Keith Ketover <keith@theketovers.com>

[ACTION REQUIRED] Some apps accessing Gmail data in your environment will be restricted beginning July 8 unless you take action

The G Suite Team <gsuite-noreply@google.com> Thu, Jun 13, 2019 at 3:53 PM
Reply-To: The G Suite Team <gsuite-noreply@google.com>
To: keith@theketovers.com

G Suite

Hello Administrator,

Your security and privacy are extremely important to Google. In order to better protect your data and help reduce the risk of data loss, we are making an important update to our policies governing third-party apps (web, Android, iOS, Chrome, and other apps) accessing your organization's Gmail data using G Suite APIs and OAuth2.

We've previously announced that apps accessing user data for non-enterprise accounts using certain Gmail APIs must be verified to ensure compliance with new privacy and security requirements using our OAuth API Application Verification. Starting on **July 8, 2019**, we will apply similar requirements for apps you may use within your domain.

What does this mean for my organization?

While existing unverified apps will continue to work for users who have installed them before July 8, after this date **we will be blocking new installs** for unverified third-party apps that access Gmail data and that you don't explicitly trust (whitelist) in the G Suite Admin console.

What do I need to do?

1. **Review unverified apps in your environment**: Please review the unverified apps currently in use in your organization's G Suite environment, and decide which apps you want to trust and allow users to continue to install. We have included a list of the unverified apps at the end of this email, including the number of users and whether or not you have trusted them in API Permissions.
2. **Trust apps that you want to allow users to continue to install:** To trust an app, use our API Permissions (OAuth apps whitelisting) feature in the Security section of Google Admin. Trusting an app also means that, if users consent, the app will have access to some G Suite user data (OAuth2 scopes) that you have otherwise restricted using this same tool. For example, if you have generally blocked access to Gmail OAuth2 scopes, trusted apps will have access for accounts where users consent.

We also recommend that you review your OAuth ecosystem more broadly by taking advantage of these best practices.

FAQs

1. **Why would an app be unverified?** Apps may not have completed the verification process for numerous reasons, some of the more common ones being an unsupported Application Type or using data in a way that is incompatible with Limited Use requirements. We have implemented this verification process to help provide users both confidence and consistency with their privacy expectations. As apps are verified, we will post updates on this FAQ.
2. **If I am an app developer as well as a user, how do I get an app verified?** Review the OAuth API Application Verification FAQ and submit a request for verification from the API Developer Console.
3. **What will happen to unverified apps after July 8?** Users who have installed unverified apps before July 8 will continue to have access to them, unless you restrict access to G Suite APIs in the Security section of the Google Admin console. New users will not be able to install unverified apps unless you trust them using the OAuth apps whitelisting feature (API Permissions).
4. **What happens when I trust an app?** Users that haven't already installed it before July 8 will now be able to install it, whether or not the app is verified by Google. Additionally, the app will have access to any G Suite APIs (OAuth2 scopes) that you have restricted using the API Permissions settings.
5. **What if I don't want to trust any apps?** If you take no action, new users will be blocked from accessing unverified third-party apps that access Gmail data beginning July 8. Additionally, you can further restrict, limit or block access by

all apps, including previously installed apps, to Gmail by using API Permissions.

We’re here to help

If you have additional questions or need assistance, please contact G Suite support. When you call or submit your support case, reference issue number 132979135. We’ve also announced these changes on G Suite Updates.

Sincerely,

The G Suite Team

Unverified Apps in your Domain

The following are unverified apps in your domain that will be restricted for installation starting July 8. Included in this list are apps that are both trusted and untrusted by your Organization. Internal apps that were created by users in your Organization may also be listed. This list is subject to change as apps leave the list when they complete the verification process and are added to the list based on new usage by your users or newly identified non-compliance. For a complete list of all apps accessing OAuth2 scopes in your domain, please review API Permissions in Google Admin.

App Name	OAuth2 Client ID	User Count	Users in Last 30 Days	Trusted Status
SMS Backup+	959061759285-uqnem9qtjr97856o7b6pkuek0ref5dnd.apps.googleusercontent.com	1	0	No

Was this information helpful?

YES NO

You have received this important update about your G Suite account because you designated this email address as a primary or secondary contact for mandatory service communications in your Google Admin console profile.