Account Roles, Tiers, and Permissions

Admin · https://coreel.ai/help/account-roles-tiers-and-permissions/

This guide explains who can do what in coReel and how account tier affects feature access.

Roles Overview

Each user in an organization has a role:

- **Owner**
- **Manager**
- **User**

Role controls what actions a person can perform.

Tier controls which features are available to the organization.

Owner Permissions

Owners typically have full control, including:

- Manage billing/subscription
- Upgrade/downgrade/reactivate account
- Manage organization settings
- Add/remove users
- Manage organization-level controls (including extension controls, where enabled)
- Connect/disconnect organization-level integrations

Manager Permissions

Managers can usually:

- Add/manage users (based on org policy)
- Manage selected org settings
- Perform many integration management tasks

Managers typically cannot perform full owner-only billing/subscription actions unless explicitly allowed.

User Permissions

Standard users can:

- Use assigned product features
- Record/send videos (if enabled by plan + account state)
- Use integrations already configured for their access scope

Users generally cannot manage billing, org-wide settings, or org-level integration administration.

Account Tiers (Feature Access)

coReel has multiple account tiers (for example: Starter/Business/Premium based on your account model).
Key points:

- Some features are available only on higher tiers.
- Tier is applied at the **organization account level**.
- Users in the org inherit access based on that account tier.

Trial Behavior

- Trial accounts map to Premium-level access during trial.
- Trial is time-limited (for example, 30 days in your current setup).
- After trial, an active paid subscription is required to retain full access.

Source of Truth for Tier

Account level is determined from subscription plan data (Keap plan ID) at the account-owner level and stored for organization use.

In practice:

- Tier is synced on key events (login sync/webhook updates).
- App uses stored account-level value for normal feature checks.
- This avoids unnecessary per-request plan lookups.

Extension Access and Permissions

The Chrome extension is available across tiers, but:

- Feature availability inside extension follows account tier/permissions.
- Owners/Managers can disable extension access at org level (if configured).
- If extension access is disabled, users cannot use extension functionality.

Integrations and Permissions

Integration behavior depends on role and account state:

- Organization-level integration actions may require Owner/Manager.
- If no active integration is connected, send/track features are restricted.
- Inactive subscription status may limit access to sending features.

Active vs Inactive Accounts

Active Account

- Full access according to tier + role.

Inactive Account (no active subscription)

- Access is restricted.
- Owners may still access account-related pages needed for reactivation.
- Sending/recording/video-email workflows may be limited until reactivated.

Common Permission Scenarios

“Why can my teammate log in but not send?”

Possible causes:

- No active integration
- Role limitation
- Tier limitation
- Account inactive

“Why can’t I disconnect a provider?”

- You may not be Owner/Manager for that provider’s management scope.

“Why does admin show Trial instead of Premium?”

- Trial may temporarily grant Premium-level features while still labeled as Trial status.

Best Practices

- Keep billing + critical integration ownership with Owner.
- Grant Manager role only to trusted operators.
- Review user roles quarterly.
- Document which features are tier-dependent for your team.

Need Help?

If permissions don’t match expectations, provide support with:

- Organization name
- User email + role
- Expected action vs actual behavior
- A screenshot of the blocked action or warning message