



Northstar Cloud Documentation

Eliza Lenz | Technical Writing Portfolio

Fictional product sample | Product 1.1.0 | 29 September 2026

Twelve guides covering account administration, authentication, reporting, and sign-in recovery for a fictional B2B SaaS product.

Contents

About Northstar Cloud	2
Set Up Your Organization	3
Invite Your First Users	5
Manage Users	9
Create and Manage Teams	12
Roles and Permissions	15
Configure SSO	17
Configure MFA	20
Configure Notifications	23
Generate Activity Reports	24
Troubleshoot Sign-In Problems	26
Release Notes	29

AI-assisted working edition for editorial review. UI images are static illustrations.
No implemented application or production testing is represented.

Contents numbers refer to PDF pages. Each standalone guide retains its own numbering.



About Northstar Cloud

Northstar Cloud manages access to your organization's Northstar accounts. Use it to invite colleagues, assign roles, organize teams, configure sign-in requirements, and review administrative activity.

Fictional portfolio sample. This documentation describes an original, fictional product. Interface images are static mockup illustrations. Northstar Cloud is not an available service.

Find the Right Guide

Task	Guide
Review the organization and invite colleagues	Set Up Your Organization; Invite Your First Users
Change access or organize people	Manage Users; Create and Manage Teams; Roles and Permissions
Configure authentication	Configure SSO; Configure MFA
Choose personal email preferences	Configure Notifications
Investigate activity or sign-in issues	Generate Activity Reports; Troubleshoot Sign-In Problems
Review the latest changes, updates, and fixes.	Release Notes

Important Notes

- Each account belongs to one organization and has one role: **Owner**, **Administrator**, or **Member**. Roles determine permissions. Teams group people without changing their access.
- Owners configure organization and authentication settings. Owners and Administrators manage users, teams, and activity reports. Members manage their own profile, security, and notification preferences and view their team memberships.
- Northstar does not provision accounts in other applications. Its single sign-on connection is its only integration. Bulk imports, custom roles, nested teams, and scheduled reports are outside version 1.0.
- These guides assume your organization already exists. Start with **Set Up Your Organization** if you are its first Owner. The separate AI documentation triage project is not part of Northstar Cloud.



Set Up Your Organization

Review your organization's name before inviting colleagues. The organization is provisioned in advance; this procedure does not create a new organization or account.

Before You Begin

Sign in as an active **Owner**. Your initial Owner account already has a password and multi-factor authentication (MFA) configured. Administrators and Members cannot change organization settings.

Review the Organization Details

1. Open **Settings > Organization**.
2. Check **Organization ID** to confirm the organization you are administering. The ID is read-only.
3. If needed, update **Organization name**. Enter 2–80 characters; surrounding spaces are ignored.
4. Select **Save changes**.

A screenshot of the Northstar Cloud user interface showing the 'Organization' settings page. The page has a light blue header with the 'Northstar Cloud' logo on the left and the user's name 'Alder Field Services | Morgan Ellis' on the right. Below the header, the breadcrumb 'Settings / Organization' is shown. The main title 'Organization' is in a large, bold font. There are two input fields: 'Organization name' with the value 'Alder Field Services' and 'Organization ID (read-only)' with the value 'org_alder_001'. A note below the fields states: 'The organization ID does not change when you rename the organization.' A 'Save changes' button is located at the bottom right of the form area.

Northstar Cloud Alder Field Services | Morgan Ellis

Settings / Organization

Organization

Organization name Alder Field Services

Organization ID (read-only) org_alder_001

The organization ID does not change when you rename the organization.

Save changes

Organization settings with an editable name and read-only ID. Northstar Cloud 1.0 — fictional product mockup.

The updated name appears throughout Northstar. Changing the name does not change the organization ID.

Save changes is unavailable until you change a value.

Prepare for Onboarding

Choose how colleagues will sign in before sending invitations. Password sign-in is available by default. If you plan to require single sign-on (SSO), configure and test the connection first.

