Clearlogin - Securing Access

In This Article

Overview

Clearlogin provides a central access point to your organization's applications including hosted desktops and SaaS web apps. With this centralized access Clearlogin allows you to easily manage access by individual users or by groups of users. With this in mind, it is very important to plan and configure Clearlogin's access controls including:

- Sign in options
- Account recovery
- Multi-Factor authentication
- Access controls
- Admin access

Sign In Options

Clearlogin allow you to choose how your users will sign in. It can be as simple as just a username and password, or a more complex process involving multi-factor authentication. For more information, refer to these articles:

- Password and Lockout Settings
- Multi-Factor Authentication
- Guardian MFA

Account Recovery

Depending on the identity sources connected to Clearlogin, you can allow users to recover their accounts on their own. No need for them to contact your support or help desk team.

For account recovery to work, make sure your users complete the account recovery setup process:

- Sign In and Set Up

Multi-Factor Authentication

Clearlogin's multi-factor authentication (MFA) features allow you to provide numerous ways for a user to apply MFA:

- App push notifications (Clearlogin Mobile App)
- App 6-digit codes (MS Authenticator, Google Authenticator, etc.)
- Hardware U2F USB keys

Check the Multi-Factor Authentication article for more information.

Access Controls

Access controls are the rules that determine how, when, and where a user can sign into Clearlogin. For more information, refer to these articles:

- Password & Lockout Settings
- Multi-Factor Authentication
- Access Rules
- User Profiles & Profile Management
- Help Desk Challenge

Admin Access

As an administrator of Clearlogin, you have different methods for signing in and accessing the Clearlogin Admin portal. Refer to the following for more information: