What's New

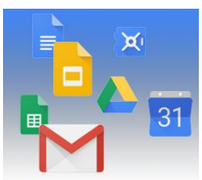
G Suite

January 2020

Featured launch: Manage Windows 10 devices through the G Suite Admin console

Work together

Use a phone for audio in a Hangouts Meet video call
Present to meetings using the HDMI cable on Hangouts Meet hardware

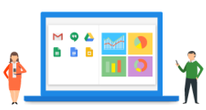


Simple to use

G Suite Add-ons now generally available in Calendar, Gmail, and Google Drive
Use phones as security keys in the Advanced Protection Program
Use an iPhone as a security key for 2-Step Verification
Originality reports & rubrics now generally available for Google Classroom users
More options for copying presentations in Google Slides

Business ready

New system to improve data loss prevention (DLP) in Google Drive
Grant SAML app access to specific groups
Password recovery for super admins and a new interface for security settings
Get email alerts and see associated tickets for Access Transparency logs
Break out a single value within a pie chart in Google Sheets
Manage Hangouts Meet and classic Hangouts video calls with one setting
View data for only selected call participants in the Meet Quality Tool
New controls for displaying sender attribution for shared mailboxes
Google App Maker will be shut down on January 19, 2021



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 Launch Team, January 2, 2020

Featured launch: Manage Windows 10 devices through the G Suite Admin console

Announced January 16, 2019 | Admin feature | - back to top -

What's changing
We're enabling enhanced desktop security for Windows with a new beta. This will allow you to manage and secure Windows 10 devices through the Admin console, just as you do for Android, iOS, Chrome, and Jamboard devices today. It will also enable SSO so users can more easily access G Suite and other SSO-enabled applications on Windows 10 devices.

With these new controls G Suite admins can:

- Enable their organization to use existing G Suite account credentials to login to Windows 10 devices, and easily access apps and services with SSO
- Protect user accounts with anti-phishing, anti-hijacking, and suspicious login detection technologies
- Ensure that all Windows 10 devices used to access G Suite are updated, secure, and within compliance
- Perform admin actions, such as wiping a device and pushing device configuration updates, to Windows 10 devices from the cloud without specific network requirements

Who's impacted
Admins

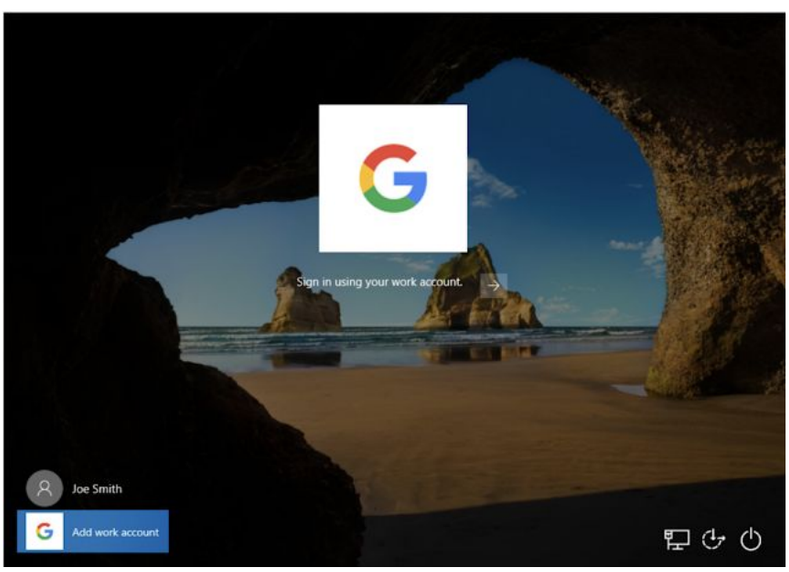
Why you'd use it
Automatic device registration, the ability to secure all of your devices in a single Admin console, and cloud-based policy and device configuration deployment will simplify device management and security for your organization. Additionally, the ability to remotely wipe devices can help increase your organization's data security.

Additionally, this makes life easier for users by reducing the hurdles and logins needed to access applications and get work done. Users need to log in just once to their Windows 10 device using their G Suite login credentials, and they'll be able to access Google apps and any other enterprise cloud applications with SSO enabled without further logins.

Additional details

Set policies, push configurations to devices, and wipe devices as needed
Admins can deploy policies and device configuration updates from the cloud, removing any network or other restraints for installing these updates on user devices. Policies and updates that can be applied by admins include BitLocker, Windows Update, and desktop customization. Additionally, admins can block or wipe devices if needed from the device page in the Admin console.

Getting started
- **Admins:** Learn more and sign up for the beta here.
- **End users:** No action required until admins activate the beta.



ā

Work together

Use a phone for audio in a Hangouts Meet video call

Announced on January 29, 2019 | Share with your organization | - back to top -

What's changing

You can now different sources for your audio and video feeds in a Hangouts Meet video call. Specifically, you can use a phone call for audio while still using your computer's camera and web browser for video.

This can be done by dialing into the call directly, or by having Meet call your phone. You can use your phone for audio immediately upon joining, or anytime after joining if you'd like to switch.

Who's impacted

Admins

Why you'd use it

You can use your phone for audio on Hangouts Meet calls to ensure you have consistent and reliable audio quality, even if your network connection is poor, or if your computer's microphone and speaker aren't working. You'll still be able to share and see video and presentations in the meeting.