1. Review **Roles and Permissions** and decide which colleagues need administrative access.
2. If you use an identity provider, follow **Configure SSO** to test and enable the connection.
3. Review **Configure MFA** to decide whether to require MFA for Members who sign in with a password.
4. Follow **Invite Your First Users**. Use the same email address that your identity provider supplies if the person will use SSO.
5. After users accept their invitations, follow **Create and Manage Teams** to organize them.

Retain Owner Access

An organization must retain at least one active Owner. Invitations cannot assign the Owner role. After a colleague activates their account, an existing Owner can assign that role through user details.

Owners retain password sign-in with mandatory local MFA even when SSO is required. Keep your recovery codes available so you can use this recovery route if the identity provider is unavailable.

Dates and Times

Activity timestamps and report date ranges use UTC. There is no organization timezone setting.

Related guides: Invite Your First Users; Roles and Permissions; Configure SSO; Configure MFA.



Invite Your First Users

Invite colleagues to Northstar Cloud and assign the access they need. Invitations are sent individually and expire after seven days.

Before You Begin

You must have the **Owner** or **Administrator** role. Confirm the email address the person will use to sign in. For single sign-on (SSO), use the email address supplied by your identity provider.

Send an Invitation

1. Select **Users** in the sidebar, then select **Invite user**.
2. Enter the person's email address in **Email address**.
3. Select **Member** or **Administrator** from **Role**. **Member** is selected by default.

Members can view their own profile and team memberships and manage their personal settings.

Administrators can also manage users and teams and view and export activity reports. Administrators cannot manage Owners or configure organization authentication settings.

A screenshot of the "Invite user" dialog box. The title is "Invite user" in bold. Below it is a subtitle "Invite a colleague to Alder Field Services." There are two input fields: "Email address" with the value "alex.chen@example.com" and "Role" with a dropdown menu showing "Member". Below the dropdown is a note: "Members can view their own profile and team memberships." and another note: "The invitation expires after seven days." At the bottom are two buttons: "Cancel" and "Send invitation".

Invite user

Invite a colleague to Alder Field Services.

Email address

Role

Member

Members can view their own profile and team memberships.

The invitation expires after seven days.

CancelSend invitation

The Invite user dialog with Member selected.

4. Select **Send invitation**.

Check the Invitation

Northstar sends the invitation and adds the person to the user list with the status **Invited**. Their name appears after they accept the invitation.

Users

Manage access to your organization.

Invite user

Invitation sent to alex.chen@example.com.

Search users

Search by name or email address

Status

All statuses

Role

All roles

Name	Email address ↑	Role	Status	Last sign-in
—	alex.chen@example.com	Member	Invited	Never
Casey Tran	casey.tran@example.com	Member	Active	29 Sep 2026, 09:15 UTC
—	jordan.lee@example.com	Member	Invited	Never
Morgan Ellis	morgan.ellis@example.com	Owner	Active	29 Sep 2026, 13:40 UTC
Priya Shah	priya.shah@example.com	Administrator	Active	29 Sep 2026, 11:20 UTC
Rowan Bell	rowan.bell@example.com	Member	Deactivated	24 Sep 2026, 16:05 UTC

6 of 6 users

Previous

Next

The Users page after an invitation is sent.

The recipient opens the invitation, enters their name, and completes authentication. They create a password or use SSO, depending on your organization's settings. If SSO is required, they must use SSO.

For password sign-in, Administrators must set up multi-factor authentication (MFA). Members must set it up if your organization requires it. For SSO, MFA requirements are managed by the identity provider.

The user becomes **Active** after completing these steps. You can then add them to a team. An existing Owner can also assign the **Owner** role after activation; it is not available when sending an invitation.

Resend an Invitation

Resend an invitation if it has expired or the recipient needs a new link. Resending invalidates the previous link and starts a new seven-day acceptance period. Ask the recipient to use the newest invitation.

