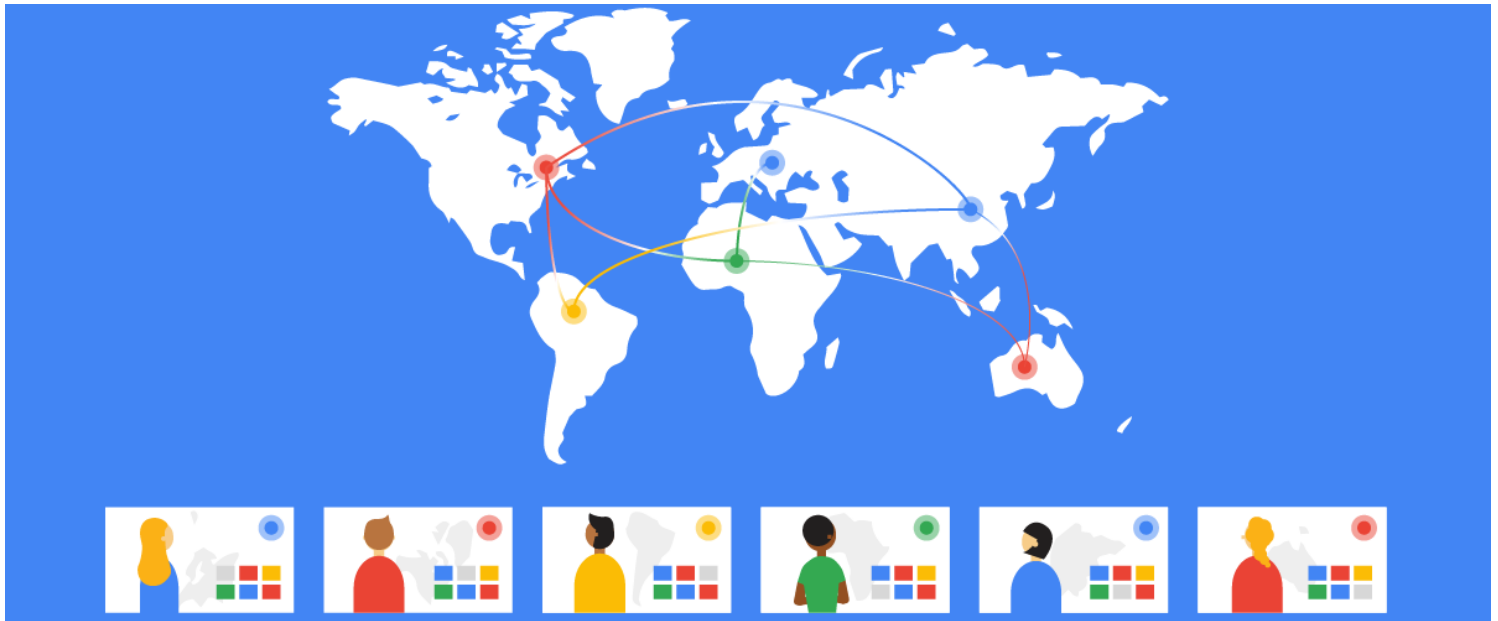


G SUITE

# Secure connections: How Google Meet keeps your video conferences protected



[Latest stories](#)

[Products](#)

[Topics](#)

[About](#)

[RSS Feed](#)

## Proactive protections to combat abuse and block hijacking attempts

Google Meet employs an array of counter-abuse protections to keep your meetings safe. These include anti-hijacking measures for both web meetings and dial-ins.

Google Meet makes it difficult to programatically brute force meeting IDs (this is when a malicious individual attempts to guess the ID of a meeting and make an unauthorized attempt to join it) by using codes that are 10 characters long, with 25 characters in the set. We limit the ability of external participants to join a meeting more than 15 minutes in advance, reducing the window in which a brute force attack can even be attempted. External participants cannot join meetings unless they're on the calendar invite or have been invited by in-domain participants. Otherwise, they must request to join the meeting, and their request must be accepted by a member of the host organization.

In addition, we're [rolling out](#) several features to help schools keep meetings safe and improve the remote learning experiences for teachers and students, including:

- Only meeting creators and calendar owners can mute or remove other participants. This ensures that instructors can't be removed or muted by student participants.
- Only meeting creators and calendar owners can approve requests to join made by external participants. This means that students can't allow external participants to

[Latest stories](#)[Products](#)[Topics](#)[About](#)[RSS Feed](#)

*Request and approval to join a meeting*

## Secure deployment and access controls for admins and end-users

To limit the attack surface and eliminate the need to push out frequent security patches, Google Meet works entirely in your [browser](#). This means we do not require or ask for any plugins or software to be installed if you use Chrome, Firefox, Safari, or Microsoft Edge. On mobile, we recommend that you install the Google Meet app.

To help ensure that only authorized users administer and access Meet services, we support multiple 2-Step Verification options for accounts that are secure and convenient. These include [hardware](#) and [phone-based](#) security keys and [Google prompt](#). Additionally, Google Meet users can enroll their account in our [Advanced Protection Program](#) (APP), which provides our [strongest protections](#) available against phishing and account hijacking and is specifically designed for the highest-risk accounts.

For G Suite Enterprise and G Suite for Education customers, we offer [Access Transparency](#), which logs any Google access to Google Meet recordings stored in Drive, along with the reason for the access (support team actions that you might have requested, for example). Customers can also use [data regions functionality](#) to store select/covered data of Google Meet recordings in specific regions (i.e. US or Europe).

[Latest stories](#)[Products](#)[Topics](#)[About](#)[RSS Feed](#)

- **Compliance certifications:** Our Google Cloud products, including Google Meet, regularly undergo independent verification of their security, privacy, and compliance controls, including validation against standards such as [SOC](#), [ISO/IEC 27001/17/18](#), [HITRUST](#), and [FedRAMP](#). We support your compliance requirements around regulations such as [GDPR](#) and [HIPAA](#), as well as [COPPA](#) and [FERPA](#) for education.
- **Incident management:** We have a rigorous process for managing data and security incidents that specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting customer data.
- **Reliability:** Google's network is engineered to accommodate peak demand and handle future growth. Our network is resilient and engineered to accommodate the increased activity we've seen on Google Meet.
- **Transparency:** At Google Cloud, we're clear about our [commitments](#) regarding customer data: we process customer data according to your instructions; we never use customer data for advertising purposes; and we publish the locations of our Google data centers, which are highly available, resilient, and secure.

During COVID-19 and beyond, we will continue to protect Google Meet users and their data, and keep innovating with new features to make our tools helpful, secure, and safe.

---

#### RELATED ARTICLE

[Latest stories](#)[Products](#)[Topics](#)[About](#)[RSS Feed](#)



Get started

Blog

Menu ▾

Google

[Privacy](#) [Terms](#) [About Google](#) [Google Cloud Products](#)

Language ▾

 Help