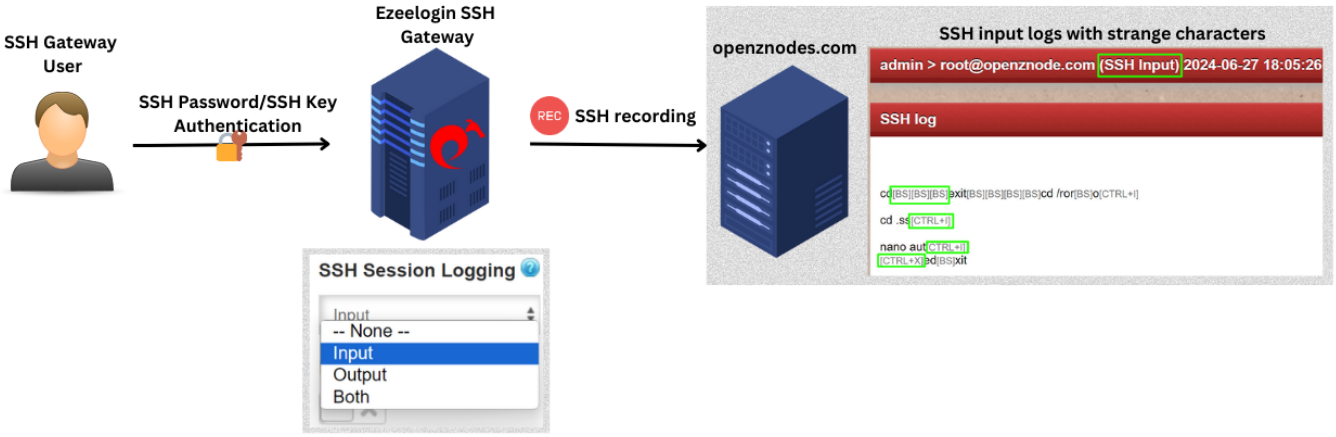
strange characters in the SSH logs recordings

63 admin October 1, 2024 Common Errors & Troubleshooting, Features & Functionalities 8717

Invisible control characters in the SSH logs recorded

Overview: This article describes how the SSH session recording logs every key press of the Ezeelogin gateway users which appear as strange characters in the logs and explains the different modes in SSH session logging.



The SSH session recording feature logs every single key press including non-printable ones like the backspace key, CTRL keys, function keys, and others, resulting in the appearance of unusual characters in the logs.

```
qui[BS][BS][BS]cd /roo[BS][BS][BS]root --------> [BS] would be a backspace
cd .ssh
ls -la
nano au[CTRL+I]
[CTRL+X]exit
```

Different modes in SSH Session Logging:

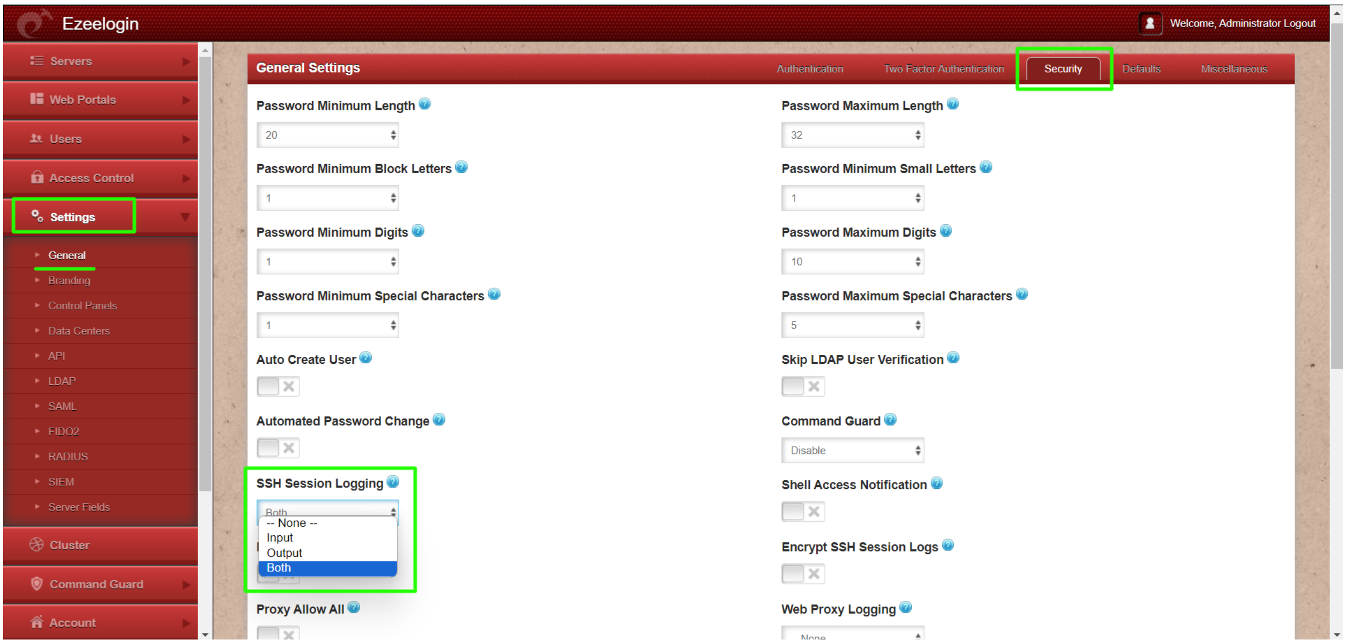
- **None:** When the SSH session recording mode is '**None**', it means no logging.
- **Input:**When the SSH session recording is set to '**Input**' mode, it logs **every single**

