Command Cloud™ End User Authentication

At Command Alkon, we ‘ve invested heavily in the security of our users’ access to Command Cloud. Users log in using a username and password, ensuring a straightforward yet secure authentication process. We are actively developing Multi-Factor Authentication (MFA) support, which will include SMS, email, and TOTP (Time-based One-Time Password) methods, adding an extra layer of security to user accounts.

APIs

All API calls within Command Cloud are secured using JWT (JSON Web Token) tokens. These tokens are issued and scoped to the specific tenant, ensuring that even if a user has access to multiple tenants, they cannot cross-pollinate or contaminate data between tenants they are not actively working in. Additionally, all API calls require an API key, further enhancing the security of our platform.

Passwords

User passwords are stored securely in AWS Cognito, a robust identity management service, and Command Alkon does not store the passwords itself anywhere, ensuring that sensitive credential information remains protected.

Access

Access to individual modules and applications within Command Cloud is managed through role-based authorization. This means that access permissions can be configured for each user, ensuring they have access only to the resources necessary for their role. This granular level of access control helps maintain the integrity and security of our platform, providing our customers with confidence in the protection of their data and operations.

The information provided here pertains exclusively to Command Cloud™ and is accurate as of the time of writing. For any questions or concerns, please contact your account manager, who can arrange a discussion with our security team. We are committed to addressing all your security needs and inquiries promptly and effectively.