Record ssh sessions

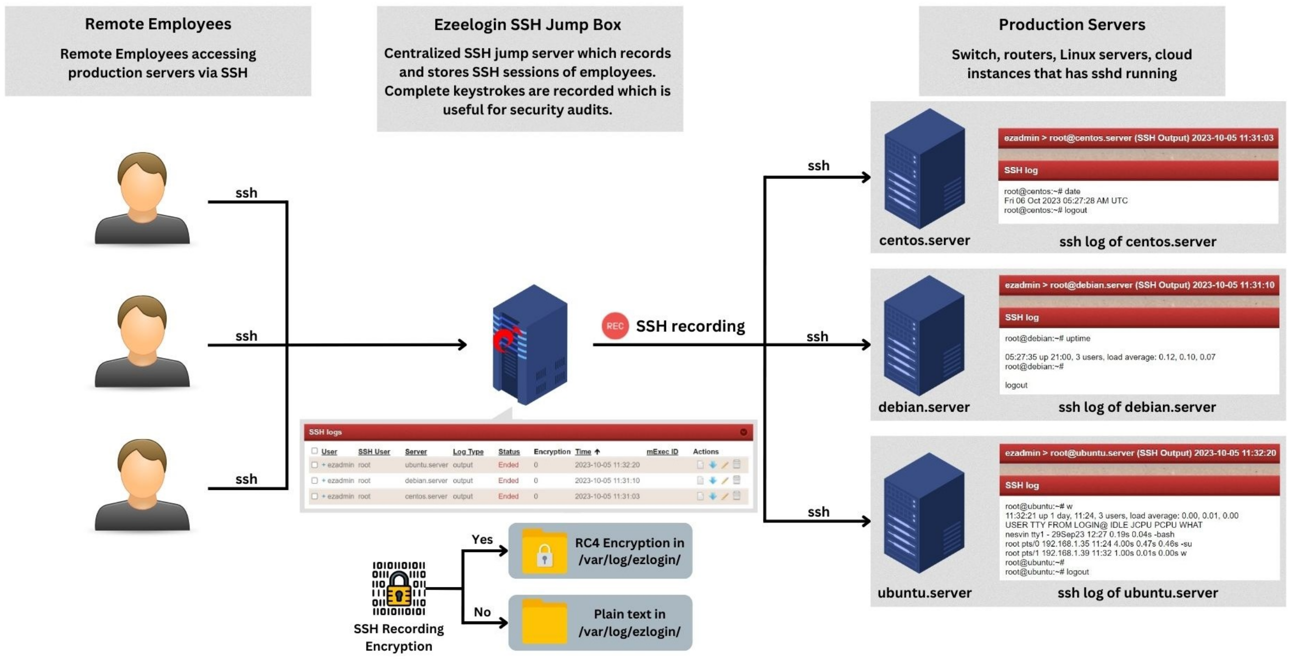
208 admin October 30, 2023 Security Features 11747

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?

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.).


Remote Employees
Remote Employees accessing production servers via SSH
Ezeelogin SSH Jump Box
Centralized SSH jump server which records and stores SSH sessions of employees. Complete keystrokes are recorded which is useful for security audits.
Production Servers
Switch, routers, Linux servers, cloud instances that has sshd running
ssh
ssh
ssh
REC
SSH recording
ssh
ssh
ssh
centos.server
ssh log of centos.server
debian.server
ssh log of debian.server
ubuntu.server
ssh log of ubuntu.server
SSH Recording Encryption
Yes
RC4 Encryption in /var/log/ezlogin/
No
Plain text in /var/log/ezlogin/

SSH logs

□	User	SSH User	Server	Log Type	Status	Encryption	Time ↑	mExec ID	Actions
□	+ ezadmin	root	ubuntu.server	output	Ended	0	2023-10-05 11:32:20		
□	+ ezadmin	root	debian.server	output	Ended	0	2023-10-05 11:31:10		
□	+ ezadmin	root	centos.server	output	Ended	0	2023-10-05 11:31:03		

ezadmin > root@centos.server (SSH Output) 2023-10-05 11:31:03

SSH log

```
root@centos:~# date
Fri 06 Oct 2023 05:27:28 AM UTC
root@centos:~# logout
```

ezadmin > root@debian.server (SSH Output) 2023-10-05 11:31:10

SSH log

```
root@debian:~# uptime

05:27:35 up 21:00, 3 users, load average: 0.12, 0.10, 0.07
root@debian:~#

logout
```

ezadmin > root@ubuntu.server (SSH Output) 2023-10-05 11:32:20

SSH log

```
root@ubuntu:~# w
11:32:21 up 1 day, 11:24, 3 users, load average: 0.00, 0.01, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
nesvin tty1 - 29Sep23 12:27 0.19s 0.04s -bash
root pts/0 192.168.1.35 11:24 4.00s 0.47s 0.46s -su
root pts/1 192.168.1.39 11:32 1.00s 0.01s 0.00s w
root@ubuntu:~#
root@ubuntu:~# logout
```

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.