Additional details

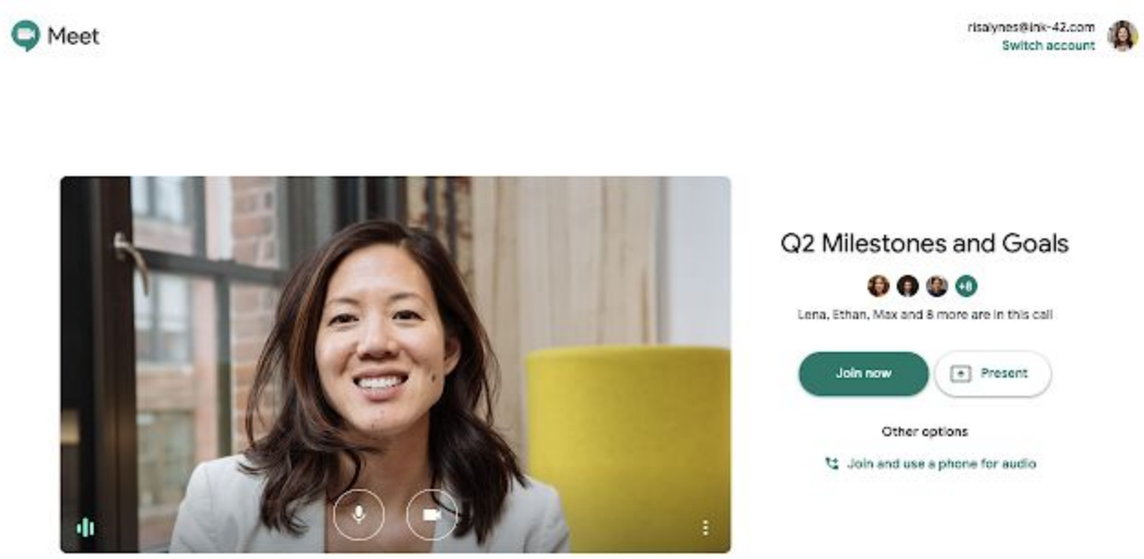
Please note that the Meet dial-out option is currently only available in the US and Canada.

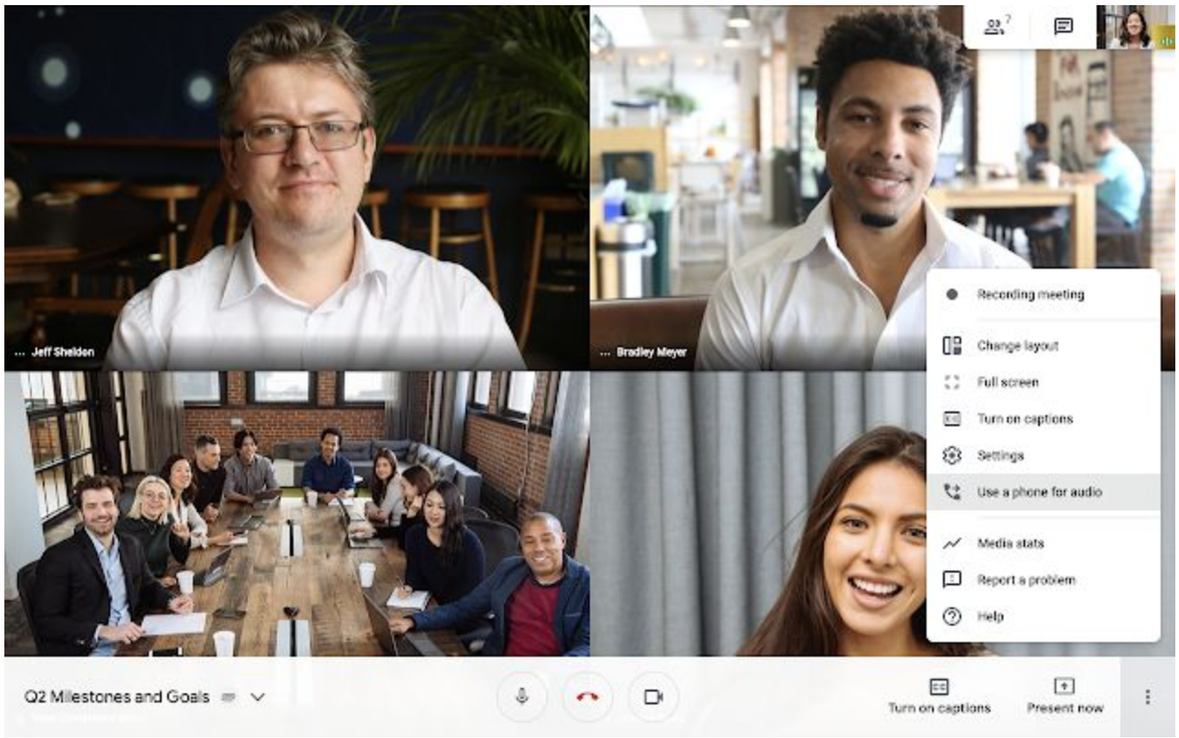
Getting started

Admins: This feature will be ON by default if dial-in functionality is enabled. If you'd like to disable the dial-in functionality for Meet meetings, it can be done at the domain, OU, or group level. To disable this feature, in the Admin console go to *Apps > G Suite > Settings for Google Hangouts > Meet settings* and disable the setting "Provide a phone number and PIN for each video meeting."

Visit the Help Center to learn more about turning dial in/out on or off for your organization.

