BitGo

The Admin Console User Guide

Welcome to the BitGo Admin Console

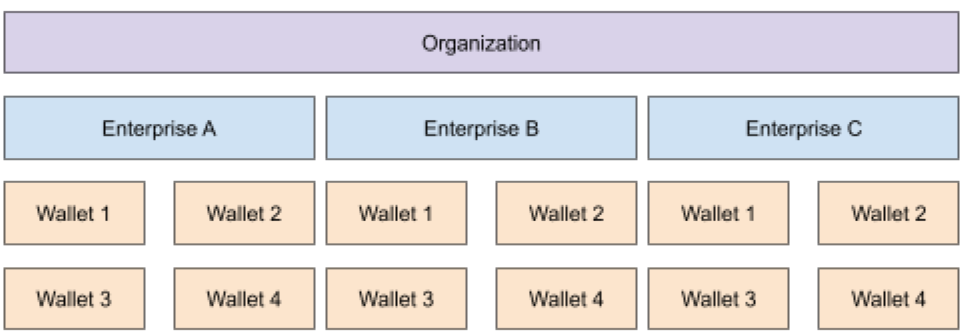
The Admin Console is a powerful tool designed to help you manage your users' roles and permissions in one place within the BitGo platform. This centralized dashboard provides an adaptable framework for user management that can be easily scaled or modified to meet your needs. Easily onboard new members, offboard members, and update permissions from an intuitive interface while maintaining complete control and visibility into who can do what within your organization.

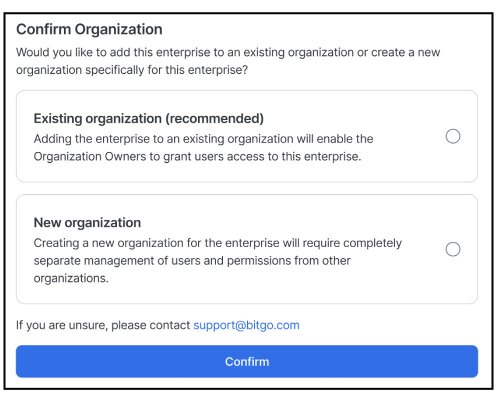
> ⭐ Before getting started, [watch this short walkthrough video](#) (less than four minutes) that takes you through the different features of the Admin Console.

Admin Console Basics

Architecture

An Organization groups multiple Enterprises together to allow streamlined role and permission management. An Enterprise groups wallets together and allows for easier wallet management.





If your company adds/creates new enterprises these can be added to an existing Organization (recommended) or you can create a new Organization to add it to.

Access

The Admin Console can only be accessed by **Organization Admin** to manage their organization's users. If an Organization Admin is tied to multiple Organizations, they will have the ability to switch between Organizations from the Admin Console as well.

KYC

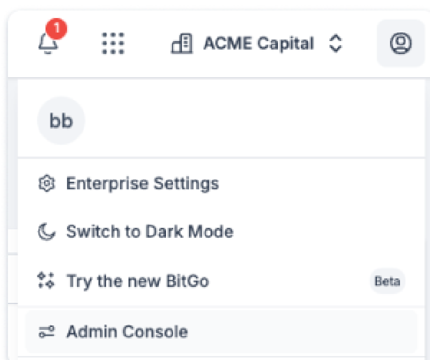
All members within an organization, including the Organization Admins, are required to fulfill know-your-client (KYC) requirements for each enterprise that they have access to. Additionally, if the organization has enterprises that span multiple jurisdictions, its members will be required to fulfill the highest level of requirements depending on the jurisdiction.

Members

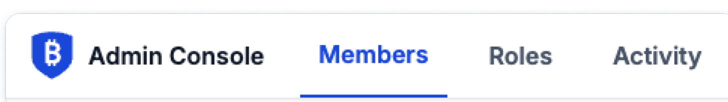
Members can belong to multiple organizations and be assigned to Default or Custom roles with specific permissioning across wallets and enterprises in the Organization. For more information on roles and permissions, refer to the Roles and Permissions section.

Getting Started (Quick Start)

- Access the Admin Console by clicking the profile icon in the top right corner



- The three tabs within the Admin Console allow you to see the following information:



    - Members = these are all users within your organization along with their permissions and access
    - Roles = these are all of the roles in use for your organization, here you can see:
        - What permissions the role provides
        - Which enterprises and wallets are covered by this role
        - And which members are assigned to this role
    - Activity = pending changes to your organization awaiting approval
- A note on roles:

- BitGo creates **default roles** for you to utilize. These have a default set of permissions and access that will apply to current and future enterprises and wallets within the organization. This is meant to provide you with a quick and easy way to manage users at scale. They cannot be modified or deleted.
  - You also have the option to create **custom roles** better suited for your organization. These allow you to have more control over permissions and access.
  - For more information about roles and permissions, review Roles and Permissions Matrix in the Appendix.
- Once you have reviewed the default roles and/or created custom roles, you can start adding members to them which will grant them access and permissions.

Roles and Permissions

Default Roles and their Permissions

Default roles have been created to enable faster onboarding. Members who belong to default roles will be automatically added to all new wallets and enterprises in the organization with the respective permissions. The default roles have the following permissions across all wallets and enterprises.

- Organization Admin = a member managing user permissions and access
- Enterprise Admin = a member creating wallets within the enterprise, managing enterprise-level policies
- Wallet Admin = a member managing wallet-level policies and whitelist
- Wallet Spender = a member initiating transactions
- Wallet Trader = a member initiating trades, can also view all wallets in the enterprise
- Viewer = a member view wallet balances and transactions
- Auditor = a member viewing activity logs

For more information about roles and permissions, please refer to the Roles and Permissions Matrix in the Appendix.

