What's New

G Suite

Featured launch: Defend high-risk users with the Advanced Protection Program for enterprise beta

Work together

Making Google Voice easier to use on your computer

Simple to use

More controls and customizations for headers and footers in Google Docs
Import questions from previously existing forms into a new Google form
Remove or select a custom color for chart borders in Google Sheets
Improving active account awareness when opening files with multiple sign-ins
Dark mode now available for Google Keep on web
A revamped home for all your G Suite apps

Business ready

Request and review formal document approvals with a new beta
Anomaly detection in the G Suite alert center now in beta
Titan Security Keys: now available in Japan, Canada, France, and the UK
Limiting access to less secure apps to protect G Suite accounts
Use groups to control more G Suite apps and settings
Whitelist and manage domains more easily in the Admin console
Coming Soon: Transformation reports from Google for Education

Learn more about G Suite

Cloud Connect: The community for G Suite administrators
G Suite on Social
G Suite Learning Center

To help you better track the full breadth of G Suite launches, including those that aren't announced on the G Suite Updates blog, check out the What's new in G Suite page in the Help Center.

We'd really appreciate your thoughts on how we can make this resource work best for you.

- The G Suite Team, August 1, 2019

Featured launch: Defend high-risk users with the Advanced Protection Program for enterprise beta

What's changing

Today, we're announcing the beta of Google's Advanced Protection Program for G Suite customers. With Advanced Protection Program for enterprise, you'll be able to enforce a set of enhanced security policies for employees in your organization that are most at risk for targeted attacks. These policies include:

- Requiring the use of security keys for maximum protection against phishing.
- Automatically blocking access to non-whitelisted third-party apps.
- Enhanced email scanning for threats.
- Download protections for certain file types when signed into Google Chrome.

Advanced Protection for enterprise will be rolling out in beta over the next several days. See below for more details on how to get started.

Who's impacted

Admins and end users

Why you'd use it

While the individual policies currently included in the Advanced Protection Program are available to G Suite users outside of this beta, the Advanced Protection Program beta offers a simple bundle of our strongest account security settings for your organization's high-risk users.

Some users who would benefit from the protections of Advanced Protection are:
- IT admins,
- Executives,
- Employees in regulated or high-risk verticals such as finance or government.

How to get started

- **Admins:** Turn the beta on by going to *Admin console > Security > Advanced Protection Program* and select "Enrollment is enabled" for one or more organizational units (OUs).

- **End users:** Once the program is enabled in your domain, users in those OUs specified by their admin can enroll in the Advanced Protection Program by going to g.co/advancedprotection.
  - Note that users will need two security keys to complete enrollment.

Additional details

Once the beta is enabled for their domain, users will be able to opt in at g.co/advancedprotection. We'll automatically enforce a specific set of policies for the users you identify as most at risk:

- **Requiring the use of security keys.** Physical security keys, such as our Titan Security Keys, go further than traditional 2-Step Verification to help secure accounts against phishing and account takeovers.

- **Automatically blocking access to high-risk third-party apps.** When a user signs up for new apps or services, they're sometimes asked to give access to high-risk data in their G Suite account. Advanced Protection allows only Google apps and select third-party apps, including those whitelisted by G Suite admins, to access high-risk user data.
  - Note: Third party apps that do not require high-risk scopes to function will not be automatically blocked by Advanced Protection. However, they can be blocked through a separate admin policy.

- **Enhanced email scanning.** Incoming email will have all available screening for phishing attempts, viruses, and attachments with malicious content.

- **Stricter account recovery:** Users who lose both of their security keys will need admin help to regain access to their accounts on new devices. This prevents automated recovery flows from becoming an attack vector.

- **Download protections in Google Chrome.** We're adding a new feature in Google Chrome that will reduce a user's exposure to potentially risky downloads. When signed into Chrome, users will receive a warning that indicates that Safe Browsing could not verify whether a file is safe. This will signal to users to proceed with caution and check the reputation of the source of the file to further validate the legitimacy of the file.

Find out more about the policies enforced in the Advanced Protection Program at g.co/advancedprotection.

G Suite

Work together

Making Google Voice easier to use on your computer

What's changing
We're making some improvements to the Google Voice web app. These will make it easier to find the right contact, quicker to place calls, and simpler to control audio settings. Specific improvements include:

- Always-visible call panel
- One-click calling
- Quick access to mic and audio settings

See more information below.

Who's impacted
End users

Why you'd use it
It's important for a telephony system to be quick and intuitive to use. These improvements will make it simpler to use Google Voice, so users spend less time navigating the product interface and more time communicating through it.

How to get started
- **Admins:** No action needed.
- **End users**: See our Help Center to learn more about how to make calls or change the audio settings for Google Voice on the web.

Additional details

Always visible call panel
The new call panel will be in the same place regardless of what you're doing in the Google Voice app—checking messages, listening to voicemails, or something else. This will make it quicker and easier to place calls when you need to.

One-click calling
A new quick call option will appear when users hover over a contact in their call list. This will allow users to make calls faster.

Quick access to mic and audio settings
A new icon in the main action bar will give instant access to common audio settings. These include what microphone and audio output to use before or during a call, as well as what device should ring for incoming calls.

Simple to use

More controls and customizations for headers and footers in Google Docs

	Announced on July 23, 2019	🔗 Share with your organization	- back to top -

What's changing
We're giving you more options to control and customize headers and footers in Google Docs.

Previously, you could set a single header or single footer for your entire document, with an option to make it different on the first page only. Now you can also define a specific header or footer for each section of your document, or use different headers and footers on odd and even page numbers.

Set a different header or footer on odd and even page numbers.

To use different headers or footers per page, see this article in the Help Center.

Import questions from previously existing forms into a new Google form

	Announced on July 1, 2019	🔗 Share with your organization	- back to top -

What's changing
We're adding the ability to import questions from your existing Google Forms and forms shared with you into a new form.

Who's impacted
End users

Why you'd use it
You've told us that the ability to import relevant questions from other forms into a new form is important. For example, educators frequently reuse questions from existing forms or forms shared with them for collaboration by others, to create quizzes. Or you could use this feature to quickly create forms that are distributed on a monthly or quarterly basis, like surveying your employees about workplace amenities.

Previously, it was only possible to do this manually, a process that often took a great deal of time.