End users: This feature will be ON by default for all calls with dial-in/out enabled. Visit the Help Center to learn more about using a phone for audio in a video meeting.





Present to meetings using the HDMI cable on Hangouts Meet hardware

Announced on January 14, 2019 | Share with your organization | - back to top -

Quick launch summary
You can now present high-quality video content with audio in your meeting using the HDMI cable included with Hangouts Meet hardware kits.

Please note: Hangouts Meet already supported using this HDMI cable for local presentations. This additional functionality allows users to present into meetings with remote participants as well.

Getting started

- **Admins:** There is no admin control for this feature.
- **End users:** This feature will be ON by default.

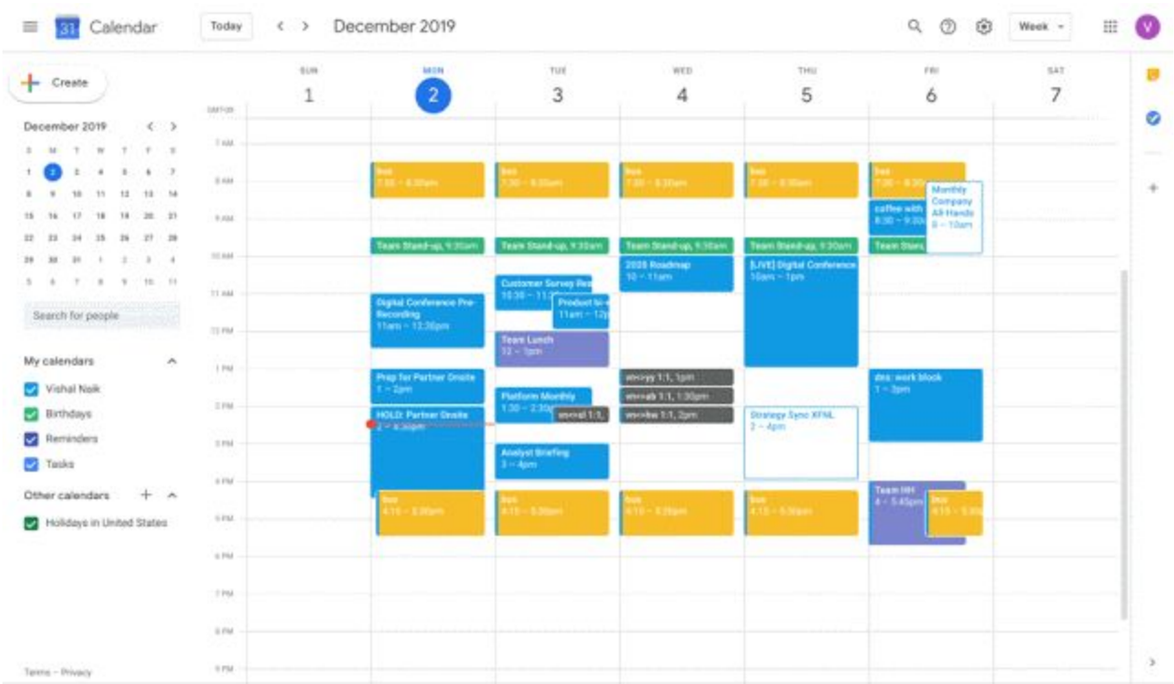
Simple to use

G Suite Add-ons now generally available in Calendar, Gmail, and Google Drive

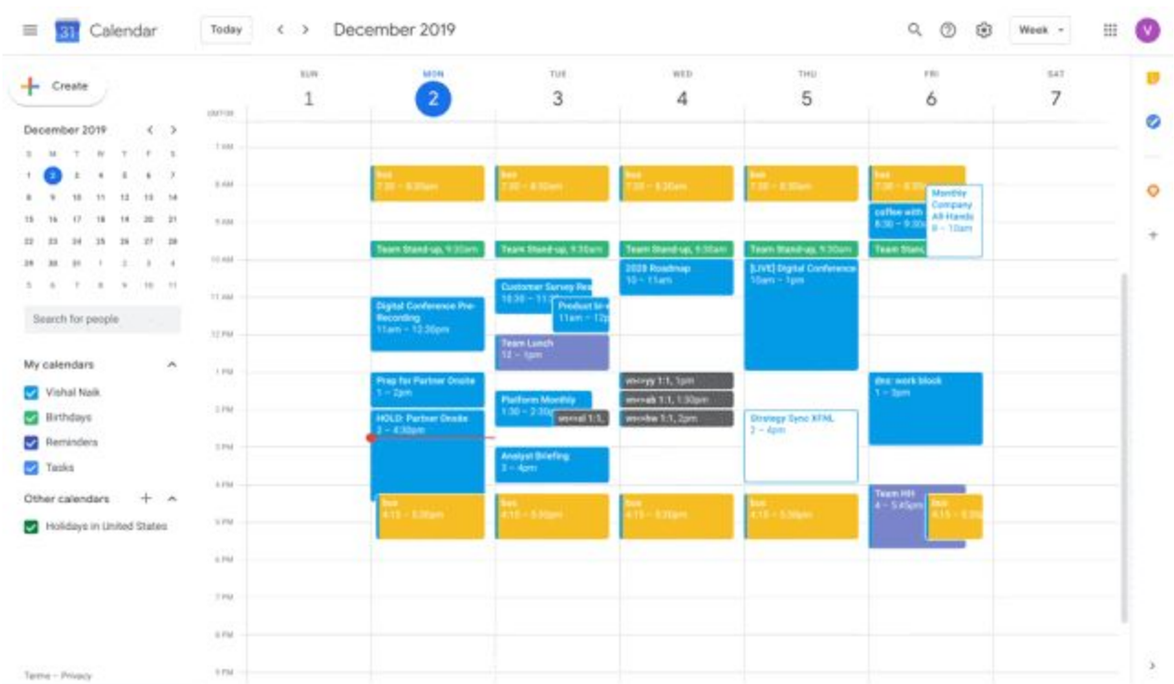
Announced on January 21, 2019 | Share with your organization | - back to top -

What's changing
Last year we announced the beta of G Suite Add-ons, a new cross-suite platform that connects G Suite to your favorite workplace apps. Beginning today, G Suite Add-ons will begin rolling out to all users.