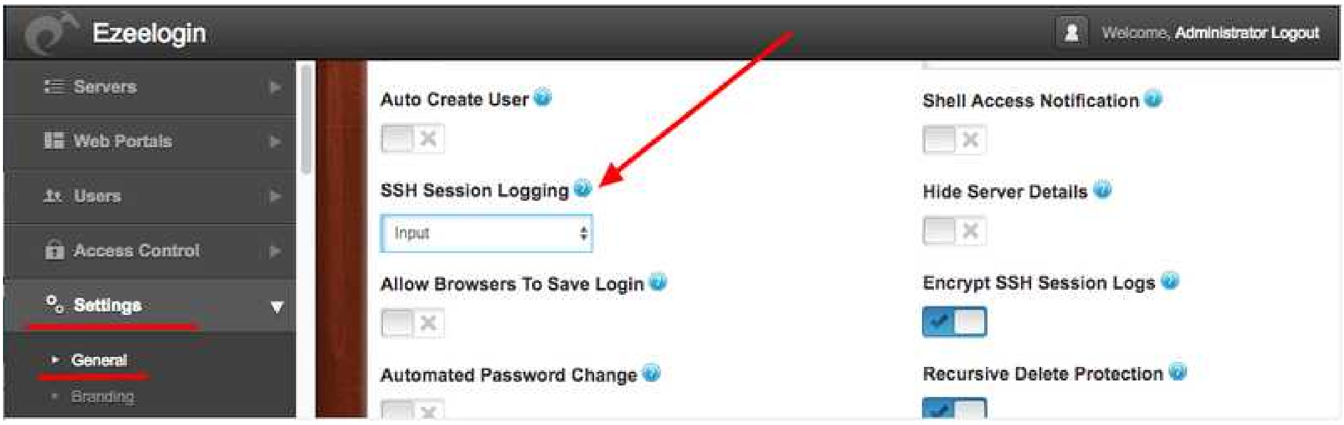
IMPORTANT

`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 compliances like pci dss, hippa, nist , nerc, ffiec as record ssh session 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



Auto Create User ☒

SSH Session Logging: Input

Allow Browsers To Save Login ☒

Automated Password Change ☒

Shell Access Notification ☒

Hide Server Details ☒

Encrypt SSH Session Logs ✓

Recursive Delete Protection ✓

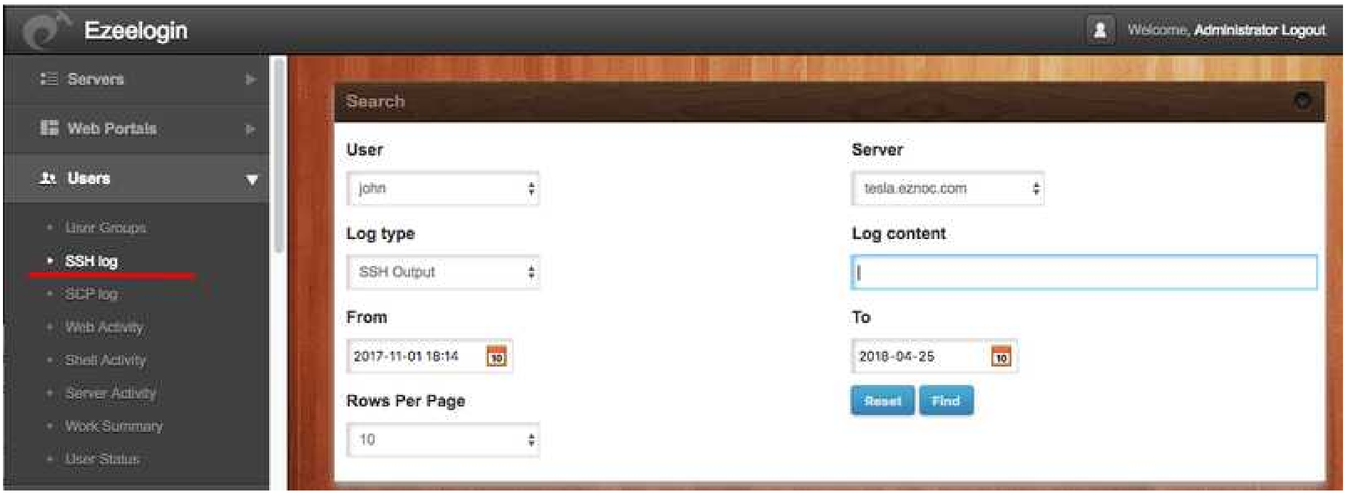
There are 3 settings to record the ssh sessions

1. None - This would disable ssh session recording.
2. Input - This would record only the STDIN, which would be the keyboard inputs of the ssh jump server user.
3. Output - This would record only the STDOUT which would be the outputs on the screen of the jump server user.
4. 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 compliances like PCI DSS, HIPPA, MAS, NIST, GDPR, FFIEC, 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?