Creating a Custom Role

If you determine that custom roles need to be created for your organization, this can be done by the Organization Admins. Once the custom role is created you can add members to it. This will require approval if your organization has more than one Organization Admin.

BitGo

- Click on the Roles tab
- Click on Create Role
- Name the Role
- Select the permissions that you want this role to have
- Select the Enterprises that you want these permissions to apply to
    - All Enterprises = All enterprises that exist today and all future enterprises that are added the organization
    - Select Enterprises = If you only want this role to apply to certain enterprises
- Choose to grant access to all wallets, or individually pick specific wallets for each enterprise:
    - All Wallets = All wallets that exist today and all future wallets that are added the enterprise
    - Select Wallets = If you only want certain wallets within the respective enterprise

Roles that apply to “all enterprises” and “all wallets” will be applied to all existing enterprises and wallets as well as any new enterprises and wallets that are added to the organization in the future.

When to Use Default vs. Custom Roles

Here are some things to consider when determining whether to leverage BitGo’s default roles for your organization or create custom roles:

- Do the default roles have the correct set of permissions?
- Should members in these roles have these permissions across enterprises and wallets, now and in the future?
- Are the default roles sufficient?
- Does my organization require a unique combination of permissions and/or wallet and enterprise access?

Updating Roles

Only **<u>ONE</u>** update can be made to a role at a time. This update must be approved before other updates can be made to the same role. For example, if you want to add members, remove members and update permissions, you will only be able to do one after the other.

Note:

- Members must already exist to be added to a role in the Roles tab. If they are not in the Organization yet, they can be added from the Members tab.
- Custom roles can be deleted from the Roles tab by going into the Role and clicking Delete Role. This will remove the associated access from all users with that role.
- Every member must have at least one role to remain in an Organization.

BitGo

Removing Members

Members can be removed from your organization on the Members tab of the Admin Console. Click Edit Member next to the member that you wish to remove then click Remove Member from Organization.

A note on self-custody wallets:

- If you are removing a member who is the last key holder of a self-custody wallet, removing this user could freeze access to this wallet and funds could be lost. Ensure another member has key access to this wallet before proceeding. See Self-Custody Wallet Sharing for more information.

Organization Management

Creating a New Wallet

When a new wallet is created:

- The wallet will be added to the Admin Console
- The wallet will be available to select when establishing or updating roles
- Any member that has access to “All Wallets” within their roles will be granted access to the newly created wallet.
- If the creator of the wallet belongs to a custom role with Enterprise Admin and does not have “All Wallets” selected, the wallet will be added to the custom role.

Members that have the ability to create wallets may not automatically be Wallet Admins. This requires the necessary permission within the role. See the Roles and Permissions Matrix in the Appendix for more information.

A note on self-custody wallets:

- Due to the nature of self-custody wallets keys, self-custody wallets will need to manually be shared with any members in a “Spender” role. See Self-Custody Wallet Sharing for more information.

Creating a New Enterprise

When you onboard with BitGo you will be able to create your new enterprise(s). If you are an existing client you can reach out to the BitGo team to create a new enterprise.

BitGo

When a new enterprise is created it will need to be added to an organization to be able to manage members in a consistent manner. This also means that when a new enterprise is created:

- Primary Contacts have the ability to add a newly created enterprise to a new or existing organization
- Organization Admins will need to add or remove members to the enterprise
- Any members that belong to a role with “All Enterprises” will be granted access to this new enterprise

Creating a New Organization

You will have the option to create a new organization when creating a new enterprise. If an enterprise is added to a new Organization vs. an existing one, this means that there will be completely separate management of members and roles between the two Organizations.

Self-Custody Hot Wallet Sharing

Self-custody hot wallets are unique because one of the private keys is encrypted to the user’s password. This means that any member with spend permission on a hot wallet needs to enter their password when:

- Creating a self-custody hot wallet = Enterprise Admins that create wallets are the first member with the private key encrypted against their password. Once the wallet is created, a key sharing request will be generated for this member to access from the Activity page. They will need to share this wallet with all other members in the Organization with Spend permissions on “All Wallets.”

- Sharing a self-custody hot wallet = if you are currently a “key holder” (i.e., you have permission to spend from a self-custody wallet), then you will be responsible for sharing the wallet with other team members when they are added to a role that grants them spend permission on the wallet. You can do this by accessing the Activity page within each enterprise. Until a key has been shared, users will be added to wallets as Viewers. Once the key is shared, members will be updated to a Spender.

- Receiving a self-custody hot wallet share = Once you have been added to a role that has Spend permission on a self-custody wallet and a key holder has shared the wallet, you will need to accept the share from the Activity page within each enterprise. You will also need to ensure that you log into the BitGo platform at least once before the key can be shared with you. If you have not logged in your pubKey has not been created which will not make key sharing possible.

Things to Note about Self-Custody Key Sharing

- Although member management is done in the Admin Console, key sharing happens **within the enterprise**.
- Enter a wallet password one-by-one and we will apply it to all of the wallets that use that password. Continue entering new wallet passwords until you complete all shares.
- You do not need to be an Organization Admin to share a self-custody wallet key. You do however need to be a current or previous Wallet Spender.

Activity

The Activity tab allows you to monitor platform activity as it happens so you can stay informed, ensure accountability, and quickly identify anything unusual. Review, approve or reject pending actions directly from this screen.

Approvals

If your organization has at least two Organization Admins, the following actions will require one approval by default:

- Inviting a member
- Removing a member
- Creating a role
- Editing a role
- Deleting a role
- Adding a user to a role
- Removing a user from a role

Appendix

For more information about the different roles and permissions within the BitGo platform, refer to the Roles and Permissions Matrix below.