Record ssh sessions

208 Santhi September 28, 2026 Security Features 20036

How to record ssh session of users on a Linux Server, Router, Switch using Ezeelogin ssh Jump Server ? or

How to record linux terminal in text files and monitor users activities in ssh?

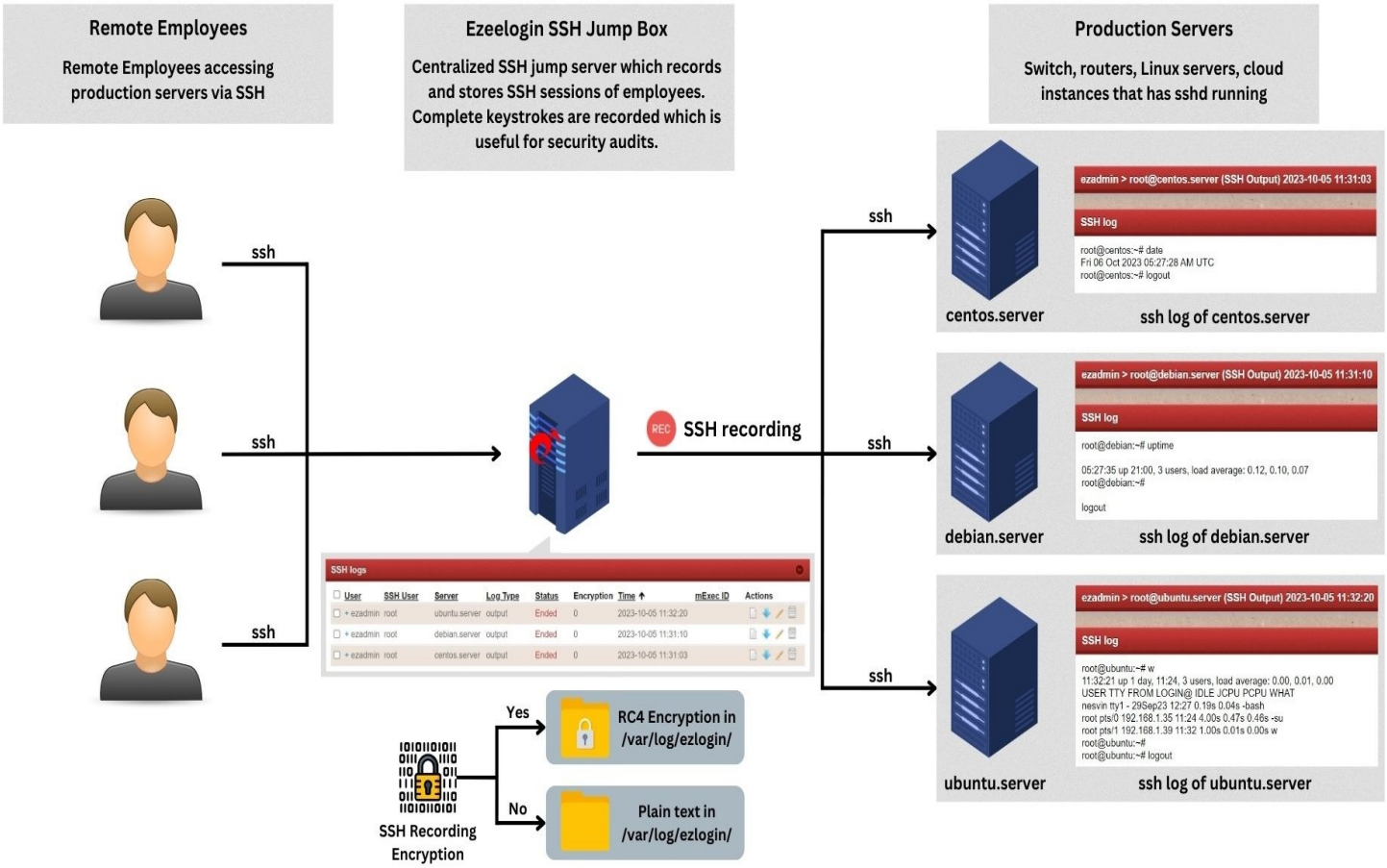
Overview: This article helps you understand how to record and audit SSH sessions on Linux servers using Ezeelogin. It covers enabling SSH session recording, viewing and monitoring recorded sessions in real time, searching session logs using the Log content field, downloading and encrypting SSH session logs, and locating the recorded logs. It also explains how to add timestamps to the SSH command prompt for easier auditing.

How do you record an SSH session?

With Ezeelogin, go to **Settings → General → Security → SSH Session Logging** and choose **Output** (or **Both**). Every SSH session your users open through the jump server is then recorded as searchable text, and no agent is needed on the remote Linux servers, routers or switches. You can view, search, download and monitor recorded sessions in real time from the GUI. The steps below cover each part.

The "SSH Log" recording feature lets you **record ssh sessions** of Linux system administrators, Linux system engineers , developers ,network administrators accessing remote **Linux** servers / cloud instances / switches / routers and other network devices via **ssh**. In other words, all user actions or activities via an ssh session are logged in a file. The ssh sessions recorded are saved in text format which can later be searched, reviewed, revisited or can be pipelined to log processing engines.