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



User: john

Server: tesla.eznoc.com

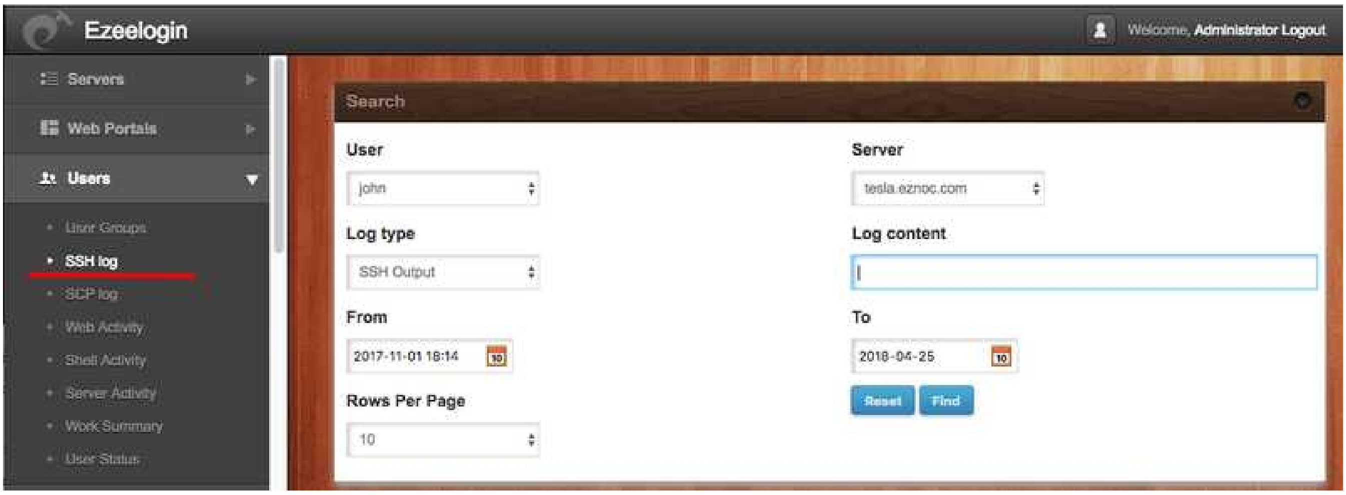
Log type: SSH Output

Log content:

From: 2017-11-01 18:14

To: 2018-04-25

Rows Per Page: 10



User: john

Server: tesla.eznoc.com

Log type: SSH Output

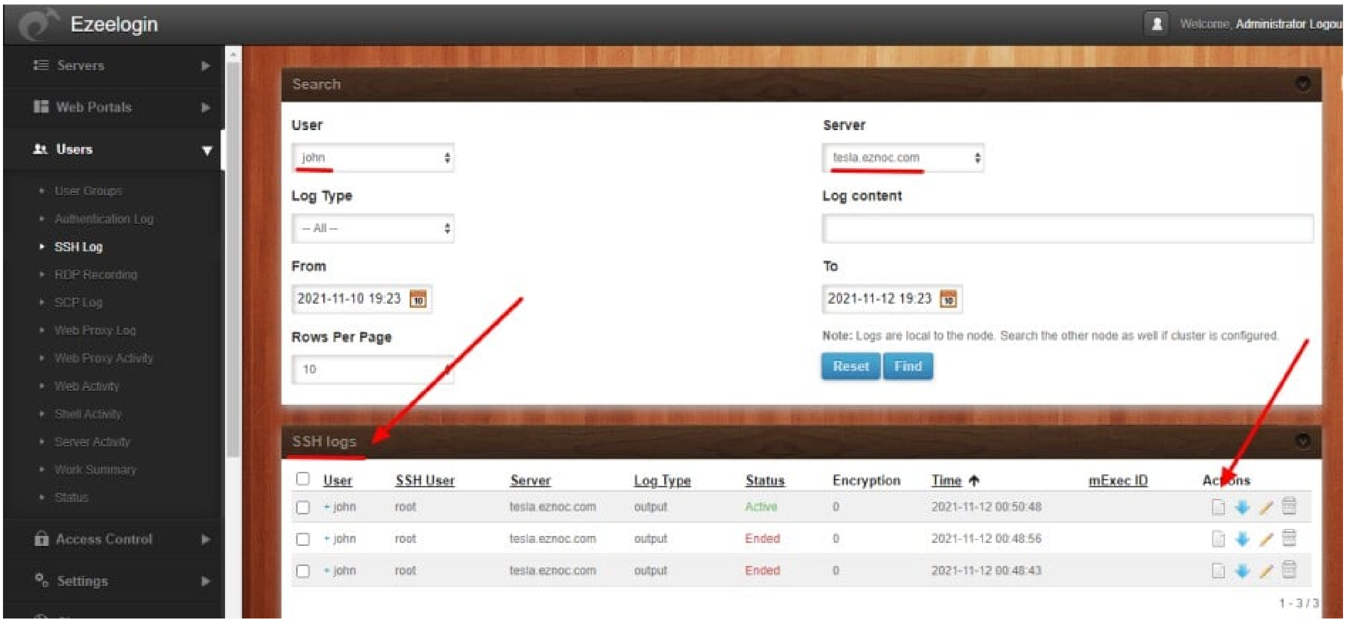
Log content:

From: 2017-11-01 18:14

To: 2018-04-25

Rows Per Page: 10

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.



