

Atlassian Confluence

Tolleiv Nietsch - 2024-09-09 - Connect Application



Was ist Atlassian Confluence?

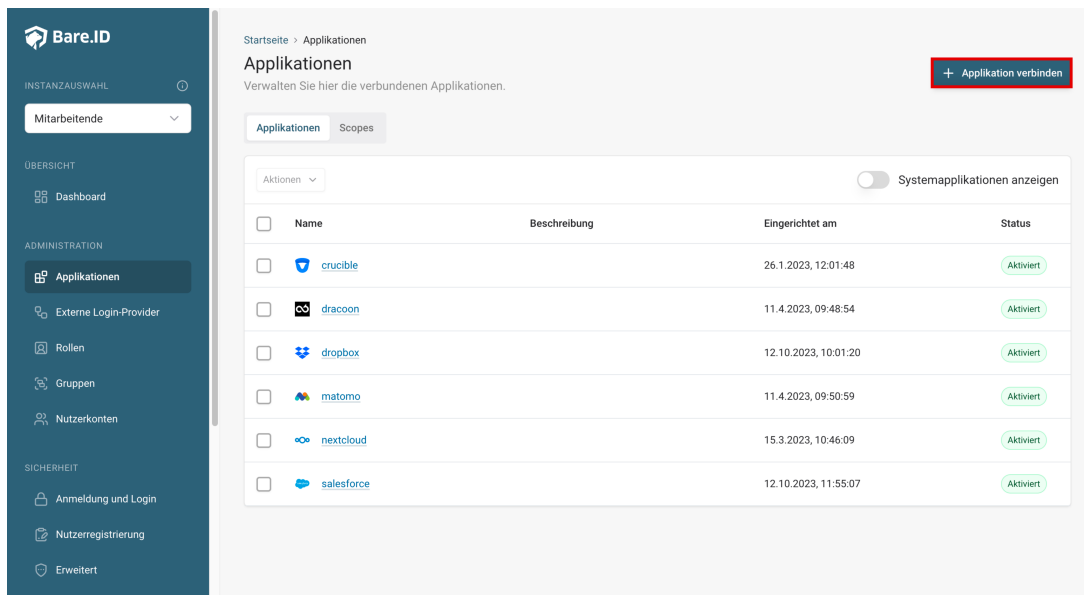
- Applikation kurz beschreiben, was sie macht und wofür sie potentiell genutzt werden kann

Bare.ID-Instanz mit Atlassian Confluence verbinden

- Die vorkonfigurierte Verbindung macht die Integration von Atlassian Confluence in Bare.ID besonders einfach. Abschließend muss Bare.ID nur noch als Login-Provider in der Atlassian Confluence-Applikation hinterlegt werden.

Atlassian Confluence als Applikation mit Bare.ID verbinden

- Melde Dich mit einem Administrator-Konto bei Bare.ID unter app.bare.id an.
- Wähle auf der Willkommensseite die Instanz aus, für die Atlassian Confluence als Applikation verbunden werden soll.
- Klicke in der Navigation links auf "Applikationen".



- Klicke auf den Button "**Applikation verbinden**" (oben rechts im Bild mit einem roten Rahmen markiert).

Es öffnet sich die Seite "**Applikation verbinden**" mit einer Übersicht an Applikationen, die bereits vorkonfiguriert sind



- Wähle die Atlassian Confluence-Applikation durch Klick auf das entsprechende Icon (oben im Bild mit einem roten Rahmen markiert).

Es öffnet sich die Seite Atlassian Confluence verbinden

- Setze alle Optionen und fülle die Felder wie gewünscht:

Startseite > Applikationen > Applikation verbinden > Atlassian Confluence

Atlassian Confluence verbinden

Atlassian Confluence Wiki

Allgemein

Client ID
confluence

Identifiziert die Anwendung. Muss eindeutig sein.

Beschreibung

Fügen Sie eine kurze Beschreibung für die Anbindung hinzu.

☐ Zugriff beschränken

Aktivieren Sie diese Option, um nur Benutzern mit entsprechender Rolle die Anmeldung an dieser Applikation zu gewähren.

☒ Verbindung aktiviert

Aktivieren oder deaktivieren Sie die Verbindung zur Applikation. Nur im aktiven Zustand können sich User über Bare.ID an der Applikation anmelden.

