Quick Start Guide

Tolleiv Nietsch - 2024-09-09 - Schneller Einstieg

Dieser Artikel soll Administratoren den Einstieg in die Nutzung der Bare.ID-Lösung erleichtern. Dabei werden die wesentlichen Schritte beschrieben, um Nutzern die abgesicherte Anmeldung an einer mit Bare.ID verknüpften Applikation zu ermöglichen. Detailliertere Anleitungen zu den einzelnen Funktionen von Bare.ID finden sich im Bare.ID Handbuch

An Bare.ID anmelden

Nach der Auswahl einer Subscription zu einem passenden Tarif, erfolgt das Setup der gebuchten Bare.ID-Lösung durch den Bare.ID-Support. Dabei wird ein initiales Administrator-Konto mit gewünschtem Benutzernamen für die angegebene E-Mail-Adresse angelegt. Dieses Konto verfügt über alle administrativen Rechte zur Verwaltung der Bare.ID-Funktionalitäten. Weitere Administrator-Konten mit dedizierten Rechten, z.B. zur Verwaltung von Applikationen oder Nutzerkonten, können auf Anfrage vom Bare.ID-Support ergänzt werden.

- Für die erste Anmeldung mit dem initialen Administrator-Konto an Bare.ID muss zunächst ein sicheres Passwort festgelegt werden. Die E-Mail mit entprechender Aufforderung zur Passwortänderung wird an die im Konto hinterlegte E-Mail-Adresse verschickt.

- Die weiteren Schritte entsprechen dem Standard-Vorgehen bei erforderlicher Passwortänderung und sind, zusammen mit den Passwortrichtlinien, im Kapitel Passwort ändern des Handbuchs beschrieben. Folge den dort beschriebenen Schritten.
- Melde Dich anschließend mit dem Benutzernamen oder der E-Mail-Adresse und dem neuen Passwort unter https://app.bare.id/ an.

- War die erste Anmeldung erfolgreich, ist jetzt die Benutzeroberfläche von Bare.ID sichtbar und alle gebuchten Funktionen stehen zur Verfügung.

Mehr Details zum Ändern des Passwort eines Administrator-Kontos finden sich im Kapitel Passwort ändern des Handbuchs.

Instanz anlegen lassen

Nach der ersten erfolgreichen Anmeldung an Bare.ID mit einem Administrator-Konto muss zunächst eine erste Instanz erstellt werden. Eine Bare.ID-Instanz entspricht einem Keycloak-Realm und bildet einen abgeschlossenen Datensatz. Nutzer- und Konfigurationsdaten sind isoliert von den Daten anderer Instanzen und müssen daher separat gepflegt werden.

- Kontaktiere hierfür den Bare.ID-Support über das Support-Center.
- Fülle das Kontaktformular aus und erläutere die
    - Anzahl der gewünschten Instanzen
    - Namen der gewünschten Instanzen
    - Namen der Subsciptions denen die Instanzen jeweils zugeordnet werden sollen

Der Bare.ID-Support wird die gewünschten Instanzen dann zeitnah erstellen.

- Melde Dich mit deinem Administrator-Konto neu an Bare.ID an.
- Wähle auf der Willkommensseite eine Instanz aus, um auf die Funktionalitäten für diese Instanz zuzugreifen.

Es werden jetzt alle Funktionalitäten der gewählten Bare.ID-Instanz angezeigt.

Mehr Details zum Anlegen einer Instanz finden sich im Kapitel Instanz anlegen lassen des Handbuchs.

Einstellungen vornehmen

Sobald eine Instanz in Bare.ID angelegt wurde, können diverse Sicherheits- und System-Einstellungen für diese Instanz vorgenommen werden. Dabei können die eigenen Anforderungen an Sicherheit, Branding und E-Mail-Versand abgebildet werden.

- Melde Dich zunächst mit einem Administrator-Konto bei Bare.ID an.
- Sind mehrere Instanzen angelegt, wähle auf der Willkommensseite die Instanz aus, für die Einstellungen angepasst werden sollen.

Sicherheit

Zunächst sollten einige grundlegende Sicherheitseinstellungen für die Instanz vorgenommen werden, um die verbundenen Applikationen abzusichern. Die Möglichkeiten unterscheiden sich dabei je nach gebuchtem Tarif.

- Klicke in der Navigation links in der Rubrik "SICHERHEIT" auf die Kategorie, die geändert werden soll.

