How to truncate the ssh session logs recorded

168 admin October 5, 2024 Features & Functionalities, Migration & Maintenance 7990

SSH log rotation or prune recorded SSH logs

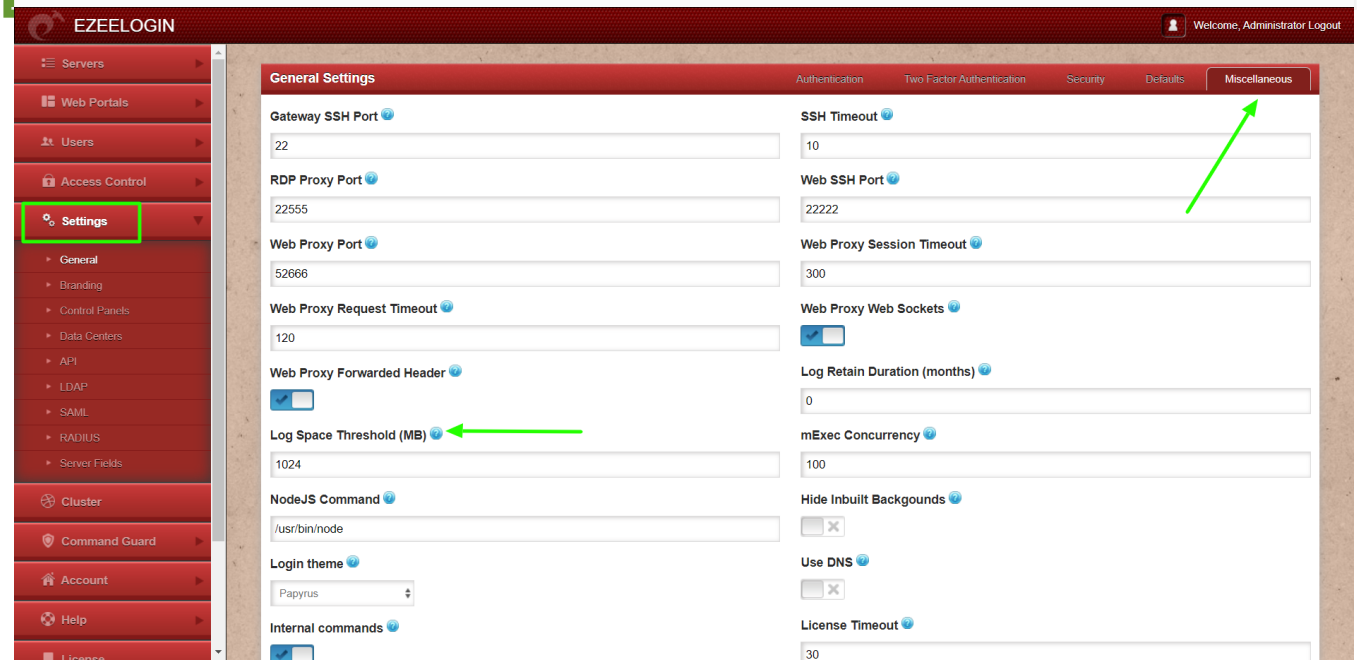
Overview: This article outlines how to manage SSH log rotation and pruning in Ezeelogin, including setting log space thresholds, and retention durations, and configuring cron jobs for automatic log deletion based on size or age to prevent disk overflow.

---

1. Setting Log Space Threshold.

Step 1(A): To prevent a full disk it is important to prune the ssh log files regularly. It is possible to auto-delete logs when the log size exceeds a limit. To Enable it Navigate to **Settings** -> **Miscellaneous** -> **Log space threshold**