1. On **Users**, search for the email address. You can filter **Status** to **Invited**.
2. Select the email address to open the user details.
3. Select **Resend invitation**.

alex.chen@example.com

Role: Member · Status: Invited

Teams: None

Invitation expires: 6 October 2026, 14:00 UTC

CloseResend invitationRevoke invitation

A pending invitation with resend and revoke actions.

An expired invitation retains the **Invited** status and displays an **Expired invitation** indicator.

Revoke an Invitation

Revoke an invitation if the person no longer needs access or you used the wrong email address. Revoking invalidates the link and removes the pending user record. Invitation activity remains in activity reports.

1. On **Users**, select the pending user's email address.
2. Select **Revoke invitation**.
3. Review the email address in the confirmation dialog, then select **Revoke invitation**.

Email addresses cannot be edited. To correct an address, revoke the pending invitation and send a new invitation to the correct address.

If the Email Address Already Exists

Find the existing user record and check its status before taking another action.

Status	Action
Invited	Resend the existing invitation if the recipient needs a new link.
Active	The person already has an account. Direct them to sign in.
Deactivated	Reactivate the existing account if access should be restored. A new invitation is not required.



Manage Users

Use the user directory to review account status, change roles, and remove or restore access. Accepted accounts are retained when deactivated; Northstar does not permanently delete them.

Before You Begin

You must be an **Owner** or **Administrator**. Administrators can manage other Administrators and Members, but cannot change an Owner's role, status, or multi-factor authentication (MFA). You cannot change your own role, deactivate yourself, or reset your own MFA through user administration.

Find a User

1. Select **Users** in the sidebar.
2. Enter a name or email address in **Search users**. Use **Status** and **Role** to narrow the results; the filters work together.
3. Select the user's email address to open their details.

Northstar Cloud

Alder Field Services | Morgan Ellis

Users / casey.tran@example.com

Casey Tran

Email address: casey.tran@example.com

Role: Member Status: Active

Teams: Client Support

Last sign-in: 29 September 2026, 09:15 UTC

Change role

Deactivate user

Reset MFA

Casey Tran's active account, viewed by an Owner. Northstar Cloud 1.0 — fictional product mockup.

An invited user has no name until they accept. An expired invitation still has the status **Invited**, with an **Expired invitation** indicator. Email addresses cannot be edited.

Change a Role

Role changes end the affected user's existing sessions. At their next sign-in, Northstar applies the new permissions and authentication requirements. You can change roles only for **Active** users.

1. Open the user's details and select **Change role**.
2. Select the required **Role**. Only an Owner can assign or remove **Owner**.
3. Select **Save changes**.

For an Administrator, password sign-in requires local multi-factor authentication (MFA). A newly promoted user must enroll if they have not already done so. The last active Owner cannot be demoted or deactivated.

Deactivate a User

Deactivation immediately blocks both password and single sign-on (SSO) access and ends existing sessions. The account retains its role and team memberships.

1. Open the active user's details and select **Deactivate user**.
2. Review the affected user and the access consequences.
3. Confirm by selecting **Deactivate user**.

Reactivate a User

1. On **Users**, filter **Status** to **Deactivated** and open the account.
2. Select **Reactivate user**.
3. Review the retained role and confirm by selecting **Reactivate user**.

The user becomes **Active** with their previous role and team memberships. They must still meet current SSO and MFA requirements. Northstar does not send a new invitation.

For a pending invitation, use **Resend invitation** or **Revoke invitation** instead. See **Invite Your First Users**.

Reset Another User's MFA

Reset local MFA when a user cannot use their authenticator or recovery codes. An Owner can reset another user's MFA. An Administrator can reset MFA only for another Member. This action does not change MFA at your identity provider.

A reset removes the local enrollment and all recovery codes and ends the user's sessions. If the user's role or organization policy requires MFA, the user must enroll again at their next password sign-in.

1. Open the user's details and select **Reset MFA**.
2. Check that the confirmation identifies the correct account.
3. Confirm by selecting **Reset MFA**.

