About DLP

Archived: 2026-04-05 17:24:40 UTC

Supported editions for this feature: Frontline Standard and Frontline Plus; Enterprise Standard and Enterprise Plus; Education Fundamentals, Education Standard, and Education Plus; Enterprise Essentials Plus. Compare your edition

Drive DLP and Chat DLP are also available to Cloud Identity Premium users who also have a Google Workspace license (Enterprise, Business, or Education editions).

DLP rules

Using data loss prevention (DLP), you can create and apply rules to control the content that users can share in files outside the organization. DLP gives you control over what users can share, and prevents unintended exposure of sensitive information such as credit card numbers or identity numbers. 

DLP rules trigger scans of files for sensitive content, and prevents users from sharing that content. Rules determine the nature of DLP incidents, and incidents trigger actions, such as the blocking of specified content.

You can allow controlled sharing for members of a domain, organizational unit, or group.

Summary of DLP flow:

- You define DLP rules. These rules define which content is sensitive and should be protected. DLP rules apply to both My Drive and Shared drives.
- DLP scans content for DLP rule violations that trigger DLP incidents.
- DLP enforces the rules you defined and violations trigger actions, such as alerts.
- You are alerted to DLP rule violations.

For details on:

- Drive DLP, go to Create DLP for Drive rules and custom content detectors.
- Chat DLP, go to Prevent data leaks from Chat messages and attachments.

Use an audit-only rule to test new DLP rules

You can test DLP rules by creating rules that don't have an optional action, such as blocking or warning users. If these rules are triggered, data related to the incident is written to the Rule log events. For details, go to **Step 1: Plan your rules** at Create DLP for Drive rules and custom content detectors.

DLP sample use cases

You can use DLP to:

- Audit the usage of sensitive content in Drive that your users may have already shared to gather information on sensitive files uploaded by users.
- Directly warn end users not to share sensitive content outside of the domain.
- Prevent sharing of sensitive data (such as a Social Security Number) with external users
- Alert administrators or others about policy violations or DLP incidents.
- Investigate details of an incident with information on the policy violation.

DLP features

The following table describes the DLP features:

DLP Features	Details
Author DLP rules with scope, condition, and actions	Scope • Author policies based on organizational units or groups • Organizational unit and group inclusion and exclusion - define policy based on organizational units in the environment. The rule scans files owned by users in the selected organizations or groups. See also DLP for Drive FAQ. Conditions • Contents of scanned files or content • Rule templates • Reusable content detectors • Keyword and word Lists • Regular expressions (Regex) • Predefined detectors to allow inspection on numerous content types. Go to How to use predefined content detectors for details. • Nested conditions. Go to DLP for Drive rule nested condition operator examples for details. • Set detection confidence threshold levels • Extended match count Actions • Set alert and notification rules • Block externally shared links • Warn end users • Audit Drive file content violations

DLP Features	Details
Incident Management	• Sends an alert summary to DLP administrators to enable quick detection of DLP incidents validation of false positives. Go to View alert details for details. • You receive a DLP alert in the alert center when a DLP rule is triggered. From the Admin console Home page, go to **Security** and then **Alert center**. Go to View alert details for details. • Reporting and investigation dashboard for policy violations (DLP incidents and Top Policy Incidents). Go to About the security dashboard for details.
Rule investigation	• For rule investigation, use the security investigation tool. Go to About the security investigation tool for details. • You must have the privilege **Security Center** and then **Investigation Tool** and then **Rule** and then **View Metadata and Attributes** to access the investigation tool. • Use the Investigation tool to identify, triage, and take action on security and privacy issues in your domain.
Admin privileges	• View DLP Rules—Allows delegated administrators to view DLP rules • Manage DLP Rules—Allows delegated administrators to create, edit and investigate DLP rules. Note that you must enable both *View* and *Manage permissions* to have complete access for creating and editing rules. For the investigation tool only: **Security Center and then Investigation Tool and then Rule and then View Metadata and Attributes**.

Applications and file types scanned by DLP

Scanned applications

Applications scanned include:

- Google Sheets
- Google Docs
- Google Slides
- Google Forms—The following content is scanned:
    - Files submitted in response to file upload questions. Responders might be warned or blocked from submitting their responses if they attempt to upload sensitive content.

    - Form content (questions and options).
- Google Vids

Content that isn't scanned by DLP:

- Comments in Docs, Sheets, Slides, and Google Drawings
- Comment email notifications
- Sites content
- Forms responses (other than file uploads)

Scanned file types

File types scanned for content include:

- Document file types: .doc, .docx, .html, .pdf, .ppt, .pptx, .txt, .wpd, .xls, .xlsx, .xml
- Image file types: .bmp, .eps, .fif, .gif, .img_for_ocr, .jpeg, .png, .ps, .tif
- Compressed file types: .bzip, .gzip, .rar, .tar, .zip
- Custom file types: .hwp, .kml, .kmz, .sdc, .sdd, .sdw, .sxc, .sxi, .sxw, .ttf, .wml, .xps

Video and audio file types are not scanned.

Note: The actual scanned files can differ by application. For example, for the file types that DLP for Drive supports, go to What content is scanned in each Drive file?

Administrator requirements

To create and set DLP rules and content detectors, you must be a super administrator or a delegated admin with these privileges:

Learn more about administrator privileges and creating custom administrator roles.

- Create DLP for Drive rules and custom content detectors
- DLP for Drive rule nested condition operator examples
- View DLP for Drive dashboard incidents, alerts, and audit events
- View DLP content and rule size limits
- DLP for Drive FAQ
- Rule log events
- How to use predefined content detectors