User: john

Server: tesla.eznoc.com

Log Type: -- All --

Log content:

From: 2021-11-10 19:23

To: 2021-11-12 19:23

Rows Per Page: 10

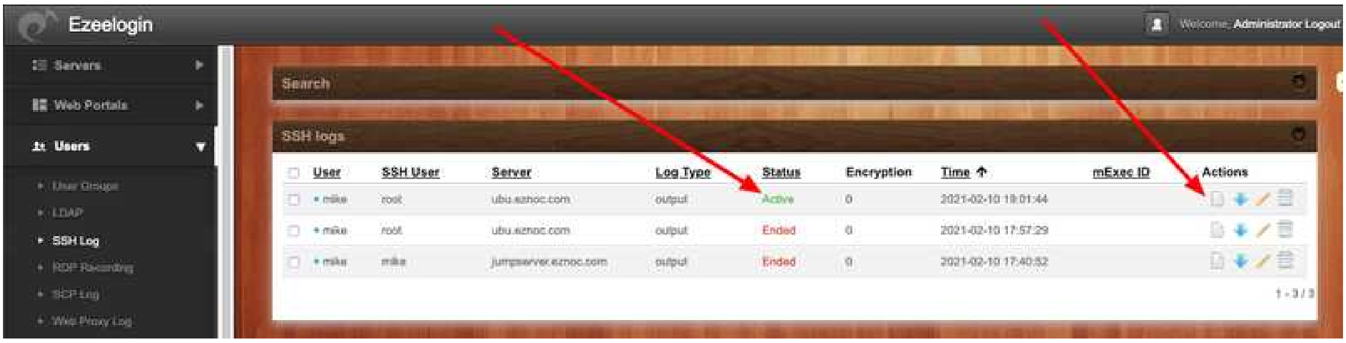
Note: Logs are local to the node. Search the other node as well if cluster is configured.

	User	SSH User	Server	Log Type	Status	Encryption	Time ↑	mExec ID	Actions
□	john	root	tesla.eznoc.com	output	Active	0	2021-11-12 00:50:48		
□	john	root	tesla.eznoc.com	output	Ended	0	2021-11-12 00:48:56		
□	john	root	tesla.eznoc.com	output	Ended	0	2021-11-12 00:48:43		

1 - 3 / 3

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

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

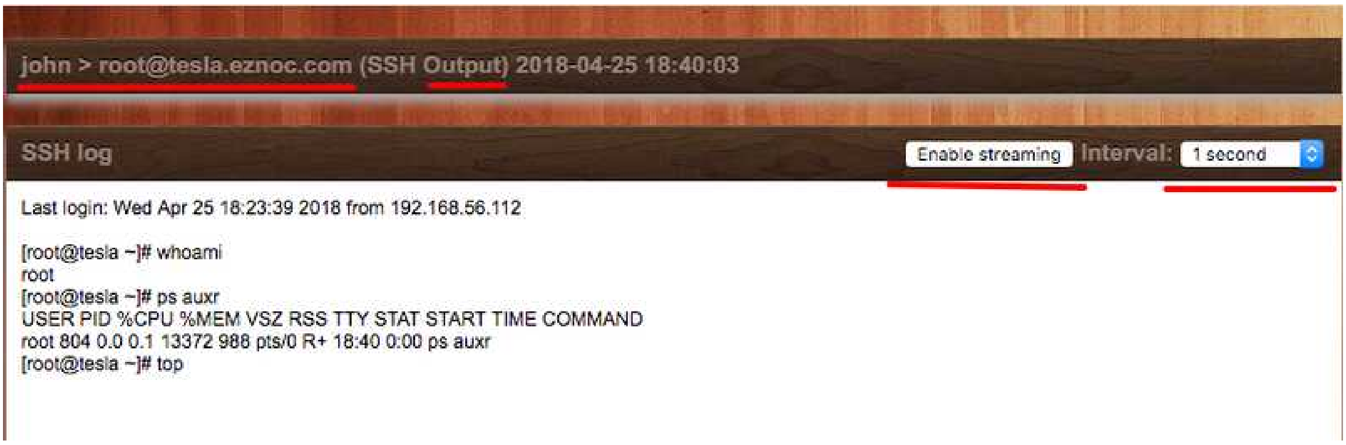


	User	SSH User	Server	Log Type	Status	Encryption	Time ↑	mExec ID	Actions
□	mike	root	ubu.eznoc.com	output	Active	0	2021-02-10 18:01:44		
□	mike	root	ubu.eznoc.com	output	Ended	0	2021-02-10 17:57:29		
□	mike	mike	jumpserver.eznoc.com	output	Ended	0	2021-02-10 17:40:52		

1 - 3 / 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.


john > root@tesla.eznoc.com (SSH Output) 2018-04-25 18:40:03
SSH log
Enable streaming
Interval:
1 second

```
Last login: Wed Apr 25 18:23:39 2018 from 192.168.56.112

[root@tesla ~]# whoami
root
[root@tesla ~]# ps auxr
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 804 0.0 0.1 13372 988 pts/0 R+ 18:40 0:00 ps auxr
[root@tesla ~]# top
```