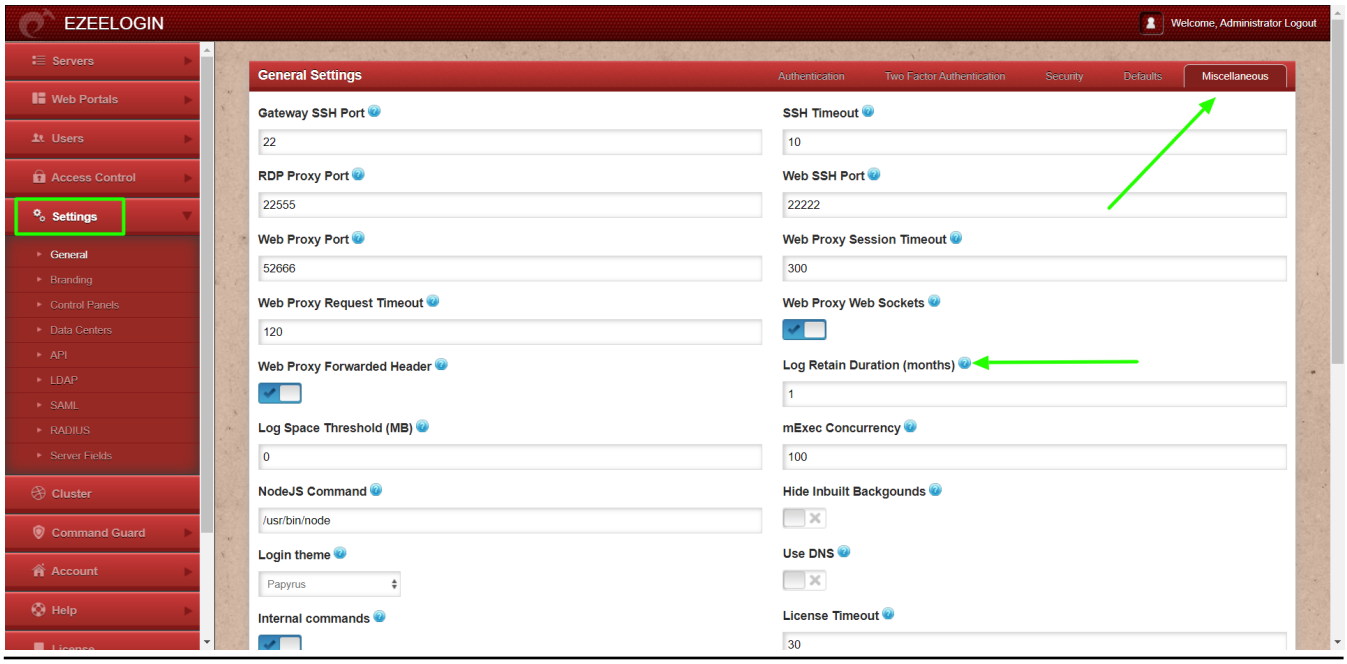
Refer Manual: https://www.ezeelogin.com/user_manual/Miscellaneous.html



2. Configuring Log Retain Duration.

Step 2(A): You can also set the period for which the SSH user log and the RDP user logs have to be retained in the system after which it would be truncated by daily cronjobs. A value of **0** means the **logs** would be **retained forever**.

To set **Log Retain Duration,** navigate to **Settings** -> **Miscellaneous** -> **Log Retain Duration**



3. Automation Log Deletion with Cron.

Step 3(A): Set a cronjob for the root user to run daily or once a week so that log files stored on the server in the directory (/var/log/ezlogin/) are truncated when they exceed a particular size or when it older than the specified number of days.

The path to the command that needs to be set in cron is,

```
0 6 * * * php /usr/local/ezlogin/house_keeping.php
```

Note:

Log file locations:

