

Google Workspace Data Access Terms - Gmail Inbound And Google Drive

Gmail Readonly Restricted-Scope Terms

These terms explain the Gmail inbound access DynamicMail requests when an authorized tenant user or administrator connects Gmail inbound document intake for tenant document workflows.

Google Sign-In identity scopes such as `openid`, `email`, and `profile` are separate from this Gmail data-access consent. Signing in with Google does not mean you have accepted Gmail inbound access.

Requested Scope

DynamicMail requests `https://www.googleapis.com/auth/gmail.readonly` only when an authorized tenant user or administrator connects Gmail inbound document intake. The scope lets DynamicMail view Gmail messages and settings for the connected Google account. DynamicMail uses the scope for read-only inbound processing and does not use it to send, modify, delete, archive, label, or move Gmail messages.

DynamicMail should not request or process Gmail data that is unrelated to the visible inbound document intake feature.

Data DynamicMail May Access

When Gmail inbound is connected, DynamicMail may access the Gmail data needed to find and process inbound business documents, including:

- message IDs, thread IDs, history IDs, label references, and sync cursors;
- sender, recipient, subject, date, headers, and other message metadata;
- message bodies and snippets needed to identify document context;
- attachments and inline files that may contain invoices, notices, agreements, receipts, or other tenant documents;
- Gmail settings only where the Gmail API requires them for the readonly scope or account sync behavior;
- derived data created from Gmail content, such as parsed document fields, OCR text, classification labels, extraction results, summaries, audit events, and document records.

Why DynamicMail Uses Gmail Data

DynamicMail uses Gmail readonly data to provide the Gmail inbound source selected by the tenant. The intended purposes are:

- detecting inbound messages that may contain tenant business documents;
- importing attachments or message content that the tenant chooses to process;
- extracting, classifying, and routing documents into DynamicMail workflows;
- reconciling sync state so the same message is not repeatedly imported;
- showing connection, sync, and processing status to authorized tenant users;
- troubleshooting, security, audit, and legal-compliance activities allowed by the applicable policies and the tenant agreement.

DynamicMail must not sell Gmail data, use it for advertising or retargeting, transfer it to data brokers, use it for surveillance, or use it to determine creditworthiness or lending eligibility.

Retention

DynamicMail retains Gmail-derived data only as needed for the visible inbound document feature, tenant document retention settings, audit records, security, dispute handling, or legal compliance. OAuth tokens and sync metadata are retained only while needed to operate the connected Gmail inbound source or to preserve required audit records.

Raw Gmail message content, attachments, and derived document data should be deleted or anonymized when they are no longer needed for the disclosed purpose, unless a legal, security, audit, or tenant-retention obligation requires continued retention.

Deletion

An authorized tenant user or administrator may request deletion of Google-derived cached data, imported attachments, extracted text, and derived document records. DynamicMail should delete or anonymize the requested data when permitted by the tenant's retention settings and applicable law.

Deleting imported DynamicMail records does not necessarily delete the original email or attachment from Gmail, because the Gmail readonly scope does not grant DynamicMail permission to modify or delete Gmail messages.

Revocation And Disconnect

The tenant can disconnect Gmail inbound in DynamicMail. After disconnect or local consent revocation, DynamicMail must stop using stored OAuth tokens for Gmail inbound and must stop reading additional Gmail messages from the connected account.

The Google account owner can also revoke the app authorization in Google account settings. If Google authorization is revoked, DynamicMail must stop Gmail API access when token refresh or API calls fail, and the connection should be shown as disconnected or requiring reconnection.

Local revocation does not automatically remove already imported DynamicMail documents. Those records are handled through the deletion and retention rules above.

AI, OCR, And Extraction Use

DynamicMail may use OCR, parsing, classification, summarization, and other AI-assisted processing on Gmail-derived message content and attachments only to provide or improve the visible inbound document workflow for the tenant. Gmail data and derived data must not be used to create, train, or improve a general-purpose machine-learning or AI model outside the tenant's requested feature.