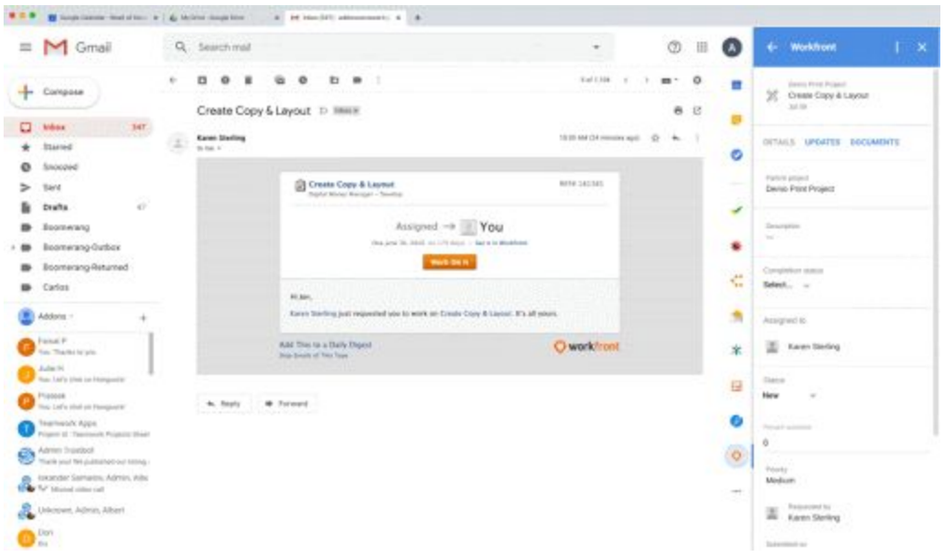
With G Suite Add-ons, workflows that require third-party applications can be executed inside G Suite, allowing users and teams to use the applications they want without leaving G Suite. For example, you can install the Workfront add-on for quick access across Calendar, Gmail, and Google Drive.



Installing the Workfront add-on directly from Calendar



Access G Suite Add-ons from the side panel of Calendar, Google Drive, and Gmail



Take action without leaving G Suite

Who's impacted
Admins and end users

Why it's important
G Suite Add-ons connect G Suite with third-party applications so you can work directly from the G Suite app you're using, rather than toggling from one app to another. They also surface relevant information and suggest actions based on what you're working on.

Add-ons from SignEasy, WebEx, Workfront, Lucidchart and more are available now and can be installed from the G Suite Marketplace.

Organizations can also build their own add-ons using Apps Script. Note that the developer feature will be fully available in early February — we'll provide an update here once it's fully rolled out.

Additional Details
G Suite Add-ons will work across G Suite products, allowing developers to create a single add-on that works across G Suite, rather than building a separate add-on for each application within G Suite.

G Suite Add-ons are currently accessible in Calendar, Gmail, and Google Drive, with support for other G Suite products coming later this year.

Getting started

Admins: This feature will be available by default. If you allow users to install only whitelisted applications from the G Suite Marketplace, you can specify those apps within the Admin console. Or, you can install chosen G Suite Add-ons for your entire domain via the G Suite Marketplace.

End users: This feature will be available by default. You'll be able to install G Suite Add-ons using the "+" button in the G Suite quick access side panel. The add-ons you install will appear in the side panel across G Suite apps.

Use phones as security keys in the Advanced Protection Program

Announced on January 15, 2019 | Share with your organization | - back to top -

What's changing
You can now use your mobile phone as a security key in the Advanced Protection Program for the enterprise. This means you can use your Android or iOS device's built-in security key for 2-Step Verification, which makes it easier and quicker to protect high-risk users with our strongest account security settings.

Users can learn more and sign up for the Advanced Protection Program at g.co/advancedprotection.

Who's impacted
Admins and end users

Why you'd use it
The Advanced Protection Program for the enterprise enforces a package of several security policies, which can help protect the accounts of employees who are most at risk for targeted attacks. By adding the option to use your phone as a security key with this program, we hope more G Suite users will be able to take advantage of the protection it offers due to:

- Simpler enrollment - Users can sign up quickly using devices they already have.
- Intuitive user experience - Users are familiar with the phone interface, and often already carry phones with them.
- Lower costs - This reduces the need to purchase security keys.

Additional details
Targeted attacks describe sophisticated, low volume handcrafted attacks that are often carried out by highly motivated professional or government backed groups. Employees at risk of targeted attacks that may benefit from the program include, for example, IT admins, executives, and employees in regulated industries such as finance or government.

