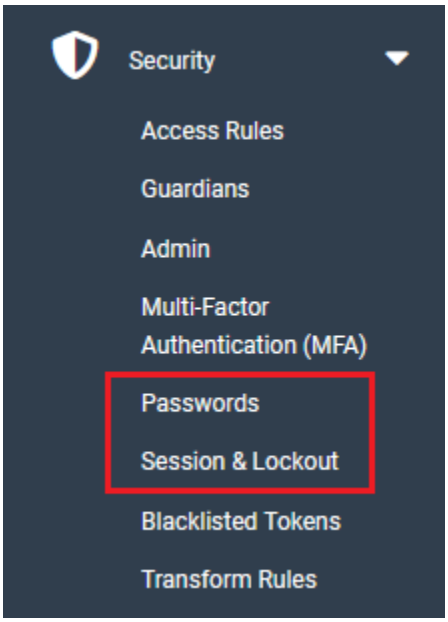
Clearlogin - Password and Lockout Settings

In This Article

Overview

In this article we cover the password and lockout settings, which are managed in the **Security** section of the Clearlogin admin portal.



Password Settings

In the left navigation menu, browse to: **Security** > **Passwords**

Allow Password Change	Allows your users to update their password as long as they remember their current password.
Custom Change Password URL	If you set a URL here Clearlogin will redirect to the URL when users want to change their password. This allows you to link to a separate website for password changes.
Allow Password Reset	Allows your users to set their password if they have forgotten it. Password resets are only allowed after users have completed the security question and phone number verification processes.
Redirect to Account Recovery on Login	When selected, users will be redirected to their My Settings page to complete their recovery verification information (Security Question & Recovery Phone Number). Once a user completes their recovery verification information, Clearlogin will stop redirecting to their My Settings page.
Show Password Expiration Warnings from Identity Source	When selected, Clearlogin will redirect users to a page that shows a password expiration warning from the identity source. The number of days remaining is based on the user's password expiration date. If the number of days is set to 14, the user will start being notified 2 weeks before their password expires.

Password Policy Settings

Minimum Password Length	The minimum password length. • Range: 5 - 64 characters • Default: 8
Custom Password Tips	Clearlogin will show default password tips, but you can use the editor to replace them with your own definitions and instructions.
Enforce Evolve IP Password Policy	If enabled, the following rules will show on the password change/forgot pages: • You may not reuse your previous password • Must be at least 8 characters long • Must be comprised of the following characters: 0-9, A-Z, a-z, / # @ - | _ ~ ! . ^ & * % $ + = • Must not be longer than 40 characters • May not repeat any character more than 2 times in a row • May not contain a sequence of characters more than 2 long • Must contain at least 1 capital letter • Must contain at least 1 number • Must contain at least 1 special character • Must contain at least 1 lower case letter

Security Question Settings

Minimum Security Question Length	The minimum amount of characters required for the security question. • Range: 1 - 999 • Default: 16
Minimum Security Answer Length	The minimum amount of characters required for the security answer. • Range: 1 - 999 • Default: 8

Help Desk Challenge

The Help Desk Challenge feature is an additional security layer that allows your support team to verify an end-user by using a call-and-response process. When an end-user contacts your support team the support team can verify the identity of the end-user via a passphrase or a question and answer.

For more information about the help desk challenge feature including configuration guidance, refer to the **Help Desk Challenge** article.

Disabled	The help desk challenge feature is disabled.
Question and Answer	The help desk challenge feature is enabled and the challenge method is a question and answer.
Passphrase Only	The help desk challenge feature is enabled and the challenge method is a passphrase.

Session Settings

In the left navigation menu, browse to: **Security** > **Session & Lockout**

Session Timeout	This is the length of time that a user's session will remain active after they login. The default is 24 hours. If kept at the default, the session will be terminated upon browser closing. If modified from the default, then closing the browser will not terminate the session. • Range: 1 hr - 24 hrs • Default: 24 hrs
Concurrent Logins	This allows users to login to Clearlogin using multiple browsers and from multiple locations. Enable | Disable
Refresh Cookie Expiration	This allows the cookie expiration time to refresh when a user is active. When this is enabled, the user will be logged out of their session after however many hours are set from the time of the last click. When this is disabled, the user will be logged out of their session after however many hours are set from the time of authentication. Enable | Disable

Lockout Settings

Lockout Max Attempts	Account Lockout will be enforced after this number of attempts within the period of Lockout Time. • Range: 3 - 50 • Default: 10
Lockout Time	The amount of time a user will be locked out as well as the time period during which failed attempts are tracked and counted. • Range: 5 min - 360 min (in 5 min increments) • Default: 15 min