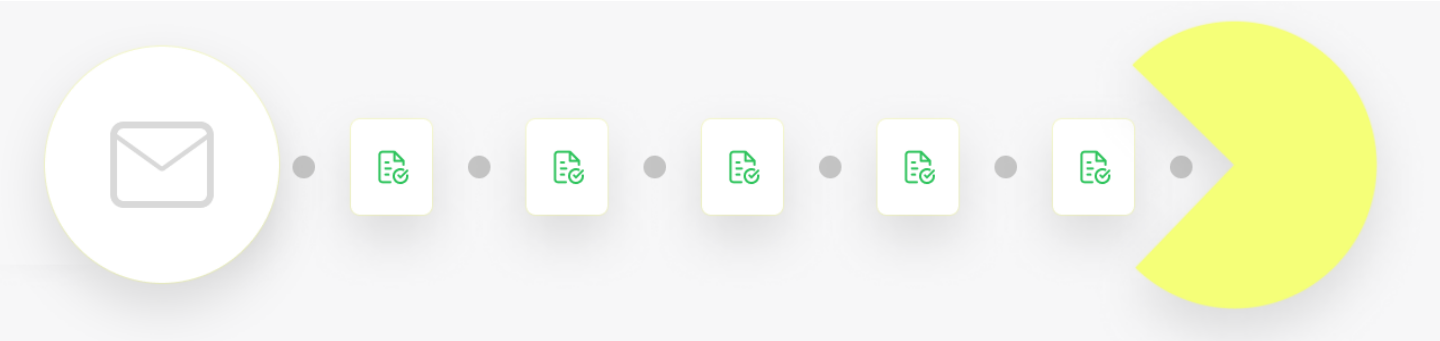


Ramp email integrations: security brief

Ramp's industry-first Gmail and Outlook Integrations collect receipts from your business's email automatically. Companies with the integration enabled collect the majority of receipts without any human touch.

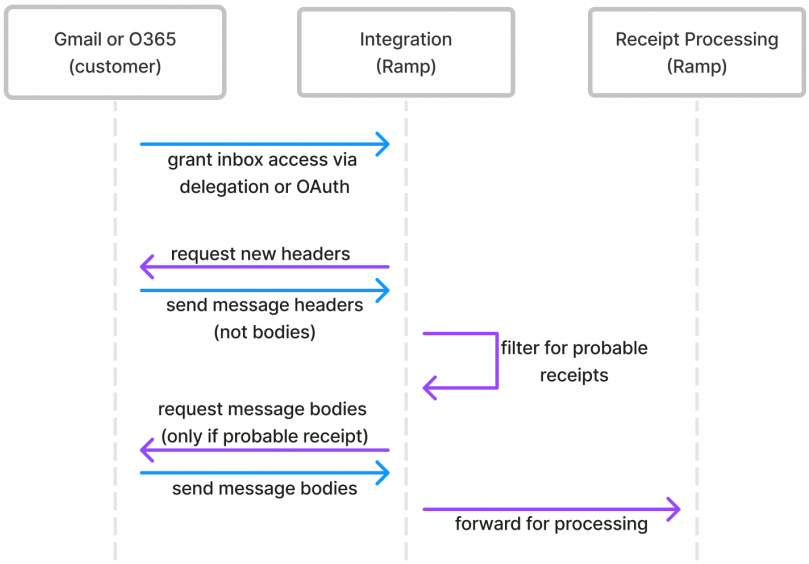
Customer trust is foundational to our business. When you enable these integrations, you trust Ramp with access to your business's emails. Our email integrations were designed with this trust in mind: we implemented a variety of integration-specific measures to further restrict our access and protect your data.

Product Overview: Email Integrations

Our email integrations are entirely automated. There is no human in the loop—at your business or at Ramp—on the receipt matching process.

To achieve this we periodically query your company's inboxes for new email messages. If any exist, we pull the message headers (e.g., who it was sent to, who it was sent from, and the subject line) and run a series of algorithms to determine if the message is likely to contain a receipt. For messages likely to contain a receipt, we pull the message body and attachments, then run a second set of algorithms to match the potential receipt to a specific transaction. We do not access the bodies of messages unlikely to contain a receipt.

Here's an overview of how our integration works



Ramp's Overall Security Posture

Ramp maintains a SOC 2 Type II report which provides validation from an independent third-party auditor that our security program meets industry standards to keep your data protected. This report is updated on an annual basis—you can download the latest version and learn more about our security program at trust.ramp.com.

Threat Model: Email Integrations

Two notable potential attack vectors that we considered in implementing our email integrations are:

- **Compromise of account access:** if Ramp's access to your email accounts is compromised, an attacker could access your emails.
- **Compromise of Ramp's storage and admin systems:** if Ramp itself is compromised, an attacker could access information stored in Ramp's systems, including any retained email contents.

To mitigate these attack vectors, Ramp minimizes the data accessed by our email integrations wherever possible, avoids storing information we don't need, and robustly protects the data and credentials that we do store. The remainder of this document details these mitigations.

Mitigations

Access to your Inboxes

For Gmail

Our Gmail Integration uses a Google API integration called domain-wide delegation. Domain-wide delegation enables a Google Workspace administrator to configure API access to every email message within an organization without requiring each employee to manually enable access themselves.

Once this delegation is enabled, Ramp's Google Cloud Platform (GCP) Gmail Integration project is allowed to make API requests to Gmail on behalf of your business. Access to this project is controlled by Google's IAM system. Our software uses a Google Service Account to access this project and make requests. Credentials for this service account are available to only a small subset of engineers actively supporting our integration.

Ramp interacts with the delegated access by directly using Google's APIs over encrypted connections.