The individual policies currently included in the Advanced Protection Program are also available to G Suite admins and users outside of the program. However, the Advanced Protection Program for the enterprise offers an easy-to-use bundle of our strongest account security settings

Getting started
Admins: By default, users will be able to sign up for the Advanced Protection Program. You can disable it at the OU level. Visit the Help Center to learn more about managing the Advanced Protection Program in your organization.

End users: Android users can go directly to g.co/advancedprotection to enroll their phone as a security key. iPhone users must first activate the security key with Google's Smart Lock app, then enroll in the Advanced Protection Program.

Use an iPhone as a security key for 2-Step Verification

Announced on January 15, 2019 | Share with your organization | - back to top -

What's changing
We're adding an option to use your iPhone as a security key for your Google Account. Security keys provide the strongest form of 2-Step Verification (also known as two-factor authentication or 2FA) to help protect your account against phishing, and are an essential part of the Advanced Protection Program for the enterprise. To use your iPhone as a security key, you need to install the Google Smart Lock app.

Read more about this launch in our Security Blog post, or use our Help Center to learn more about security keys and 2-Step Verification. Also see our other announcement today - Use phones as security keys in the Advanced Protection Program.

Who's impacted
Admins and end users

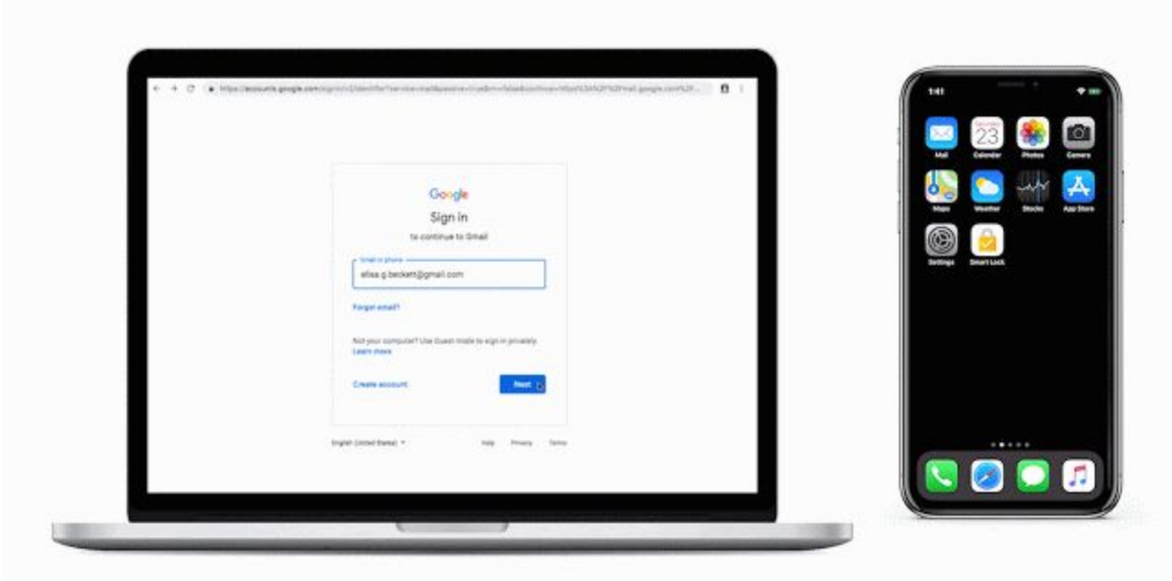
Why you'd use it
2-Step Verification adds another layer to your account security, making it more resistant to phishing and account takeover attacks. By adding the option to use iPhones as a security key, we're making the strongest form of phishing protection more accessible and convenient. As a result, we hope you'll be able to implement Advanced Protection in your organization more quickly, while also minimizing user training and overall costs.

We previously announced that you can use the security key built into your Android phone, in addition to physical security keys, including Google's Titan Security Keys.

We also announced today that you can use phones as security keys in the Advanced Protection Program for the enterprise. We hope that these launches bring the added protection of security keys to more users, including making it easier to enrol in the Advanced Protection Program, and helps ensure that all users have access to more convenient forms of security.

Additional details
- The iPhone security key is enabled through the Google Smart Lock app.
- Installation of the Google Smart Lock app is only available on devices running iOS 10.0 and up.
- The security keys on iPhones are compatible with Bluetooth-enabled Chrome OS (version 79 and up), iOS, macOS, or Windows 10 devices with a Chrome browser.

Getting started
- **Admins**: If 2-Step Verification or Security Key Enforcement is turned on for an organization, iOS devices will be available as an option for security keys by default. Use our Help Center to see how to enforce the use of security keys in your organization.
- **End users**: Use the Help Center to see how to activate the security key on your phone or enroll in the advanced protection program.

