

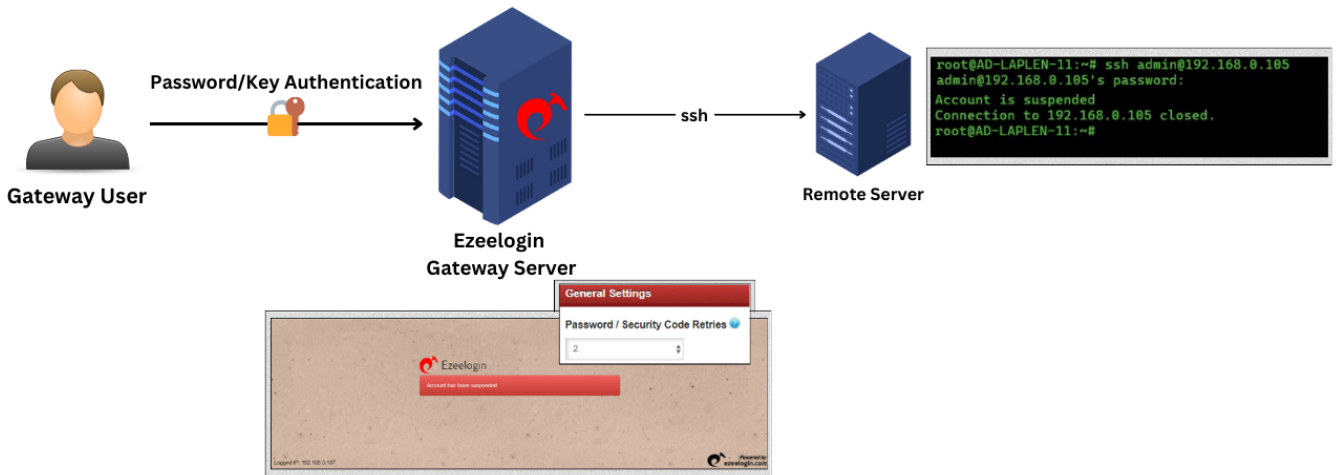
Account lockout Threshold

735 Rakhi September 19, 2024 [Features & Functionalities](#) 79

How can you setup an Account lockout threshold?

Overview: The account lockout threshold defines the maximum number of failed login attempts allowed before a user account is locked; typically set to three, while a value of zero means the account will never lock out.

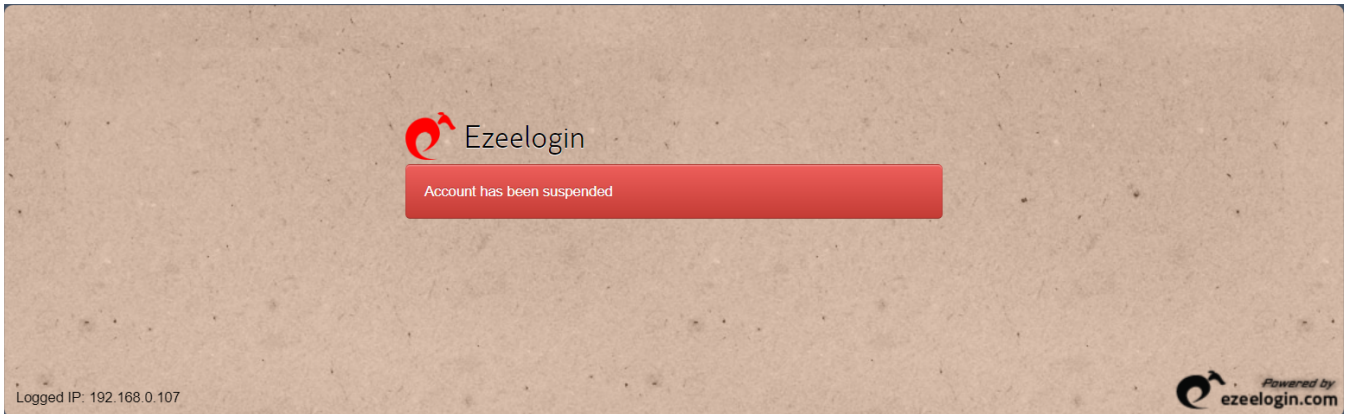
This feature allows you to configure the number of allowed retries for the password or security code when a user logs into the Ezeelogin shell. Users can attempt to enter their security code multiple times without their account being suspended or locked. However, if the user exceeds this limit while trying to log in via the web panel, their account will be suspended.



- You can set a lockout threshold for a gateway user under [Settings > General](#). In the below screenshot, the retries are set to '2'.

The screenshot shows the Ezeelogin administrative interface. The left sidebar contains a menu with the following items: Servers, Web Portals, Users, Access Control, Settings (highlighted), General (highlighted), Branding, Control Panels, Data Centers, API, LDAP, SAML, FIDO2, RADIUS, SIEM, and Server Fields. The main content area displays the **General Settings** configuration page. The **Authentication** tab is selected. The **Password / Security Code Retries** dropdown menu is highlighted with a green box and set to **2**. Other settings include **Web Panel Authentication** (Internal), **reCAPTCHA Sitekey** (with a link to [Get reCAPTCHA API Key](#)), **User Password Lifetime** (0), **Allow Browsers To Save Login** (disabled), **Remote SSH Public Key Authentication** (disabled), **Login captcha** (Disable), **External SSH Auth** (checked), **reCAPTCHA Secret**, **User SSH Key Lifetime** (0), **Maximum Days Without Login** (0), and **Remote SSH Password Authentication** (checked). **Cancel** and **Save** buttons are visible at the bottom right.

- The GUI account would be suspended after the user retries with the incorrect password twice.



The backend would be suspended after the user retries with the incorrect password twice.

```
root@AD-LAPLEN-11:~# ssh admin@192.168.0.105
admin@192.168.0.105's password:
Account is suspended
Connection to 192.168.0.105 closed.
root@AD-LAPLEN-11:~#
```

Related Articles:

[Set Password history limit for Gateway users.](#)

[To Unsuspend the user from the backend.](#)

Online URL: <https://www.ezeelogin.com/kb/article/account-lockout-threshold-735.html>