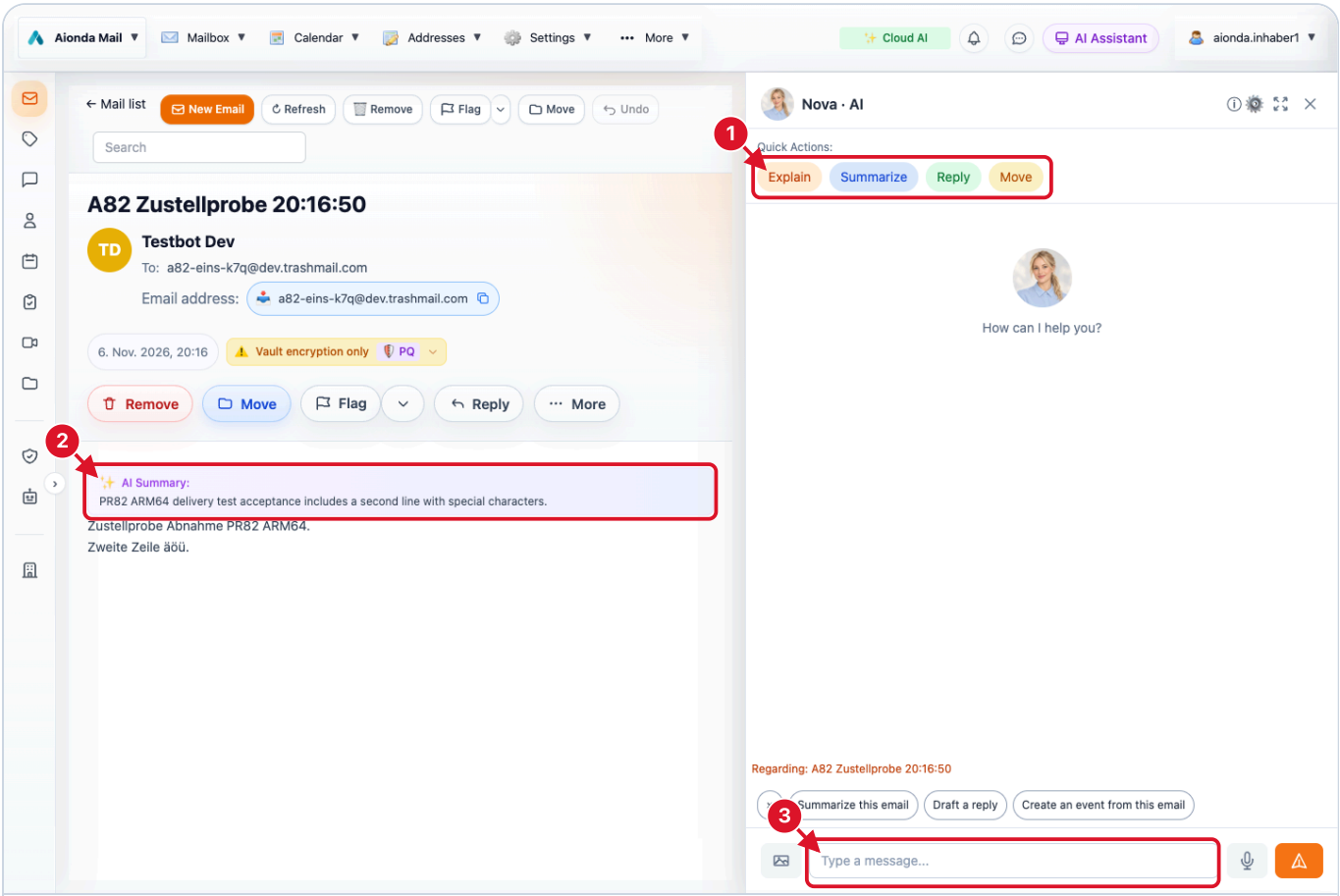
Limits and verification

Models can misunderstand intent, invent facts or misread documents. Confirm recipients, amounts, dates and requested actions before relying on output. Text inside emails, web pages and attachments is untrusted source material, not an authorization to perform unrelated actions.