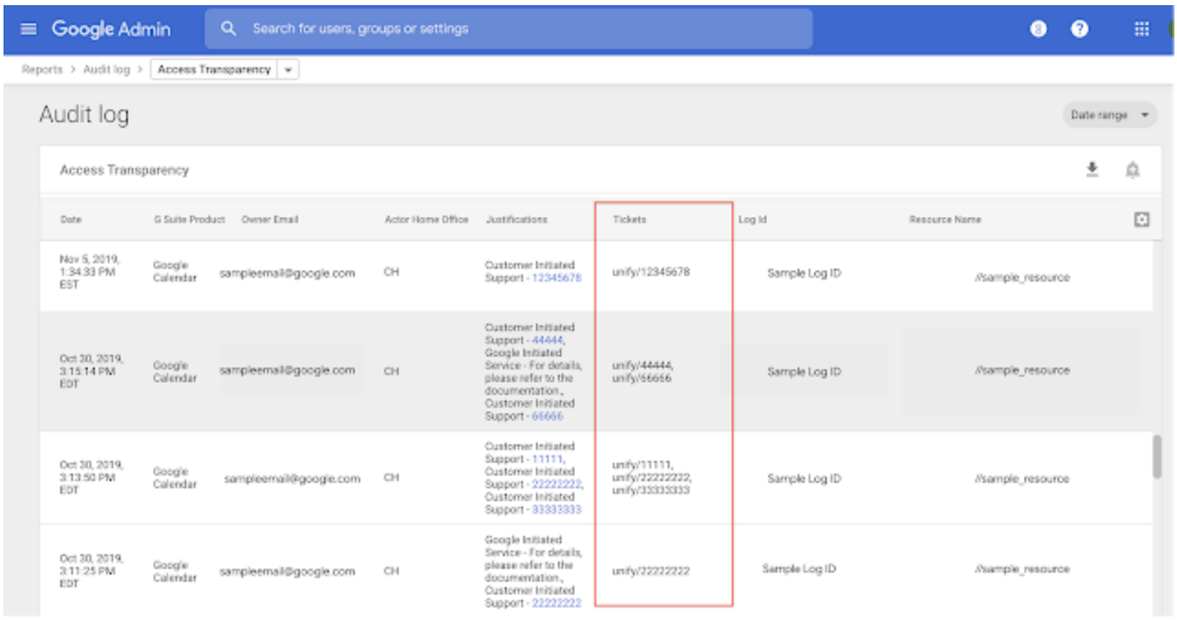


Originality reports and rubrics now generally available for Google Classroom users

Announced on January 21, 2019 | Share with your organization | - back to top -

What's changing
Last year, we announced betas for originality reports and rubrics, two new tools for Google Classroom. Beginning today, these features are generally available for G Suite for Education and G Suite Enterprise for Education Classroom users.

Who's impacted
End users



You can see support ticket numbers in the Access Transparency audit log

Getting started

- **Admins:** Email alerts will be OFF by default, support ticket information in the audit log will be ON by default. Learn more about Access Transparency logs, or how to set up alerts.
- **End users:** Feature is not visible to end users.

Break out a single value within a pie chart in Google Sheets

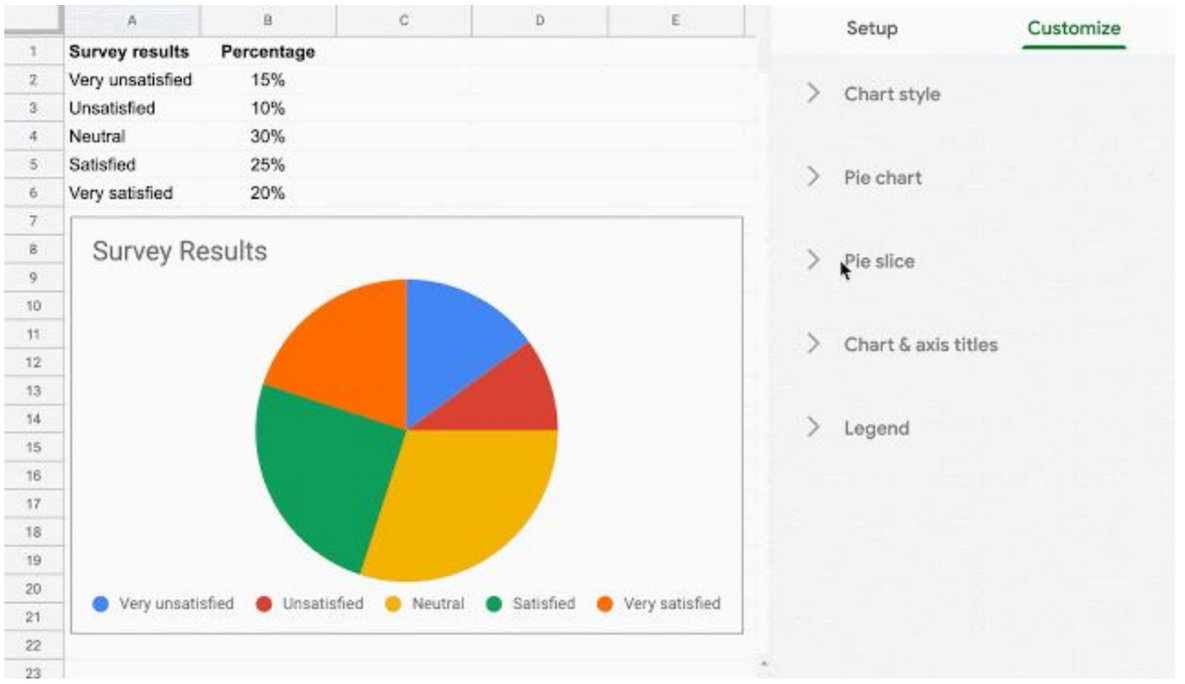
Announced on January 8, 2019 | Share with your organization | - back to top -

Quick launch summary

You can now “pull out” and highlight a slice from a pie or donut chart in Google Sheets. This feature gives you more ways to control the look of your charts and better display the most important data in Sheets.

Getting started

End users: This feature is available by default. Visit the Help Center article to learn more about using this feature.



