

Multi-party approval for sensitive actions

Supported editions for this feature: *Enterprise Standard and Enterprise Plus; Education Standard and Education Plus; Enterprise Essentials Plus*. [Compare your edition](/admin/getting-started/editions/compare-google-workspace-editions) (/admin/getting-started/editions/compare-google-workspace-editions)

As a Google Workspace administrator, you can protect against malicious actions in the Google Admin console by using multi-party approval. When multi-party approval is on, a second administrator must approve changes to sensitive settings.

You can use multi-party approval for certain security, Google Groups, Domains, Google Calendar, and Google Vault settings. To review all Admin console settings that multi-party approval can protect, go to [Multi-party approval settings](#) (#index) (later on this page).

Note: Apps and services can also access certain Admin console settings through APIs. Separate multi-party approvals protect sensitive actions performed through public API calls.

Before you begin

- To review requests for sensitive Admin console actions, any admin who isn't a super administrator must have either the **Can review Multi-Party Approvals for all sensitive actions** privilege or the privilege required to perform the sensitive action.
- If you turn off multi-party approval for your organization, pending requests remain active until they are approved, denied, canceled, or expire.
- If multi-party approval is turned on in a resold customer's domain, and a reseller admin tries to update a sensitive setting, the approval request is sent only to the resold admins. Only these admins can approve, deny, or view the request.

Step 1: Turn multi-party approval on or off

You must be signed in as a [super administrator](/admin/users/prebuilt-administrator-roles#super_admin) (/admin/users/prebuilt-administrator-roles#super_admin) for this task.

1. In the Google Admin console, go to Menu



Security



Authentication



Multi-party approval settings.

Go to Multi-party approval settings (<https://admin.google.com/ac/managedsettings/352555445522/multiartyapprovalsettings>)

2. Click **Multi-party approval settings**.
3. Check or uncheck the **Require multi-party approval for sensitive actions** box.
4. Click **Save**.

5. Click a settings category and a setting. [Learn about the settings](#) (#index) (later on this page).
6. To require multi-party approval for a setting, check the box.
7. Click **Save**.

Step 2: Give admins multi-party approval privileges

You must be signed in as a [super administrator](/admin/users/prebuilt-administrator-roles#super_admin) (/admin/users/prebuilt-administrator-roles#super_admin) for this task.

1. [Create one or more custom admin roles](/admin/users/create-edit-and-delete-custom-admin-roles) (/admin/users/create-edit-and-delete-custom-admin-roles), each of which includes the multi-party approval privileges you want admins to have.

Tip: Some Admin console actions require being a super admin, such as turning 2-Step Verification (2SV) on or off. If multi-party approval is turned on for one of these actions, a second super admin must review any associated multi-party approval requests. For details, go to [Make a user a super admin](/admin/users/make-a-user-an-admin#make_user_superadmin) (/admin/users/make-a-user-an-admin#make_user_superadmin).

2. Assign the custom admin role that you created in step 1 to one or more admins. For details, go to [Assign specific admin roles](/admin/users/assign-specific-admin-roles) (/admin/users/assign-specific-admin-roles).
3. Save the role configuration that you assigned in step 2.

Step 3: Review multi-party approval requests

You can review multi-party approval requests that you created, as well as requests from others that you're authorized to review.

1. In the Google Admin console, go to Menu



Security



Authentication



Multi-party approval requests.

Go to Multi-party approval requests (<https://admin.google.com/ac/list/security/mpa>)

You must be signed in as a [super administrator](/admin/users/prebuilt-administrator-roles#super_admin) (/admin/users/prebuilt-administrator-roles#super_admin) for this task.

2. To approve or deny a request, click the request name
>
Approve request or **Deny request**.
3. To cancel a request that you submitted, click **Requests submitted**
>
request name
>
Cancel request.

Multi-party approval settings

Multi-party approval for security settings

> 2-Step Verification

Check the box to require multi-party approval for changes to your organization's 2SV settings. A super admin must approve the request. For details, go to [Protect your business with 2-Step Verification](/admin/security/protect-your-business-with-2-step-verification) (/admin/security/protect-your-business-with-2-step-verification).

> Account recovery

Requires multi-party approval to change your organization's account recovery settings. A super admin must approve the request. For details, go to [Set up password recovery for users](/admin/users/set-up-password-recovery-for-users) (/admin/users/set-up-password-recovery-for-users).

> Google session control

Requires multi-party approval to change your organization's Google session control settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review security actions
- Security > Control security settings read and write

For details, go to [Set session length for Google services](/admin/security/set-session-length-for-google-services) (/admin/security/set-session-length-for-google-services).