If an Action Is Unavailable

Situation	What to check
Change role is unavailable	The account must be Active. You cannot change your own role or remove the last active Owner.
Owner controls are missing	An Administrator cannot manage an Owner. Ask another authorized Owner.
Reset MFA is unavailable	Check your authority and whether the user has a local enrollment. You cannot reset your own MFA here.
The email address already exists	Find the existing account. Resend an invitation or reactivate it, as appropriate; do not create a duplicate.

Related guides: Roles and Permissions; Configure MFA; Troubleshoot Sign-In Problems.



Create and Manage Teams

Teams organize users without granting permissions. A user can belong to more than one team, or none. Teams have no separate owner, manager, or role.

Before You Begin

You must be an **Owner** or **Administrator**. Users must be **Active** before you can add them. Invited users must accept their invitations first.

Create a Team

1. Select **Teams** in the sidebar, then select **Create team**.
2. Enter a **Name** of 2–60 characters. The name must be unique; capitalization and surrounding spaces do not distinguish names.
3. Optionally, enter a **Description** of up to 200 characters.
4. Select **Create team**.

A screenshot of the 'Create team' form in the Northstar Cloud interface. The form is titled 'Create team' and is part of the 'Teams / Create team' section. It has two input fields: 'Name' with the value 'Service Desk' and 'Description' with the value 'Coordinates incoming service requests.' At the bottom right, there are two buttons: 'Cancel' and 'Create team'.

Create a team with a name and optional description. Northstar Cloud 1.0 — fictional product mockup.

The team is created without members. Add users from its details page.

Add or Remove Members

1. On **Teams**, find the team using **Search teams**, then select its name.
2. Select **Add members**.
3. Select the active users to add, then select **Add members**.

Northstar Cloud Alder Field Services | Morgan Ellis

Teams / Client Support

Client Support

Description: No description

2 members Add members

Name	Status	Action
Casey Tran	Active	Remove from team
Rowan Bell	Deactivated	Remove from team

Edit team Delete team

Client Support includes one active and one deactivated member. Northstar Cloud 1.0 — fictional product mockup.

The membership list shows each user's status. If a member is later deactivated, they remain in the team and its member count. Deactivation does not remove the membership.

Remove a Member

1. Open the team's details and find the person in the membership list.
2. Select **Remove from team** for that person.
3. Check the person and team in the confirmation, then select **Remove from team**.

Removing a membership does not deactivate the account or change its role. Active users receive membership emails if their personal **Team membership changes** preference is on.

Edit a Team

1. Open the team's details and select **Edit team**.
2. Update **Name** or **Description**. The same length and unique-name rules apply as when creating a team.
3. Select **Save changes**.

Delete a Team

Deleting a team removes all of its memberships. It does not delete or deactivate the user accounts, and it does not change their roles.

1. Open the team's details and select **Delete team**.
2. Review the team name and the effect on its memberships.
3. Confirm by selecting **Delete team**.

Active users whose membership-change emails are on receive a removal email. Deactivated users receive no optional emails, and those missed events are not sent after reactivation.

If You Cannot Add Someone

Check their status in **Users**. An invited user must accept first. A deactivated user must be reactivated before a new membership can be added. Existing retained memberships do not need to be added again.

Related guides: Manage Users; Roles and Permissions; Configure Notifications.



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.



Configure SSO

Configure a single SAML 2.0 connection so users can sign in through your identity provider. Single sign-on (SSO) authenticates existing accounts; it does not create accounts, assign roles, synchronize teams, or reactivate users.

Before You Begin

You must be an **Owner** in Northstar and have permission to configure a SAML application at your identity provider. Keep access to your Owner password, authenticator, and recovery codes during configuration.

Configure the provider to send the user's email address as **NameID**. The email must match the Northstar account or pending invitation, ignoring capitalization. Provider-specific configuration steps are outside this guide.

Exchange Connection Values

1. Open **Settings > Authentication > Single sign-on**.
2. Copy **Service provider entity ID** and **Assertion consumer service URL** into the corresponding fields for your SAML application at the identity provider.
3. Copy the provider values into the Northstar fields listed below.
4. Select **Save configuration**. Valid fields are saved with the status **Draft**.