View data for only selected call participants in the Meet Quality Tool

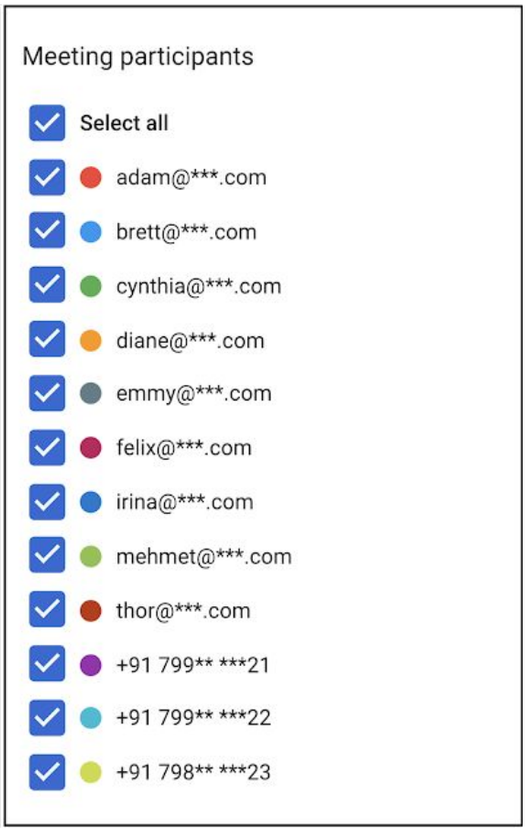
Announced on January 22, 2019 | Admin feature | - back to top -

Quick launch summary
You can now select specific participants when viewing meetings in the Meet Quality Tool. This allows you to display data and statistics for just a subset of the participants. When viewing calls with many participants, this helps limit the amount of information displayed on the screen at one time. By fitting just the most relevant information into the view, pagination can often be avoided even for very large meetings.

Getting started

Admins: This feature will be available by default when using the Meet Quality Tool. To select participants, use the participant list on the left-hand side of the Meeting Details page. As selections are made, the information displayed to the right will update accordingly.

End users: This feature has no impact on end users.



Manage Hangouts Meet and classic Hangouts video calls with one setting

Announced on January 7, 2019 | Admin feature | - back to top -

What's changing
Video calling from Hangouts Meet and classic Hangouts is now controlled by the same setting. This means that the setting in the Admin console that controls classic Hangouts video calling now also controls Hangouts Meet.

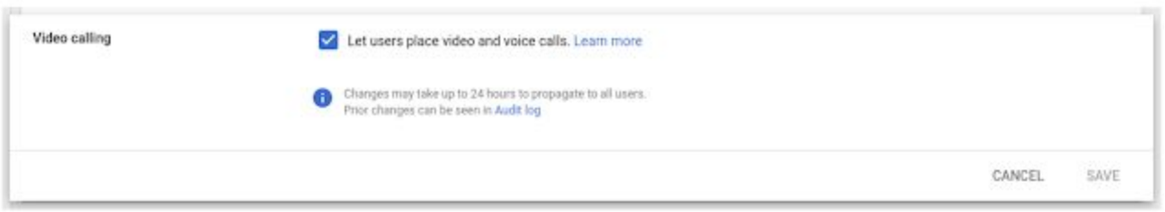
Why it matters

By combining these settings, we're making it easier for you to manage all video calling within your organization.

Getting started

Admins: You can find the new, consolidated setting in the Admin console at *Apps > G Suite > Settings for Google Hangouts > Meeting Settings*. The new setting will respect your previous setting. For new G Suite customers, video calling will be enabled by default.

End users: There is no end user setting for this feature.



New controls for displaying sender attribution for shared mailboxes

Announced on January 7, 2019 | Share with your organization | - back to top -

What's changing
We're adding new controls for how the "Sender Attribution for Shared Mailboxes" is displayed. Currently, sender attribution is always enabled — this will remain the default setting unless disabled by the admin or the end user.

For end users, there's a new setting in Gmail where you can specify what information is included in the email header of messages sent by delegates.

For admins, there's a new setting in the admin console that allows you to hide all attribution for shared mailboxes in your domain or organizational unit (OU). **This will override and disable the user setting in Gmail.**

Who's impacted
Admins and end users

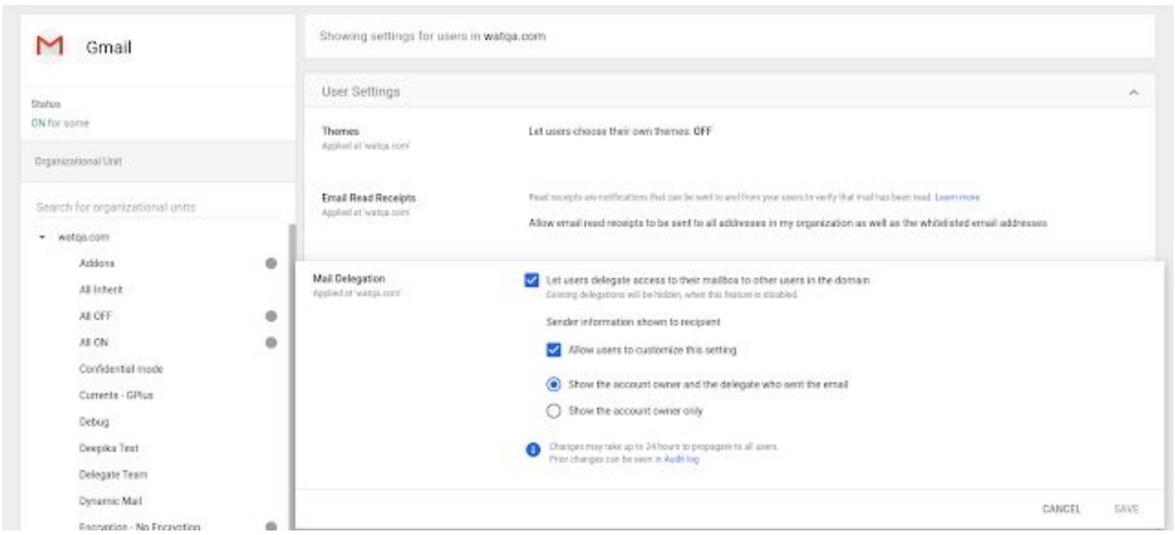
Why you'd use it
Organizations use shared mailboxes in Gmail in multiple ways. For example, if an executive admin is responding on behalf of a CEO, from the CEO's mailbox, sender attribution makes it clear who specifically drafted and sent the email.

