

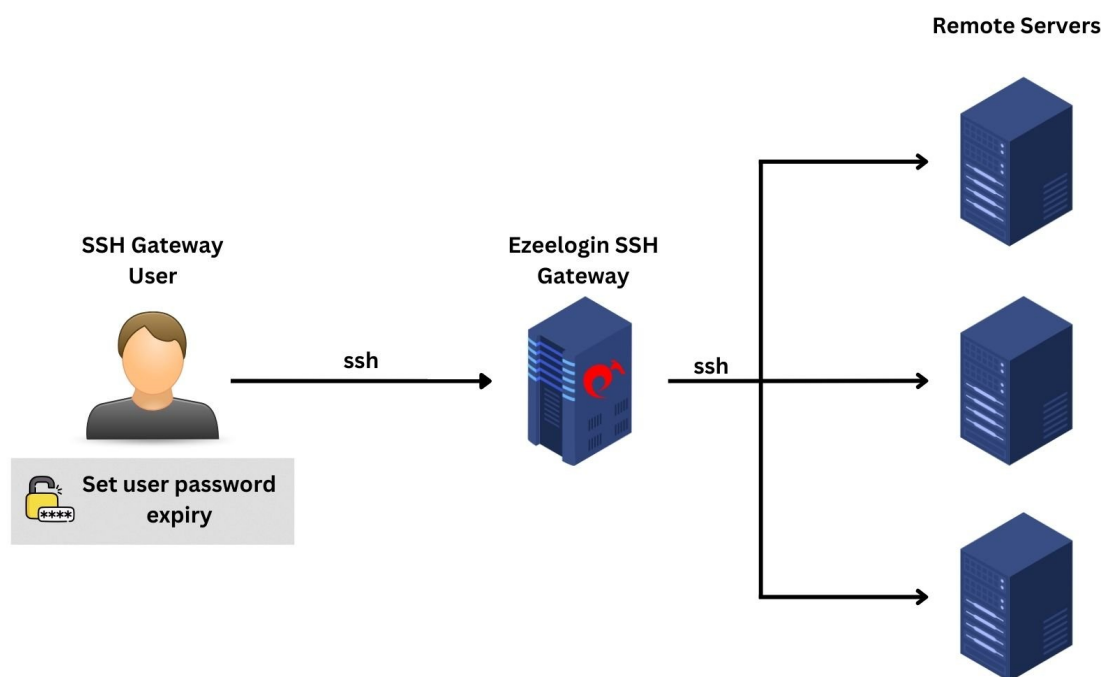
Set SSH gateway user password lifetime

297 admin July 22, 2025 [Features & Functionalities](#) 5780

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.



Step 1: To force the gateway user to reset the password after **30 days**, navigate to **Settings -> General -> Authentication -> User Password Lifetime** and enter the value **30**.

Ezeelogin

Welcome, Administrator Logout

Servers

Web Portals

Users

Access Control

Settings

General

Branding

Control Panels

Data Centers

API

LDAP

SAML

RADIUS

General Settings

Authentication

Two Factor Authentication

Security

Defaults

Miscellaneous

Password / Security Code Retries

2

Web Panel Authentication

Internal

reCAPTCHA Sitekey

Get reCAPTCHA API Key

reCAPTCHA Secret

User Password Lifetime

0

Allow Browsers To Save Login

Login captcha

reCAPTCHA v2

PAM Authentication

Maximum Days Without Login

0

Cancel

Save

Note: A value of **0** indicates that passwords **never expire**, while a value like **30** enforces gateway user to reset password **every 30 days**.

Related Articles

[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>