Northstar field	Use this value
Identity provider entity ID	The entity identifier supplied by the identity provider.
Sign-in URL	The provider's SAML sign-in endpoint.
X.509 certificate	The certificate supplied by the provider for the SAML connection.

Use the values from your own organization and provider. Illustrative example URLs are not working endpoints.

Test and Enable the Connection

A test must authenticate the Owner currently configuring the connection. Saving fields alone does not enable SSO.

1. Select **Test connection**.
2. Complete sign-in at the identity provider using the email address of your current Northstar Owner account.
3. Return to Northstar and check the test outcome. Resolve any mismatch or configuration error before continuing.
4. After a successful test, select **Enable SSO**.

The screenshot shows the 'Single sign-on' configuration page in Northstar Cloud. The page header includes 'Northstar Cloud' and the user 'Alder Field Services | Morgan Ellis'. The breadcrumb trail is 'Settings / Authentication / Single sign-on'. The main heading is 'Single sign-on'. Below this, the status is 'Status: Draft Test outcome: Successful'. The configuration fields are as follows:

- Service provider entity ID (read-only): `https://northstar.example/saml/org_alder_001`
- Assertion consumer service URL (read-only): `https://northstar.example/saml/org_alder_001/acs`
- Identity provider entity ID: `https://idp.example/entity`
- Sign-in URL: `https://idp.example/saml`
- X.509 certificate: Certificate contents omitted in this illustration

Below the fields, there is a note: 'Example URLs are nonfunctional. No certificate contents are shown. Owners retain password sign-in with local MFA when SSO is required.' At the bottom, there are three buttons: 'Save configuration', 'Test connection', and 'Enable SSO'.

A saved Draft connection after a successful test. Northstar Cloud 1.0 — fictional product mockup.

The status changes to **Enabled**. SSO is initially optional, so Members and Administrators can still use password sign-in. Connection fields become read-only.

Editing Draft fields invalidates the test result. Test again after each change before enabling the connection.

Require SSO

Requiring SSO blocks password sign-in for Members and Administrators and ends their existing sessions. Confirm that affected users can authenticate at the provider before applying this setting.

Owner recovery access: Owners retain password sign-in with mandatory local multi-factor authentication (MFA), even when SSO is required. Owners can also use SSO.

1. On **Single sign-on**, check that the connection is **Enabled**.
2. Turn on **Require SSO**.
3. Review the impact on Members and Administrators, then confirm by selecting **Require SSO**.

Disable or Replace the Connection

Disabling SSO clears **Require SSO** and ends all sessions. Users who have never set a password must use **Forgot password** before signing in with a password. Local MFA requirements still apply.

1. On **Single sign-on**, select **Disable SSO**.
2. Review the effect on sign-in, then confirm by selecting **Disable SSO**.
3. To replace the connection values, edit the retained Draft fields and select **Save configuration**.
4. Test the revised connection and enable it again. If required, turn on **Require SSO** again.

Northstar does not add a local MFA challenge after successful SSO. Configure the provider's MFA requirements at the identity provider.

Related guides: Configure MFA; Troubleshoot Sign-In Problems.



Configure MFA

Multi-factor authentication (MFA) adds an authenticator-app code to password sign-in. Northstar supports one authenticator enrollment per account and supplies ten single-use recovery codes.

Understand Who Must Enroll

User	Local MFA for password sign-in
Owner or Administrator	Always required, regardless of organization policy.
Member	Optional unless Require MFA for password sign-in is on.
User signing in with SSO	Provider MFA applies. Northstar does not add a local challenge.

Require MFA for Members

Only an **Owner** can change this policy. Turning it on ends password-authenticated sessions. Users without an enrollment must set up MFA at their next password sign-in. Single sign-on (SSO) sessions are unaffected.

1. Open **Settings > Authentication > Multi-factor authentication**.
2. Turn on **Require MFA for password sign-in**.
3. Select **Save changes**.