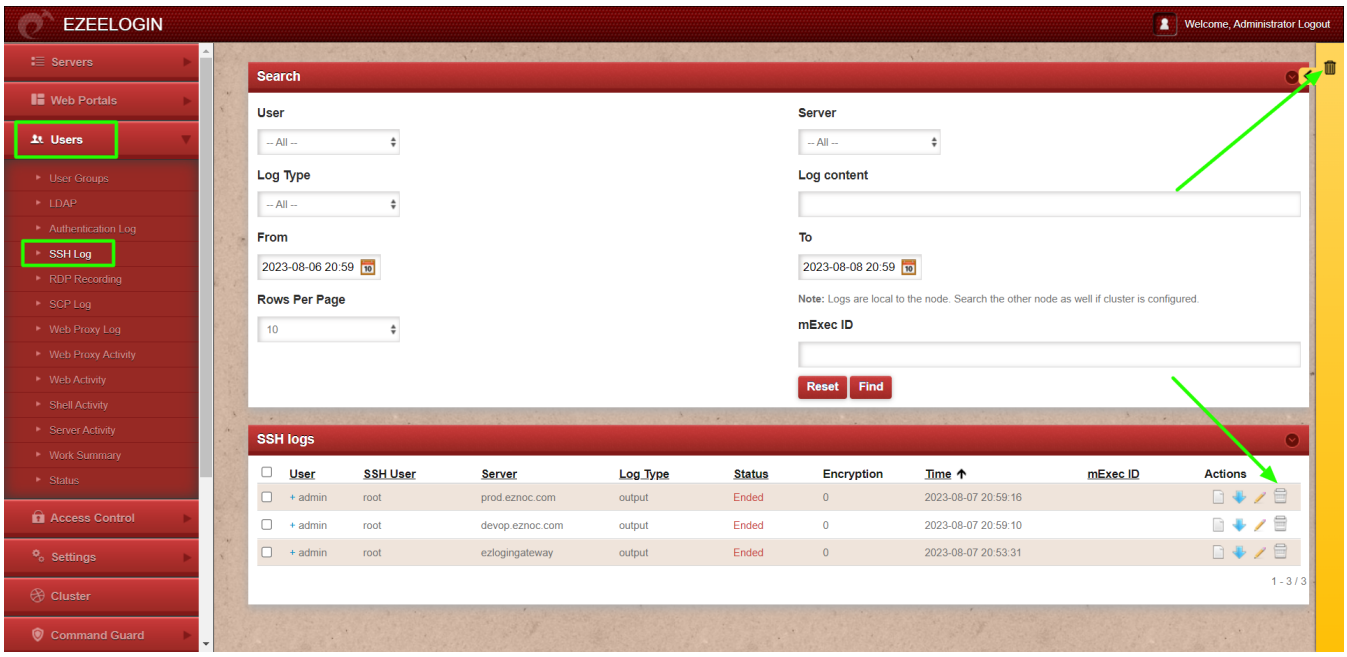
The SSH log files recorded are stored in the directory **/var/log/ezlogin/full** , **/var/log/ezlogin/input**, **/var/log/ezlogin/output**, **/var/log/ezlogin/rdp**.

- The '**full**' directory stores the **entire** SSH sessions.
- The '**input**' directory stores the recording from the **STDIN**
- The '**output**' directory stores the recording from the STDOUT and the 'rdp' directory stores the rdp session recorded.

.

4. Deleting SSH recording from the GUI.

Step 4(A): You can also **delete** the **ssh log** from the GUI by selecting the ssh log session and by clicking on the **trash icon**.



Note:

Ensure the housekeeping script is set to run in cron (0 6 * * * php /usr/local/ezlogin/house_keeping.php) so that the ssh sessions recorded which are stored in files are deleted from the backend server. You may also run the command manually to ensure that files are deleted from the backend almost instantly. You may wonder why the ssh log recorded stored in the directory **/var/log/ezlogin** is not deleted when the ssh recording is deleted from the GUI, this is because the webserver user does not have the privileges to delete the ssh log recording in the ownership of the ssh gateway user.

EMERGENCY CLI METHOD:

1. Run the below command on the gateway server to set the **Log Space Threshold** from the database. Replace the value with the value of your choosing.

```
root@gateway:~# php /usr/local/ezlogin/ez_queryrunner.php "update prefix_settings set value=95 where name='logs_threshold'"
```

2. Run the below command on the gateway server to set the **Log Retain Duration** from the database. You can replace the value with the value of your choosing.

```
root@gateway:~# php /usr/local/ezlogin/ez_queryrunner.php "update
prefix_settings set value=5 where name='log_retain_duration'"
```

If you are unable to log in to Ezeelogin software GUI, you can **delete the log files** from the **database**.

Step 1(A): Run the below command on the gateway server to **list the log files** in the directory "**/var/log/ezlogin**" that are **older than 365 days**.

```
root@gateway:~# find /var/log/ezlogin -type f -mtime +365 -exec ls -al {} ;
```

Step 1(B): Run below command on the gateway server to the **find log files** older than **365 days** in the directory "**/var/log/ezlogin**" and **delete them**.

```
root@gateway:~# find /var/log/ezlogin -type f -mtime +365 -exec rm {} ;
```

Related Articles:

Deleting entries in the MySQL database table gwactivity_logs.

An Issue with Log Retain Duration.