How to get started

- **Admins:** No action required.
- **End users:**
  - First, open a form and from the action toolbar on the right, select *Import Questions*.
  - Then, from the dialogue box, select the form with the questions you want to import.
  - From the right hand sidebar menu, you can:
    - Import all questions by choosing *Select All > Import Questions*
    - Or, you can select specific questions to import and then select *Import Questions*.
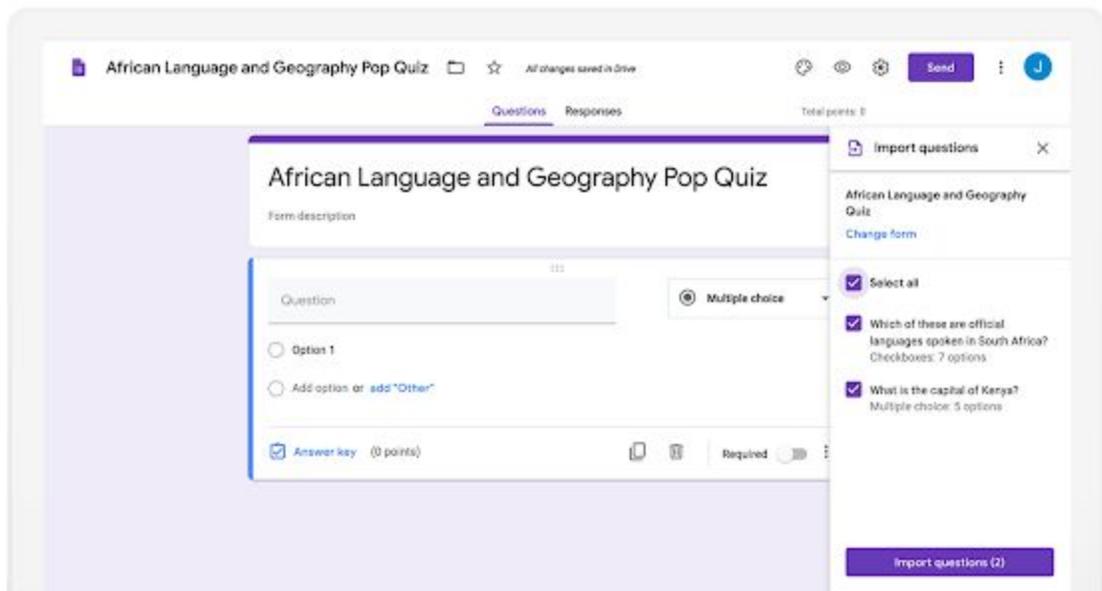
Remove or select a custom color for chart borders in Google Sheets

Announced on July 8, 2019   Share with your organization   - back to top -

Quick launch summary
You now have more options for customizing chart borders in Google Sheets. Currently, the default border for a chart is dark gray — now, you can change the border to a custom color or remove the border:

- Double click on any chart to open the Chart editor and select the Customize tab.
- Under Chart style, you can select a border color or select "None" to remove the border.
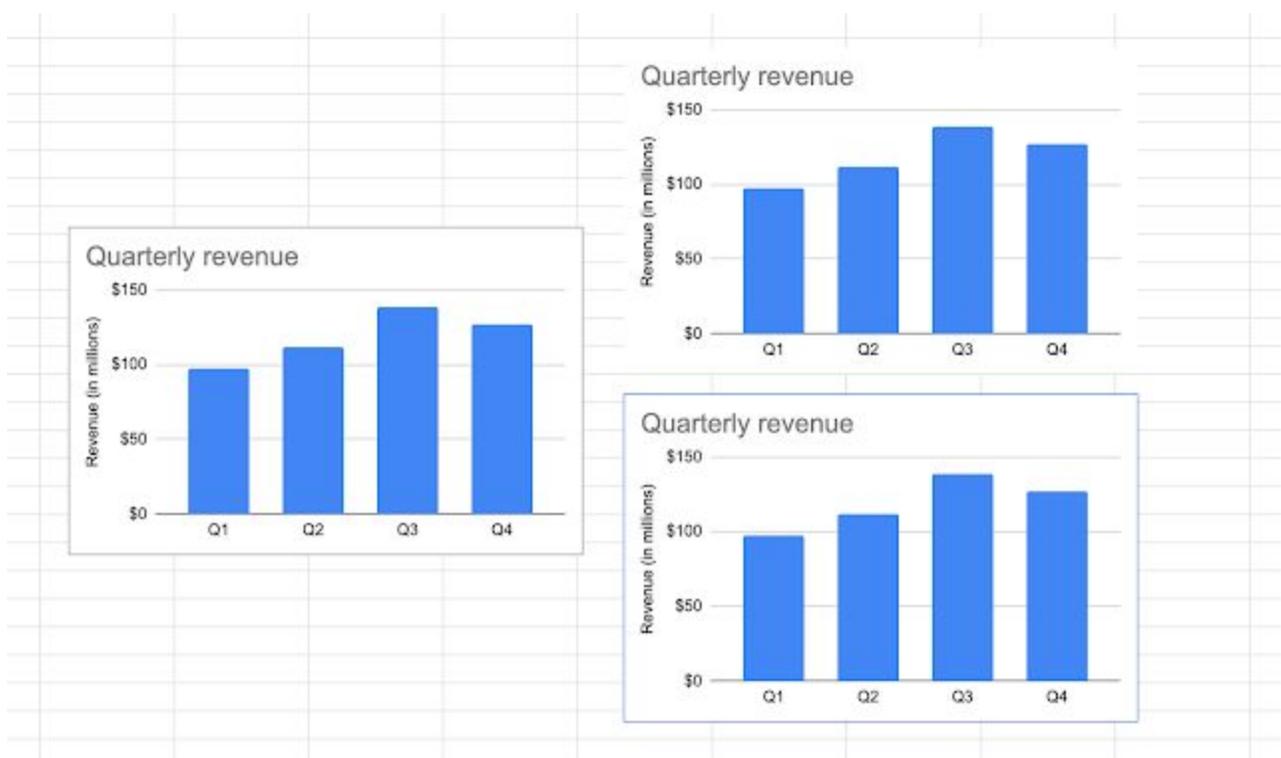
The default border is shown on the left, customization options shown on the right.

We hope this new feature helps you better customize your Sheets.

Improving active account awareness when opening files with multiple sign-ins

|		
Announced on July 9, 2019	Share with your organization	- back to top -

What's changing
We're making it easier for you to identify which Google account is active when opening and contributing to Docs, Sheets, and Slides files.

When you're logged into multiple accounts, like switching between your work and personal accounts, it can sometimes be confusing to determine which account is active when opening and collaborating on a Doc, Sheet, or Slide.