AI-assisted results can be wrong. DynamicMail should present extracted data as workflow output that authorized users can review, correct, approve, reject, or delete according to the product flow.

Support And Human Access

DynamicMail personnel, contractors, or subprocessors should not read specific Gmail messages, attachments, extracted text, or derived Gmail data unless one of these conditions applies:

- the user has explicitly asked for support that requires access to specific data;
- access is necessary for security investigation, abuse prevention, or incident response;
- access is necessary to comply with law, legal process, or a binding tenant instruction;
- the data is aggregated or anonymized for internal operations and no specific user's Gmail content is readable.

Support access should be least-privilege, time-limited where practical, and logged for auditability.

References

- DynamicMail restricted-scope contract:
Documentation/DynamicMail/LocalizedIntegrations/google-restricted-scope-compliance-contract-2026-06-02.md
- Google API Services User Data Policy: <https://developers.google.com/terms/api-services-user-data-policy>
- Google Workspace API user data and developer policy:
<https://developers.google.com/workspace/workspace-api-user-data-developer-policy>
- Gmail API scopes: <https://developers.google.com/workspace/gmail/api/auth/scopes>
- Google restricted-scope verification guidance:
<https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification>

Google Drive Restricted-Scope Terms

These terms explain the Google Drive access DynamicMail requests when an authorized tenant user or administrator connects Google Drive for tenant document workflows.

Google Sign-In identity scopes such as `openid`, `email`, and `profile` are separate from this Google Drive data-access consent. Signing in with Google does not mean you have accepted Google Drive access.

Requested Scope

DynamicMail requests <https://www.googleapis.com/auth/drive> only when an authorized tenant user or administrator connects Google Drive for tenant document workflows. This is a broad restricted Drive scope that can permit DynamicMail to view and manage all files in the connected Google Drive account, including files the user owns, files shared with the user, folders, and shared-drive content available to that account.

DynamicMail must use the Drive scope only for disclosed, visible Drive document workflows selected by the tenant. DynamicMail should not request, browse, copy, download, modify, delete, or otherwise process Drive data that is unrelated to the visible Drive document workflow.

Data DynamicMail May Access

When Google Drive is connected, DynamicMail may access the Drive data needed to provide the selected tenant workflow, including:

- file IDs, names, MIME types, checksums, size, timestamps, descriptions, labels, folder references, parent folders, and other file metadata;
- folder metadata, shared-drive metadata, and search/listing results needed to locate tenant documents;
- file content, previews, thumbnails, exports, downloads, uploads, and generated or edited file payloads;
- sharing and permission metadata when needed to show or complete a visible Drive file operation;
- account-level Drive summary information needed to confirm the connected account and connection status;
- stored copies or cached extracts of Drive files imported into DynamicMail;
- derived data created from Drive files, such as OCR text, parsed document fields, classification labels, extraction results, summaries, audit events, and document records.

Why DynamicMail Uses Google Drive Data

DynamicMail uses Google Drive data to provide tenant-selected Drive document workflows. The intended purposes are:

- letting authorized users connect Drive as a document source or destination;
- finding, listing, importing, downloading, exporting, uploading, or updating tenant business documents selected through the product flow;
- extracting, classifying, and routing Drive documents into DynamicMail workflows;
- showing connection, file-operation, sync, and processing status to authorized tenant users;
- maintaining audit records and operational logs that prove what Drive operation was requested and completed;
- troubleshooting, security, abuse prevention, dispute handling, and legal-compliance activities allowed by the applicable policies and the tenant agreement.

DynamicMail must not sell Google Drive data, use it for advertising or retargeting, transfer it to data brokers, use it for surveillance, or use it to determine creditworthiness or lending eligibility.

