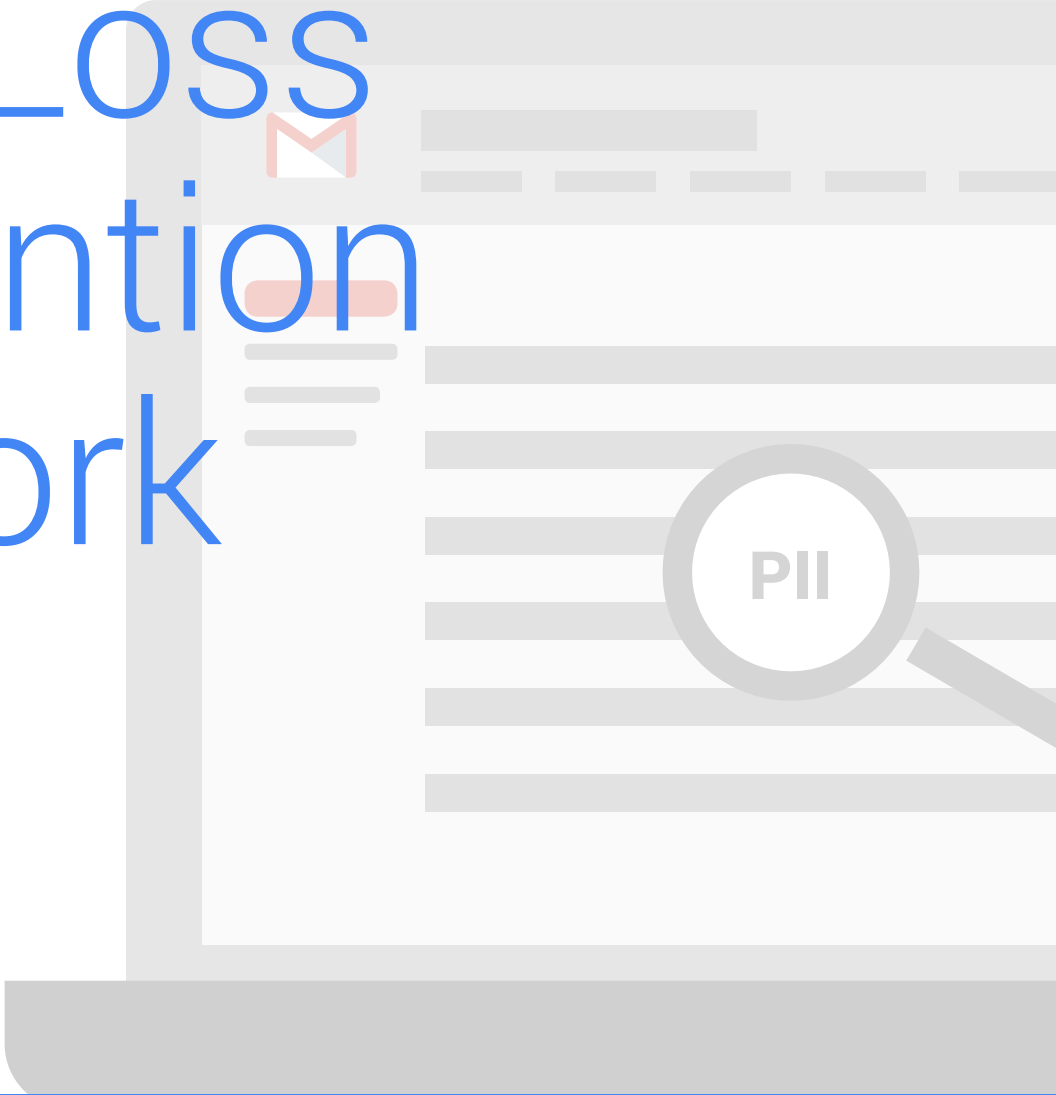


INTRODUCING

Google Data Loss Prevention for work



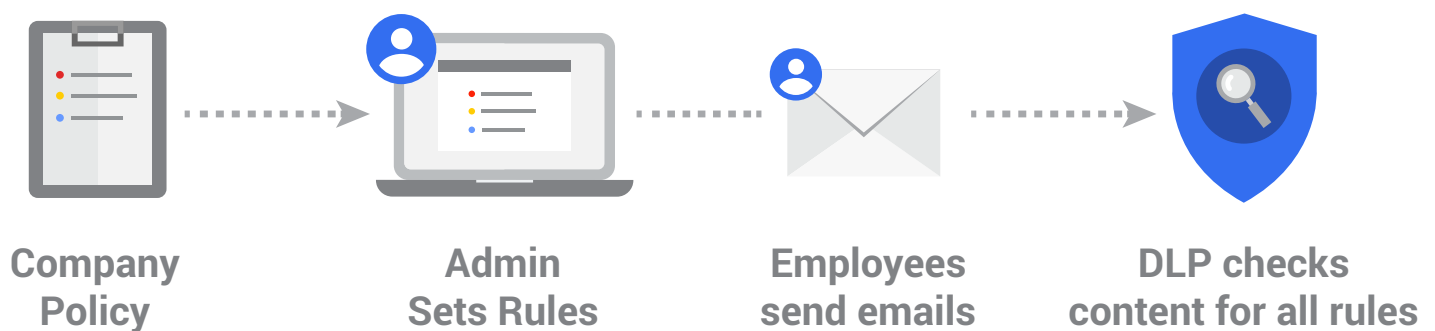
Data loss prevention made easy

We all care about keeping our data safe and private. Google DLP keeps sensitive data from slipping out of your organization.

Google Apps for Work helps admins manage security needs across all information with features like encryption, audit reports, sharing controls, mobile management, and two-factor authentication. Data Loss Prevention (DLP) adds another layer of protection to prevent sensitive or private information from leaking outside of an organization. Gmail DLP is a tool that enables rules to prevent people from either accidentally or maliciously sending confidential data and is the first step in a long term investment to bring rule based security across Google Apps. We're working on bringing DLP to Google Drive in 2016, along with other rule based security systems.

Why is Gmail DLP important?