Now when you open a file, you may see a message that indicates which account is active, and gives you the option to quickly change accounts to ensure you're using the best one. This will help eliminate confusion and ensure you're using the correct account when contributing to content.
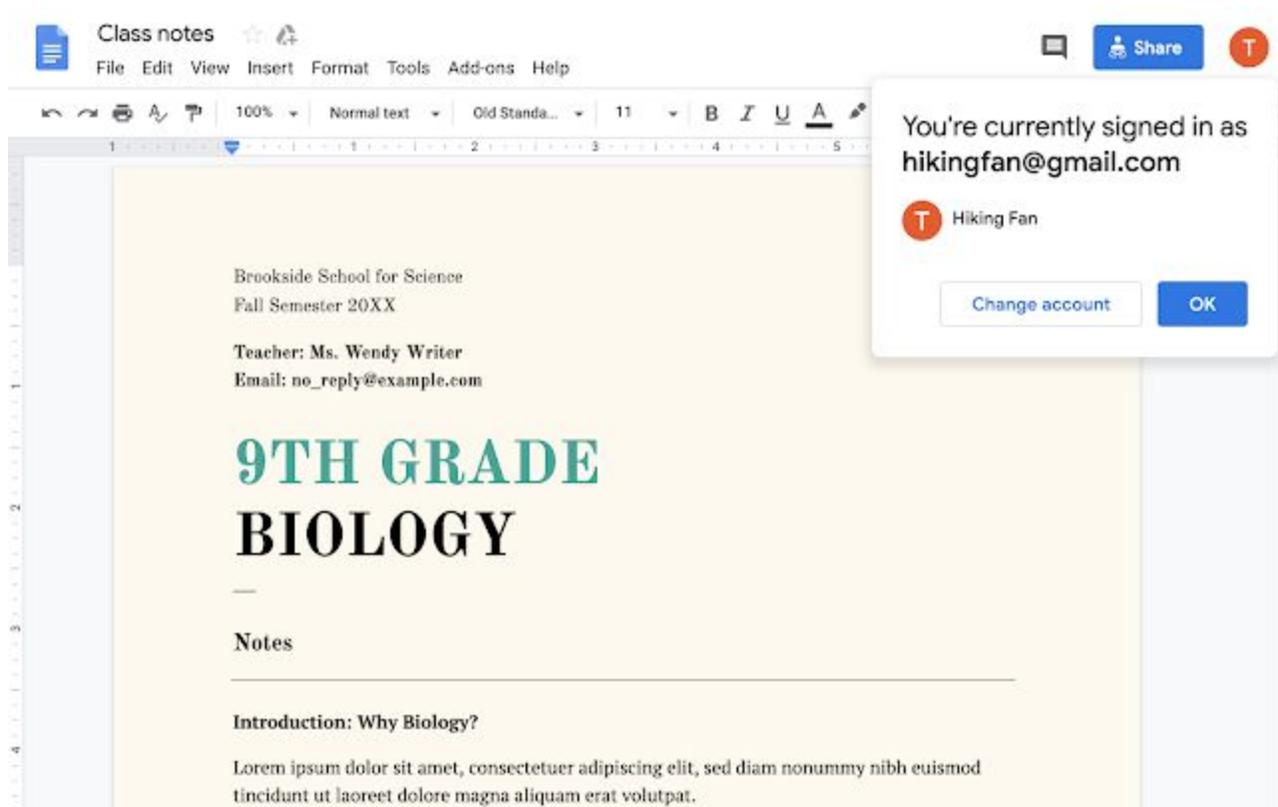
## Dark mode now available for Google Keep on web

Announced on July 9, 2019	Share with your organization	- back to top -

What's changing
You can now enable Dark mode for Keep on the web. To activate Dark mode, click Settings (gear icon) in the top bar and select "Enable Dark mode" from the dropdown menu.

Note that Dark mode must be enabled on a per-device basis. You can also enable Dark mode for Keep on Android.

Dark mode is a popular feature that's frequently requested by Calendar and Keep users. It creates a better viewing experience in low-light conditions by reducing brightness.
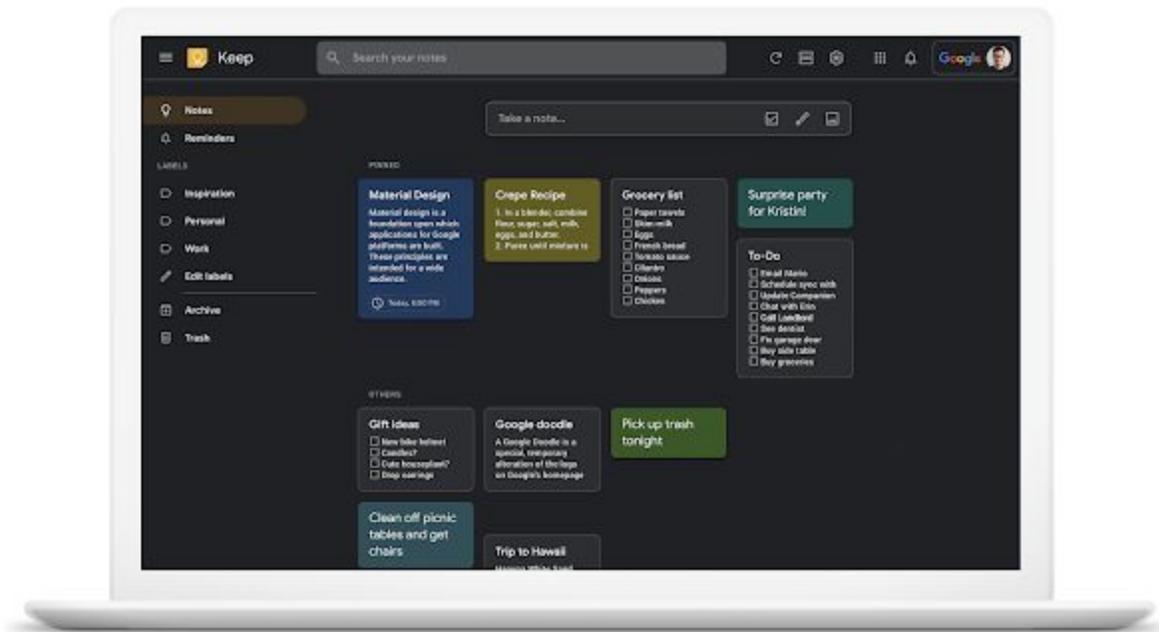
Dark mode for Keep on web.

A revamped home for all your G Suite apps

Announced on July 9, 2019   Share with your organization   - back to top -

What's changing
You can see a list of all the core G Suite apps enabled for your organization in the User Dashboard at gsuite.google.com/dashboard. After a recent redesign, this page is now better-looking and easier to navigate, with a search bar that allows users to quickly find apps.

