



Roles and Permissions

Every user has one organization role. That role applies throughout Northstar Cloud. Team membership does not add permissions or restrict the role's access.

Role	Scope
Owner	Manages users, teams, reports, organization settings, and authentication. Can assign or remove the Owner role.
Administrator	Manages other Administrators and Members, teams, and reports. Cannot administer Owners or organization authentication.
Member	Manages their own profile, security, and notifications and views their own team memberships.

Compare Permissions

Capability	Owner	Administrator	Member
View own profile and memberships	Yes	Yes	Yes
Change own name and notifications	Yes	Yes	Yes
View user directory and all teams	Yes	Yes	No
Invite as Administrator or Member	Yes	Yes	No
Resend or revoke invitations	Yes	Yes	No
Create and Manage Teams	Yes	Yes	No
View roles reference and reports; export CSV	Yes	Yes	No
Edit organization settings	Yes	No	No
Configure SSO and MFA policy	Yes	No	No

Permissions for Account Changes

The following actions apply to other users. You cannot change your own role, deactivate yourself, or administratively reset your own multi-factor authentication (MFA).

Action	Owner	Administrator
Change Member to Administrator or reverse	Yes, for Active users	Yes, for Active users
Assign or remove Owner	Yes, for Active users	No
Deactivate or reactivate an Administrator or Member	Yes	Yes
Deactivate or reactivate another Owner	Yes, with Owner safeguards	No
Reset local MFA	Other users	Other Members only

Ownership Safeguards

An organization must always have at least one active Owner. Northstar blocks changes that would remove the last active Owner. Invitations can assign only **Administrator** or **Member**; an Owner can promote a user after activation.

Roles cannot be changed for Invited or Deactivated accounts. Role and status changes end the affected user's sessions. Unauthorized actions are hidden; temporarily unavailable actions are disabled with an explanation.

Personal MFA and Single Sign-On

Owners and Administrators must use local MFA for password sign-in and cannot disable it. Members may disable local MFA only when organization policy allows it. With single sign-on (SSO), MFA is managed by the identity provider.

Even when SSO is required, Owners retain password sign-in with local MFA as a recovery route.

Related guides: Manage Users; Configure SSO; Configure MFA.