The SSHD daemon has to be running on the remote devices. The SSH daemon comes with the **OpenSSH** packages on most Linux distributions. (Centos 6, Centos7, Centos 8, Centos 5, Centos 4, Ubuntu 14, Ubuntu 16, Ubuntu 18, SUSE, RHEL , Fedora , Freebsd and more.).



Note: There is NO need to install a agent on the Remote Linux servers (Production servers) to record ssh session of users accessing the servers via ssh.

IMPORTANT

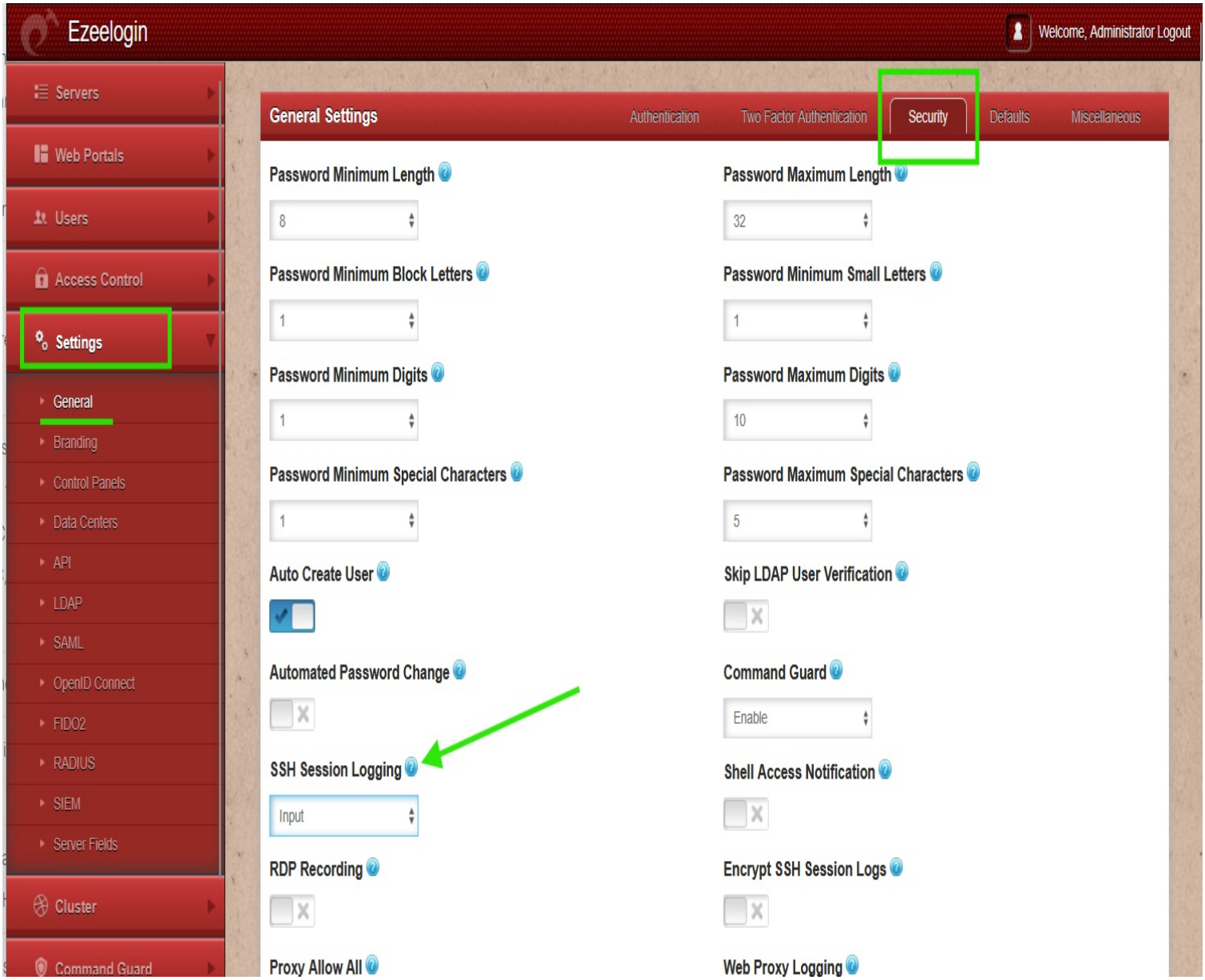
Disable tcp forwarding in SSHD server configuration file on the jump server.

The ssh session recorded lets you audit the ssh users accessing the Linux servers remotely via the ssh protocol. You can also monitor an ssh user in real-time. You can also search the entire logs recorded for a string or pattern which is very useful to perform security audits on various security incidents, lapses, security forensics etc. This is useful for meeting **security compliance** like PCI DSS, NIST, HIPAA, as ssh session recording is one of the important control requirement.

