BLUEBEAM TECHNICAL SUPPORT

Single Sign-on User List Preconfiguration

Part of the onboarding process for Bluebeam single sign-on (SSO) involves using email domains managed by your identity provider to identify users who already have accounts in Bluebeam Studio.

After you configured the SSO application in Microsoft Entra ID (Formerly Azure Active Directory) or in Okta, you logged into accounts.bluebeam.com and submitted information to Bluebeam.

Note: We currently support SSO for only Microsoft Entra ID and Okta.

After we receive your information, we'll send you a Studio User Activity Report, which is a CSV formatted file that lists all users under your managed domain who currently have Bluebeam IDs (BBIDs). Use the activity report to ensure your users' BBIDs match their entries in Microsoft Entra ID or their usernames in Okta (depending on which identity provider your organization uses) to ensure your users retain access to all the Sessions, Projects, and other Studio work they spent valuable time creating.

User information included in the Studio User Activity Report

The Studio User Activity Report file contains the following headings:

- User Status (PreCreated, Active, Closed, Suspended)

  Note: "Closed" and "Suspended" are legacy statuses that are no longer used. You can ignore these statuses if they appear for any users in the User Activity Report. The user status is reset when those users sign in through your identity provider.

- Email Address

- Sessions Owned

- Projects Owned

- Sessions Attended/Invited

- Project Memberships/Invites

- Last Studio Access
  Note: You should format this column to "Time" to display human readable time.

Reconcile the user report with your users’ BBIDs

Bluebeam matches your existing users’ BBIDs to a value that must be in email address format.

- **Microsoft Entra ID:** Use the Email property specified for each user.
- **Okta:** Use the Okta Username attribute (which should be in email address format).

To ensure this match, use the Studio User Activity Report to compare the BBID values in the Email Address column to users’ Microsoft Entra ID entries or Okta usernames to ensure the values match.

If you find discrepancies between the BBIDs listed in the Studio User Activity Report and those users’ Entra ID or Okta username values, we recommend that you have those users make changes at https://accounts.bluebeam.com/.

Potential discrepancies between the Bluebeam ID list we provide and your identity provider:

- The Bluebeam ID (email) doesn’t exist with the identity provider. This scenario can occur for any BBIDs in your organization that were created with shared or generic email addresses. To solve this discrepancy, be sure those BBIDs have an associated Entra ID or Okta account with the email property set to that email address, or those users will be unable to sign in after you enable SSO.
- Terminated employees, alias, or nickname emails used as an alternative to the identity provider email property.
- The email changed with the identity provider, and is no longer the same as the Bluebeam ID.
- Typos with the Bluebeam ID that differ from what’s registered with the identity provider.
- Other unexpected authentication problems that may prevent a successful implementation.

Important: If, after SSO is enabled for your organization, you encounter issues after changing a user’s BBID, contact Bluebeam Technical Support about the requested changes, and include the following information:

- The current email listed for the user in https://accounts.bluebeam.com/.
- The desired new email address for the user.

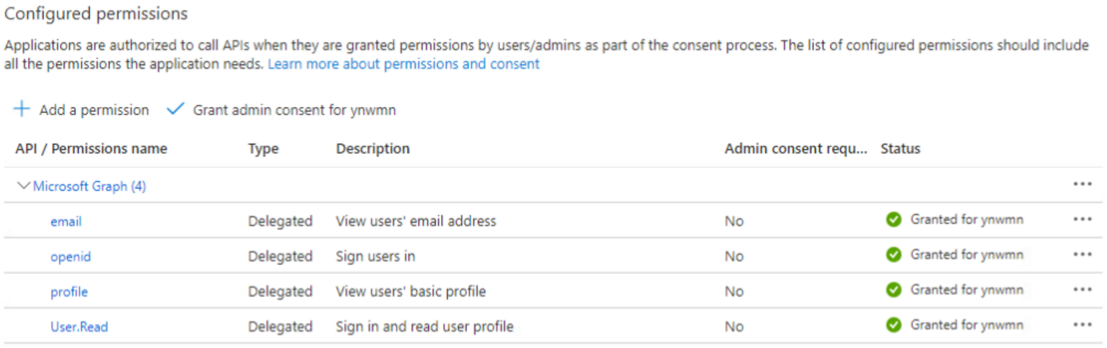
Technical Support will analyze the state of the two email accounts and reply with the resolution for the issue.

How user accounts are synced with Entra ID

When you configure the SSO application in Entra ID, you will grant specific API Permissions and Optional Claims to the Bluebeam SSO application. The following images show the minimum requirements for Entra ID. Bluebeam requires you provide values for all fields.

Important: If either of the fields in the Optional Claims section are empty, that user will be unable to sign in via SSO.

- API Permissions

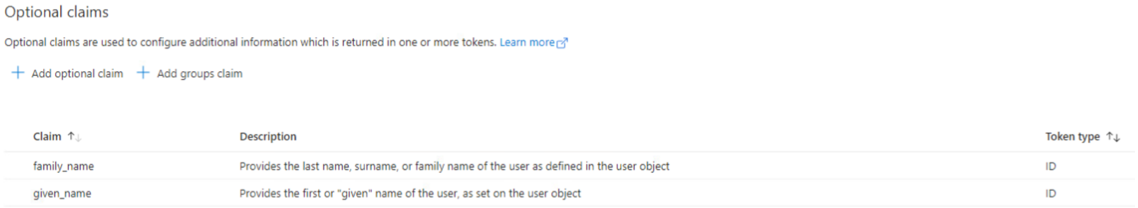


Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
email	Delegated	View users' email address	No	✓ Granted for ynwmn
openid	Delegated	Sign users in	No	✓ Granted for ynwmn
profile	Delegated	View users' basic profile	No	✓ Granted for ynwmn
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for ynwmn

- Optional Claims



Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim ↑↓	Description	Token type ↑↓
family_name	Provides the last name, surname, or family name of the user as defined in the user object	ID
given_name	Provides the first or "given" name of the user, as set on the user object	ID

Bluebeam matches Entra ID users to existing Bluebeam users only by the Entra ID Email property. To successfully link user accounts in Entra ID to user accounts in Bluebeam, the value for the users' Entra ID Email property must match their email address values in Bluebeam Studio.

When a user logs in to Studio for the first time after SSO is active, Bluebeam will attempt to sync the user signing in with an existing user in the Bluebeam databases. If no user account already exists, a new user will be created in Bluebeam Studio.