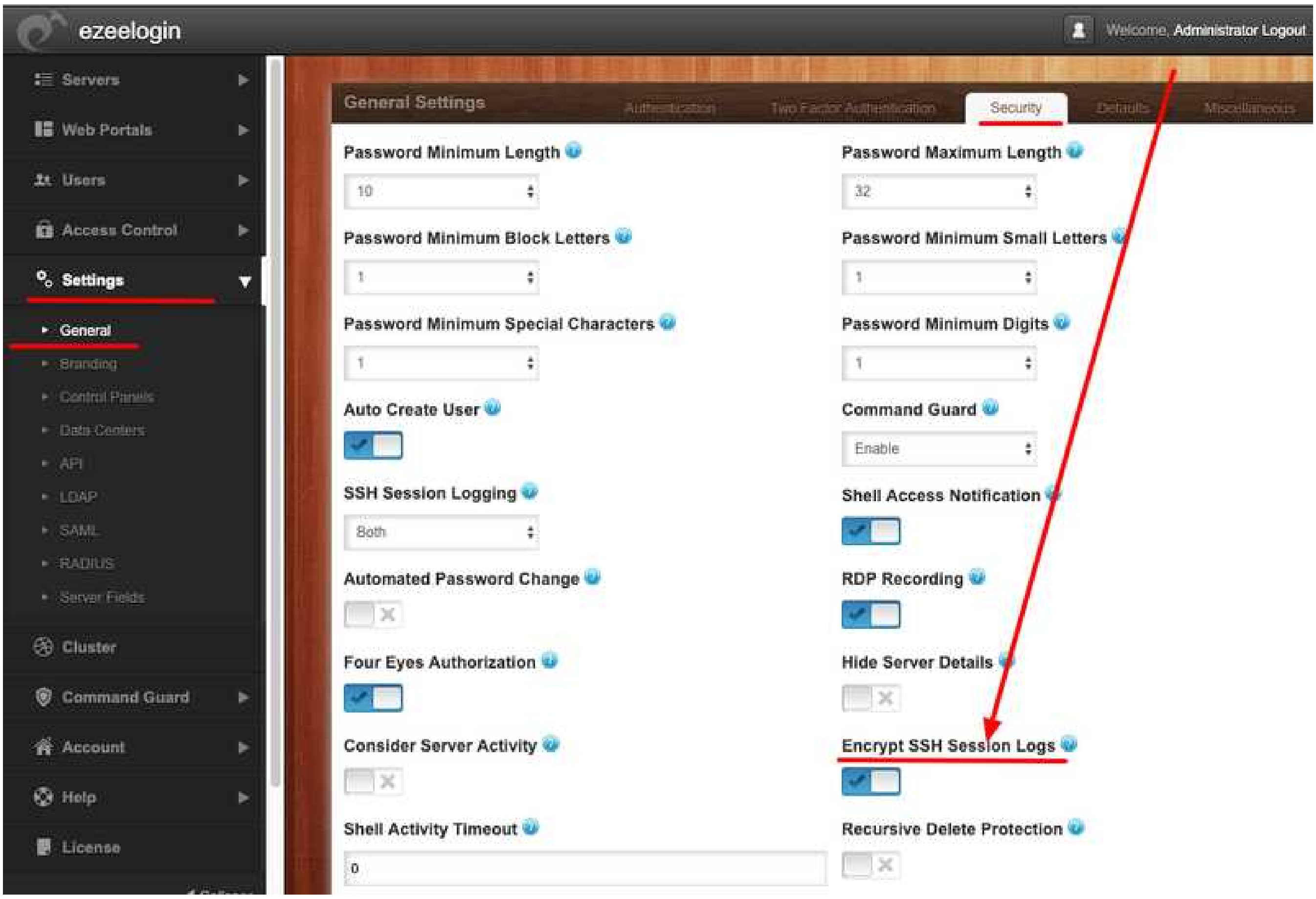
The ssh logs recorded for every gateway user is stored in the filesystem directory /var/log/ezlogin/input/{username}. The input directory stores only the inputs from STDIN devices such as keyboard, mouse etc hence the input log would contain every keypress of the user including password and invisible 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.