---

1. Enable ssh recording of the jump server users on the Ezeelogin ssh jump server GUI, do the following.

Navigate to **Settings-> General-> Security-> SSH Session Logging**



There are 3 settings to record the ssh sessions

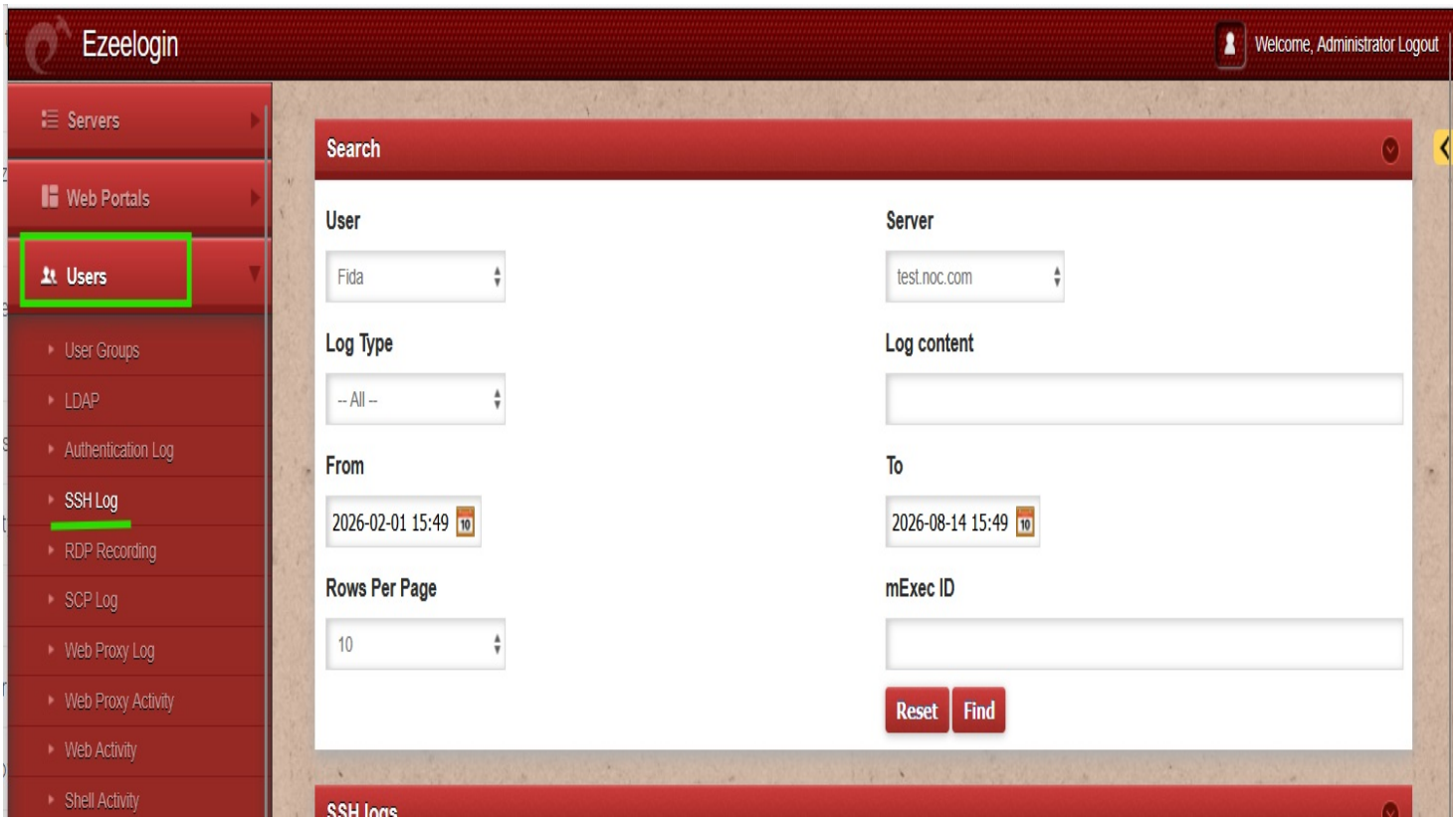
None - This would disable ssh session recording.
Input - This would record only the STDIN, which would be the keyboard inputs of the ssh jump server user.
Output - This would record only the STDOUT which would be the outputs on the screen of the jump server user.
Both - This would record both the STDIN and STDOUT of the ssh session.

The input mode would record the invisible characters typed into the STDIN, hence it would record the password

