

User Management

Introduction

This page covers day-to-day user administration across the commercial hierarchy (platform, distributor, partner, tenant). It includes adding, editing, disabling, deleting users, assigning roles and scopes, and handling password/MFA resets.

The screenshot shows the CloudAxis Users management interface. The sidebar on the left contains navigation options: Dashboard, Notifications, Subscriptions, Billing, Relationships, Pricing, Settings, Regions, and Users. The main content area displays a table of users with the following columns: Role, Full Name, Description, Email Address, and Role Scope. The table contains three rows of user data.

Role	Full Name	Description	Email Address	Role Scope
Platform Administrator	Platform Admin	Default Platform Admin.	default@admin.local	All Relationships
Tenant Administrator	Hannah Lewis	Accounts Payable	hlewis@council.gov.au	City Council
Tenant Administrator	Simon Platt	CIO	splatt@council.gov.au	City Council

Add a new User

Purpose

Add a new user to the system.

Permission Level

- Platform Administrator
- Partner Administrator
- Distributor Administrator
- Tenant Administrator

Steps

1. Go to Settings→ Users.
2. Select Create.
3. Enter First Name, Last Name, Email Address, and optionally Phone Number.
4. Select User Role. Select Distributor, Partner, and Tenant to define the user's scope.
5. (Optional) Toggle MFA Required if your policy requires MFA at next sign-in.
6. (Optional) Toggle Federated Only to prevent local password login for this user.

7. Save.

Modify an existing User

Purpose

Modify an existing user's details, role, scope, or security options.

Permission Level

- Platform Administrator
- Partner Administrator
- Distributor Administrator
- Tenant Administrator

Steps

1. Go to Settings → Users.
 2. Select the user you want to edit.
 3. Update First Name, Last Name, Email Address, or Phone Number if required.
 4. Adjust User Role.
 5. Update Distributor, Partner, and Tenant scope as needed.
 6. Adjust toggles: MFA Required, Federated Only, Disabled, or Locked Out.
 7. Select Save.
-

Disable or Enable a User

Purpose

Temporarily block or restore user access without deleting the account.

Permission Level

- Platform Administrator
- Partner Administrator
- Distributor Administrator
- Tenant Administrator

Steps

- Go to Settings → Users.
 - Select the user you want to edit.
 - Toggle **Disabled** on to suspend, off to re-enable.
 - Select **Save**.
-

Unlock a User

Purpose

Clear a lockout after failed login attempts.

Permission Level

Platform Administrator
Distributor Administrator
Partner Administrator
Tenant Administrator

Steps

1. Go to Settings → Users.
 2. Select the user you want to edit.
 3. Unset the **Locked Out** indicator.
 4. Select **Save**.
-

Enforce MFA

Purpose

Require the user to register or re-register MFA at next sign-in.

Permission Level

Platform Administrator
Distributor Administrator
Partner Administrator
Tenant Administrator

Steps

1. Go to Settings → Users.
 2. Select the user you want to edit.
 3. Toggle **MFA Required** on.
 4. Select **Save**.
-

Force Federated Only

Purpose

Restrict the account to federated sign-in only (no local password).

Permission Level

Platform Administrator

Distributor Administrator
Partner Administrator
Tenant Administrator

Steps

1. Go to Settings → Users.
 2. Select the user you want to edit.
 3. Toggle **Federated Only** on.
 4. Select **Save**.
-

Delete a User

Purpose

Remove a user account permanently.

Permission Level

Platform Administrator
Distributor Administrator
Partner Administrator
Tenant Administrator

Steps

1. Go to Settings → Users.
 2. Select the user you want to delete.
 3. Choose **Delete**.
 4. Confirm the deletion.
-

Revision #4

Created 21 September 2025 11:57:18 by AutoBot

Updated 25 September 2025 03:19:20 by AutoBot