Or, if you use an info@company.com mailbox to communicate with customers, customers will view all responses as equally valid, without knowing whether they were sent by sally@company.com, or jim@company.com.

With these new settings, you can now control and customize how attribution is handled for your domain, by OU, or on an individual user level.

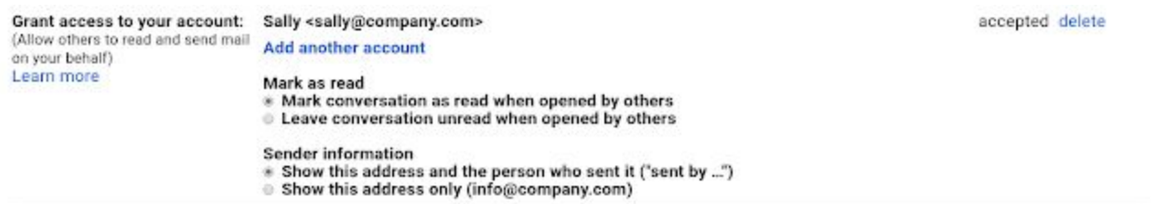
Getting started

Admins: Sender attribution is on by default and can be disabled at the OU or domain level. The new setting can be found in the Admin console under *Apps > G Suite > Gmail > User settings > Mail Delegation*. Note that the default setting will be "Allow users to customize this setting" and "Show the account owner and delegate who sent the email."



Settings for Mail Delegation in the Admin console

End users: Sender attribution is ON by default. You can view and set sender attribution parameters by going to *Settings > Account > Grant access to your account* in Gmail. If your admin has hidden sender attribution for your domain or OU, no action can be taken.



End user settings for sender attribution in Gmail

If disabled at the OU or domain level, end users can take no action in Gmail

Google App Maker will be shut down on January 19, 2021

Announced on January 27, 2019 | Share with your organization | - back to top -

What's changing
Due to low usage, Google App Maker will be turned down gradually over the course of 2020 and **officially shut down on January 19, 2021**. Prior to the shutdown, you'll need to review App Maker usage in your domain and take any necessary action.

See the Additional details section below for a timeline of the shutdown and alternatives you can deploy in your organization.

Who's impacted
Admins, end users, and developers

Why it's important
As soon as possible, review your organization's App Maker applications. App creators should review the uses cases listed in the Additional details section below and take action as necessary by the dates listed in the turndown schedule.

Additional details

Turndown schedule

App Maker will be disabled gradually according to the schedule below:

- **Today**, existing apps continue to work. Though App Maker is no longer under active development, the service will continue to be maintained.
- Starting **April 15, 2020**, you will no longer be able to create new App Maker apps. You will still be able to edit and deploy existing apps.
- Starting **January 19, 2021**, existing App Maker apps **will stop working** and you will no longer have access to them. App maker data stored in Cloud SQL will remain unchanged and continue to follow the policies established by your Google Cloud Platform (GCP) account.

Alternative solutions

Due to the specific source code used for App Maker, you can't directly migrate your apps to another platform. Depending on your use case, we recommend the following:

- **If you use App Maker to automate business processes**: Use AppSheet, a new addition to our application development portfolio that has capabilities similar to App Maker. App Maker data is stored in Cloud SQL, and App Sheet supports Cloud SQL databases. This allows you to build an application on the existing database tied to your App Maker app.
- **If you use App Maker to develop apps**: Use App Engine to build and deploy applications on a fully managed platform. App Maker data is stored in Cloud SQL, allowing you to build an App Engine application on the existing Cloud SQL database tied to your App Maker app.
- **If you use App Maker for data collection**: Use Google Forms, which has many new features that were not available when App Maker launched.

Deleting apps

If you no longer use apps created with App Maker, please follow these steps to fully delete each app:

- (Optional) Export the app before deleting to save database information.
- Delete the app in App Maker
- Delete the associated Cloud project.

Data retention

Your App Maker data belongs to your organization. App Maker user data is stored in CloudSQL and will continue to be retained according to the policies established by your GCP account. Data composing the App Maker app itself can be exported from within the App Maker editor until January 19, 2021.

Getting started

Admins: We recently emailed the primary admin in your domain and provided a CSV file with a list of the App Maker apps being used in your organization. This list includes the application name, creator name, and last modified date for each app. It also contains a link to your Admin console with application-specific usage stats and project information.

Notify app creators in your domain as necessary of the upcoming shutdown and alternative solutions.