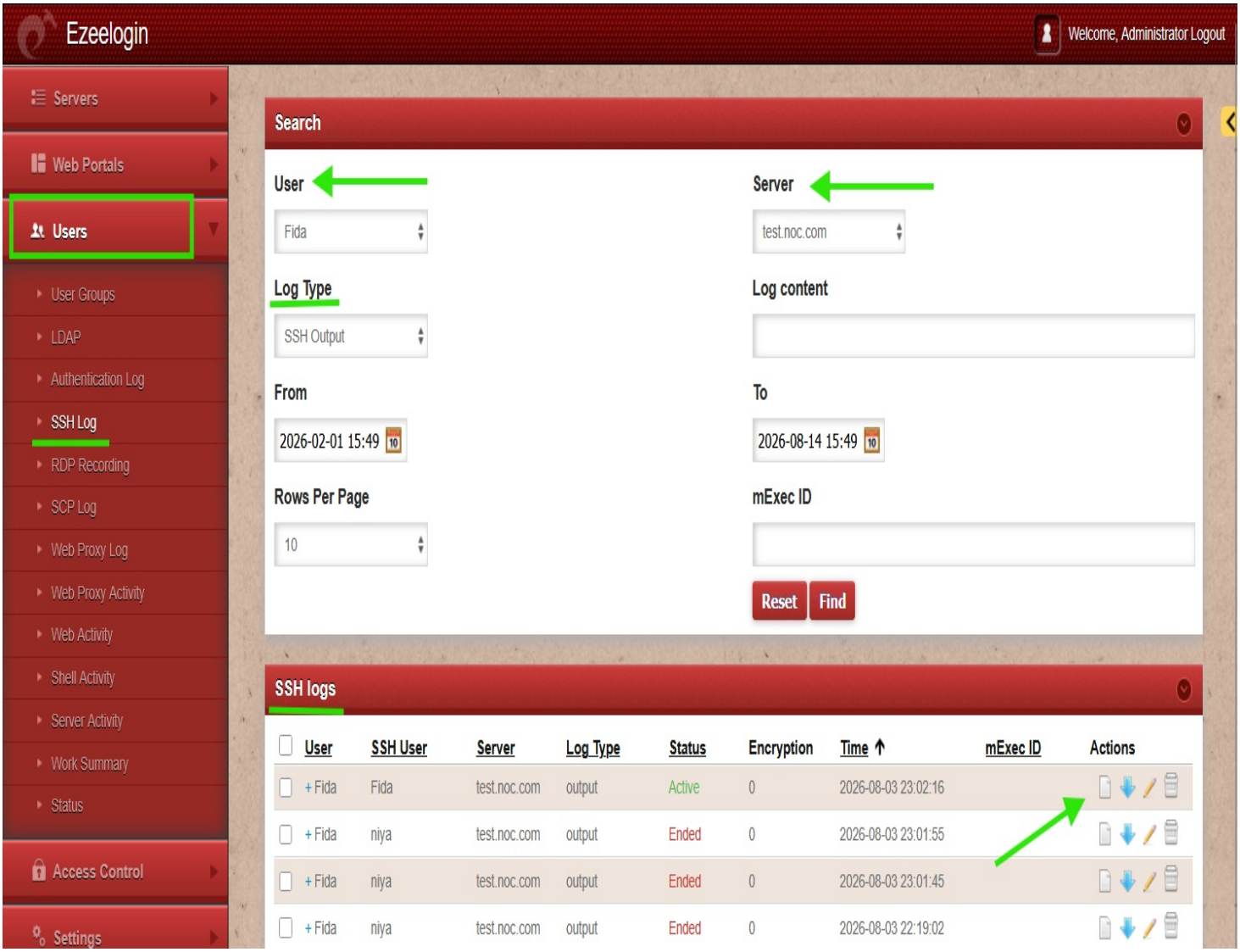
changes of a user that is done using the password command. This would be in violation of security compliance like PCI DSS, HIPAA, NIST, GDPR, etc. We would recommend choosing output only to avoid recording the password in order to meet security compliance.

2. How to view the user ssh sessions recorded on the Ezeelogin ssh jump server GUI?

2.A) Navigate to **users->SSH log** and select the jump server user and the server to view the **recorded ssh session** for that server.