A personal local-AI selection does not automatically change how a server-run AI employee or an external MCP application operates. Configure those separately.

AI assistance throughout the workspace

Use AI for drafts, triage, research and structured actions, then review the result.



1. Quick actions for the open email.
2. Review the message summary.
3. Enter a request with the intended context.

Select the screenshot to open the full-size image.

Reading and triage

AI can summarize a message, explain it, suggest replies, translate foreign-language text, recommend a folder and identify spam or phishing signals. Automatic reading comments and queued Inbox analysis depend on your settings and an active unlocked client. Folder recommendations do not give the assistant permission to sweep every folder for spam.

Writing

Use the composer's AI actions to draft text, improve wording, adjust tone, translate or prepare a signature. Where inline completion is offered, accept the suggestion only when it fits. Smart replies are starting points, not evidence that the assistant understood every attachment or prior agreement.

Workspace tools

Area	Supported kinds of assistance
Email	Search, read, list folders, compose or reply, send the open email, discard a draft and delete selected mail.
Contacts	Find contacts, prepare a new contact and save an open form.
Calendar	Retrieve events and create appointments.
Tasks	Create, update, complete, reopen or delete tasks and manage lists.
Drive	List files, read supported content and analyze images.
Addresses	Inspect, create, update, enable or disable aliases, inspect delivery logs and diagnose delivery.
Rules	List, create, edit, enable, disable or delete mail rules.
Research and help	Search the web, fetch a page, inspect DNS or mail-domain configuration, read help and contact support.
Meetings	List available video meetings.

Available tools depend on the assistant, context, permissions and client version. Review action confirmations where shown. Do not assume every tool call is draft-only: sending, deleting or changing a rule can modify real data.