character sent to the STDIN file descriptor (**keyboard input**), capturing all the keystrokes during the SSH session, including invisible control characters.

- **Output:** When the ssh session recording is set to '**Output**' mode it would record all the characters that goes to the **STDOUT** file descriptor which would be the outputs on the screen of the Ezeelogin gateway user and will not have the invisible control characters in it.
- **Both:** When the SSH session recording mode is "**Both**", it would record both the STDIN and STDOUT.

To Switch the SSH session recording mode:

Step 1: Login to Ezeelogin software GUI and navigate to **Settings** -> **General** -> **Security** -> **SSH Session logging**.



On the Ezeelogin gateway server, the SSH session logs are stored in the directory **/var/log/ezlogin**.

- The '**Input**' session recorded are stored in the directory '**/var/log/ezlogin/input**'.
- The '**Output**' SSH sessions recorded are stored in the directory '**/var/log/ezlogin/output**'. For pipelining the logs to SIEM software, we would recommend using the '**Output**' SSH logs.

- The database stores only the metadata of the files containing the recorded SSH logs. The example below illustrates the SSH session logs stored in the database.

```
root@gateway:~# mysql $(awk '/^db_name/ {print $2}' /usr/local/etc/ezlogin/ez.conf)

MariaDB [ezlogin_mpayl]> select * from gjbpe_sshlogs;

+----+---------+-----------+-----------------+---------+-------+-------+-------+-------------------------------
-----------------------------------------------+---------+-----------+------------+------------------+----
----------------+---------+
```

```
| id | user_id | server_id | serveractivity_id | ssh_user | type | status | reason | file | comments | encryption | mexecid | created | mtime | finished |
+----+---------+-----------+-------------------+----------+--------+--------+--------+---------------------------------------------------------------------------------------+----------+------------+-------------+--------------------+---------------------+----------+
| 1 | 1 | 1 | 1 | root | full | end | NULL | /var/log/ezlogin/full/admin/root~Production Server~Tue_May_28_12:14:35_2024 | NULL | 0 | | 2024-05-28 12:14:37 | 2024-05-28 17:44:43 | 1 |
| 2 | 3 | 1 | 3 | jini | full | end | NULL | /var/log/ezlogin/full/John/jini~Production Server~Tue_May_28_12:34:00_2024 | NULL | 0 | | 2024-05-28 12:34:01 | 2024-05-28 18:04:06 | 1 |
| 3 | 3 | 1 | 4 | jini | full | end | NULL | /var/log/ezlogin/full/John/jini~Production Server~Tue_May_28_12:38:01_2024 | NULL | 0 | | 2024-05-28 12:38:04 | 2024-05-28 18:08:51 | 1 |
| 4 | 3 | 1 | 5 | jini | full | begin | NULL | /var/log/ezlogin/full/John/jini~Production Server~Tue_May_28_12:39:04_2024 | NULL | 0 | | 2024-05-28 12:39:05 | 2024-05-28 18:09:05 | 0 |
| 5 | 3 | 1 | 6 | jini | full | end | NULL | /var/log/ezlogin/full/John/jini~Production Server~Tue_May_28_12:41:32_2024 | NULL | 0 | | 2024-05-28 12:41:33 | 2024-05-28 18:11:36 | 1 |
```

Related Articles:

[Record ssh sessions]

[View SSH logs of all users]

[How to decrypt the encrypted SSH logs in Ezeelogin?]

[SSH session logs recorded are blank or unable to view]

[View the SSH logs history that was recorded for an SSH gateway user]

[Encryption type used for securing users' ssh logs in ezeelogin]

[View all ssh logs of a deleted user]

[Truncate the SSH session logs recorded]