For Outlook

Our Outlook Integration uses Microsoft's Graph API. Microsoft's standard OAuth flow enables an Office 365 administrator to grant Ramp's Outlook Integration application the following permissions:

- `User.Read`, which grants Ramp access to basic profile information for the administrator who performed the OAuth flow. This grant is required by Microsoft's standard OAuth flow, but the administrator's profile data is not collected or stored by Ramp.
- `Mail.Read`, which grants Ramp access to every email message in every mailbox in the tenant, without requiring each employee to manually enable access themselves.

As part of the OAuth flow, the administrator also registers your Azure tenant id with Ramp's email integration system.

Once the OAuth flow is complete, Ramp's email integration system uses an Azure service account along with your pre-registered Azure tenant id to obtain a short-lived access token to your tenant. We encrypt that token using a dedicated key for this data type and store it in our email integration system database. We later use that token to make API requests to Microsoft on behalf of your business. When the token expires, we automatically repeat this flow to obtain a new one.

Microsoft offers a technique to limit the `Mail.Read` permission to specific mailboxes by placing relevant mailboxes in a mail-enabled security group and then limiting Ramp's Outlook Integration application to only that set of mailboxes via an application access policy. Instructions for this setup are in Microsoft's Graph API documentation→. Ramp offers a separate opt-out process, detailed below.

Ramp interacts with Microsoft's Graph API directly over encrypted connections.

Opting-out inboxes

The Ramp email integrations give you control of which inboxes we access.

By default, Ramp queries only those inboxes that have an associated active Ramp account. We never attempt to access inboxes that do not have a corresponding Ramp user.

Additionally, you can opt-out specific email addresses which *do* have an associated Ramp account using Ramp's developer API (docs→) or by sending a request to support@ramp.com. If a user has multiple email aliases, opting out their primary email address will also opt out their aliases. When you opt-out a specific address, our email integration system continues to interact with Google and Microsoft's APIs to list email aliases, but we will never attempt to pull email metadata or bodies for messages in that address's inbox. You can see a list of email addresses that have been opted-out on the integration configuration page (Gmail→, Outlook→).

Minimizing data processed

The Ramp email integrations are designed to minimize the data processed at every point.

Our integration pulls email metadata, specifically the Message-ID and email headers (e.g., who the email was sent to, who it was sent from, and the subject line) for any new mail received by an enabled inbox. We do not pull email bodies at this time. Furthermore, we do not pull metadata for messages where the subject contains the keywords “confidential” or “privileged.”

We process the email metadata to determine the probability that a message contains a receipt. Our algorithms consider a variety of factors like particular subject-line keywords, who the message is from, etc. Because we have not accessed the email bodies at this stage, neither the contents of the email nor its attachments are available to our algorithms.

The vast majority of messages are rejected in this first round of processing and, as a result, we never access their message body or attachments. On average, Ramp accesses the message body and attachments for **less than 2%** of messages processed by the integration.

In the event that an email’s headers passed the keyword filters and the message is deemed likely to contain a receipt, we then reach out to Gmail or Outlook a second time to access the message’s body and attachments. We send the header and body of these messages to Ramp’s receipt-processing software (the same system that handles receipts forwarded by your employees to receipts@ramp.com, submitted via SMS, or uploaded via the Ramp application).

The body and attachments for messages unlikely to contain a receipt or that are rejected by our keyword filters are never requested by our system.

Minimizing data stored

The Ramp email integrations avoid storing unnecessary data and delete data after it is no longer needed.

For each email that we pull, we potentially store three separate pieces of information:

- **Email Message-ID:** We store the email Message-ID for every email processed by the integration. This opaque identifier helps us recognize which emails we’ve already processed and which still need to be processed. This information is not deleted.
- **Email Headers:** During our first processing step we temporarily store email headers (e.g., who the email was sent to, who it was sent from, and the subject line). If the headers indicate that the message is unlikely to contain a receipt, we delete the headers immediately. When a message is deemed likely to contain a receipt and moves to the second processing step, we store the headers for up to 30 days.
- **Email Bodies and Attachments:** Email bodies contain the actual contents of the email (any text, html, or attachments). As noted above, we do not access message bodies for messages

that fail our keyword filters or are unlikely to contain a receipt. When a message is deemed likely to contain a receipt and we access its message body, the body and headers are sent to Ramp's receipt processing software (the same system that handles receipts manually forwarded by your employees to receipts@ramp.com, submitted via SMS, or uploaded via the Ramp application), and may also be stored in our email integration system for up to 30 days.

After 30 days, the only piece of information left in the integration system will be the Message-ID of each email we have processed. Messages which are sent to Ramp's receipt-processing software are retained by that software for a longer period of time (similar to how that system handles receipts manually forwarded by your employees to receipts@ramp.com).

In order to ensure service availability, Ramp regularly snapshots and backs up our databases. Database snapshots and backups are regularly removed after 30 days, though may be retained for up to three years in some cases. They are encrypted at rest.

Protecting stored data

All information pulled by the Ramp email integrations is encrypted at rest in our database and file storage system. The database for the email integrations uses a separate set of encryption keys from other Ramp databases, and sensitive information stored in it (like message subjects and headers, before they are purged) is further encrypted at a row level. Access to this information is not generally available to other systems or to humans through any application (including administration applications internal to Ramp).

Emails that are sent to Ramp's receipt processing software are also encrypted at rest, and are treated the same way as emails manually forwarded by your employees to receipts@ramp.com, submitted via SMS, or uploaded via the Ramp application.

Our platform, including where we process and store data for the email integrations, runs on Amazon Web Services. Following the principle of least privilege, only engineers actively maintaining this integration have access to manage related databases.