About 2-Step Verification

Sumo Logic offers 2-Step Verification, also known as two-factor authentication, as an optional feature for customers to enhance security and secure sensitive data stored in Sumo Logic. When 2-Step Verification is configured, the user is prompted for an additional security code after authenticating with their username and password. The user obtains the additional security code from a configured device.

2-Step authentication is used only during the login process with username and password (Sumo Logic native authentication). 2-step verification is not applied when using SAML/SSO for authentication.

The following 2-Step Verification options are available:

- Require all users to authenticate with 2-Step Verification.
- Allow each user to decide whether to require 2-Step Verification when signing in.

With multi-account access, user sign-in is governed by the strictest setting across all organizations. If a user has accounts in two organizations, one of which requires 2-Step Verification and one which doesn’t, the user will always be required to perform 2-Step Verification when signing in.

To implement 2-Step Verification:

1. By default, 2-Step Verification is optional, but an administrator can make it required for an organization. See [2-Step Verification for Administrators](#).
2. Users configure 2-Step Verification for their individual accounts. See [2-Step Verification for Users](#).

The following Time-based One-Time Password (TOTP) apps have been tested to work with 2-Step Verification (any RFC 6238 compatible app should work):

- For Android, IOS and Blackberry: [Google Authenticator](#)
- For Android and IOS: [Duo Mobile](#)
- For Windows Phone: [Authenticator](#)