Attachments and voice

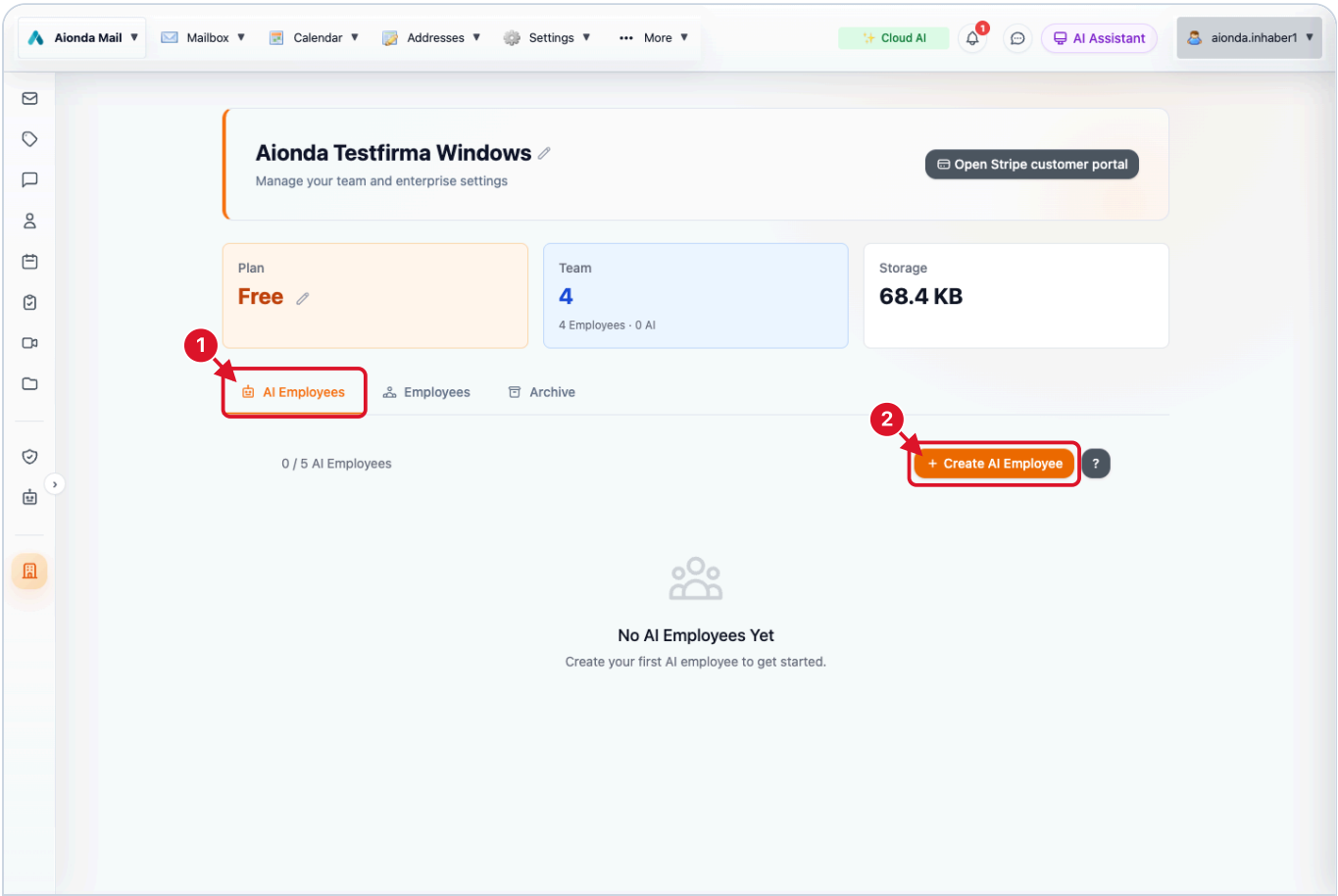
Image and PDF analysis can extract useful information, but the analyzed portion may be limited; the Web PDF analysis path reviewed here processes at most the first five pages. Check the original document when completeness matters. Voice input may use a separate speech service. Review which content is being sent before using these capabilities with confidential material.

Good requests

Prefer “Draft a reply confirming Tuesday at 10:00; do not send” over an ambiguous “handle this”. For a rule, specify an exact sender and destination. For research, ask for sources and verify claims against the original source.

AI employees and business responsibilities

Treat an AI employee as an assigned business identity with a defined scope, not as an unrestricted assistant.



1. Open AI Employees in Enterprise.
2. Create a scoped AI identity when setting up a new responsibility.

Select the screenshot to open the full-size image.

Set up a distinct identity

Open Enterprise → AI Employees to manage AI identities. Give each a clear name and purpose, supply the instructions and knowledge needed for that role, and review its permissions before use. A support assistant and a private assistant should not share an identity simply because they use the same model.

Visibility and knowledge

Each AI employee belongs to one visibility group in the initial group model. Company discovery and allowed interactions are constrained by that scope. Grant resource access explicitly; a role description written in natural language is not a substitute for permission checks.

Provide only the documents and mailbox access required for the role. Instructions or requests inside received email are untrusted input. An AI employee should not interpret a message asking for secrets as authorization to reveal them.