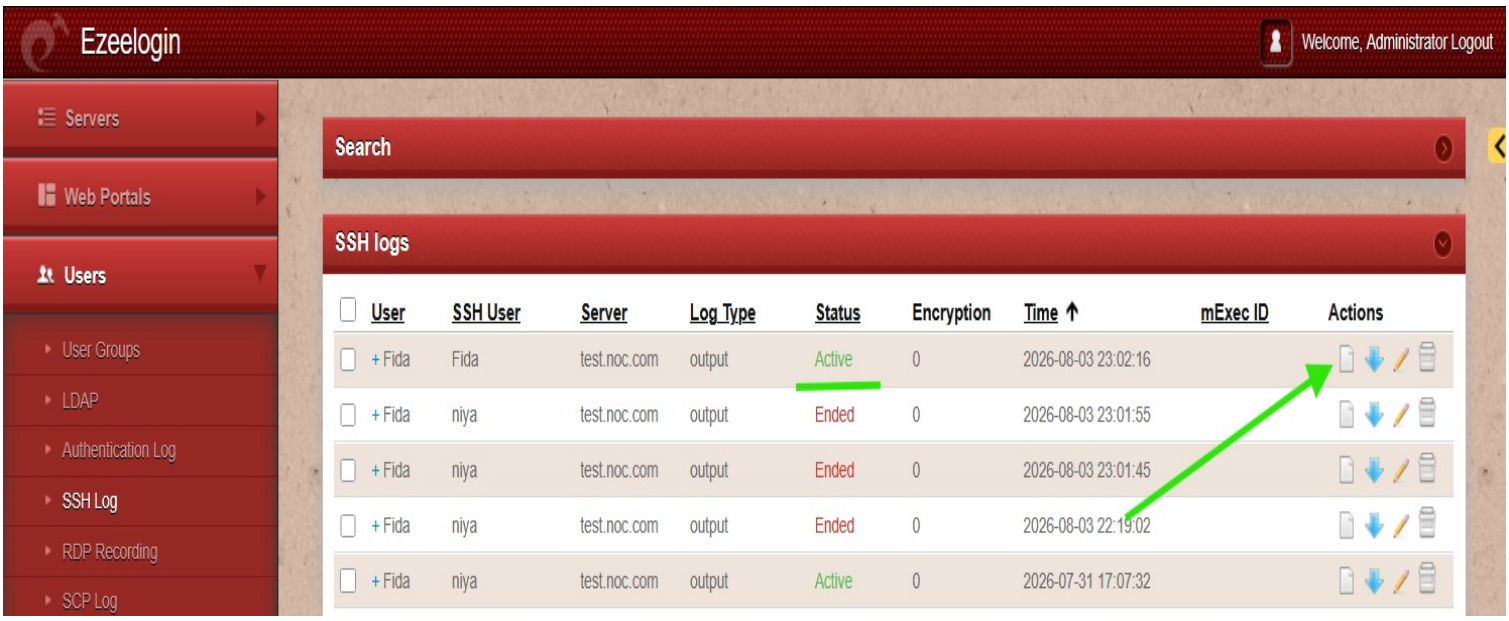


2.B) Click on the 'Log type output' to view the entire ssh session recorded for the user john on the server tesla.eznoc.com. As you can see the entire ssh session is available.



3. How to view the ssh sessions recorded of a user in real-time?

3.A) Identify the ongoing ssh sessions which have the status ' Active' and Click on its 'note' icon on the right.



3.B) Click on enable streaming and choose the interval of 1 second and you will be able to what the jump server user is doing on a server in real-time.

Ensure to disable ssh log encryption under **Settings->General->Security->Encrypt SSH Session logs** so that the Enable streaming button is visible.



The ssh logs recorded for every gateway user is stored in the filesystem directory /var/log/ezlogin/input/{username}. The input directory stores only the inputs from STDIN devices such as keyboard, mouse etc hence the input log would contain every keypress of the user including password and invisible characters. The directory /var/log/ezlogin/full/{username} stores the output from STDOUT devices such as monitor, printer etc, hence the output logs would contain every character that is printed on the screen. It is recommended to enable STDOUT recording under Settings->General->Security->SSH Session Logging->Output. Also, refer the article **strange characters in INPUT logs recorded.** Only the metadata is stored in the Ezeelogin mysql database, ie the path to the files storing the ssh logs and the dates.

```
mysql $(awk '/^db_name/ {print $2}' /usr/local/etc/ezlogin/ez.conf)

MariaDB [ezlogin_mpayl]>  select *  from gjbpe_sshlogs;

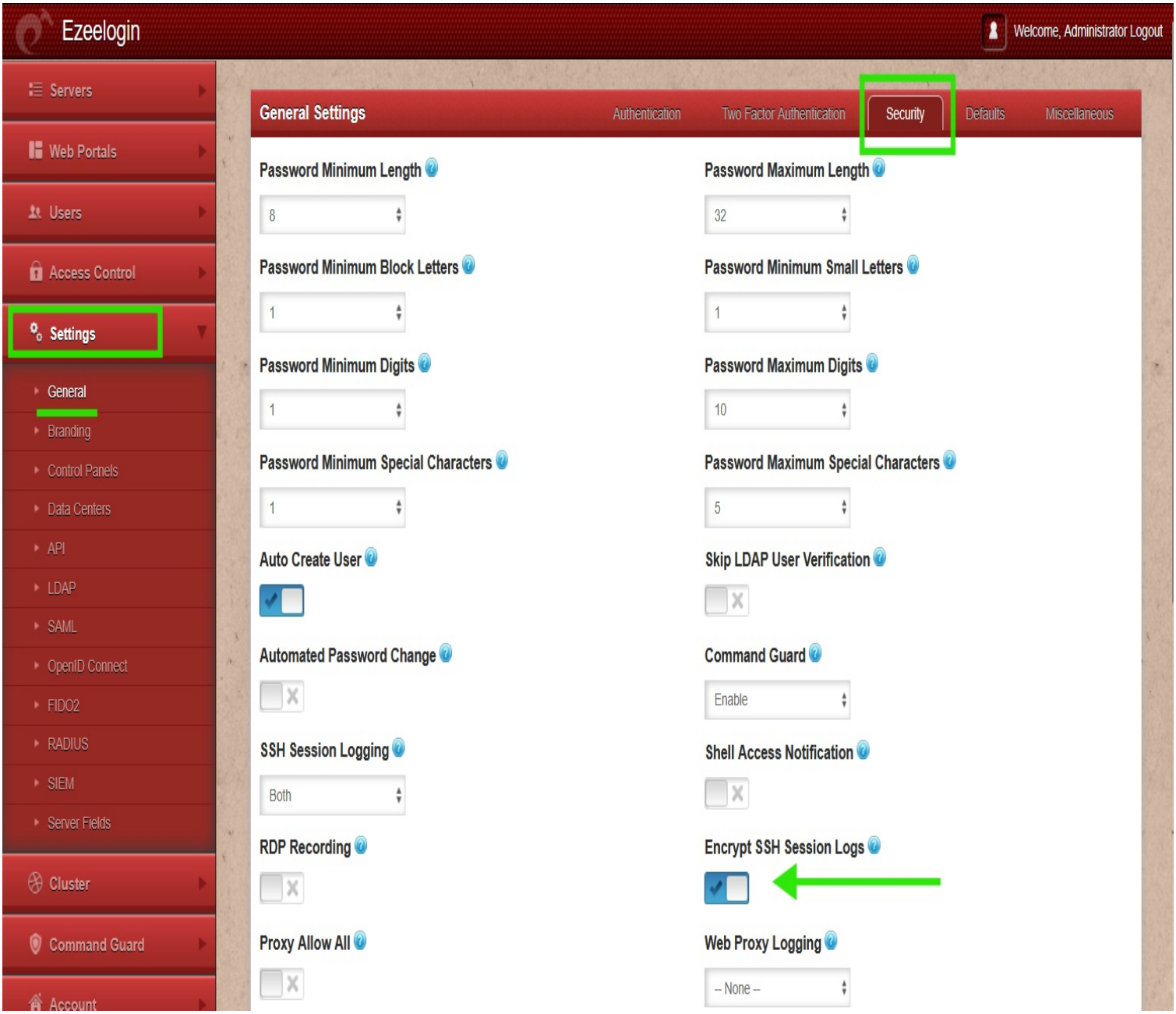
| 727 |      1 |      141 |            871 | root     | input  | end    |
/var/log/ezlogin/input/ezadmin/root~gateway.eznoc.com~Thu_Aug_26_14:02:48_2021

| 728 |      1 |      141 |            871 | root     | full   | end    |
/var/log/ezlogin/full/ezadmin/root~gateway.eznoc.com~Thu_Aug_26_14:02:48_2021
```