Anmeldung und Login

- Bleibe im Reiter "AUTHENTIFIZIERUNG" und lege die gewünschten Methoden zur Authentifizierung fest.
- Schalte die Abfrage eines zweiten Faktors an.
- Lege fest, ob Nutzer-Passwörter gegen die haveIBeenPwned-Datenbank geprüft werden sollen.
- Wähle die gewünschten Methoden zur Mehr-Faktor-Authentifizierung.
- Soll Authentifizierung per Security-Token (WebAuthN) oder die App "Sicherer Login für Webdienste" (protect4use) genutzt werden, müssen auch diese Funktionen hier angeschaltet werden.
- Wähle den Reiter "PASSWORTRICHTLINIEN".
- Definiere hier Richtlinien für die Nutzer-Passwörter und parametriere sie so, dass die erforderlichen Sicherheitsstandards erfüllt sind.
- Wähle den Reiter "BRUTE-FORCE-SCHUTZ".
- Aktiviere den Brute-Force-Schutz, um Angriffe durch das (automatisierte) Ausprobieren vieler Passwörter abzuwehren.
- Konfiguriere die Auslöser und Dauer von Kontosperren durch den Brute-Force-Schutz.

Mehr Details zu den Einstellungen für Anmeldung und Login finden sich in den Kapiteln Authentifizierung, Passwortrichtlinien und Brute-Force-Schutz des Handbuchs.

Nutzerregistrierung

- Wenn gewünscht, schalte im Reiter "REGISTRIERUNG" die Option "Geschäftsbedingungen akzeptieren" ein, um bei der Registrierung eines neuen Nutzerkontos das Akzeptieren der verlinkten Geschäftsbedingungen zu verlangen.

Mehr Details zu den Einstellungen für die Nutzerregistrierung finden sich im Kapitel Registrierung des Handbuchs.

Erweitert

- Konfiguriere bei Bedarf Token, ergänze HTTP-Header oder parametriere Nutzer- und Client-Sessions.

Mehr Details zu den erweiterten Sicherheits-Einstellungen finden sich in den Kapiteln Token, Session und HTTP-Header des Handbuchs.

System

In den Systemeinstellungen werden grundlegende Einstellungen für die Instanz festgelegt, das Aussehen der für Nutzer sichtbaren Seiten gestaltet und Einstellungen für den E-Mail-Versand festgelegt. Die Möglichkeiten unterscheiden sich dabei je nach gebuchtem Tarif.

- Klicke in der Navigation links in der Rubrik "SYSTEM" auf die Kategorie, die geändert werden soll.

Grundeinstellungen

- Lege hier einen Anzeigenamen und eine Beschreibung für die Instanz fest.
- Aktiviere über entsprechende Schalter die Möglichkeit für alle Nutzer der Instanz, Änderungen an ihrem Konto vorzunehmen oder ein neues Nutzerkonto zu registrieren.
- Lege die unterstützten Sprachen fest und wähle eine Standard-Sprache.

Mehr Details zu den Grundeinstellungen finden sich in den Kapiteln Allgemein und Sprachen des Handbuchs.

Branding

Die Branding-Einstellungen bieten die Möglichkeit, die für die Nutzer sichtbaren Oberflächen von Bare.ID an das gewünschte Erscheinungsbild anzupassen und die Bare.ID-Lösung in die Corporate Identity eines Unternehmens zu integrieren.

- Bleibe im Reiter "LOGO".
- Hinterlege hier ein Logo und ein Favicon für die Anzeige auf den Nutzer-Seiten.

- Wähle den Reiter "HINTERGRUND".
- Gestalte den Hintergrund mit einem Hintergrundbild oder definiere Farben für eine individuelle Optik.
- Wähle den Reiter "LOGIN-BOX".
- Gestalte die Anmeldemaske auf der Anmeldeseite für Nutzer.
- Entscheide (je nach gebuchtem Tarif möglich), ob der Copyright-Hinweis auf Bare.ID angezeigt werden soll
- Wähle den Reiter "ELEMENTE".
- Definiere Aussehen einzelner Elemente.
- Wähle den Reiter "LINKS".
- Definiere Links zu Impressum, Datenschutz und anderen Zielen.
- Wähle den Reiter "TEXTE".
- Ändere Übersetzungstexte für Nutzer in allen übersetzten Sprachen.

Mehr Details zu den Branding-Einstellungen finden sich in den Kapiteln Logo, Hintergrund, Login-Box, Elemente, Links und Texte des Handbuchs.

E-Mail-Versand

In den Einstellungen zum E-Mail-Versand lassen sich Optionen für die von Bare.ID versandten E-Mails vornehmen.

- Lege hier Einstellungen für die von Bare.ID versandten E-Mails und deren Antwort-E-Mails fest.
- Soll ein eigener E-Mail-Server genutzt werden, aktiviere die entsprechende Option und konfiguriere und teste die Server-Verbindung.

Mehr Details zu den E-Mail-Versand-Einstellungen finden sich in den Kapiteln Allgemein und Eigenen E-Mail-Server verwenden des Handbuchs.

Applikation verbinden

Damit sich alle zukünftigen Nutzer zentral über Bare.ID an einer Applikation anmelden können, muss diese einmal mit Bare.ID verbunden werden.

- Melde Dich hierfür mit einem Administrator-Konto bei Bare.ID an und wähle auf der Willkommensseite die Instanz aus, mit der eine neue Applikation verbunden werden soll.
- Klicke in der Navigation links auf "Applikationen".