Northstar Cloud

Alder Field Services | Morgan Ellis

Settings / Authentication / Multi-factor authentication

Multi-factor authentication

Require MFA for password sign-in

On

Owners and Administrators always require local MFA for password sign-in.
This policy does not change SSO sessions or identity-provider MFA.

Save changes

Organization MFA policy with the Member requirement turned on. Northstar Cloud 1.0 — fictional product mockup.

To make MFA optional for Members again, turn off the same setting and select **Save changes**. Owners and Administrators still require local MFA. Owners retain password sign-in with MFA when SSO is required.

Set Up Your Authenticator

Have an authenticator app available. If MFA is mandatory, Northstar prompts you to enroll before completing password sign-in. For optional enrollment, use your profile settings.

1. Open the profile menu, select **My profile**, and open **Security**.
2. Select **Set up MFA**.
3. Scan the displayed QR code with your authenticator app, or enter the setup key into the app.
4. Enter the app's six-digit **Authentication code**, then select **Verify code**.
5. Save the ten recovery codes somewhere you can access if the authenticator is unavailable.
6. Select **I have saved my recovery codes**, then select **Finish setup**.

The Security page shows that MFA is enabled. At password sign-in, use the code from the enrolled app. Each recovery code can be used once in place of an authenticator code.

Protect Setup Information

The setup key and recovery codes provide access to your account. Do not include them in screenshots or messages. This sample intentionally does not display a scannable QR code, setup key, or usable recovery code.

If Setup Does Not Complete

Check that you entered the six-digit code for the Northstar enrollment you just added. You must verify a code and acknowledge that you saved the recovery codes before enrollment is complete.

Disable Optional MFA

This option is available only to Members when organization policy does not require MFA. Owners and Administrators cannot disable local MFA.

1. Open **My profile > Security** and select **Disable MFA**.
2. Enter your **Password** and an **Authentication code**, or select **Use a recovery code** and enter an unused code.
3. Confirm by selecting **Disable MFA**.

Recover Access

If your authenticator is unavailable, select **Use a recovery code** at the MFA prompt and enter an unused recovery code. A password reset does not remove MFA.

If you have no recovery code, ask an authorized administrator to reset your local MFA. An Owner can reset another user's MFA; an Administrator can reset MFA only for another Member. A reset removes the enrollment and recovery codes and ends existing sessions.

If MFA is still mandatory, enroll again at your next password sign-in. A sole Owner without an authenticator or recovery code must contact Northstar support. This sample does not define support identity verification or promise an automatic bypass.

Related guides: Manage Users; Configure SSO; Troubleshoot Sign-In Problems.



Configure Notifications

Choose which optional emails Northstar sends to you. These preferences apply only to your account; they do not change notifications for the organization.

Change Your Preferences

Any active user can change their own notification preferences. Both optional categories are on by default.

1. Open the profile menu and select **My profile**.
2. Open **Notifications**.
3. Turn **Team membership changes** and **Product updates** on or off as needed.
4. Select **Save changes**.

A screenshot of the Northstar Cloud user interface showing the 'Notifications' settings page. The page has a header with the Northstar Cloud logo on the left and the user's name 'Alder Field Services | Morgan Ellis' on the right. Below the header, there is a breadcrumb 'My profile / Notifications' and a main heading 'Notifications'. A table-like structure contains two rows: 'Team membership changes' and 'Product updates', each with a toggle switch set to 'On'. At the bottom left, a note states 'Required account emails cannot be turned off.' and at the bottom right is a 'Save changes' button.

Northstar Cloud		Alder Field Services Morgan Ellis
My profile / Notifications		
Notifications		
Team membership changes	On	
Product updates	On	
Required account emails cannot be turned off.		Save changes

Personal notification preferences with both optional categories on. Northstar Cloud 1.0 — fictional product mockup.

Team membership changes sends an email when you are added to or removed from a team, including removal when a team is deleted. **Product updates** controls optional product emails.