Users will be directed to the User Dashboard after signing the G Suite Terms of Service, but they can also bookmark it for quick access in the future. Visit the Help Center for more information.
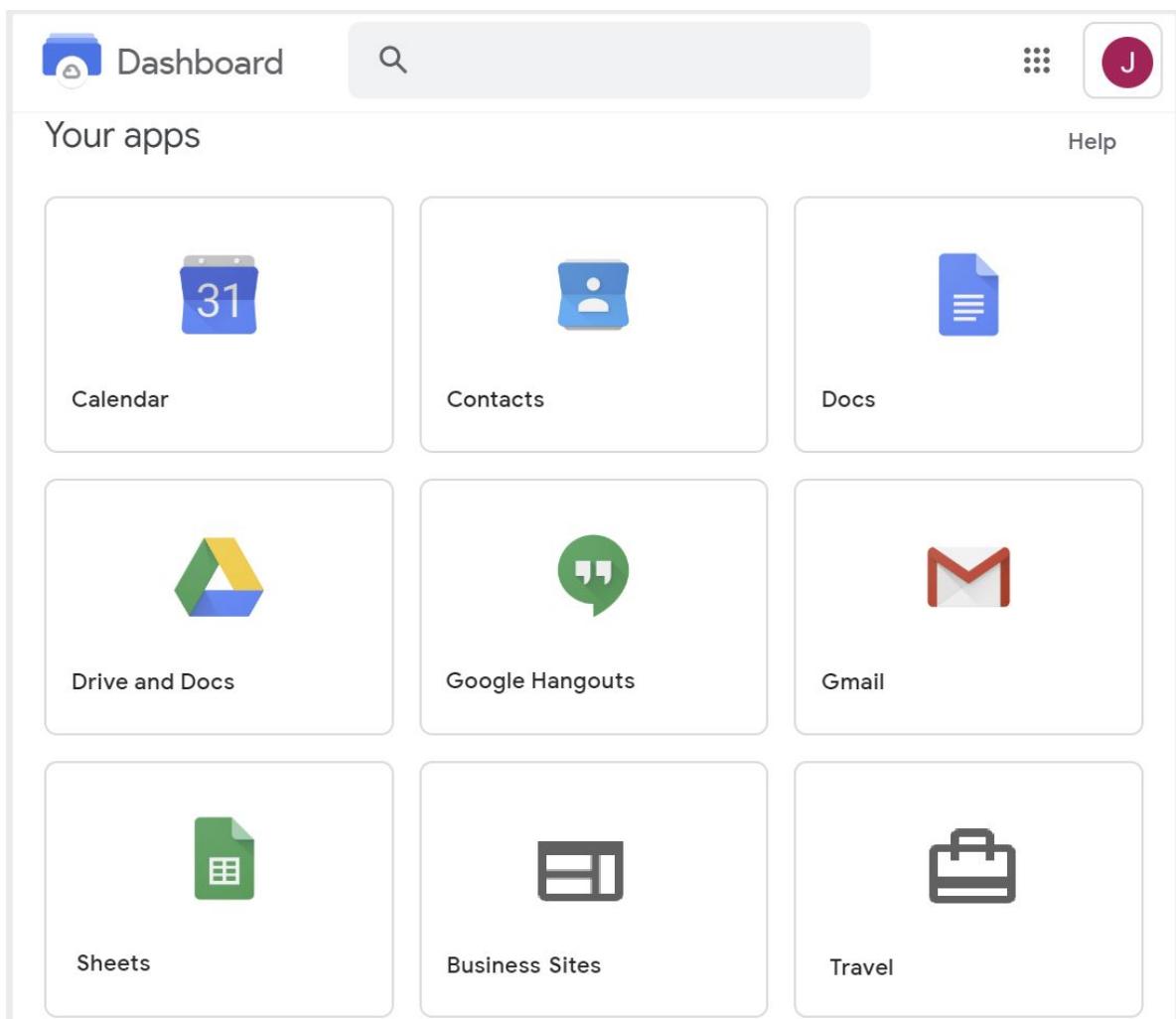
G Suite

Business ready

Request and review formal document approvals with a new beta

What's changing
We're launching a new beta that allows you to request and review formal approvals on Google Docs, Sheets, and Slides. This feature gives you a direct way to get binding approvals on a file, and to see who's approved them.
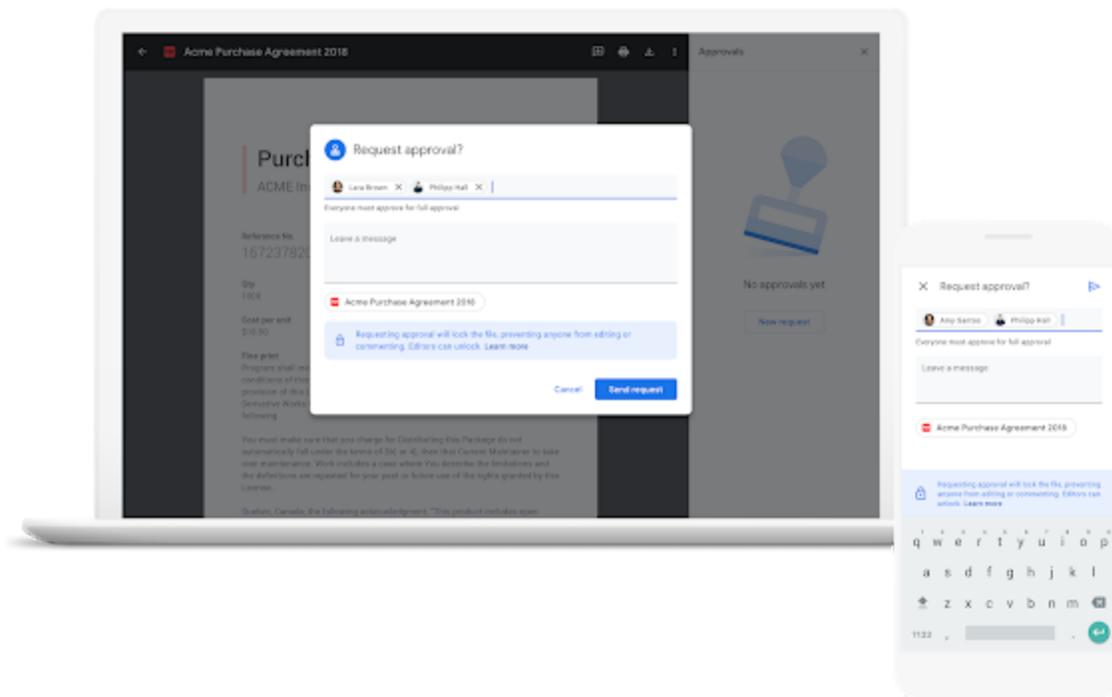
To learn more about this beta and to apply, see here.

Who's impacted
Admins and end users

Why you'd use it
With this beta, you can easily request approval on specific files from a single or multiple reviewers. Once you add a reviewer to a file, they'll receive a notification via email.

You'll also have the option to specify a due date when requesting an approval. As the due date approaches, reviewers will receive reminders via email that their approval is needed. Reviewers will also receive reminders if their approval is past due.

For a single reviewer, the file is automatically approved or rejected once the reviewer makes their choice. For multiple reviewers, the file gets approved once **all** reviewers have selected "approve" and rejected once **any** reviewer selects "reject."

