

Users and Access

Users and Access

Purpose and security boundary

Use user records to give one person an identifiable Brisk sign-in and only the access required for that person's work. User administration is restricted setup work. Never copy passwords, recovery codes, API tokens, or customer information into documentation or support notes.

Review users

Mon, Aug 10, 2026

Search Here

Search For...

My site > Setup > User List

Create New User

User List

« First Previous Page 1 of 1 Next Last »

Search & Filter Options

User	Last Login	Username	First Name	Last Name	Email Address	Active	Date Jo
__codexcheck__	None	__codexcheck__			codex@example.com	True	March 3
docdemo_cashier	Aug. 10, 2026, 12:47 p.m.	docdemo_cashier	Cashier	Demo	cashier@example.invalid	True	Aug. 10
docdemo_inventory_clerk	Aug. 10, 2026, 12:47 p.m.	docdemo_inventory_clerk	Inventory Clerk	Demo	inventory_clerk@example.invalid	True	Aug. 10
docdemo_office_manager	Aug. 10, 2026, 12:45 p.m.	docdemo_office_manager	Office Manager	Demo	office_manager@example.invalid	True	Aug. 10
docdemo_service_technician	Aug. 10, 2026, 12:45 p.m.	docdemo_service_technician	Service Technician	Demo	service_technician@example.invalid	True	Aug. 10
docdemo_administrator	Aug. 10, 2026, 12:47 p.m.	docdemo_administrator	Administrator	Demo	administrator@example.invalid	True	Aug. 10
docdemo_support_developer	Aug. 10, 2026, 1:11 p.m.	docdemo_support_developer	Support Developer	Demo	support_developer@example.invalid	True	Aug. 10

The Users and Access list screen in the Brisk documentation demo.

Open **Setup** → **Users** and review active accounts regularly. Investigate accounts that no longer have an owner or need. Use the user's detail page to review their profile before changing access.

Create a user

Mon, Aug 10, 2026

Search Here

Search For...

My site > Setup > User List > New user

Save Cancel < Previous Next >

User Entry - New user

First name

Last name

Username

Password

Email address

Active ☒

Sales Transaction Warehouses

Available

Search available...

DOC-W-001 - Documenta

Selected

Search selected...

Add >

Add All >>

< Remove

<< Remove All

Groups

Available

Search available...

Documentation Demo - Ca
Documentation Demo - Inv
Documentation Demo - Off
Documentation Demo - Sei
Documentation Demo - Ad
Documentation Demo - Su

Selected

Search selected...

Add >

Add All >>

< Remove

<< Remove All

User permissions

Available

Search available...

Accounting | account | Can
Accounting | account | Can
Accounting | account | Can
Accounting | account | Can
Accounting | account categ
Accounting | account categ
Accounting | account categ
Accounting | account categ
Accounting | Account Daily
Accounting | Account Daily
Accounting | Account Daily
Accounting | Account Daily
Accounting | Account Rollu
Accounting | Account Rollu
Accounting | Account Rollu
Accounting | Account Rollu
Accounting | Account Rollu

Selected

Search selected...

Add >

Add All >>

< Remove

<< Remove All

Save Cancel < Previous Next >

The Users and Access create screen in the Brisk documentation demo.

1. Create a distinct account for the person; do not share a generic sign-in.
2. Enter the required identity and sign-in fields.
3. Assign only reviewed groups and permissions for the person's job.
4. Set an initial password through the protected password workflow, then have the user configure account security.
5. Test a representative task as that role without exposing another user's session or credentials.

View a user

The detail page is the starting point for profile, access, preference, and password administration. Treat staff and superuser flags as elevated access, not convenience settings.

Update a user

Change identity or access only with authorization. Removing access can interrupt current work; adding broad access can expose financial or administrative functions. Record the business reason using your organization's access-review process.

Manage another user's settings

User preference pages change account-specific Brisk behavior. Adjust only the relevant section, and distinguish user preferences from system-wide settings before saving. See the [User Preferences Reference](#) for every preference grouped by its screen section.

Change a user's password

Use the dedicated password action. Do not transmit a reusable password through ordinary notes or documentation. Follow the organization's identity-verification and secure-delivery procedure.

Remove or disable access

Historical records may refer to a user, so deletion can be inappropriate or blocked. Prefer the approved deactivation process where audit history must remain attributable.

Navigation

In this module

- [Return to setup and administration](#)

Revision #4

Created 2026-08-10 16:10:05 UTC by Brisk

Updated 2026-08-11 06:01:45 UTC by Brisk