Password Minimum Length: 10

Password Minimum Block Letters: 1

Password Minimum Special Characters: 1

Auto Create User: ✓

SSH Session Logging: Both

Automated Password Change: ✗

Four Eyes Authorization: ✓

Consider Server Activity: ✗

Shell Activity Timeout: 0

Password Maximum Length: 32

Password Minimum Small Letters: 1

Password Minimum Digits: 1

Command Guard: Enable

Shell Access Notification: ✓

RDP Recording: ✓

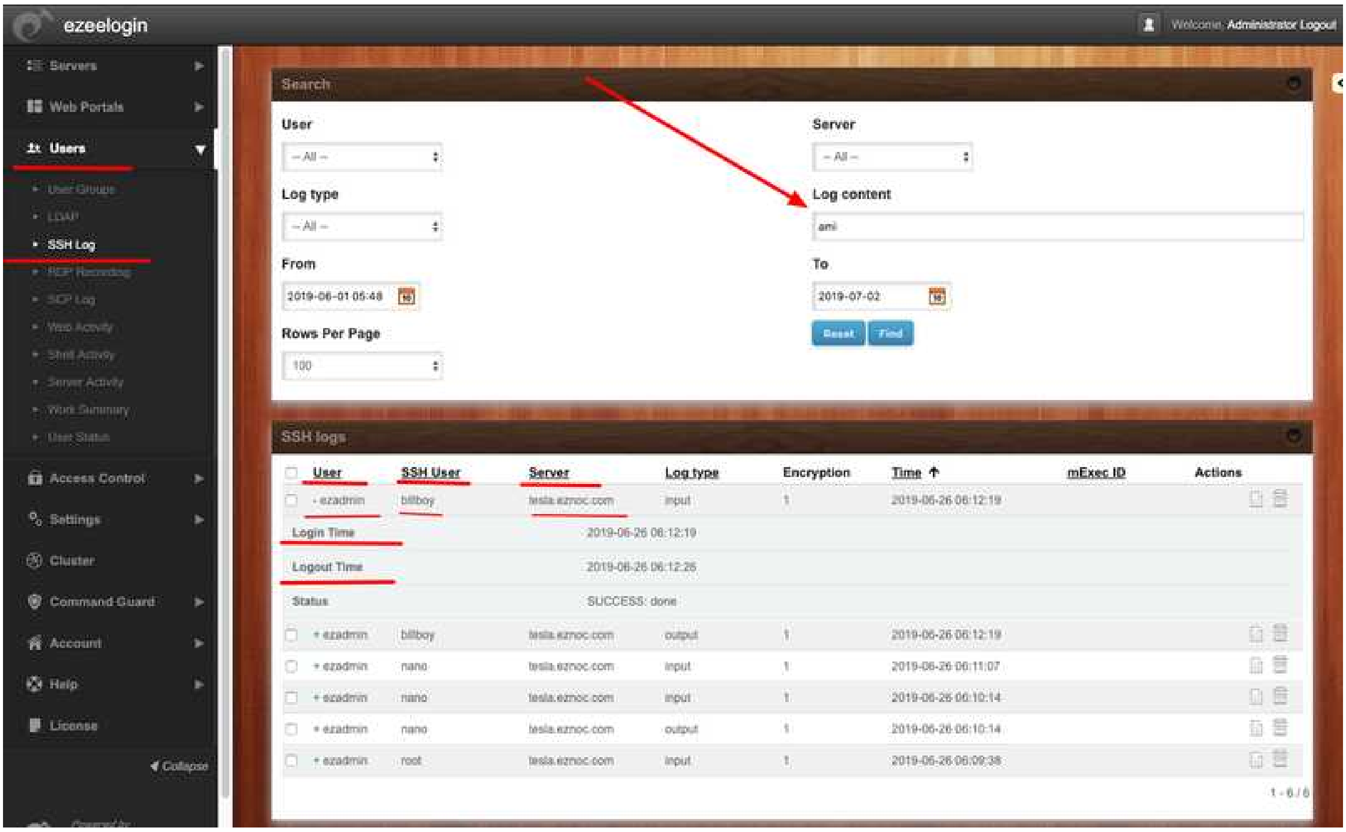
Hide Server Details: ✗

Encrypt SSH Session Logs: ✓

Recursive Delete Protection: ✗

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.