If you need to add additional reviewers to a request, you can do so as long as an approval is still pending. In addition, editors and pending reviewers can choose to re-assign a review request to a more appropriate party.

How to get started

- **Admins:** To apply for the Google Drive Approvals beta, see here.
- **End users:**
  - **Once this feature is enabled for your domain, to request an approval:**
    - In Google Drive, right-click the file you want to get approved and select "Approvals" from the list of options.
    - If you have the file open in preview mode, this option is also available in the actions listed in the three-dot drop-down menu.

- ○ **To approve or reject a file:**
    - ■ If your approval is requested on a document, you'll receive a notification email and can take action within Gmail:
        - ● You can approve or reject the document in the preview pane, and add comments.
        - ● From Drive, you can see a pending request for approval in the action items associated with a file, or by right-clicking and choosing "View approvals."

Additional details

Once you send a file for review, the content of the file cannot be modified, including leaving and resolving comments within the document. Only comments regarding the approval itself can be added.

Only editors can unlock the file, in which case the review request is cancelled. Reviews can be requested again once all revisions are made.

Anomaly detection in the G Suite alert center now in beta

Announced on July 31, 2019   ⭐ Admin feature   - back to top -

What's changing

We're launching the beta of anomalous alert activity for Google Drive. Super admins and admins with delegated privileges for the alert center for G Suite will be alerted when potential data exfiltration risks occur based on unusual Google Drive behavior. Our machine learning models analyze security signals within Google Drive to detect potential security risks such as data exfiltration or policy violations related to unusual external file sharing and download behavior.
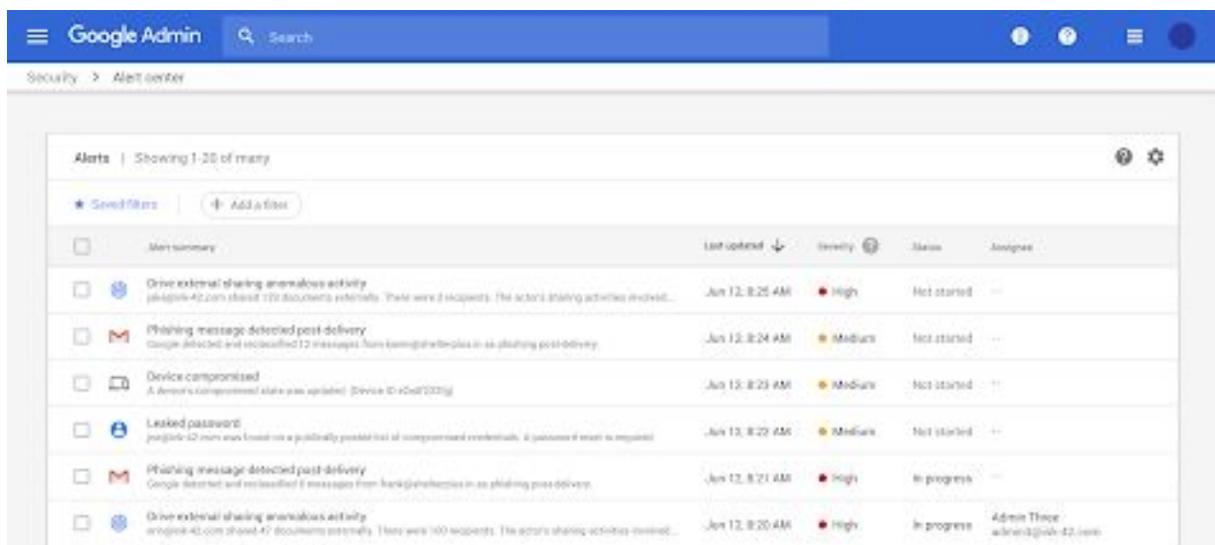
Who's impacted

Admins only

Why you'd use it

Staying on top of activity that impacts the organization's security is top of mind for most admins.

Once in beta, we'll proactively notify you of potential security risks including data exfiltration and unusual user behavior patterns that can otherwise be more difficult for security admins to discover.

Additionally, since the alert center integrates with the security center investigation tool for G Suite, organizations can directly launch remediation efforts from within the alert center.

How to get started

- ● **Admins:** Sign up for the beta using this form.
- ● **End users:** No action needed.

Additional details

With this beta program, we're launching two new types of alerts:

- **Drive External Sharing Anomalous Activity alert:** This alert informs security admins of potential data exfiltration risks based on unusual user Drive sharing behavior to external users.
- **Drive Download Anomalous Activity alert:** This alert informs security admins of potential data exfiltration risks based on unusual user Drive downloading behavior.

Titan Security Keys: now available in Japan, Canada, France, and the UK

Announced on July 31, 2019   ⭐ Admin feature   - back to top -

Quick launch summary
Last year, we launched Titan Security Keys in the United States to help companies protect their users' accounts against phishing and account takeovers. Now, Titan Security Keys are available on the Google Store in Japan, Canada, France, and the United Kingdom (UK).

Titan Security keys can be used anywhere FIDO security keys are supported, including Google's Advanced Protection Program, and help provide strong protection against automated bots, bulking phishing, and targeted attacks.

Admins can learn more about enabling security key enforcement for G Suite, GCP, and Cloud Identity users by visiting our Help Center.

Limiting access to less secure apps to protect G Suite accounts

Announced on July 29, 2019   ⭐ Admin feature   - back to top -

What's changing
On October 30, 2019, we'll begin removing the setting to "Enforce access to less secure apps for all users" from the Google Admin console. This setting should disappear from your Admin console by the end of year.
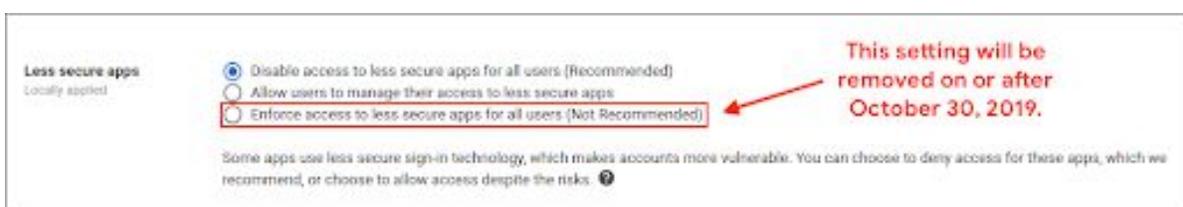
If the "Enforce access to less secure apps for all users" setting is selected for your domain when this change takes place, we'll automatically select "Allow users to manage their access to less secure apps" instead. You'll no longer have the option to enforce access to LSAs at the domain level.

Following this change, if you "Allow users to manage their access to less secure apps," users will still have the option to access LSAs, provided the "Less secure app access" setting is enabled at the individual user account level. To minimize disruption in domains where we've automatically changed the setting from "Enforce access" to "Allow users to manage their access," this account-level setting will be on by default at the time of the change for all *active* users of LSAs.