- Klicke auf den Button "APPLIKATION HINZUFÜGEN".

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

Vorkonfigurierte Applikation verbinden

- Befindet sich darunter die gewünschte Applikation, wähle diese aus, indem Du auf den "VERBINDEN"-Button klickst.
- Fülle auf der angezeigten Seite alle erforderlichen Felder aus und setze die Optionen wie gewünscht.

Eine detaillierte Beschreibung der Felder und Optionen um eine Applikation zu verbinden, findet sich in Kapitel vorkonfigurierte Applikation verbinden des Handbuchs.

- Lasse die Option "Zugriff beschränken" deaktiviert, um allen Nutzern zunächst eine Anmeldung an diese Applikation zu ermöglichen.
- Sind alle Angaben gemacht, schalte die Applikation über die Option "Verbindung aktiviert" aktiv und klicke auf den "SPEICHERN"-Button.
- Melde Dich jetzt in der Applikation an und konfiguriere Bare.ID als SSO-Provider.

Die Applikation muss noch ihrerseits für die Benutzung von Bare.ID konfiguriert werden.

Anleitung zur Konfiguration einzelner Applikationen sind an dieser Stelle der Wissensdatenbank zu finden.

Applikation selbst konfigurieren

Alternativ können weitere Applikationen über den OpenID Connect oder SAML-Standard mit Bare.ID verbunden werden.

- Klicke hierfür auf "VERBINDEN" in der entsprechenden Kachel des gewünschten Standards.
- Folge dann den Anweisungen des entsprechenden Artikels in der Wissensdatenbank.

Applikation verbinden lassen

Ist eine Applikation noch nicht aufgeführt, kann diese auf Wunsch vom Bare.ID-Entwicklungsteam implementiert werden.

- Kontaktiere hierfür den Support unter: https://support.bare.id/de/new-ticket.

Sind Änderungen an den Einstellungen der Applikation notwendig oder die Verbindung mit der Applikation soll deaktiviert werden, kann jede hinzugefügte Applikation nachträglich bearbeitet werden. Mehr Details dazu finden sich im Kapitel Applikation bearbeiten des Handbuchs.

Nutzerkonto anlegen
Für jeden Nutzer, der Bare.ID zur Anmeldung an einer Applikation nutzen möchte, muss ein Nutzerkonto mit entsprechenden Rechten in Bare.ID hinterlegt sein.

Externe Identitätsquelle anbinden
Nutzerkonten können per OpenID Connect- oder LDAP-Standard aus externen Identitätsquellen, wie einem Active Directory oder einem weiteren SSO-System, eingespeist werden.

- Kontaktiere bei benötigter Hilfe den Support unter: https://support.bare.id/de/new-ticket

Nutzerkonten über die Bare.ID-Benutzeroberfläche hinzufügen
Alternativ können alle Nutzerkonten und ihre Rechte über die Benutzeroberfläche von Bare.ID verwaltet werden.

- Melde dich hierfür mit einem Administrator-Konto bei Bare.ID an und wähle auf der Willkommensseite die Instanz aus, für die du ein Nutzerkonto anlegen möchtest.
- Klicke in der Navigation links auf "Nutzerkonten"

- Klicke auf den Button "NUTZERKONTO HINZUFÜGEN". Es öffnet sich eine Eingabemaske.

- Fülle alle erforderlichen Felder aus und setze alle Optionen, wie sie für diesen Nutzer gewünscht sind. Eine detaillierte Beschreibung der einzelnen Optionen und Eingabefelder befindet sich im Kapitel Nutzerkonto erstellen des Handbuchs.
- Um dem Nutzer Zugang zur Anmeldung über Bare.ID zu gewähren, lasse die Optionen "neues Passwort vergeben" und "via E-Mail versenden" aktiv. Der Nutzer muss dann zunächst ein persönliches Passwort anlegen und bekommt eine entsprechende E-Mail-Aufforderung.

- Stelle sicher, dass die Option "Aktiviert" aktiv gesetzt ist und klicke anschließend auf den "SPEICHERN"-Button. Das Nutzerkonto ist jetzt in Bare.ID hinterlegt.

Sind Änderungen an den Einstellungen des Nutzerkontos notwendig oder das Konto soll deaktiviert werden, kann jedes erstellte Nutzerkonto bearbeitet werden. Details zum Bearbeiten von Nutzerkonten finden sich im Kapitel Nutzerkonto bearbeiten des Handbuchs.

Rollen und Gruppen

Zur Vereinfachung der Rechteverwaltung von Nutzerkonten, lassen sich mehrere Nutzer zu Gruppen zusammenfassen. Diesen Gruppen oder einzelnen Nutzer können Rollen zugewiesen werden, um ihnen ein Set an Rechten zu gewähren.

Mehr Details zu Rollen und Gruppen finden sich in den Kapiteln Globale Rolle erstellen, Applikationsspezifische Rolle erstellen und Gruppe erstellen des Handbuchs.