Required Account Emails

You cannot turn off invitations, password resets, account status and role notices, or local multi-factor authentication (MFA) notices. Provider MFA changes are managed outside Northstar.

Deactivated users receive no optional emails. Northstar does not send missed events after the account is reactivated.

Related guides: Create and Manage Teams; Manage Users.



Generate Activity Reports

Filter administrative and sign-in activity, then export the matching events as a CSV file. You must be an **Owner** or **Administrator**.

Choose a Reporting Period

Northstar retains events for 90 days. The default range covers the last seven UTC calendar dates, including today. Custom ranges include both the start and end date, cannot include future dates, and must stay within the retained period.

Filter Activity

1. Select **Activity reports** in the sidebar.
2. Choose a **Date range**. For **Custom**, enter the **Start date** and **End date**.
3. Choose an **Actor** and **Category**, or leave them unrestricted.
4. Select **Apply filters**.

Northstar Cloud

Alder Field Services | Morgan Ellis

Activity reports

Activity reports

Date range

23–29 Sep 2026 (UTC)

Actor

All actors

Category

Users

Apply filters

Timestamp (UTC)	Actor	Action	Target	Result
28 Sep 2026, 14:00	Morgan Ellis	Invitation sent	jordan.lee@example.com	Success

1 event | Newest first

Export CSV

Activity filtered to Users for 23–29 September 2026 UTC. Northstar Cloud 1.0 — fictional product mockup.

Results appear newest first, with 25 rows per page. The table shows **Timestamp (UTC)**, **Actor**, **Action**, **Target**, and **Result**. Results are **Success** or **Failure**.

If **No activity found** appears, broaden the dates or remove an actor or category filter, then select **Apply filters** again. **Export CSV** is unavailable when no events match.

Export the Filtered Result

1. Review the active filters and select **Apply filters** if you have changed them.
2. Select **Export CSV**.

The CSV contains every event matching the applied filters, not just the visible page. Timestamps use ISO 8601 UTC. The export action is recorded after the export dataset is captured, so the export does not contain its own activity event.

Choose a Category

Category	Events included
Users	Invitation actions, account activation, and role or status changes.
Teams	Team and membership changes.
Authentication	SSO changes, local MFA policy and enrollment or reset changes, and sign-in successes or failures.
Organization	Organization-name changes.
Reports	CSV exports.
All categories	All of the categories above.

Understand Report Limits

Personal name edits and notification-preference changes are not recorded in this version. Unknown identities in failed sign-ins appear as **Unknown user**; attempted email addresses are not exposed.

Passwords, tokens, certificates, and MFA secrets are not report fields. Reports do not provide scheduled delivery or a custom report builder.

Related guides: Manage Users; Troubleshoot Sign-In Problems.



Troubleshoot Sign-In Problems

Start with the account's current status and sign-in method. Resetting a password does not bypass deactivation, required single sign-on (SSO), or multi-factor authentication (MFA).

Invitation and Account Problems

Symptom	Likely cause	Action
The invitation has expired	Invitation links last seven days.	Ask an Owner or Administrator to resend it. Use the newest link; resending invalidates the previous one.
An old link no longer works	The invitation was resent or revoked.	Use the latest invitation, or ask an administrator to check whether the pending record was revoked.
You cannot sign in after deactivation	Deactivated accounts cannot use password sign-in or SSO.	Ask an authorized administrator to review and reactivate the account if access should be restored.
A new invitation is rejected	That email address already has an account or invitation.	An administrator should find the existing record and resend or reactivate it as appropriate.
SSO invitation acceptance fails	The provider email does not match the invited email.	Ask the provider administrator to check the email sent as NameID against the invitation. Capitalization is ignored.

An expired invitation remains **Invited**, with a separate **Expired invitation** indicator. It does not become Deactivated.

Related guides: Invite Your First Users; Manage Users.