User: -- All --

Server: -- All --

Log type: -- All --

Log content: ami

From: 2019-06-01 05:48

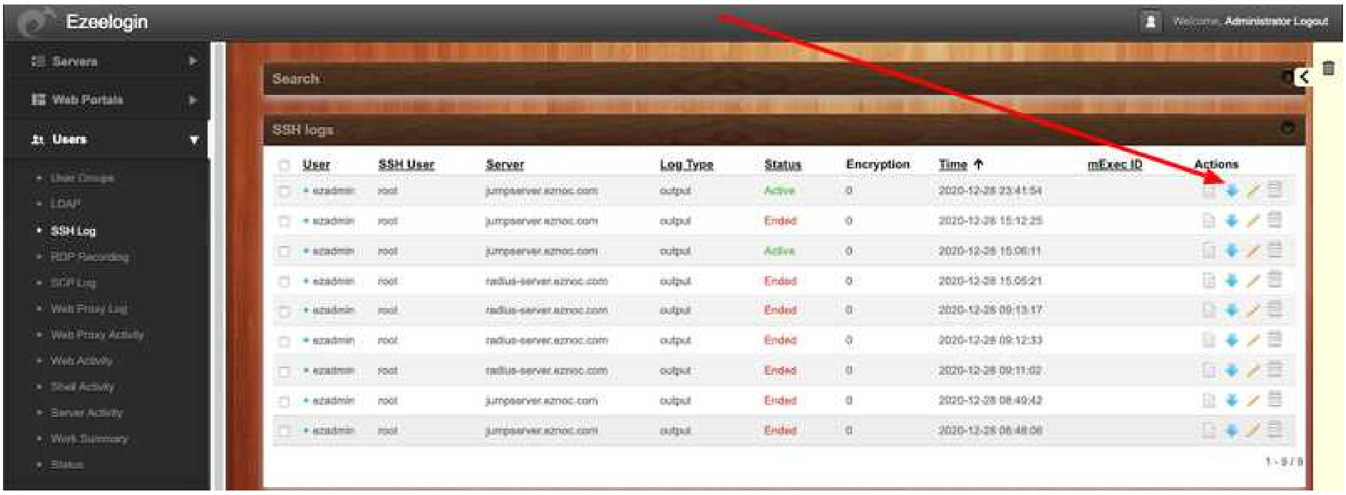
To: 2019-07-02

Rows Per Page: 100

☐	User	SSH User	Server	Log type	Encryption	Time ↑	mExec ID	Actions
☐	- ezadmin	billboy	tesla.eznoc.com	input	1	2019-06-26 06:12:19		
Login Time			2019-06-26 06:12:19					
Logout Time			2019-06-26 06:12:26					
Status			SUCCESS: done					
☐	+ ezadmin	billboy	tesla.eznoc.com	output	1	2019-06-26 06:12:19		
☐	+ ezadmin	nano	tesla.eznoc.com	input	1	2019-06-26 06:11:07		
☐	+ ezadmin	nano	tesla.eznoc.com	input	1	2019-06-26 06:10:14		
☐	+ ezadmin	nano	tesla.eznoc.com	output	1	2019-06-26 06:10:14		
☐	+ ezadmin	root	tesla.eznoc.com	input	1	2019-06-26 06:09:38		

1 - 6 / 6

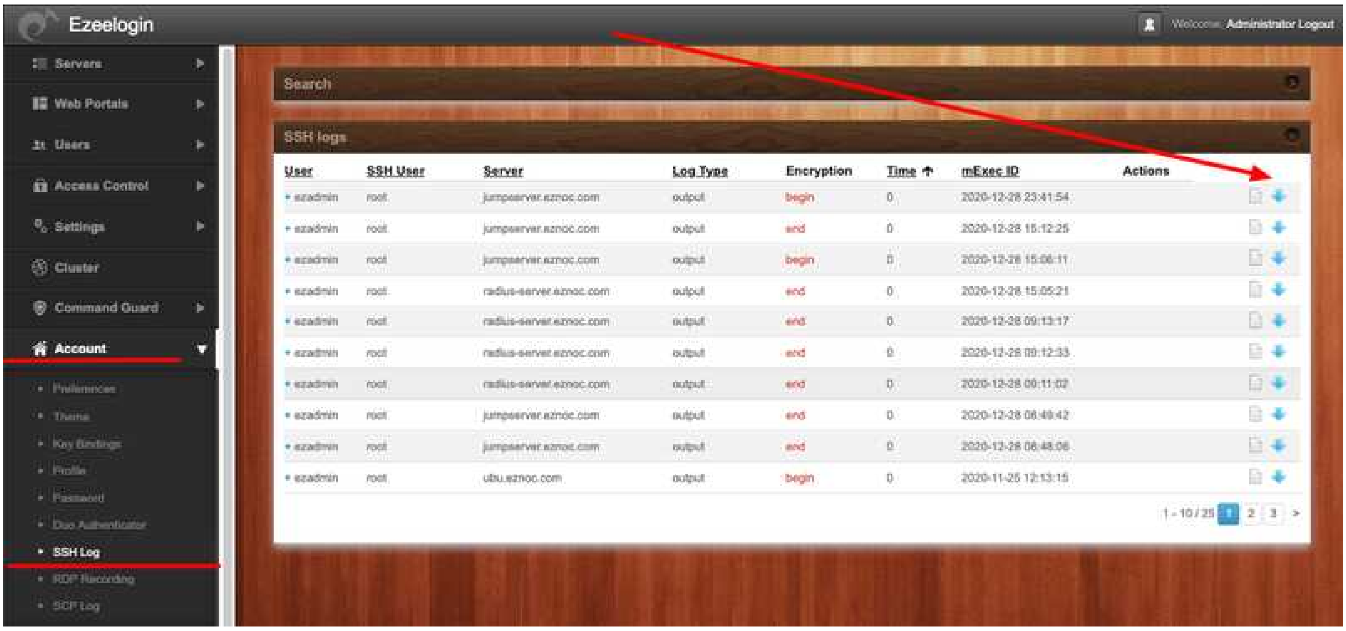
6. The Administrator user can download any users ssh session to remote devices as a text file by clicking on the blue arrow as shown below.



User	SSH User	Server	Log Type	Status	Encryption	Time ↑	mExec ID	Actions
ezadmin	root	jumpserver.eznoc.com	output	Active	0	2020-12-28 23:41:54		
ezadmin	root	jumpserver.eznoc.com	output	Ended	0	2020-12-28 15:12:25		
ezadmin	root	jumpserver.eznoc.com	output	Active	0	2020-12-28 15:06:11		
ezadmin	root	radius-server.eznoc.com	output	Ended	0	2020-12-28 15:05:21		
ezadmin	root	radius-server.eznoc.com	output	Ended	0	2020-12-28 09:13:17		
ezadmin	root	radius-server.eznoc.com	output	Ended	0	2020-12-28 09:12:33		
ezadmin	root	radius-server.eznoc.com	output	Ended	0	2020-12-28 09:11:02		
ezadmin	root	jumpserver.eznoc.com	output	Ended	0	2020-12-28 08:49:42		
ezadmin	root	jumpserver.eznoc.com	output	Ended	0	2020-12-28 08:48:06		