← **Less secure app access**

Some apps and devices use less secure sign-in technology, which makes your account more vulnerable. You can **turn off** access for these apps, which we recommend, or **turn on** access if you want to use them despite the risks. Learn more

Allow less secure apps: ON
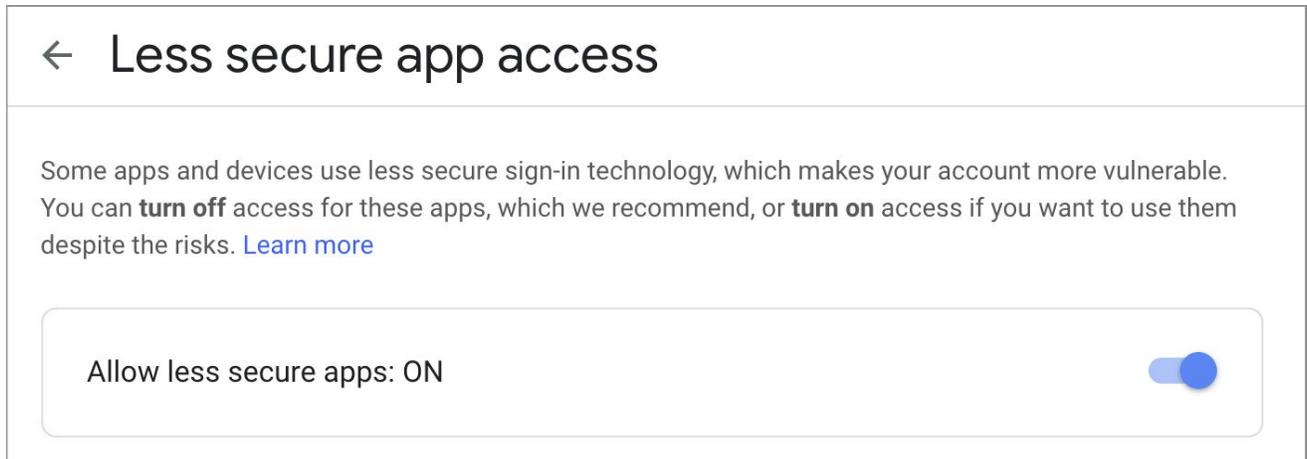
If a user has previously opted to let LSAs access their account, but no LSAs have connected to their account in some time, we'll turn this account-level setting off for them. They can manually reenable this setting at any time at myaccount.google.com/lesssecureapps (provided their admin allows them to do so).

Who's impacted
Admins and end users

Why it's important
We're making this change to protect your users. LSAs connect to Google accounts using only a username and password, which makes them vulnerable to hijacking. Whenever possible, users should connect to their accounts via OAuth, a more secure method. OAuth allows third-party apps to use Google account information without seeing a user's password, and it gives admins security controls like the ability to whitelist certain apps and offer scope-based account access.

Visit the Help Center to learn more about managing OAuth-based access to connected apps.

How to get started

- **Admins:** No action is required, but we recommend the following:
  ○ If you currently enforce access to LSAs in your domain, change your setting to disable access or allow users to manage their access as soon as possible, as LSAs can make Google accounts vulnerable to hijackers.
  ○ Encourage your users to use OAuth-based protocols (like OAuth-based IMAP) to give non-Google apps access to their Google accounts, including their email, calendar, and contacts.
  ○ Review our list of alternatives to less secure apps.
  ○ Prepare your users and internal help desks for the change.
  ○ Update any user guides you've previously published to recommend the use of OAuth or to instruct users on how to turn on LSAs.
  End users: Visit the Help Center to learn more about LSAs and your account.

Additional details

See below for FAQs.

What is a less secure app (LSA)?
A less secure app (LSA) is an app that connects to Google accounts using only username and password verification for access and not OAuth. Generally, you should only allow your users to use external apps that connect to Google accounts via OAuth, as LSAs make user accounts more vulnerable to hijacking.

I have an app that cannot use OAuth; what do I do?
Choose the "Allow users to manage their access to less secure apps" option in the Admin console, and ensure that users who need to use the app enable the "Less secure app access" setting at myaccount.google.com/lesssecureapps. We also recommend contacting the app's developer and asking them to provide support for OAuth, as this is the more secure option.

Use groups to control more G Suite apps and settings

What's changing
Last year, we announced that you could control access to G Suite apps and services using groups. We're now expanding what G Suite features you can control using groups. You can now use groups to control default settings for:

- **App Maker** database settings
- **Currents** settings (for organizations enrolled in the Currents beta program)
- **Directory** editability, such as what profile information (e.g. name, birthday, gender, etc.) users can edit
- **Google Drive and Docs** policies for sharing files and link visibility
- **Google Voice** settings (for organizations who have signed up for Google Voice)
- **Hangouts Meet** settings
- **YouTube** content settings, permissions, and more

Who's impacted
Admins only

Why you'd use it
Using groups can make G Suite simpler to manage while making sure the right users have access to the right apps, and have the appropriate default settings within those apps. For example, you could use groups to automatically configure G Suite for specific job functions, project teams, specific seniority levels, or geographic locations.

How to get started
- Admins: Use our Help Center to learn how to configure G Suite service settings with groups.
- End users: No action needed.
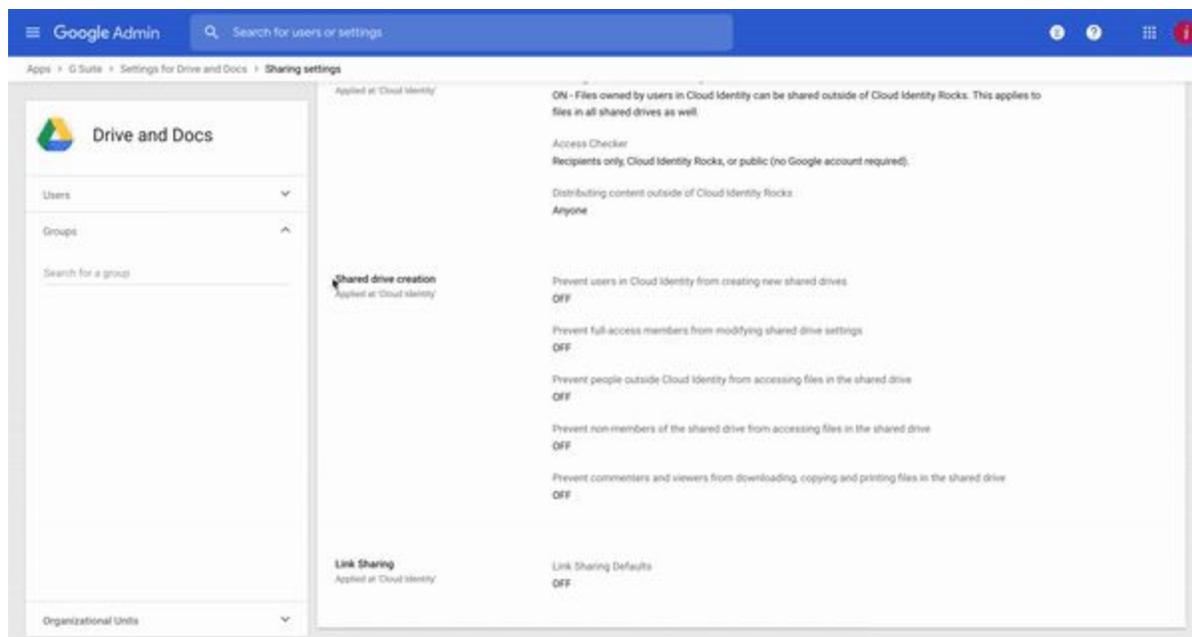
Whitelist and manage domains more easily in the Admin console

