Orgs, Spaces, Roles, and Permissions

CF uses a role-based access control (RBAC) system to grant Cloud Foundry users permissions appropriate to their role within an org or a space. This topic describes how orgs and spaces work within a CF deployment, and how different Cloud Foundry User roles operate within those contexts.

Admins, Org Managers, and Space Managers can assign user roles using the cf CLI.

💡 **Note**: Before you assign a **space role** to a user, you must assign an **org role** to the user.

Orgs

An org is a development account that an individual or multiple collaborators can own and use. All collaborators access an org with user accounts. Collaborators in an org share a resource quota plan, applications, services availability, and custom domains.

By default, an org has the status of *active*. An admin can set the status of an org to *suspended* for various reasons such as failure to provide payment or misuse. When an org is suspended, users cannot perform certain activities within the org, such as push apps, modify spaces, or bind services. For details on what activities are allowed for suspended orgs, see Roles and Permissions for Suspended Orgs.

User Accounts

A user account represents an individual person within the context of a CF installation. A user can have different roles in different spaces within an org, governing what level and type of access they have within that space.

Before you assign a space role to a user, you must assign an org role to the user. The error message `Server error, error code: 1002, message: cannot set space role because user is not part of the org` occurs when you try to set a space role before setting an org role for the user.

Spaces

Every application and service is scoped to a space. An org can contain multiple spaces. A space provides users with access to a shared location for application development, deployment, and maintenance. Each space role applies only to a particular space.

Roles and Permissions

A user can have one or more roles. The combination of these roles defines the user's overall permissions in the org and within specific spaces in that org. Roles can be assigned different scopes of User Account and Authentication (UAA) privileges. For more information about UAA scopes, see Scopes in *Component: User Account and Authentication (UAA) Server*.

For non-admin users, the `cloud_controller.read` scope is required to view resources, and the `cloud_controller.write` scope is required to create, update, and delete resources.

- **Admin** is a user role that has been assigned the `cloud_controller.admin` scope in UAA. An admin user has permissions on all orgs and spaces and can perform operational actions using the Cloud Controller API. To create an account with `cloud_controller.admin` scope for your installation, see the Create an Admin User topic.
- **Admin Read-Only** is a user role that has been assigned the `cloud_controller.admin_read_only` scope in UAA. This role has read-only access to all Cloud Controller API resources.
- **Global Auditor** is a user role that has been assigned the `cloud_controller.global_auditor` scope in UAA. This role has read-only access to all Cloud Controller API resources except for secrets such as environment variables. The Global Auditor role cannot access those values.
- **Org Managers** are managers or other users who need to administer the org.
- **Org Auditors** view but cannot edit user information and org quota usage information.
- **Org Billing Managers** create and manage billing account and payment information.

💡 **Note**: The Billing Manager role is only relevant for Cloud Foundry environments deployed with a billing engine.

- **Org Users** can view the list of other org users and their roles. When an Org Manager gives a person an Org or Space role, that person automatically receives Org User status in that Org.

- **Space Managers** are managers or other users who administer a space within an org.
- **Space Developers** are application developers or other users who manage applications and services in a space.
- **Space Auditors** view but cannot edit the space.

Roles and Permissions for Active Orgs

The following table describes the permissions for various CF roles.

Activity	Admin	Admin Read-Only	Global Auditor	Org Manager	Org Auditor	Org Billing Manager	Org User	Space Manager	Space Developer	Space Auditor
Scope of operation	Org	Org	Org	Org	Org	Org	Org	Space	Space	Space
Assign user roles	✓			✓				✓		
View users and roles	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Create and assign org quota plans	✓									
View org quota plans	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Create orgs	✓			*	*	*	*	*	*	*
View all orgs	✓	✓	✓							
View orgs where user is member	✓**	✓**	✓**	✓	✓	✓	✓	✓	✓	✓
Edit, rename, and delete orgs	✓			✓⁂						
Suspend or activate an org	✓									
Create and assign space quota plans	✓			✓						
Create spaces	✓			✓						
View spaces	✓	✓	✓	✓				✓	✓	✓
Edit spaces	✓			✓				✓		
Delete spaces	✓			✓						
Rename spaces	✓			✓				✓		
View the status, number of instances, service bindings, and resource use of applications	✓	✓	✓	✓				✓	✓	✓
Add private domains†	✓			✓						
Share private domains with other orgs	✓			✓§						
Deploy, run, and manage applications	✓								✓	
Instantiate and bind services to applications	✓								✓	
Associate routes†, instance counts, memory allocation, and disk limit of applications	✓								✓	
Rename applications	✓								✓	
Create and manage Application Security Groups	✓									
Create, update, and delete an Isolation Segment	✓									
List all Isolation Segments for an Org	✓	✓	✓‡	✓‡	✓‡	✓‡	✓‡	✓‡	✓‡	✓‡
Entitle or revoke an Isolation Segment	✓									
List all Orgs entitled to an Isolation Segment	✓	✓	✓‡	✓‡	✓‡	✓‡	✓‡	✓‡	✓‡	✓‡
Assign a default Isolation Segment to an Org	✓			✓						
List and manage Isolation Segments for spaces	✓			✓						
List entitled Isolation Segment for a space	✓	✓	✓	✓				✓	✓	✓

List which Isolation Segment an app runs on	✓	✓	✓	✓				✓	✓	✓
List application and service usage events	✓	✓	✓						✓	✓

[*]Not by default, unless feature flag `user_org_creation` is set to `true`.

[**]Admin, admin read-only, and global auditor roles do not need to be added as members of orgs or spaces to view resources.

[†]Unless disabled by feature flags.

[‡]Applies only to orgs they belong to.

[§]The user attempting to share must have permissions in both the source and target orgs.

[⁂]Org Managers can rename their orgs and edit some fields; they cannot delete orgs.

Roles and Permissions for Suspended Orgs

The following table describes roles and permissions applied after an operator sets the status of an org to *suspended*.

User Role	Admin	Admin Read-Only	Global Auditor	Org Manager	Org Auditor	Org Billing Manager	Org User	Space Manager	Space Developer	Space Auditor
Scope of operation	Org	Org	Org	Org	Org	Org	Org	Space	Space	Space
Assign user roles	✓									
View users and roles	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Create and assign org quota plans	✓									
View org quota plans	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Create orgs	✓									
View all orgs	✓	✓	✓							
View orgs where user is a member	✓[**]	✓[**]	✓[**]	✓	✓	✓	✓	✓	✓	✓
Edit, rename, and delete orgs	✓									
Suspend or activate an org	✓									
Create and assign space quota plans	✓									
Create spaces	✓									
View spaces	✓	✓	✓	✓				✓	✓	✓
Edit spaces	✓									
Delete spaces	✓									
Rename spaces	✓									
View the status, number of instances, service bindings, and resource use of applications	✓	✓	✓	✓				✓	✓	✓
Add private domains[†]	✓									
Deploy, run, and manage applications	✓									
Instantiate and bind services to applications	✓									
Associate routes[†], instance counts, memory allocation, and disk limit of applications	✓									
Rename applications	✓									
Create and manage Application Security Groups	✓									

[†]Unless disabled by feature flags.

[**]Admin, admin read-only and global auditor roles do not need to be added as members of orgs or spaces to view resources.