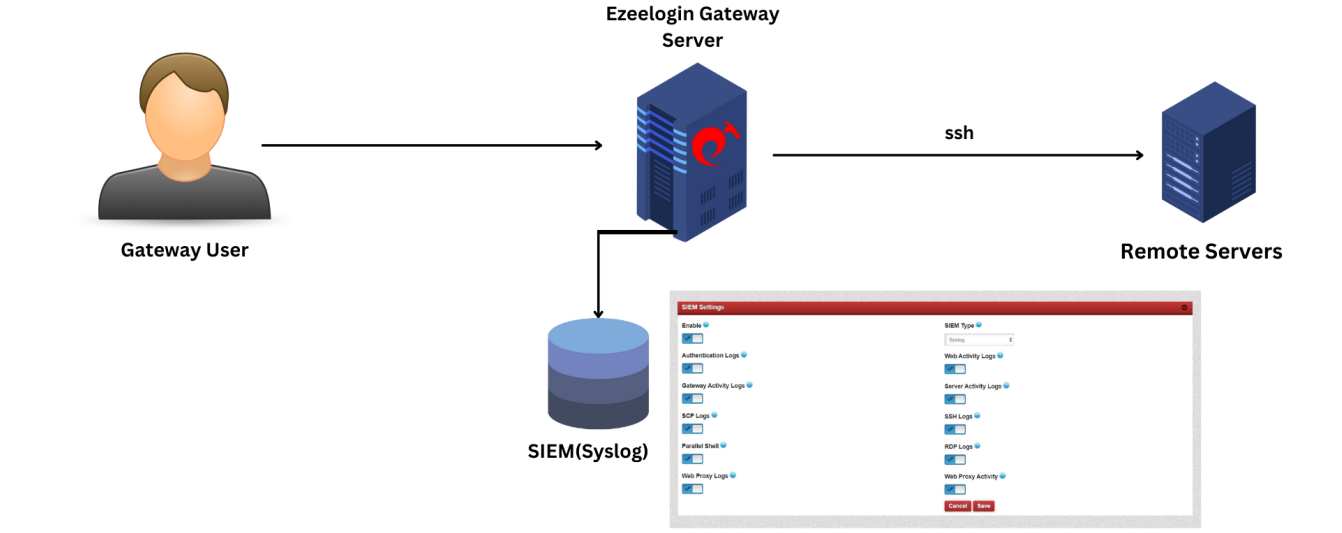
Integrate SSH Jump Server with syslog

670 Nesvin KN April 18, 2025 Productivity & Efficiency Features 1988

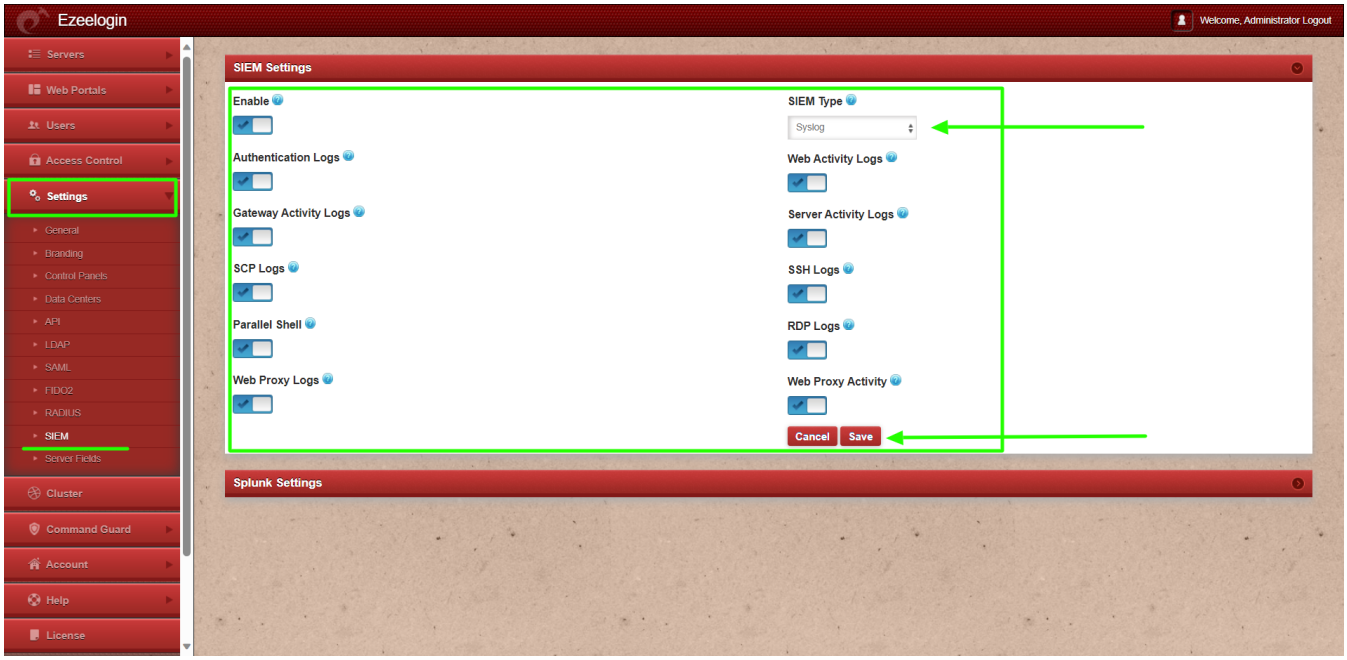
How to forward SSH Jump Server logs to syslog?

Overview: This article describes how to forward SSH Jump Server logs to the syslog by enabling SIEM settings, allowing centralized monitoring of authentication, activity, and command logs.

By enabling this feature, all active logs will be directed to the syslog of the gateway server, which you can monitor by tailing the syslog.



Step 1: Login to Web GUI and navigate to **Settings - > SIEM -> SIEM type to syslog** and **enable logs**.



By enabling this feature, all active logs will be directed to the syslog of the gateway server. You can monitor these logs by tailing the syslog and executing the SIEM script in a separate shell to analyze the forwarded logs.

```
root@gateway :~# tail -f /var/log/syslog  //for ubuntu

root@gateway :~# tail -f /var/log/messages  //for centos

root@gateway :~# php /usr/local/ezlogin/siem_push.php
```

Refer below examples for syslog logs:

- **Authentication Log**


```
Jan 22 11:57:07 gw-master ezeelogin: {"id":"898","user_id":"1","controller":"auth","function":"logout","objective":"0","description":null,"creat