Password Problems

Symptom	Cause or check	Action
Password sign-in is temporarily blocked	Five consecutive failed password attempts trigger a 15-minute block.	Wait for the block to end. Administrators cannot manually unlock the account. SSO is unaffected.
The password reset link fails	It may have expired, been used, or been replaced.	Request a new link. Links expire after 30 minutes and can be used once; a new request invalidates the previous link.
You never created a password	You may have used only SSO before it was disabled.	Use Forgot password to set a password. Meet current local MFA requirements at sign-in.

Reset Your Password

1. On the sign-in screen, enter your **Email address** and select **Forgot password**.
2. Select **Send reset link**.
3. Open the newest reset email before its 30-minute expiry.
4. Enter and confirm a new password of 12–128 characters, then select **Reset password**.
5. Return to sign-in and complete any required MFA challenge.

There is no required mix of character types. A password reset does not reset MFA, reactivate an account, or remove the requirement to use SSO.

Required SSO

When your organization requires SSO, Members and Administrators must select **Continue with SSO**. Owners can still sign in with a password and local MFA for recovery.

SSO and MFA Problems

Symptom	Action
SSO succeeds at the provider but Northstar access fails	Ask an administrator to check for an Active account or valid invitation and a matching email. SSO does not create or reactivate accounts.
The identity provider is unavailable	Ask an Owner to investigate. Owners can use their password and local MFA; Members and Administrators cannot bypass required SSO with a password reset.
Your authenticator is unavailable	Select Use a recovery code and enter an unused code. Each recovery code works once.
You have no authenticator or recovery code	Ask an authorized administrator to reset local MFA. Owners can reset other users; Administrators can reset other Members only.
You are the sole Owner with no recovery method	Contact Northstar support. Support identity verification is outside this fictional sample; no automatic recovery is promised.
MFA fails during provider sign-in	Contact your identity-provider administrator. A Northstar MFA reset does not reset provider MFA.

Information to Give Your Administrator

Provide the affected account email, the sign-in method, the approximate time in UTC, and the message shown. Do not send passwords, authenticator setup keys, or recovery codes.

Owners and Administrators can use **Activity reports** to review recorded sign-in successes and failures. Unknown identities appear as **Unknown user**; the report does not expose attempted email addresses.

Related guides: Configure SSO; Configure MFA; Generate Activity Reports.



Release Notes

Version 1.1.0 | 29 September 2026

Review the latest changes, updates, and fixes in Northstar Cloud. This release improves invitation visibility, reporting, and authentication security.

Portfolio sample: all changes, Jira references, and vulnerability examples below are fictional. CVE-DEMO identifiers are illustrative placeholders, not assigned CVE records. No real vulnerabilities or customer tickets are represented.

New Features and Enhancements

Clearer Invitation Status: Expired invitations now display an Expired invitation indicator in the user directory and invitation details. The account retains the Invited status until the invitation is accepted or revoked (NSC-1842).

More Useful Activity Exports: CSV exports now include the event ID and the applied UTC date range to help administrators correlate exported records with activity in Northstar. Existing date-range and role restrictions continue to apply (NSC-1871).

Bug Fixes

Resent Invitations: Fixed an issue where the original invitation expiry could remain visible after an invitation was resent. The displayed expiry now reflects the new seven-day acceptance period (SUP-1048, SUP-1062).

Combined User Filters: Fixed an issue where changing the Role filter could clear the selected Status filter. Both filters now remain applied when narrowing the user directory (SUP-1093).

Security Enhancements

Session Invalidation After Deactivation: Closed a gap in session invalidation that could allow an existing session to continue making requests briefly after an administrator deactivated the account. Deactivation now rejects subsequent requests from affected sessions (CVE-DEMO-2026-001, NSC-1904).

SAML Assertion Validation: Strengthened checks on SAML assertion recipients and validity periods. Assertions that do not match the configured recipient or fall outside their validity period are rejected (CVE-DEMO-2026-002, NSC-1916).

Availability and Required Action

Version 1.1.0 is deployed to all organizations in this fictional release scenario. No administrator upgrade is required. If SSO fails after deployment, verify the assertion recipient and validity period with your identity provider administrator. Owners retain password sign-in with local MFA for recovery.