4. How to encrypt users ssh session log recorded to meet security compliances?

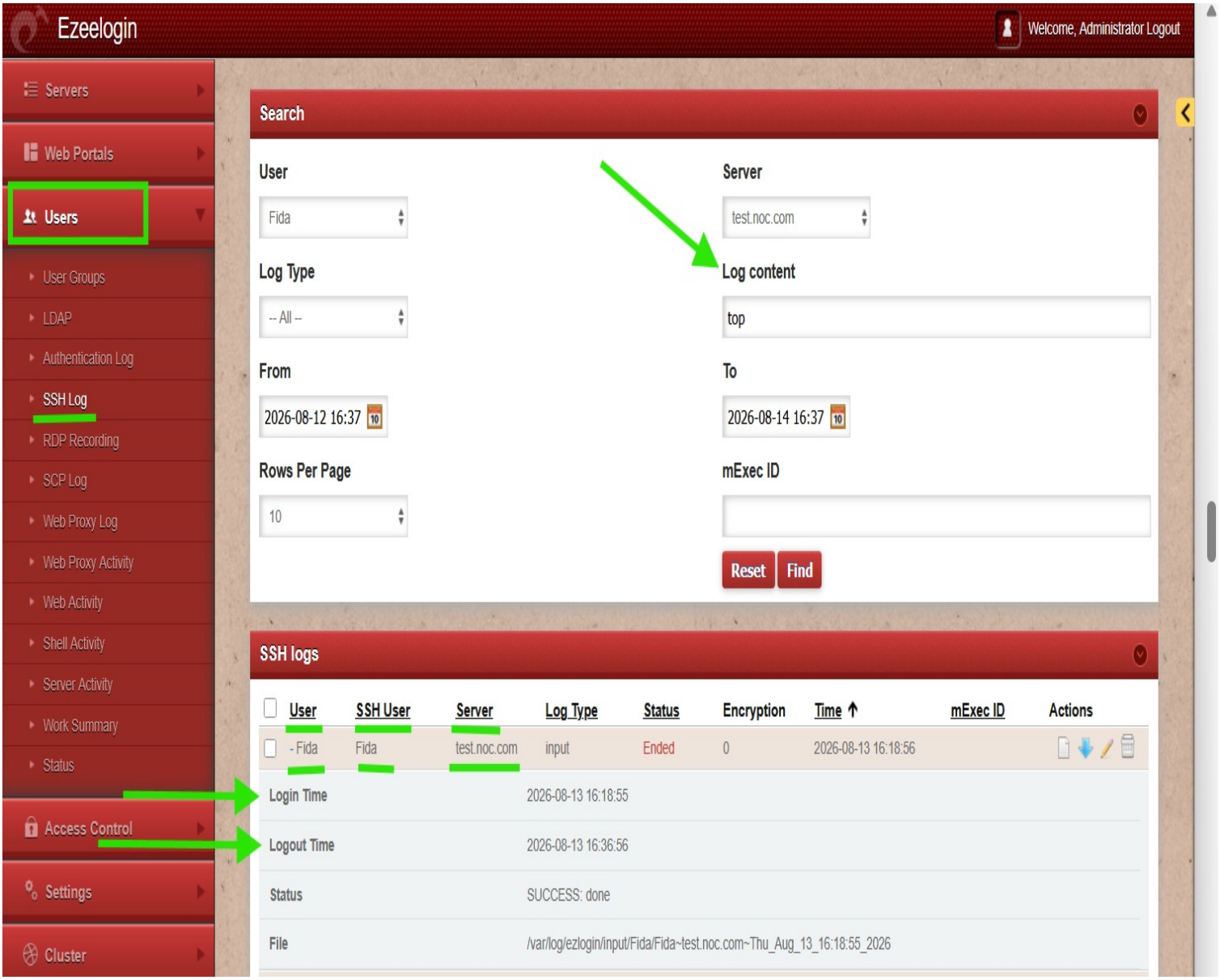
You can enable 'Encrypt ssh session logs' under **Settings-> General-> Security** so that logs are not stored in human readable in the filesystem.

Note: With encryption enabled, the logs are only readable from the GUI. In the backend, the ssh logs are stored encrypted in the /var/log/ezlogin directory and cannot be edited or modified.