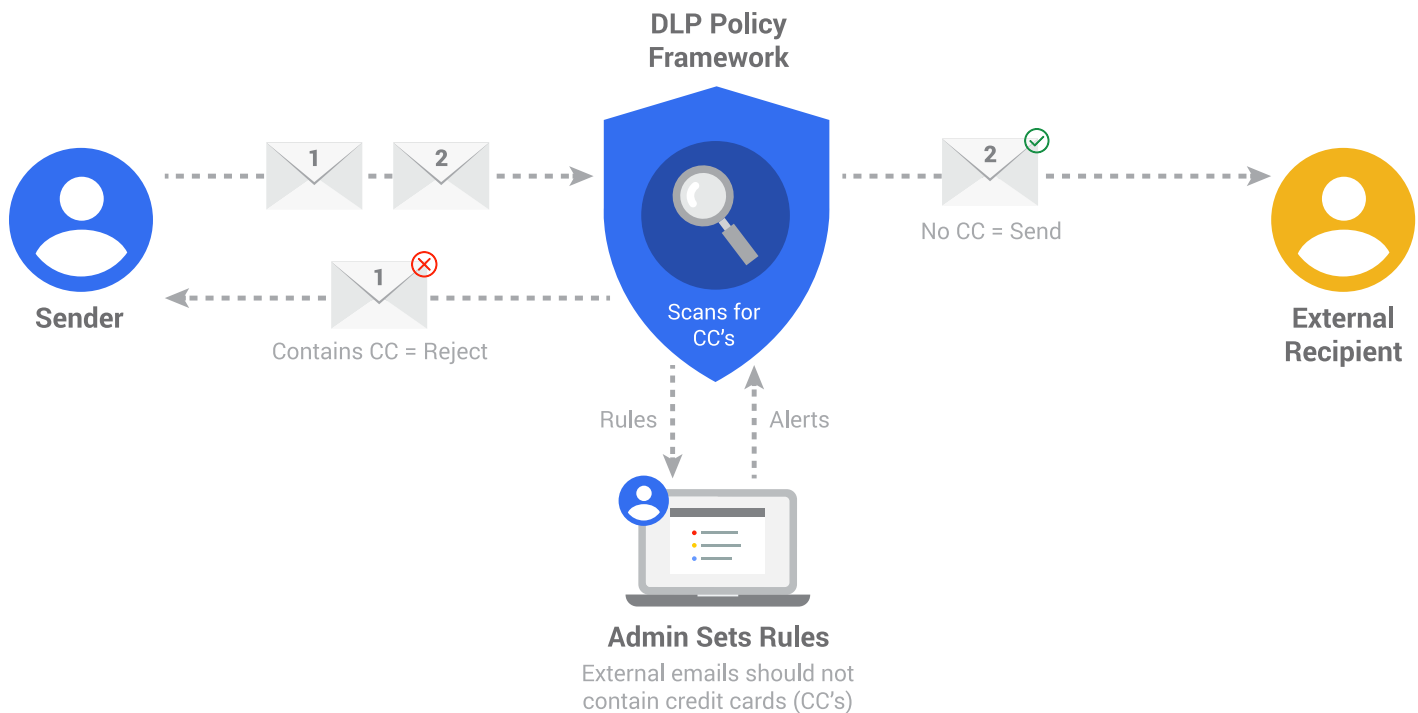
Email is the main way people communicate at work. In fact, In 2015 over 200 billion emails were sent and received each day worldwide.¹ And organizations are custodians of a lot of sensitive data, which includes both proprietary (e.g intellectual property) and third-party data (e.g. customer personally identifiable information (PII)). The cost of data leaks can be large, in the form of intellectual property loss and costly litigation. Interestingly, a large percentage of data leaks happen accidentally – someone replies all when meaning to send a private message, chooses a client instead of teammate who has a similar name, or doesn't realize how confidential certain data is. When these mistakes happen, Gmail DLP helps Google Apps customers prevent losing data.



¹ "Email Statistics Report, 2015-2019" published by The Radicati Group

How Gmail DLP works

Organizations may have a policy that the Sales department should not share customer credit cards externally. And to keep information safe, admins can easily set up a DLP policy by selecting “Credit Card Numbers” from a library of predefined content detectors. Gmail DLP will automatically check all outgoing emails from the sales department and take action based on what the admin has specified: either quarantine the email for review, tell users to modify the information, or block the email from being sent and notify the sender.



Attachment scanning

These scans don't just apply to message subject and copy, but also to content inside common attachment types—such as documents, presentations, and spreadsheets. Gmail DLP identifies each file type through a binary scan to provide more accurate data than relying on the supplied file extension, which can be inaccurate. Text is then extracted from the attachment using an algorithm specific to the file type, and processed via the DLP algorithm.