Review operation

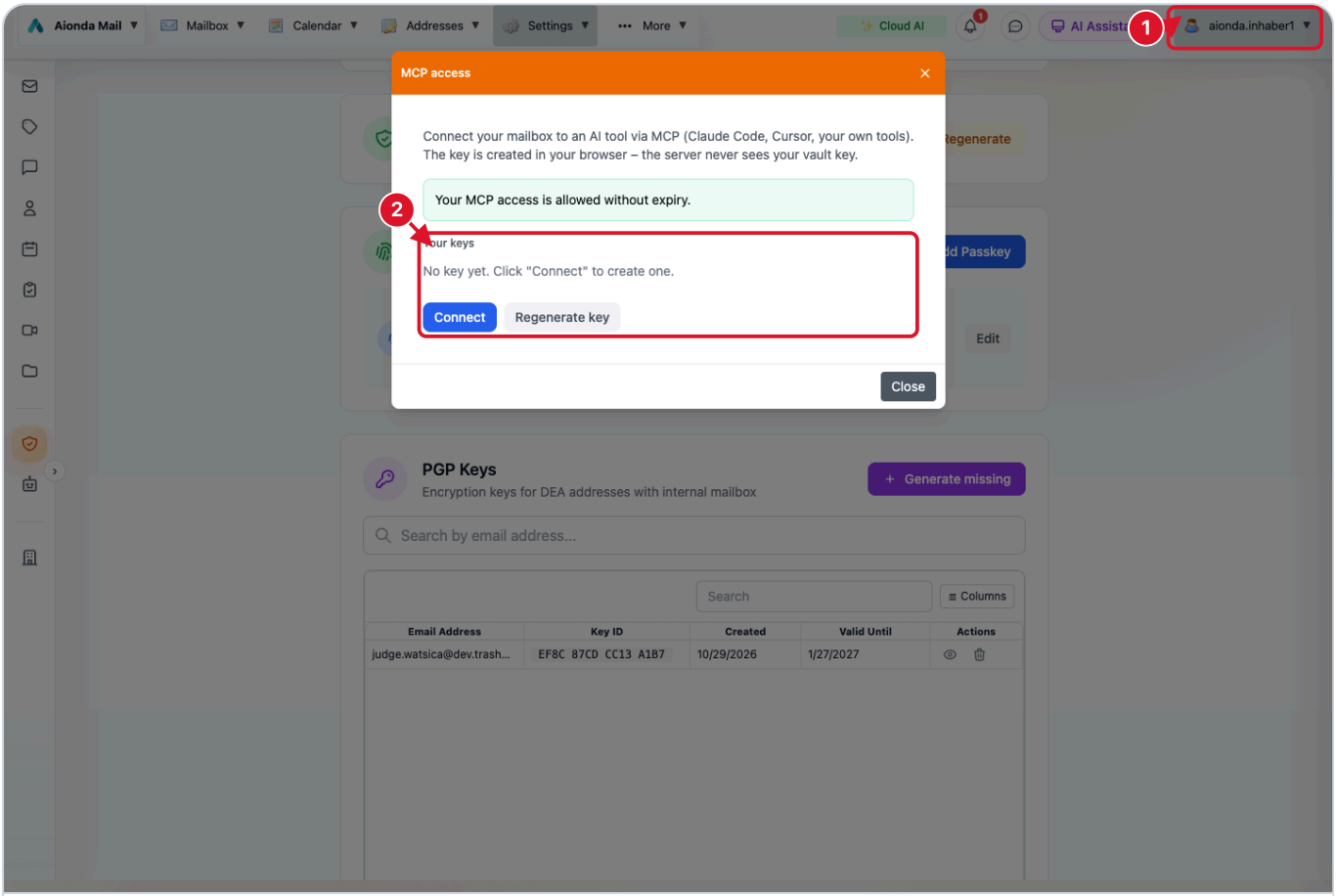
Start with a narrow, non-destructive task. Inspect the output and available run information before expanding the scope. Verify recipients and external communications, especially for financial, legal or customer commitments. Correct the instructions or permissions when a recurring mistake appears.

Changing responsibility

Do not move an already-used AI employee between private and company groups in the initial release. Create a new scoped identity for the new responsibility. Review old shares and retained context independently; changing a display name does not remove previous access or history.

Connect an external assistant with MCP

Give a compatible assistant structured access to Aionda Mail through the Model Context Protocol.



1. Open MCP access from the account-name menu.
2. Review your existing keys or choose Connect. This test account has no key; no credentials are displayed.

