Two factor authentication (2FA)

Two-factor authentication (2FA), often also called two-factor authentication, describes a user's proof of identity by means of a combination of two different and, in particular, independent components (factors). Typical examples are bank cards and PINs for ATMs, fingerprints and access codes in buildings, or passphrase and transaction number (TAN) for online banking.

2FA in BlueSpice

The extensions OATHAuth und Webauthn make it possible to implement 2FA in BlueSpice. Both extensions are deactivated in BlueSpice 3.2.x by default. They have to be configured explicitely after activation.

- OATHAuth enables 2FA via one-time password
- WebAuthn enables 2FA via FIDO sticks, Windows Hello!, etc.

Single-sign on (SSO): If an external authentication source (SAML, OpenIDConnect und LDAP) is implemented, we recommend to execute 2FA within these sources and not inside the wiki. Compatibility with SAML, OpenIDConnect or LDAP have not yet been tested in BlueSpice.

2FA is not possible with true SSO (LDAP/Kerberos).

2FA in BlueSpice

Extension	3.2x	BS 4.0 (cloud)	BS 4.1
OATHAuth	deactivated	activated	activated
Webauthn	not included, but can be installed manually	not available	activated