G Suite

What's changing

We're making a few changes to how G Suite admins manage owned and whitelisted domains in the Admin console. There will be no significant functionality changes, but the interface at *Admin console > Account > Domains* will be different. Specifically you may notice:

- A "Manage domains" section. This was previously called "Add/remove domains."
- A "Whitelisted domains" section. This was previously called "Whitelisted external domains" and is where you can whitelist domains so your users can more easily collaborate with users in those domains.
- An updated interface in both of these sections, with options rearranged to make it easier to find and perform common functions.
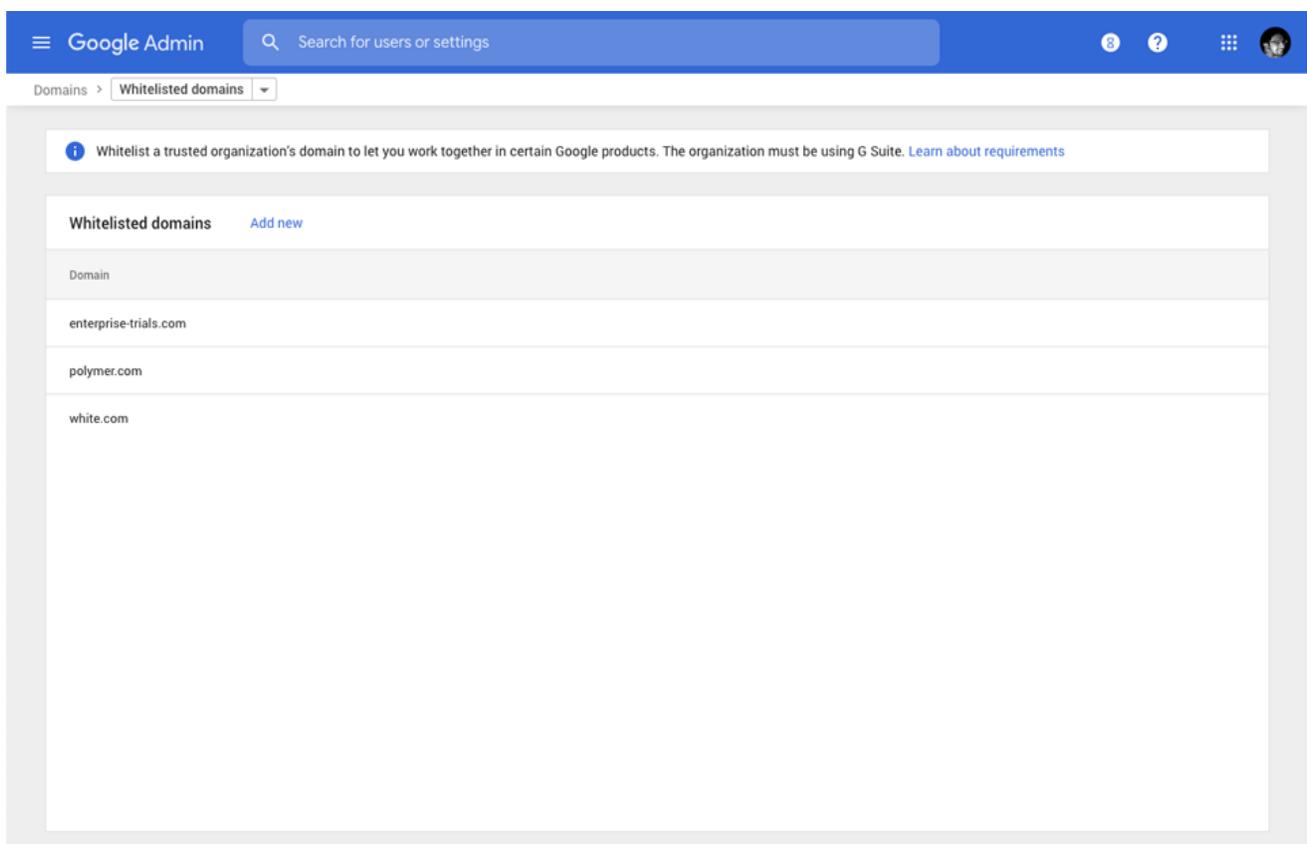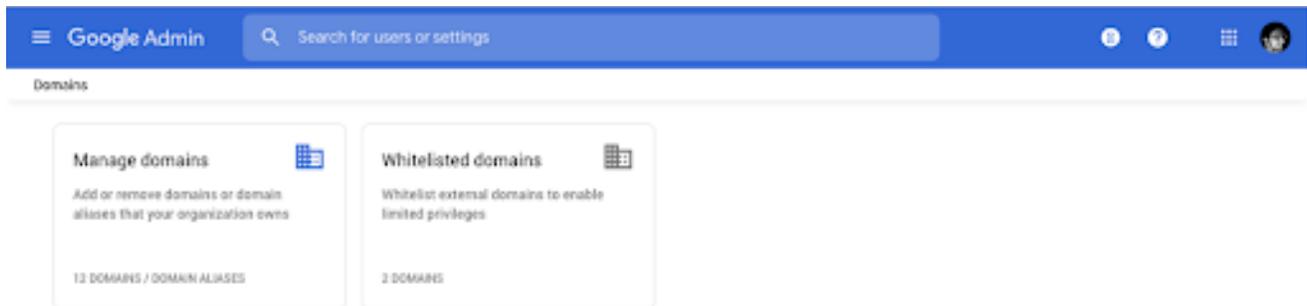
Use our Help Center to learn more about how to add more domains to your G Suite account or whitelist trusted G Suite domains.

Coming Soon: Transformation reports from Google for Education

G Suite

What's changing
This back-to-school season, we're launching Google for Education transformation reports, available to all K-12 districts and schools in the US free of charge. Admins can sign up to be notified once the tool is available by filling out this form.