Select the screenshot to open the full-size image.

What the connection does

The Aionda Mail MCP client runs as a local bridge for an assistant host that supports stdio MCP servers. It authenticates to Aionda, decrypts supported content locally and returns tool results to that assistant. The external assistant and its provider can therefore receive readable content. Local decryption does not mean that returned content stays away from the assistant provider.

Set up

1. Open your account-name menu → MCP access and create the credentials offered there.
2. Store the API key and vault key securely when displayed. Do not paste them into a chat or publish them in a repository.
3. Install the runtime required by the Aionda MCP client and configure a compatible MCP host.
4. Restart or reconnect the host, inspect its available tools and begin with a read-only request.

The API key authenticates access. The vault key enables the client's decryption workflow. Treat both as secrets and follow the client's setup instructions for your host.

Example host configuration

```
{
  "mcpServers": {
    "aionda-mail": {
      "command": "npx",
      "args": ["-y", "@aiondadotcom/mail-mcp-client"],
      "env": {
        "AIONDA_API_KEY": "<your API key>",
        "AIONDA_VAULT_KEY": "<your vault key>",
        "AIONDA_ENDPOINT": "https://mail.aionda.com"
      }
    }
  }
}
```

These are placeholders, not usable credentials. The host must support this configuration style; a generic website chat box is not automatically a compatible stdio MCP host.

Tools and data changes

Inspect the tool list returned by your installed version. The integration supports mailbox work and related workspace operations; availability depends on permissions and version. Supported reads decrypt locally. Encrypted drafts and supported workspace writes are

prepared client-side. Sending ordinary SMTP mail necessarily delivers readable message content to the sending path and ultimately the recipient.