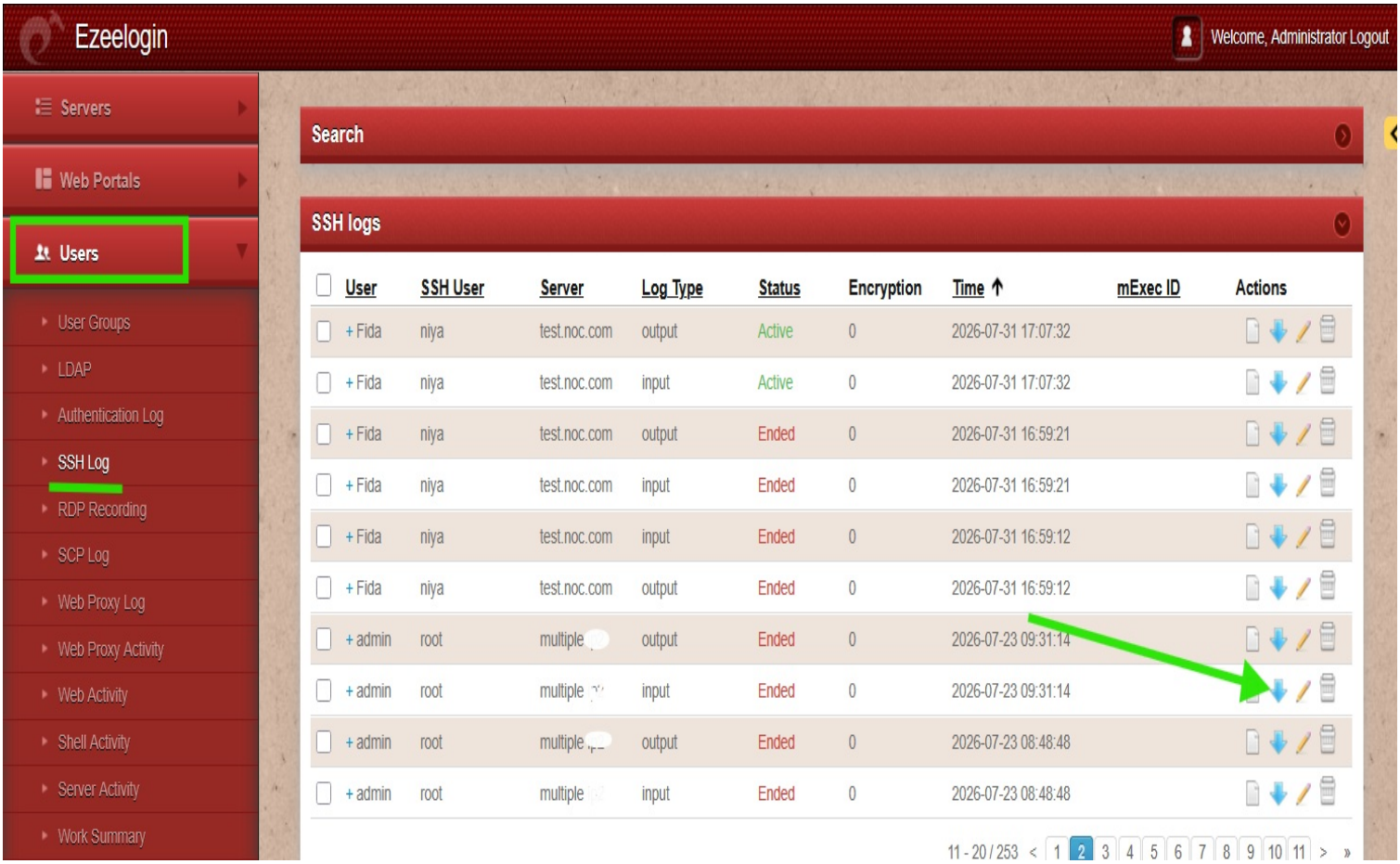


5. How to search the users recorded ssh session logs for specific strings or keywords?

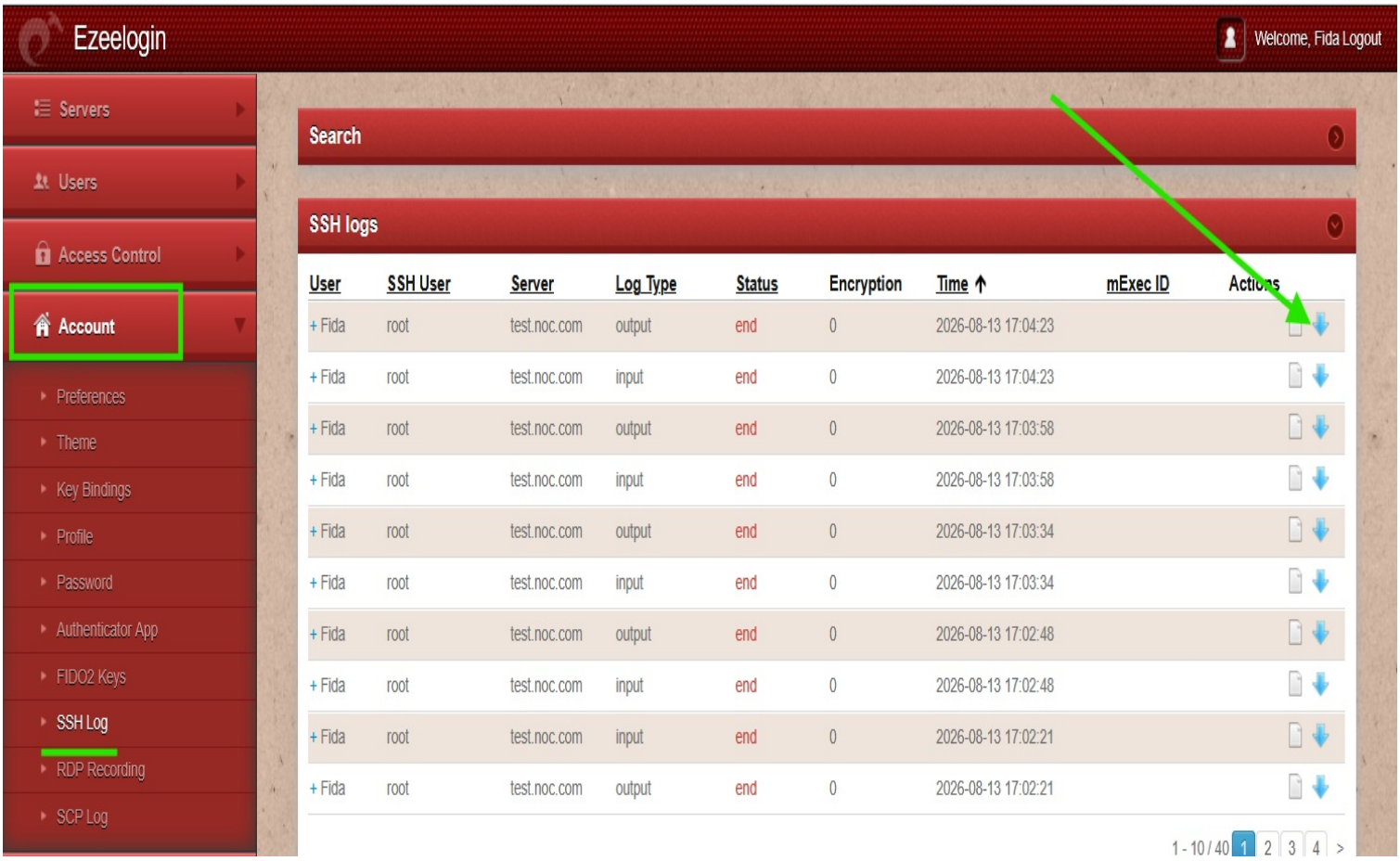
Enter the string to be searched in the field **'Log Content'**. The results show the matching logs and user, username with which the server was accessed and the login and logout times are recorded as well.



6. The Administrator user can download any users ssh session to remote devices as a text file by clicking on the blue arrow as shown below.



7. The normal gateway user can download his own ssh session logs recorded under **Accounts -> SSH Log**



8. How to get local, timestamped logging of all ssh commands?

At the moment only the ssh session start time and end time are recorded and not the times when each command is run. In order to have the timestamps of commands executed in ssh, the easiest method would be add the date in the command prompt in the bash shell as follows.

For Centos, edit bashrc file and add the line at end of the file or refer **article to modify command prompt in CentOS**

```
[root@centos ~]# vi /etc/bashrc
PS1="[\u@\h \D{%Y%m%d-%H:%M:%S}]\$ "
```

An example of adding timestamp on a Centos server.

```
[root@otp ~]# vi /etc/bashrc
PS1="[\u@\h \D{%Y%B%d-%H:%M:%S}]\$ "
```

```
[root@otp 2021March18-12:02:27]$ uptime

12:02:42 up 3 days, 14:58,  2 users,  load average: 0.00, 0.01, 0.05

[root@otp 2021March18-12:02:42]$ date

Thu Mar 18 12:02:43 IST 2021
```

