



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.