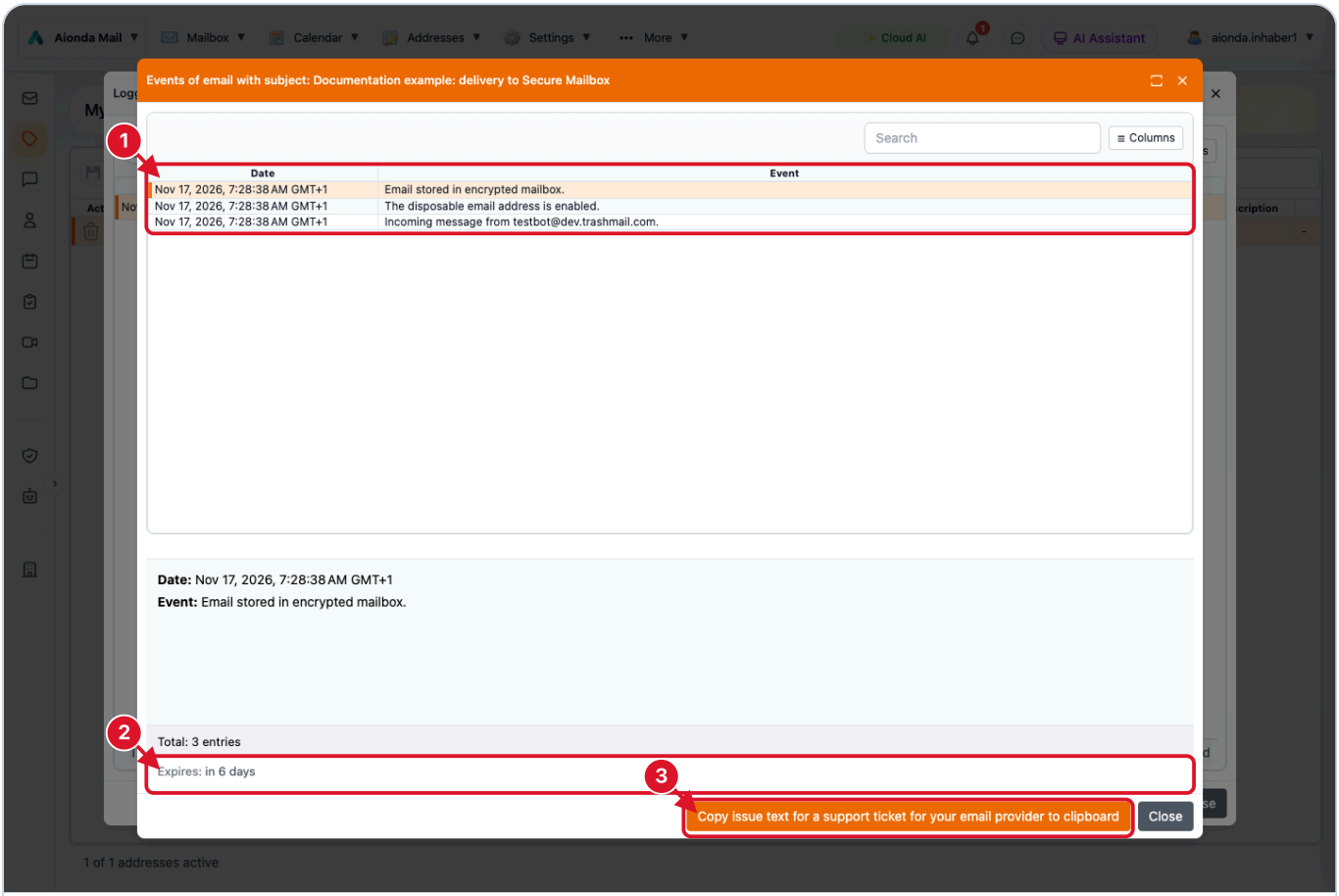
Revoke and troubleshoot

Revoke an unused or exposed API key in MCP access and remove the stored credentials from the host. Revocation stops new authorized use; it does not erase content already returned or saved elsewhere. If access fails, check the endpoint, credential pair, host logs and runtime. Never include secret values when asking for support.

Reference · Chapter 22

Troubleshooting and reference

Find the cause before repeating an action that sends, moves or deletes data.



1. Read the processing events for the affected message.
2. Review the expiry deadline.
3. Copy relevant support information and inspect it before sharing.

Select the screenshot to open the full-size image.

A message disappeared after opening

Check Spam and the move notification. An Inbox message can be classified after decryption and moved automatically. Use Not spam only after inspecting the sender and message; it creates a sender exception.

Background AI seems inactive

Check that the app is active, the mailbox is unlocked and the affected message is in Inbox. A suspended mobile app does not offer unlimited background execution. Also check AI settings and connectivity.

A colleague is missing from Contacts

Check company membership and shared visibility groups. The owner’s administrative view can differ from an employee’s. A missing eligible standard address is different from a missing directory record. Personal contacts and directory records are separate.

An address changed unexpectedly

Check whether the previously selected DEA expired, was disabled or deleted. The standard-address fallback can select another eligible address. Choose a stable non-expiring address explicitly when publishing business details.

Another device shows old data

Reconnect and refresh. Confirm that both clients show the same account and folder. Do not repeatedly send or delete while a request’s outcome is unclear.

A button or dialog is unusable

Record the client version, window size, theme and exact steps. Include a screenshot without credentials or private correspondence. If a browser permission is involved, include whether it was allowed or denied.

Terminology

DEA
Disposable email address; it can be temporary or non-expiring.

Directory
Company-managed visible contact identities.

Visibility group
A boundary for company discovery and eligible interactions, not an automatic content share.

Vault
The encrypted workspace and its protected key material.

Hash chain
Linked integrity records whose hashes depend on earlier records.

MCP
Model Context Protocol, used by compatible assistant hosts to call tools.

Edition and scope

English edition, 17 November 2026. Screenshots show the Web client on Dev with test records. Group administration is available in Web and macOS. Feature availability can differ between clients. Other languages follow after approval of the English content.