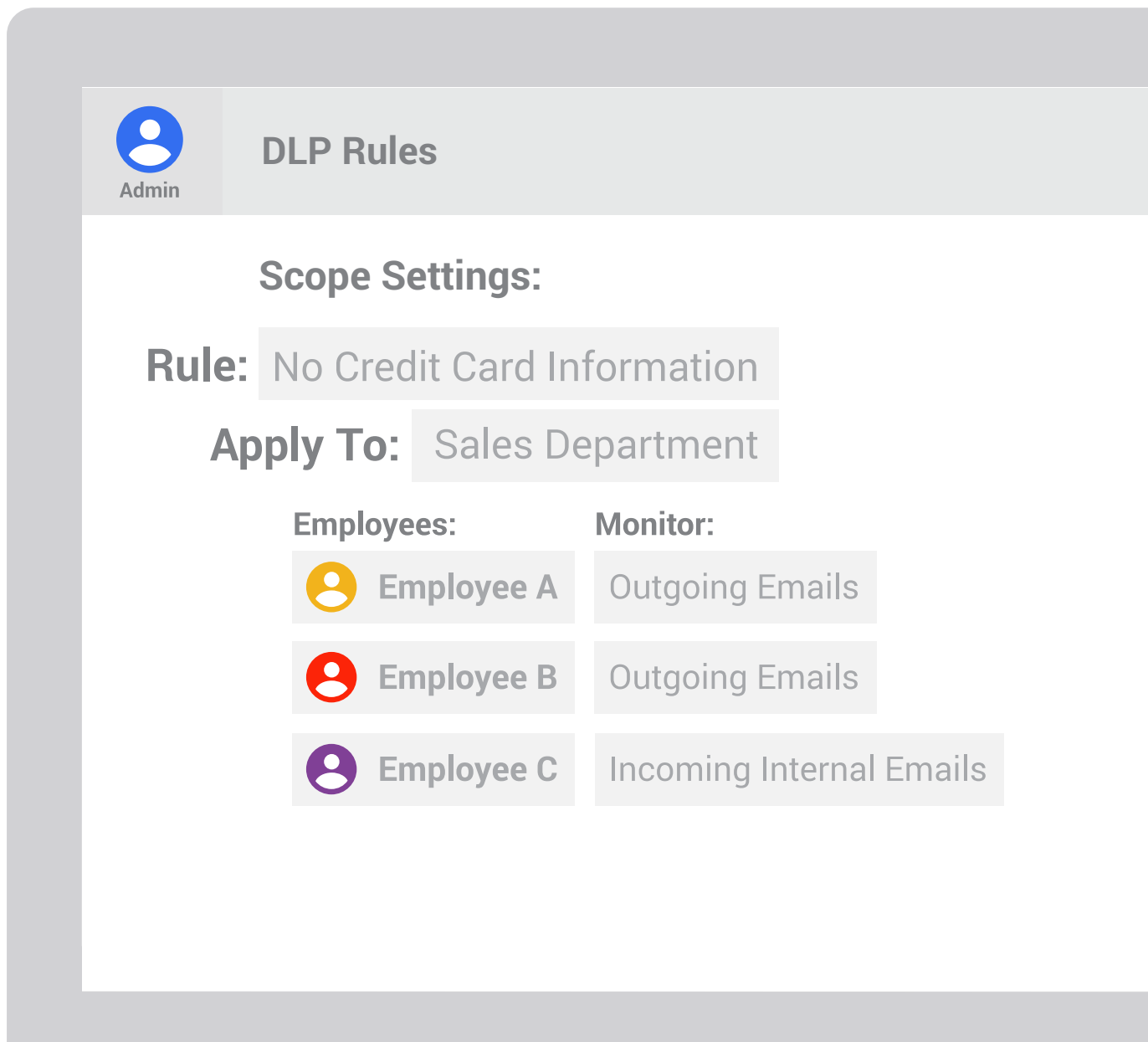
How to set up a DLP rule

1. Set the scope
2. Specify conditions to check for
3. Specify the appropriate action




Set the scope

Scope determines which set of users in your organization the rule applies to.

- Apply the rule to every message and employee
- Apply based on department or organizational unit
- Apply to only outgoing messages
- Apply to recipients to check incoming mail as well



The screenshot shows a user interface for configuring DLP rules. At the top left, there is a blue circular icon with a white person silhouette, labeled "Admin". To its right, the text "DLP Rules" is displayed. Below this, the section "Scope Settings:" is shown. Under "Scope Settings:", the "Rule:" is set to "No Credit Card Information" and "Apply To:" is set to "Sales Department". Below these settings, there are two columns: "Employees:" and "Monitor:". Under "Employees:", three entries are listed: "Employee A" with a yellow person icon, "Employee B" with a red person icon, and "Employee C" with a purple person icon. Under "Monitor:", three entries are listed: "Outgoing Emails" (corresponding to Employee A and B), and "Incoming Internal Emails" (corresponding to Employee C).

