Enabling User Provisioning (SCIM) with Existing Users

11/27/2026 3:33 pm MST

This article covers turning on user provisioning (SCIM) for a DocBoss instance that already has users. Read it before provisioning is switched on, along with the setup article for your identity provider (Microsoft Entra ID, Okta or Ping).

How existing users are matched

When your identity provider sends a user, DocBoss looks for an existing user on your instance whose **login** exactly matches the **userName** sent by the identity provider (the user's email address).

- **Match found:** the existing DocBoss user is kept, with their projects, permissions and history, and is managed from the identity provider from then on.
- **Match found, but the DocBoss user is disabled:** the user is enabled again.
- **No match:** a new DocBoss user is created. If the person already had a DocBoss user under a different login (an old email address, a different domain, a different spelling), they will now have two users, and the old one keeps their history.
- **The login is already used on another DocBoss instance:** the user is not created.

What is updated on the first sync

For every matched user, the first sync replaces these DocBoss fields with the values from your identity provider:

- **First name, last name and email** (email is set to the userName).
- **Title:** replaced with the title sent. If title is not mapped, existing titles are cleared.
- **Time zone:** replaced with the time zone sent. If timezone is not mapped, or the value does not exactly match a DocBoss time zone value (for example America/Toronto), the user's own time zone is cleared and they get the company or instance time zone.
- **Role:** replaced only if userType is sent. If userType is not mapped or is empty, the user keeps their current role. If it is mapped to a single value for everyone (for example Full), every assigned user gets that role, including existing admins.
- **Affiliate:** changed only if affiliate is sent. A value that does not match a Company Short Name in DocBoss gives the user the original affiliate.

When the role changes, permissions are reset

If the identity provider changes a user's role, DocBoss resets that user's general permissions to the defaults for the new role:

- Companies, Contacts, Relationships and Reports are set to the role default (full for Admin and Full users; view for Reviewer and View users, with no Reports access).
- Affiliate-wide project and library access is removed for every affiliate, and project access is granted again only for the user's current affiliate, at the role's level.
- Permissions on individual projects are kept.

Any custom general permissions, and affiliate-wide access to other affiliates, must be set again in DocBoss afterwards. If the role and affiliate sent match what the user already has in DocBoss, nothing is reset.

Keep a security admin

Changes from the identity provider are not checked against the rule that protects your last security admin (an Admin with the Security permission). In DocBoss, the last security admin cannot be inactivated or given another role; from the identity provider, they can. If every security admin is disabled or given a role other than Admin, nobody in your company can manage users or security settings until DocBoss Support restores access. Make sure your security admins are assigned in the identity provider with the Admin role, and take care when removing or reassigning them.

When only the affiliate changes, the user is given access to the new affiliate at their role's level, and existing affiliate access is kept.

Changing a user's role or affiliate is checked against your license. If the change would exceed the number of permitted users for that role, it is refused.

Users not in your identity provider

DocBoss users who are not assigned to the DocBoss application in your identity provider are not changed. They stay as manually managed users, and disabling someone in your identity provider does not affect them. Review these users and disable any who should no longer have access.

Before you turn provisioning on

1. Export the DocBoss user list (it includes each user's login) and compare the logins with the userName your identity provider will send. Correct any that differ, so existing users are matched rather than duplicated. DocBoss Support can help change logins.

2. Decide how roles will be set. To keep the roles and permissions already set in DocBoss, leave userType unmapped at first. Map it only when your identity provider holds the same role each user already has in DocBoss; any user whose role changes has their permissions reset (see above).

3. Map title and timezone, or accept that existing users' titles will be cleared and their time zones will fall back to the company or instance time zone. If all your users are in one time zone, map timezone to a constant value, for example America/Toronto for Ontario.

4. Assign one existing user (ideally an admin) and test with it first, for example with Provision on demand in Microsoft Entra ID. Check in DocBoss that the user was matched rather than duplicated, and that their role, title, time zone and affiliate are as expected.

5. Then assign the remaining users and turn provisioning on.

Time zone values

The timezone value must exactly match one of the DocBoss time zone values. Common values:

- America/Vancouver – British Columbia
- America/Edmonton – Alberta, Northwest Territories (GMT-06:00 all year)
- America/Regina – Saskatchewan
- America/Winnipeg – Manitoba
- America/Toronto – Ontario, Quebec

- America/Halifax – Atlantic Time (Canada)
- America/St_Johns – Newfoundland
- America/Los_Angeles, America/Denver, America/Chicago, America/New_York – Pacific, Mountain, Central and Eastern Time (US)

For other time zones, contact DocBoss Support for the value to use.