> Advanced Protection Program

Requires multi-party approval to change your organization's Advanced Protection Program settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review security actions
- Security > Control security settings read and write

For details, go to [Protect users with the Advanced Protection Program](/admin/security/protect-users-with-the-advanced-protection-program) (/admin/security/protect-users-with-the-advanced-protection-program).

> Login challenges

Requires multi-party approval to change your organization's login challenges settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions

- Multi Party Approval > Review security actions
- Security > Control security settings read and write

For details, go to [Protect Google Workspace accounts with security challenges](#) (/admin/security/protect-google-workspace-accounts-with-security-challenges).

> Passwordless

Requires multi-party approval to change your organization's passwordless settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review security actions
- Security > Control security settings read and write

For details, go to [Allow users to skip passwords at sign-in](#) (/admin/users/allow-users-to-skip-passwords-at-sign-in).

> Domain-wide delegation

Requires multi-party approval to change your organization's domain-wide delegation settings. A super admin must approve the request. For details, go to [Control API access with domain-wide delegation](#) (/admin/apps/control-api-access-with-domain-wide-delegation).

> SSO with third-party identity provider (IdP)

Requires multi-party approval to change your organization's single sign-on (SSO) with third-party IdP settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review security actions
- Security > Control security settings read and write
- Security > Control inbound SSO settings read and write

For details, go to [Setting up SSO](#) (/admin/apps/setting-up-sso).

> Context-Aware Access

Requires multi-party approval to change your organization's Context-Aware Access settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review security actions
- Security > Data Security > Access Level Management

For details, go to [Turn on and turn off Context-Aware Access](#) (/admin/security/deploy-context-aware-access#turn-on-and-off).

Multi-party approval for API access to security settings

> SSO with third-party IdP

Requires multi-party approval to change your organization's SSO with third-party IdP settings through an API. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review security actions
- Security > Control security settings read and write
- Security > Control inbound sso settings read and write

Multi-party approval for domains admin settings

> Domains API

Requires multi-party approval for these sensitive domain settings:

- [Add a user alias domain or secondary domain](#) (/admin/domains/add-a-user-alias-domain-or-secondary-domain)
- [Change your primary domain for Google Workspace](#) (/admin/domains/change-your-primary-domain-for-google-workspace)
- [Remove a domain from your managed Google Account](#) (/admin/domains/remove-a-domain-from-your-managed-google-account)

A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review domain actions
- Admin API privileges > Domain Management

Multi-party approval for calendar settings

> Calendar sharing

Requires multi-party approval to change your organization's Calendar sharing settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review calendar actions

- Calendar > All Settings > Manage settings

For details, go to [Set Google Calendar sharing options](/admin/calendar/set-google-calendar-sharing-options) (/admin/calendar/set-google-calendar-sharing-options).

> General Calendar settings

Requires multi-party approval to change your organization's Calendar general settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review calendar actions
- Calendar > All Settings > Manage settings

For details, go to [Manage Calendar for your users](/admin/calendar/manage-calendar-for-your-users) (/admin/calendar/manage-calendar-for-your-users).

> Calendar third-party archiving settings

Requires multi-party approval to change your organization's Calendar third-party archiving settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review calendar actions
- Third Party Archiving > Manage Third Party Archiving Settings

For details, go to [Integrate Calendar with a third-party archiving solution](/admin/calendar/integrate-calendar-with-a-third-party-archiving-solution) (/admin/calendar/integrate-calendar-with-a-third-party-archiving-solution).

Multi-party approval for groups settings

> Groups sharing

Requires multi-party approval to change your organization's Groups for Business sharing settings. A super admin, or an admin with one of the following privileges, must approve the request:

- Multi Party Approval > Can review multi-party approvals for all sensitive actions
- Multi Party Approval > Review Groups actions
- Groups for Business > Groups service settings

For details, go to [Set organization-wide policies for using groups](/admin/groups/set-organization-wide-policies-for-using-groups) (/admin/groups/set-organization-wide-policies-for-using-groups).

Multi-party approval for Vault settings

> Create export

Requires multi-party approval to change your organization's Google Vault export settings. A super admin, or an admin with the Multi Party Approval > Can review multi-party approvals for all sensitive actions > Review Vault actions privilege must approve the request.

For details, go to [Set up Multi-party approval for Vault exports](https://support.google.com/vault/answer/2584132#MPA_vault_exports)
(https://support.google.com/vault/answer/2584132#MPA_vault_exports).

Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0) (<https://www.apache.org/licenses/LICENSE-2.0>). For details, see the [Google Developers Site Policies](https://developers.google.com/site-policies) (<https://developers.google.com/site-policies>). Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2026-07-17 UTC.