Who's impacted
Admins only

Why you'd use it
The transformation report is a free tool designed to help quantify an organization's Google for Education implementation across our products and programs. Semester-based reports track usage trends over time and make it easy to understand how your organization is using G Suite, Chromebooks, and progressing through Certification and Transformation programs.

Based on survey responses and usage information, you'll receive tailored recommendations and resources from Google for Education to help you drive more impact across your organization.

Sample Transformation report.
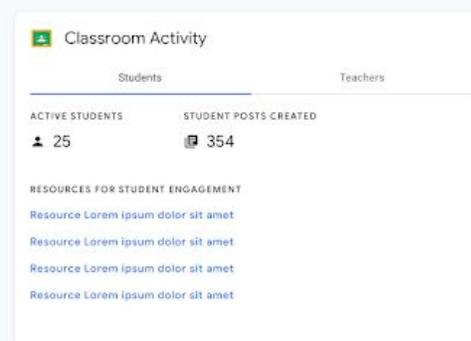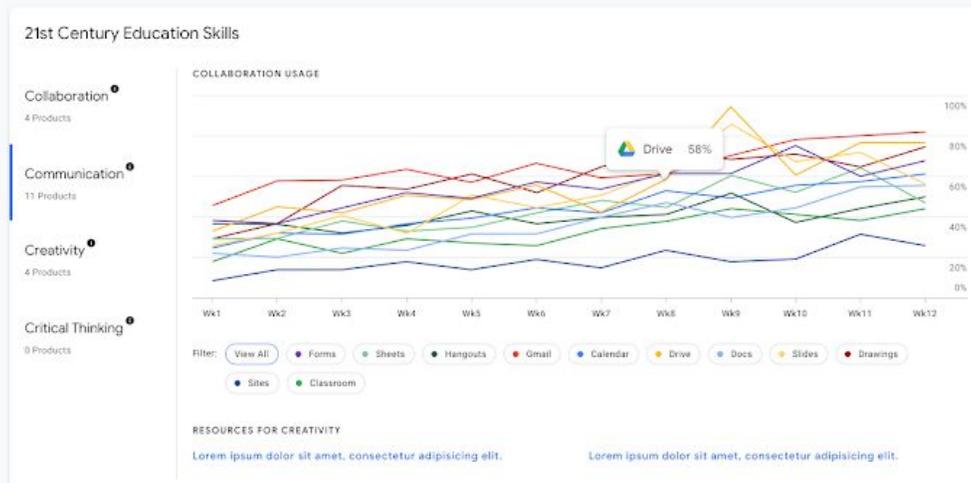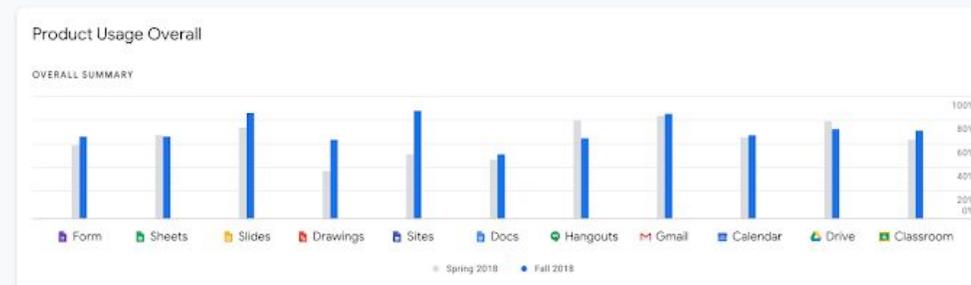
How to get started
- **Admins:** Express interest in receiving your own transformation report and receive launch updates.
  - Note: Transformation reports are only available to G Suite for Education and G Suite Enterprise for Education users *in the US only*.
- **End users**: No action required.

Additional details

The survey window will open at launch and admins will have several weeks to complete and share the transformation survey (less than 10 minutes) with others in their organization. Your custom transformation report will be generated when the survey window closes, displaying survey responses alongside product and program usage metrics. Note that a report can be generated with just an admin's response, or with no responses. If there are no survey responses, the report will not be nearly as valuable.

Reports can be generated twice a year—at the beginning of the Fall and Spring semesters—and will identify areas of improvement across seven key areas of transformation which you can learn more about here.

Additionally, you'll be able to see metrics on your active G Suite users' behavior over the course of the past semester. Specifically, you'll be able to see data around how users within your organization are using products like Google Classroom, Docs, Drive, Slides, Sites, and more for collaboration, communication, creativity, and critical thinking.

G Suite

Learn more about G Suite

Cloud Connect Community: The official community for G Suite admins
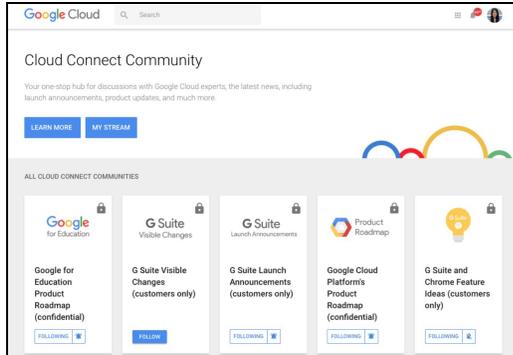
Sign in today: Cloud Connect is your one stop shop for resources to make your work with G Suite easier. Sign in today to discuss best practices, ask questions, and communicate with your peers and Googlers. Don't miss out!

G Suite on Social

Connect with us: Follow G Suite on social media to get news, product tips, and other helpful information:

Follow @gsuite on Twitter

Like G Suite on Facebook (@gsuitebygoogle)

Follow us on LinkedIn

Subscribe to our YouTube channel

G Suite Learning Center
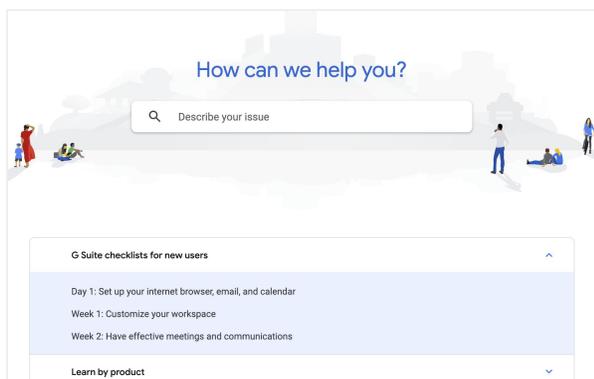
Learn more: This completely redesigned site features 300+ guides and customer-friendly enhancements, including:

- An Announcements tab with lists of new and updated Learning Center guides.
- A "Day 1" checklist to help new G Suite users get started on their first day.
- An improved search function to help you find help and training content across the G Suite Learning Center.
- Guides that are easier to print and save as PDFs or customize in Google Docs and Slides.