ed":"2024-01-22 11:57:05","username":"ezadmin"}
Jan 22 11:57:23 gw-master ezeelogin: {"id":"899","user_id":"1","controller":"auth","function":"login","objective":"0","description":null,"create
d":"2024-01-22 11:57:18","username":"ezadmin"}
```


- **Web Activity Logs**


```
Jan 22 12:00:23 gw-master ezeelogin: {"id":"901","user_id":"1","controller":"settings","function":"index","objective":"","description":null,"cre
ated":"2024-01-22 12:00:21","username":"ezadmin"}
```


- **Gateway Activity Logs**


```
Jan 22 12:02:38 gw-master ezeelogin: {"id":"79","user_id":"1","uid":"1001","remote_ip":"192.168.1.34","remote_port":"55688","local_ip":"192.168.
1.36","local_port":"22","login_time":"2024-01-22 12:02:30","logout_time":"2024-01-22 12:02:34","idle_time":"0","remote_time":"0","status":"SUCCE
SS","reason":"","username":"ezadmin"}
```


- **Server Activity Logs**


```
Jan 22 12:05:15 gw-master ezeelogin: {"id":"43","user_id":"1","server_id":"1","gwactivity_id":"79","login_time":"2024-01-22 12:05:12","logout_ti
me":"2024-01-22 12:05:13","input_idle_time":"0","output_idle_time":"0","status":"SUCCESS: login","reason":null,"type":"SHELL","username":"ezadmi
n","server":"ubuntu.server"}
```

