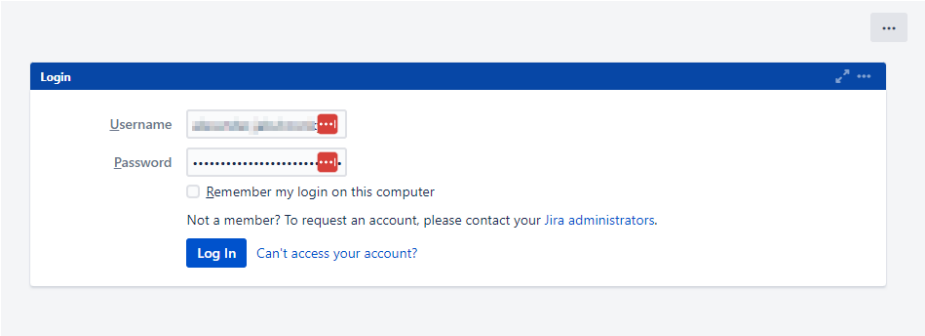
# Setup Multi-Faktor-Authentifikation für Jira/Confluence

Datum: 28.11.2023

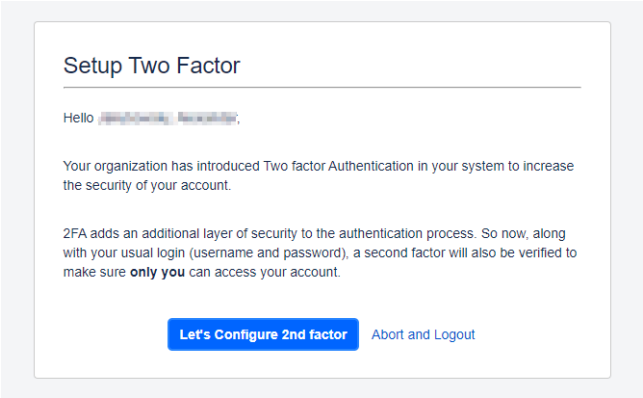
Version: 4

Autor: Geller, Silvio

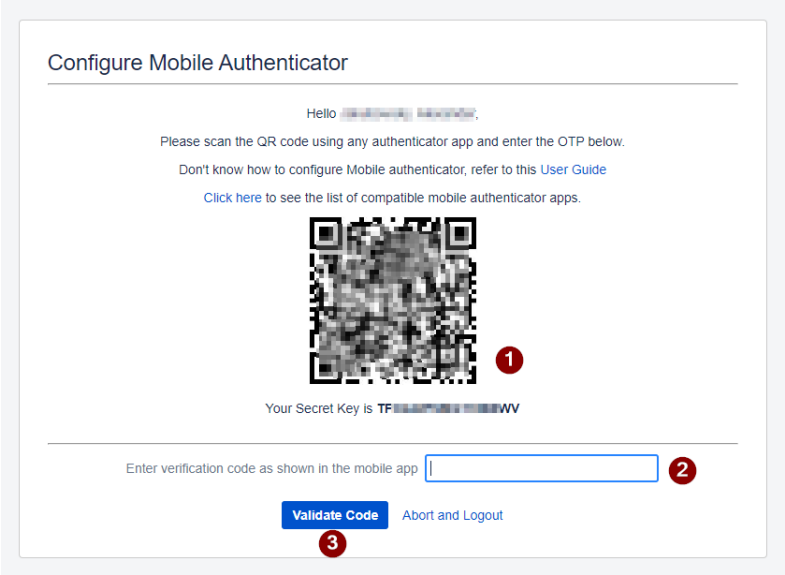
Bei der ersten Anmeldung ab dem 01.01.2024, muss jeder Benutzer einen zweiten Faktor einrichten.




Nach einer erfolgreichen Anmeldung bei Jira/Confluence wird der Benutzer aufgefordert den zweiten Faktor einzurichten.

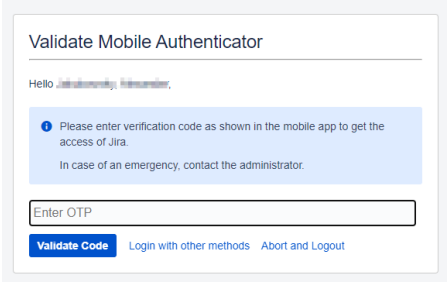



Im nächsten Schritt kann der angezeigte QR-Code (Punkt 1) entweder in eine Mobile Authenticator App (z.B. Google Authenticator, Microsoft Authenticator, etc.), auf einem Smartphone, eingescannt werden. Alternativ kann auch der angezeigte Secret Key in eine Authenticator Desktop/Web App (z.B. WinAuth, LastPass, 1Password, etc.) eingetragen werden.




Nach der Einrichtung des QR-Code oder des Secret Key werden in der gewählten Anwendung OTP-Tokens generiert. Um die Einrichtung abzuschließen, muss ein gültiger OTP-Token eingegeben werden (Punkt 2) und mit dem Button "Validate Code" bestätigt werden. (Punkt 3)

Im letzten Schritt der Einrichtung werden dem Benutzer fünfzehn Einmal-Codes angezeigt, welche er nutzen kann, wenn die ausgewählte Authenticator App nicht zur Verfügung steht. Die Codes können heruntergeladen werden und sollten sicher vor dem Zugriff Dritter gesichert werden.
Nach der Einrichtung des MFA erfolgt eine OTP-Abfrage nach einer erfolgreichen Anmeldung an Jira/Confluence.




Über das Benutzermenü "Two Factor Configuration" hat der Benutzer die Möglichkeit, wenn z.B. ein neues Smartphone eingerichtet werden soll, die Einrichtung des zweiten Faktors zurückzusetzen und neu zu starten.
Alternativ kann der Secret-Key jederzeit ausgelesen werden, um eine Web/Desktop Anwendung damit nachträglich einzurichten.