Cisco Cloud Control
RBAC

Table of Contents

Role-based access control

Cisco Cloud Control uses role-based access control (RBAC) to manage what users can view and do across Cisco Cloud Control and supported integrated products. RBAC helps ensure that users see only the features, data, and actions allowed by their assigned permissions.

RBAC controls access to these areas in Cisco Cloud Control:

- Pages and menu items
- Administrative actions
- Topology features
- Product-specific assets and services

If you do not have permission to access a feature, Cisco Cloud Control either hides the option or displays an access denied message.

Pages and menu items

Access to menu items and pages is controlled by role. Examples include the Admin Console and topology.

Administrative actions

Sensitive operations are limited to users with the required administrative privileges. Examples of restricted actions include the export of inventory data and the deletion of configurations.

Read-only users can view information but cannot perform edit or administrative actions.

Topology

Topology access is role-based. Users can have one of these experiences, depending on their role:

- Full access to topology features, including editing, deleting, and adding scopes or sites
- View-only access to topology, device details, and site information
- No topology access, with the menu item hidden and direct URL access denied

Supported roles

Cisco Cloud Control supports these roles:

Role	General access
Tenant Full Admin	Has the privileges necessary to configure and manage all tenant-level settings.
Tenant Read-Only	Can view all tenant-level settings, but cannot change them.
Integration Admin	Can manage cross-product and third-party integrations in Cisco Cloud Control, but does not have platform administration rights.

These roles determine which features, views, and actions are available to each user.

Product-specific access

Cisco Cloud Control integrates with product-specific RBAC for these products:

- Cisco Intersight
- Firewall
- Nexus Dashboard

A user can access only the assets and services that their source-product permissions allow. For example, if a user is an administrator in Cisco Intersight but does not have administrative access in Meraki, that user sees only the Cisco Intersight assets that are available through Cisco Cloud Control. This behavior helps maintain consistent access enforcement between Cisco Cloud Control and the integrated products it manages.

How RBAC works

Cisco Cloud Control applies RBAC at two levels:

- Cisco Cloud Control level
- Product level

Cisco Cloud Control retrieves user roles from the Cisco User Identity (CUI) service and includes those roles in the user access token. Cisco Cloud Control then uses those roles to control access to pages, menus, data, and actions.

For integrated products, Cisco Cloud Control also respects the permissions that a user has in the source product. This provides more granular control over which assets and services are visible in Cisco Cloud Control.

User and role management

Cisco Cloud Control unifies user management and role assignment for supported integrations. Administrators can manage user roles for integrated products, such as Nexus Dashboard, from the Cisco Cloud Control **Users** page instead of switching to separate management consoles. This includes assigning and revoking Nexus Dashboard roles for Cisco Cloud Control users.