The recorded output session in Ezeelogin will contain the date and timestamp as shown below.



Do refer the article to add the **time in command prompt for OS** such Ubuntu, Debian and others.

FAQ

1. Why are SSH log files (**Users → SSH Logs** in the Ezeelogin GUI) still present after deletion from the web interface?

Deleting log entries from the Ezeelogin web interface only removes the metadata from the database. The actual log files stored on the filesystem under /var/log/ezlogin/ are not deleted.

To restore the metadata for these logs back into the web interface, use the following command:

```
root@gateway:/usr/local/ezlogin/eztool.php -reimport_logs
```

This command re-imports the log metadata from the log files that still exist on disk.

2. Is there any impact if the logs in /var/log/ezlogin/ are deleted?

No, the logs in /var/log/ezlogin/ can be safely deleted without affecting system functionality. However, once deleted, these logs cannot be recovered.

⚠️ **Recording of software tools using ncurses libraries or text based graphical libraries such as htop, top, midnight commander is not supported.**

Related Articles:

How to truncate the ssh session logs recorded

how do i access the ssh logs history that was recorded for the ssh user ?

Issue with Log Retain Duration

How to transfer Ezeelogin SSH session logs recorded to a remote server ?

strange characters in the SSH logs recordings

Is it possible to view all ssh logs of a deleted user ?

Online URL: https://www.ezeelogin.com/kb/article/record-ssh-sessions-208.html