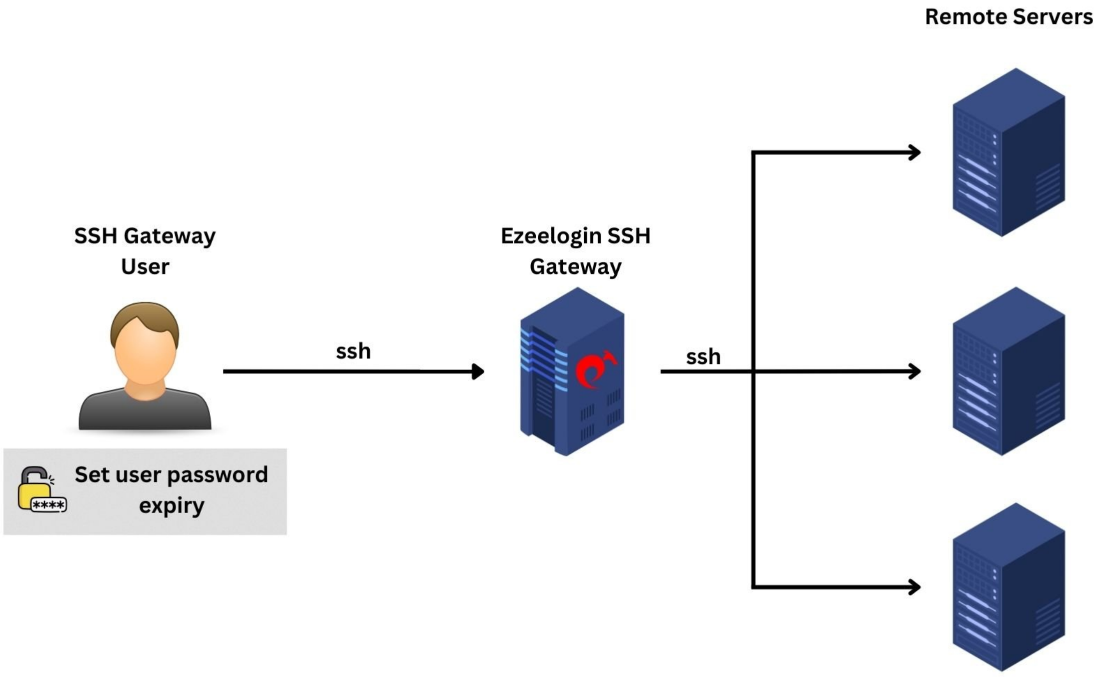
Set SSH gateway user password lifetime

297 admin July 22, 2024 [Features & Functionalities] 4003

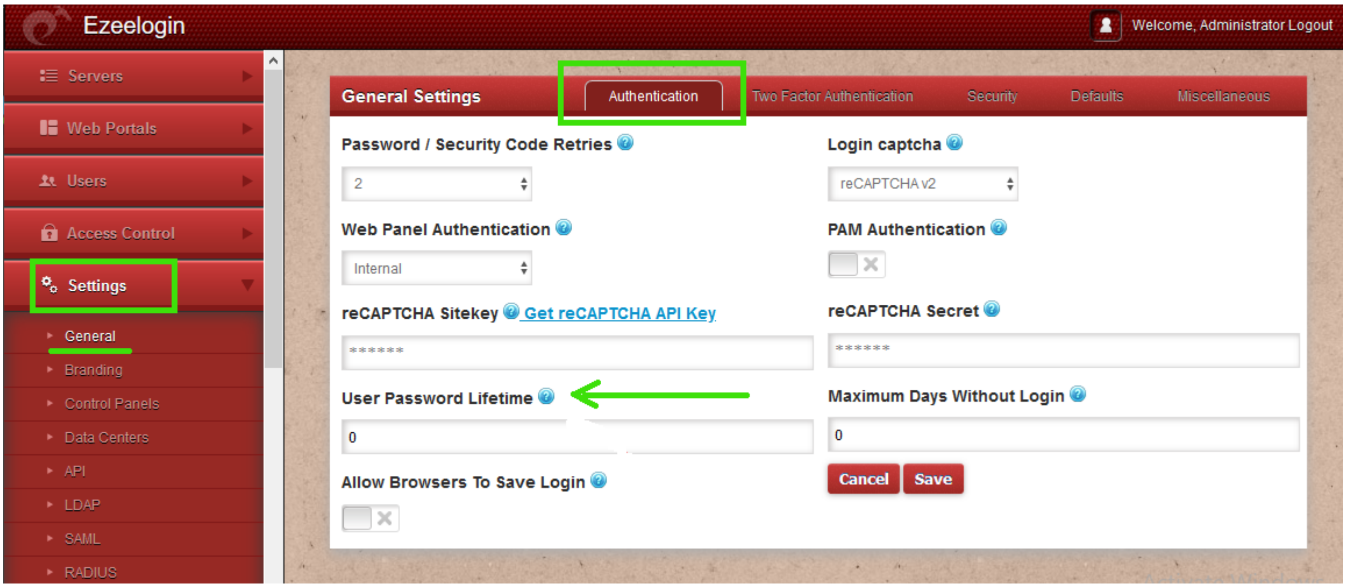
Option for setting SSH gateway user password expiration

Overview: This article explains the SSH Gateway User Password Lifetime feature, which allows you to set an expiry date for user passwords. A value of 0 indicates that passwords never expire, while a value like 30 enforces a reset every 30 days. Configuration is done through "settings -> general -> set user password lifetime.

The **SSH Gateway User Password Lifetime** feature lets you set an expiry date for the user password. The user has to set a new password to login again after its expiry. This is useful for organizations to force their employees to rotate the password of their account periodically as required by various security compliances followed.



A value 0 means the password never expires. If you want to force the user to reset the password after 30 days, you should enter the value 30. As shown below, you can set the user password lifetime by navigating to **Settings -> General -> Authentication -> User Password Lifetime.**



Password / Security Code Retries: 2

Login captcha: reCAPTCHA v2

Web Panel Authentication: Internal

PAM Authentication: ☒

reCAPTCHA Sitekey: ****** Get reCAPTCHA API Key

reCAPTCHA Secret: ******

User Password Lifetime: 0

Maximum Days Without Login: 0

Allow Browsers To Save Login: ☒

Related Article

[Disable password expiry from backend]

[Force a password change for a Ezeelogin User]

Online URL: https://www.ezeelogin.com/kb/article/set-ssh-gateway-user-password-lifetime-297.html