Einwilligungen

☐ Einwilligungen aktivieren

Einstellungen

Client Secret

Das Passwort Ihres Bare.ID Clients

Instanz-URL

Tragen Sie die URL ein, unter welcher die Applikation erreichbar ist.

+ Redirect URIs hinzufügen

Erstellen Sie eine Liste mit URLs, auf die nach der Authentifizierung weitergeleitet werden darf.

Speichern

- **Client ID:** Trage eine eindeutige Client-ID ein. Diese muss beim Einrichten in Atlassian Confluence eingetragen werden.
- **Beschreibung:** Füge eine kurze Beschreibung für die Verbindung hinzu, um sie bei der Verwaltung besser identifizieren zu können.
- Option **Zugriff beschränken:** Setze den Schalter aktiv, um nur Nutzern der Bare.ID-Instanz eine Anmeldung an Atlassian Confluence zu ermöglichen, die über die entsprechende applikationsspezifische Rolle verfügen.
- Option **Verbindung aktiviert:** Aktiviere oder deaktiviere die Verbindung zur Applikation. Lasse die Option zum Testen der Verbindung aktiv. Nur im aktiven Zustand können sich Nutzer über Bare.ID an der Applikation anmelden.
- **Client Secret:** Ein sicheres Passwort wird nach dem Speichern automatisch generiert. Dieses muss beim Einrichten in Atlassian Confluence eingetragen werden.
- **Instanz-Name:** Trage den Namen der Atlassian Confluence-Instanz aus der URL ein. Bei "https://mycompany.personio.de/" also "mycompany".
- Klicke auf den "SPEICHERN"-Button, um die Angaben zu speichern und die ausgewählte Applikation mit der ausgewählten Bare.ID-Instanz zu verbinden.

Bare.ID in Atlassian Confluence konfigurieren

Damit der SSO funktioniert, kann in der Atlassian Confluence Applikation im Bereich "Access" der Identitätsanbieter Bare.ID ausgewählt werden.

The screenshot shows the Atlassian Administration interface for 'Xtreme, Inc.' The left sidebar contains navigation links: 'Administration', 'Security', 'SAML single sign-on' (highlighted), 'Password management', 'Two-step verification', and 'Audit log'. The main content area is titled 'SAML single sign-on' and includes a 'What you need to know' section with four bullet points. The 'SAML configuration' section explains that configuration depends on the identity provider. The 'Information required by your identity provider' section lists the 'SP Entity ID' and 'SP Assertion Consumer Service URL' with 'Copy' buttons. The 'Your current SAML configuration' section shows the 'Identity provider Entity ID', 'Identity provider SSO URL', and a 'Public x509 certificate'.

Admin / Xtreme, Inc.

SAML single sign-on

Single sign-on with SAML allows your users to log in using your organization's identity provider to access all your Atlassian Cloud applications. [Learn more](#)

SAML configuration

How you configure SAML depends on which identity provider you use. See our SAML configuration [instructions for different identity providers](#).

Information required by your identity provider ⚠

To complete your SAML configuration, move the values for SP Entity ID and SP Assertion Consumer Service URL below to your identity provider:

SP Entity ID
`https://auth.atlassian.com/saml/dcd50d43-8b5a-4487-8b2b-...` [Copy](#)

SP Assertion Consumer Service URL
`https://auth.atlassian.com/login/callback?connection=saml-dc` [Copy](#)

Your current SAML configuration

Identity provider Entity ID
`http://www.okta.com/xxxxx5okhucg@q9h0h7`

Identity provider SSO URL
`https://dev-722478.oktapreview.com/app/atlassian/xxxxx5okhucg@q9h0h7/sso/saml`

Public x509 certificate
-----BEGIN CERTIFICATE----- MIIpDCCAsygAwIBAgIQAWhAw4chMAAGCSq... [Show more](#)

What you need to know

- SAML is only available for users from your [verified domains](#).
- You can only have one SAML configuration - if you have multiple domains, your SAML provider will need to be configured to handle them.
- To test your SAML configuration, open a new incognito window, go to your Atlassian login and sign in with an email address on one of your verified domains.
- When SAML single sign-on is configured, users won't be subject to Atlassian password policy and two-step verification. [Use your identity provider's equivalents](#) instead.
- During the time it takes to configure SAML single sign-on, users won't be able to log in to your Atlassian Cloud applications. Consider scheduling a day and time for the changeover to SAML, and alerting your users in