What does Bare.ID offer?

Tolleiv Nietsch - 2025-04-10 - Questions about the product

Using Bare.ID provides greater security for all users and their data stored in connected third party applications.

As a **single sign-on solution**, it replaces multiple logins to different web applications and services with a centralized login to Bare.ID. This provides an additional layer of security that can be tailored to your own standards with user-defined password policies, brute force protection, advanced multi-factor authentication (MFA) and more. At the same time, it enhances the user experience, ensuring a high level of acceptance in everyday use.

As an **identity and access management solution**, Bare.ID also offers a wide range of options for role and rights management. For example, user accounts can be combined into groups, application-specific access rights can be assigned to user accounts, groups or users with specific roles, and login activity and active sessions can be monitored. It does not matter whether the user accounts are managed through the Bare.ID user interface or imported from an external identity provider.

Pricing

Bare.ID is offered in different tariffs with varying levels of features and services. These plans can be purchased as subscriptions, with the option to purchase multiple subscriptions at different pricing levels. All plan options and their features are described at https://www.bare.id/tarife/. For the integration of Bare.ID into an existing IT environment, consulting and individual software development services are also offered.

Instances

For the subscriptions booked, so-called instances can be created and managed via the administrator account. Each instance represents a separate Keycloak realm, which is an isolated database within a Keycloak installation. Starting with the ‘Professional Edition’ tariff, this realm is located on its own dedicated cluster.

User Interface

Each Bare.ID instance can be individually configured and monitored via the Bare.ID user interface at https://app.bare.id/. This is where connected applications are managed, security and branding settings are made, and all user accounts are managed and access rights, roles and groups are assigned. A dashboard also allows you to track metrics like user and client login attempts and view all relevant URLs of the instance.

Applications

To enable users to securely log in to a third-party application using Bare.ID, the applications

are first connected to Bare.ID via the user interface. Many applications are pre-configured and can be selected from a list of existing services. Additional services can be added using the OpenID Connect (OIDC) or Security Assertion Markup Language (SAML) standards, or the Bare.ID development team takes care of the integration.

Identity Sources

User accounts and access rights can be maintained via the Bare.ID user interface as well as imported from external identity sources via OpenID Connect or the standard Lightweight Directory Access Protocol (LDAP). This can be an Active Directory (AD) or another single sign-on (SSO) system.

Multi-factor authentication

The use of multi-factor authentication (MFA) provides additional security. Standardized identification factors help to minimize the effort required to log in and lead to a high level of user acceptance. Bare.ID supports one-time passwords (OTP), facial recognition, fingerprint sensors, hardware tokens and other components in accordance with FIDO2/WebAuthN and protect4use standards.

Design

All interfaces and emails of the Bare.ID integration that are visible to users can be customized via the user interface to match any corporate design. The use of Bare.ID therefore appears to users as a fully integrated, trusted part of their organization, or may even be invisible to them.

Developer APIs

Starting with the ‘Premium Edition’, an authentication API is available for developers to integrate Bare.ID into existing systems via the OIDC or SAML protocol, as well as a management API for programmatic administration.

Certifications

Bare.ID is hosted, operated and developed exclusively in and from Germany and is therefore 100 % GDPR compliant. The SaaS solution also maps standardized legal and industry-specific security requirements and can therefore be used in a compliant manner even in highly regulated areas.

High Availability

Operated by DevOps experts, Bare.ID guarantees an availability of 99.9 %. This exceptionally high level of availability is made possible by a multi-redundant setup. Databases and application servers are hosted with multiple nodes in cluster mode and distributed across different data centers. All applications are run as containers with Kubernetes, and physically separated backups prevent data loss. Even the high requirements for critical infrastructures (KRITIS) are met by complying with the geo-redundancy required by the KRITIS regulation starting with the ‘Premium Edition’ tariff.

Service

A service team responding to monitoring and alerting is available via our support center at

https://support.bare.id/ to assist with any questions, irregularities or problems.