Employees:	Monitor:
 Employee A	Outgoing Emails
 Employee B	Outgoing Emails
 Employee C	Incoming Internal Emails

Specify conditions to check for

Specify what the rule should check for using a combination of predefined and custom detectors.

Custom content detectors

Custom detectors (e.g. confidential project keywords) can be used to cover additional use-cases. And can be combined with predefined content detectors.

Predefined content detectors

Admins can choose from a library of predefined content detectors to easily setup DLP rules without having to specify their own regular expressions (regexes) or keywords. These detectors have intelligent logic that goes beyond simple keyword or regex matching. This helps reduce false positives or negatives.



We'll continue to add additional detectors to cover other countries and verticals over time.

Specify the appropriate action

For messages that trigger the rule, admins can specify the appropriate action to take.

Modify messages

Admins can add modifications to a message that are still OK to send. So if, for instance, employees send confidential information to each other that should not be sent externally, admins can choose to automatically append [INTERNAL ONLY] to the message subject to prevent the email from being forwarded outside the organization.

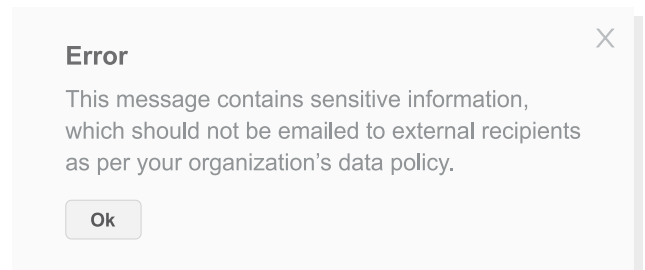
Quarantine messages

When messages are quarantined, a chosen moderator, such as a member of the policy team, can review the email before it is either delivered or held back. Inbound message can also be quarantined for review. The intended recipient has no indication of the message until the administrator releases it for delivery. Admins can allow or reject the message, or do nothing and the message will expire in 30 days.



Reject messages

Automatically reject the message if you know this information should never be sent, no exceptions. And to educate the sender, admins can craft/customizable a notice and link relevant policy documents or online resources to send when a message is rejected to avoid future mistakes.



Tips

- ★ Test your DLP rules before applying to live traffic to make sure they cover the desired use case
- ★ When introducing a new rule, start by quarantining any matches (vs automatically rejecting) to review false positives
- ★ Set policies for specific groups and organizational units, for easy targeting

FAQ

What if I am interested in a preset identifier which is not currently available?

We are working to broaden our identifier portfolio over time to include additional countries and target industries. Please file a support case if you have a request for specific identifiers, or suggestions for improving current identifiers.

DLP for Gmail is great, but Google Apps is a platform, what about other services?

We understand that customers want to protect data, not individual services. We are working to expand our DLP offering to Drive and other services.

What does Google's DLP service cost to use?

DLP is included at no additional charge with Google Apps for Work Unlimited, which costs \$10/user/month and includes unlimited storage, advanced audit and reporting capabilities and Google Apps Vault for eDiscovery and retention.

How can I learn more about Google Apps security and compliance?

The Google for [Work Security and Compliance Whitepaper](#) describes how Google protects your data, meets regulatory and compliance needs, and empowers users and administrators.

Who owns the data I put into Google Apps?

To put it simply, the data that companies, schools and governments agencies put into our systems is theirs, whether it's corporate intellectual property, personal information or a homework assignment, Google does not own that data.

Google for Work

Learn More

Already a Google Apps for Work customer?

Gmail DLP is included with Google Apps Unlimited, so get started

[Get Started](#)

If you are not already a Google Apps for Work customer, you can start a [free 30-day trial](#).