Broad-Scope And Narrowest-Scope Note

The <https://www.googleapis.com/auth/drive> scope is broad because it can permit access to all Drive files available to the connected account. DynamicMail uses this scope for the implemented Data Rooms workflow where authorized tenant users sync selected existing Google Drive folders and files, import or download Drive content, upload or update room files back to Drive, and apply user-requested sharing or permission changes on existing Drive files.

More limited Drive scopes are insufficient for the current workflow: `drive.file` would only cover files created or opened by DynamicMail and would not cover selected existing folders or all-files import; `drive.readonly` would not cover upload, update, sharing, or permission changes; metadata-only scopes such as `drive.metadata.readonly`, `appdata`, or `appfolder` scopes cannot download or process tenant document content or manage the selected existing files. If the product is redesigned around Google Picker and app-created or app-opened files only, DynamicMail should downscope before release of that redesigned workflow.

Retention

DynamicMail retains Drive-derived data only as needed for the visible Drive workflow, tenant document retention settings, audit records, security, dispute handling, or legal compliance. OAuth tokens and Drive operation metadata are retained only while needed to operate the connected Drive integration or preserve required audit records.

Drive file content, cached files, metadata, OCR text, extracted fields, and derived document data should be deleted or anonymized when they are no longer needed for the disclosed purpose, unless a legal, security, audit, or tenant-retention obligation requires continued retention.

Deletion

An authorized tenant user or administrator may request deletion of Google-derived cached data, imported Drive files, extracted text, and derived document records. DynamicMail should delete or anonymize the requested data when permitted by the tenant's retention settings and applicable law.

Deleting imported DynamicMail records does not necessarily delete the original file from Google Drive. DynamicMail should modify, move, trash, or delete original Drive files only when an authorized user explicitly requests that Drive action through a visible product workflow and the action is allowed by tenant policy and applicable law.

Revocation And Disconnect

The tenant can disconnect Google Drive in DynamicMail. After disconnect or local consent revocation, DynamicMail must stop using stored OAuth tokens for Google Drive and must stop reading, writing, downloading, uploading, modifying, or deleting additional Drive files from the connected account.

The Google account owner can also revoke the app authorization in Google account settings. If Google authorization is revoked, DynamicMail must stop Drive API access when token refresh or API calls fail, and the connection should be shown as disconnected or requiring reconnection.

Local revocation does not automatically remove already imported DynamicMail documents. Those records are handled through the deletion and retention rules above.

AI, OCR, And Extraction Use

DynamicMail may use OCR, parsing, classification, summarization, and other AI-assisted processing on Drive file content and metadata only to provide or improve the visible tenant Drive document workflow. Drive data and derived data must not be used to create, train, or improve a general-purpose machine-learning or AI model outside the tenant's requested feature.

AI-assisted results can be wrong. DynamicMail should present extracted data as workflow output that authorized users can review, correct, approve, reject, or delete according to the product flow.

Support And Human Access

DynamicMail personnel, contractors, or subprocessors should not read specific Drive files, extracted text, file metadata, or derived Drive data unless one of these conditions applies:

- the user has explicitly asked for support that requires access to specific data;
- access is necessary for security investigation, abuse prevention, or incident response;
- access is necessary to comply with law, legal process, or a binding tenant instruction;

- the data is aggregated or anonymized for internal operations and no specific user's Drive content is readable.

Support access should be least-privilege, time-limited where practical, and logged for auditability.

References

- DynamicMail restricted-scope contract:
Documentation/DynamicMail/LocalizedIntegrations/google-restricted-scope-compliance-contract-2026-06-02.md
- Google API Services User Data Policy: <https://developers.google.com/terms/api-services-user-data-policy>
- Google Workspace API user data and developer policy:
<https://developers.google.com/workspace/workspace-api-user-data-developer-policy>
- Google Drive API scopes:
<https://developers.google.com/workspace/drive/api/guides/api-specific-auth>
- Google restricted-scope verification guidance:
<https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification>