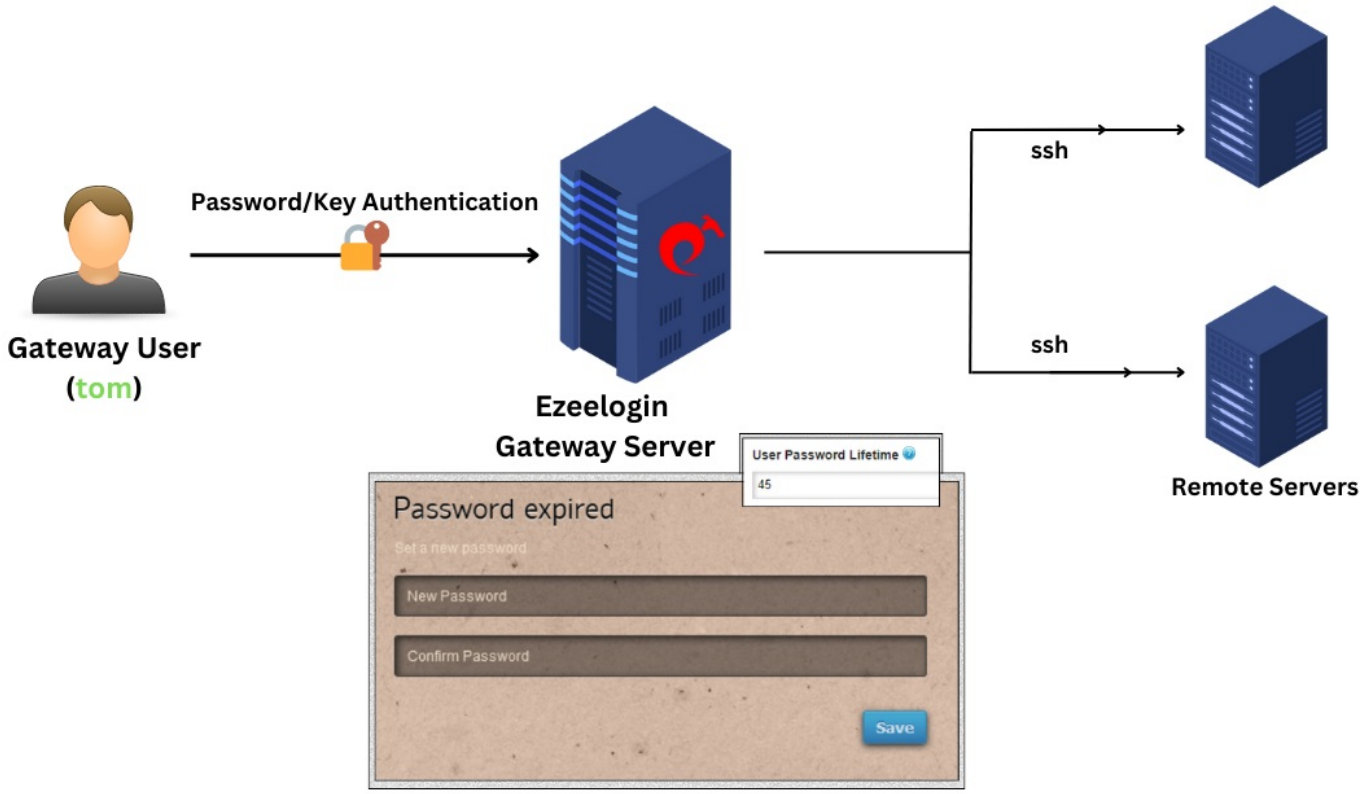
Jump server user password expired

364 admin August 27, 2024 Common Errors & Troubleshooting 8824

The Gateway SSH User password expired

Overview: This article describes how to handle the "Gateway SSH User password expired" issue by resetting the password or disabling password expiration in the database if login to the GUI fails.

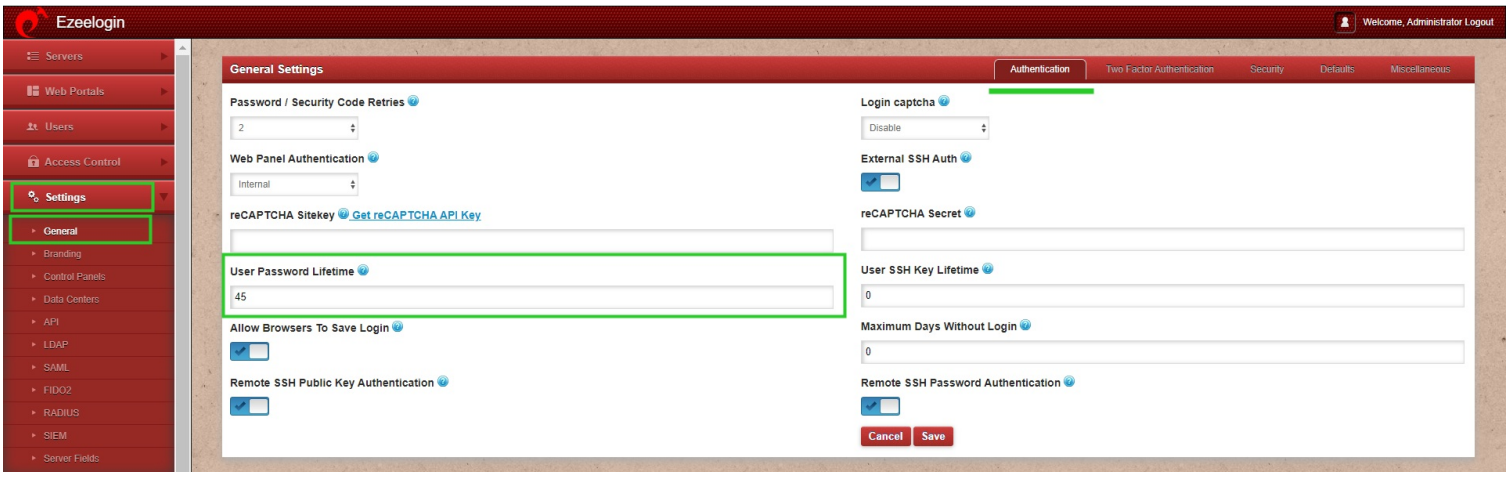


If you encounter the "Gateway SSH User password expired" message when logging into the GUI, then it's time for you to **reset the password** for the SSH gateway user and go ahead with the login.

Where was the User Password Lifetime set?

Force the user to change password every so many days. A value of 0 means the user password never expires

The duration (in days) after which a password should expire is set under "**User password Lifetime**" under **Settings > General > Authentication.**



This is a security feature as it is recommended to change the password after a preset duration of time.

However, if you are unable to reset the password or login to the GUI, follow these steps to disable password expiry directly from the database.

Method 1) Disabling password expiry

To disable password expiry if login is not possible, you can modify the "User Password Lifetime" value in the database:

The value of 45, means that the user's password would expire after 45 days and the user would be forced to change the password.

```
MariaDB [ezlogin_avmzfj]> select * from nfo_settings where name="pwexp_days";

+----+------------+-------+---------------------+
| id | name       | value | time                |
+----+------------+-------+---------------------+
| 87 | pwexp_days | 45    | 2022-08-20 00:00:54 |
+----+------------+-------+---------------------+

MariaDB [ezlogin_avmzfj]> update nfo_settings set value=0 where name="pwexp_days";
```

Method 2) Resetting user password expiry timestamp.

If you need to keep the current password valid by resetting the expiration timestamp, follow the below steps.

The following timestamp corresponds to September 12, 2024, 00:00:00 UTC on conversion to a human-readable date.

Get the current timestamp from DB and update the gateway user's time stamp field so that the user password expiry time is reset.

```
root@gateway:~# date +%s

1726108800

---

MariaDB [ezlogin_avmzfj]> update nfo_users setlpwc_ts = 1726108800 where id=1;

Query OK, 1 row affected (0.001 sec)

Rows matched: 1  Changed: 1  Warnings: 0
```

Emergency CLI Method:

Run the below command to disable user password expiry from the backend:

```
root@gateway:~# php /usr/local/ezlogin/ez_queryrunner.php "update prefix_settings set value=0 where name='pwexp_days'"
```

By following these methods, you can resolve password expiration issues and ensure continued access to your SSH gateway.

Related Article:

How to set user password lifetime for expiry

Force a password change for an Ezeelogin User

Online URL: https://www.ezeelogin.com/kb/article/jump-server-user-password-expired-364.html