User Management

- Password / Authentication Policy

Password / Authentication Policy

Created by Kyle Nehman, last modified on Mar 19, 2025

Authentication

Authentication within Cyber Crucible adheres to OAuth 2.0 standards, and is backed by AWS Cognito. All Advanced Security controls are enabled, leveraging IP address, user agent, login behavior, user behavior, and threat lists to detect a potential account compromise.

Multi-factor authentication (MFA) is strictly required for user authentication, and may be implemented with any TOTP capable app, but may not be any other, weaker, method of MFA (SMS, Email, etc.)

To reset TOTP, users must submit a request to the support.cybercrucible.com portal. The request is then verified through secondary communications with our support staff to ensure authenticity.

An account lockout is triggered after **five failed login attempts** and initially lasts **one second**. Each additional failed attempt **doubles the lockout duration**, up to a **maximum of 15 minutes**. The lockout automatically resets when a user successfully logs in or when there are no login attempts for 15 consecutive minutes.

Passwords

User password requirements have a global minimum length of 14 characters, and must contain **at least** 1 of each of the follow: lowercase letter, capital letter, number, symbol.

Password expiration is set by a group admin and managed on a group-by-group basis.

Users are not permitted to reuse their most recently used password.

Temporary passwords—for example, those used to invite a new user—expire after 3 days. After that, a new invitation or temporary password must be issued.