1 - 9 / 9

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



User	SSH User	Server	Log Type	Encryption	Time ↑	mExec ID	Actions
ezadmin	root	jumpserver.eznoc.com	output	begin	0	2020-12-28 23:41:54	
ezadmin	root	jumpserver.eznoc.com	output	end	0	2020-12-28 15:12:25	
ezadmin	root	jumpserver.eznoc.com	output	begin	0	2020-12-28 15:06:11	
ezadmin	root	radius-server.eznoc.com	output	end	0	2020-12-28 15:05:21	
ezadmin	root	radius-server.eznoc.com	output	end	0	2020-12-28 09:13:17	
ezadmin	root	radius-server.eznoc.com	output	end	0	2020-12-28 09:12:33	
ezadmin	root	radius-server.eznoc.com	output	end	0	2020-12-28 09:11:02	
ezadmin	root	jumpserver.eznoc.com	output	end	0	2020-12-28 08:49:42	
ezadmin	root	jumpserver.eznoc.com	output	end	0	2020-12-28 08:48:06	
ezadmin	root	ubu.eznoc.com	output	begin	0	2020-11-25 12:13:15	

1 - 10 / 25 1 2 3 >

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

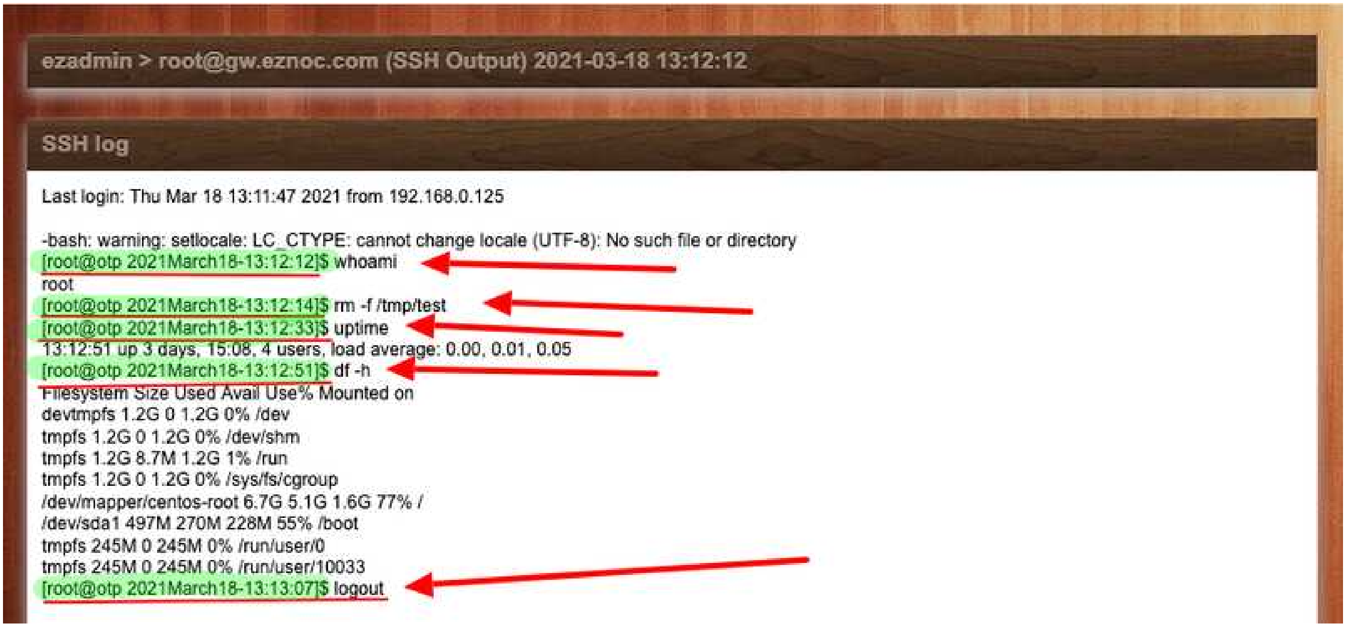
```
[root@centos ~]# vi /etc/bashrc

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.



ezadmin > root@gw.eznoc.com (SSH Output) 2021-03-18 13:12:12
SSH log

```
Last login: Thu Mar 18 13:11:47 2021 from 192.168.0.125

-bash: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file or directory
[root@otp 2021March18-13:12:12]$ whoami
root
[root@otp 2021March18-13:12:14]$ rm -f /tmp/test
[root@otp 2021March18-13:12:33]$ uptime
13:12:51 up 3 days, 15:08, 4 users, load average: 0.00, 0.01, 0.05
[root@otp 2021March18-13:12:51]$ df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 1.2G 0 1.2G 0% /dev
tmpfs 1.2G 0 1.2G 0% /dev/shm
tmpfs 1.2G 8.7M 1.2G 1% /run
tmpfs 1.2G 0 1.2G 0% /sys/fs/cgroup
/dev/mapper/centos-root 6.7G 5.1G 1.6G 77% /
/dev/sda1 497M 270M 228M 55% /boot
tmpfs 245M 0 245M 0% /run/user/0
tmpfs 245M 0 245M 0% /run/user/10033
[root@otp 2021March18-13:13:07]$ logout
```

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

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

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