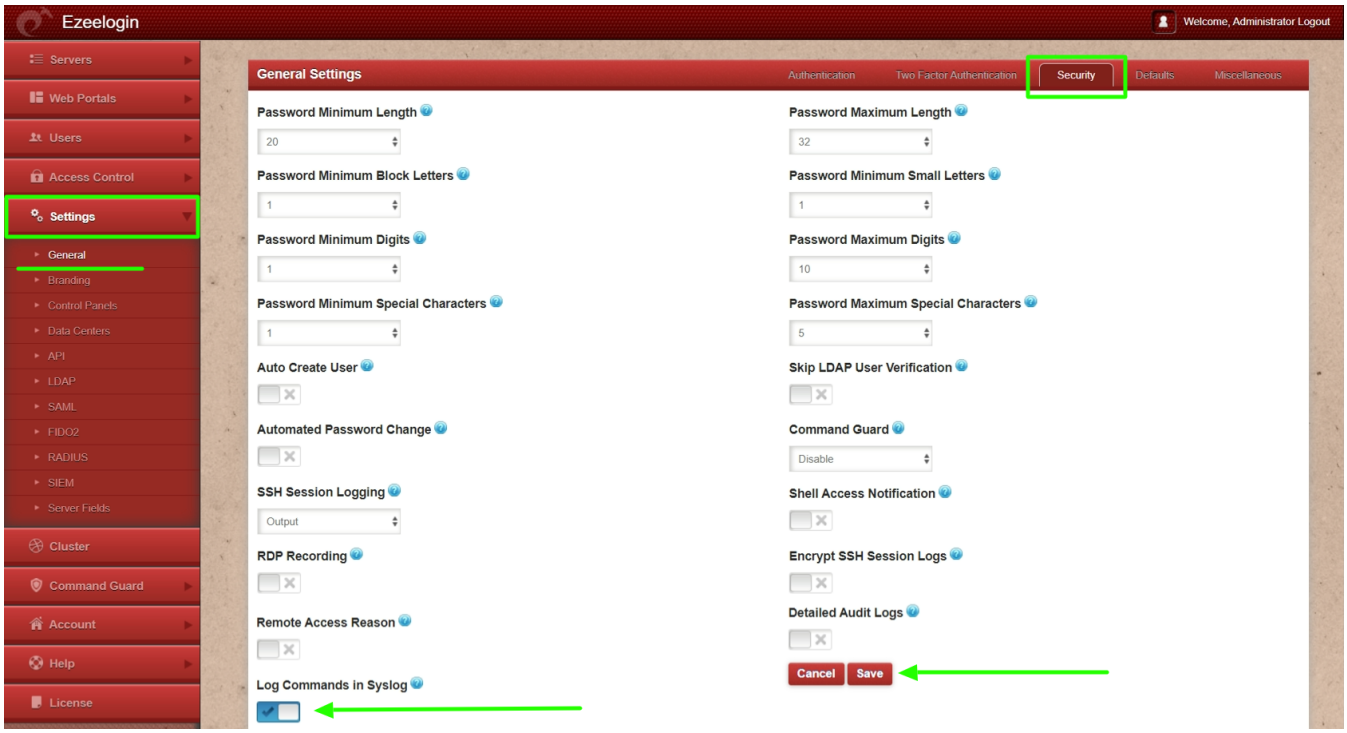

- **SSH Logs**


```
Jan 22 12:05:15 gw-master ezeelogin: {"id":"28","user_id":"1","server_id":"1","serveractivity_id":"43","ssh_user":"root","type":"full","status":
"begin","reason":null,"file":"\/var\/log\/ezlogin\/full\/ezadmin\/root~ubuntu.server~Mon_Jan_22_12:05:12_2024","comments":null,"encryption":"0",
"mexecid":"","created":"2024-01-22 12:05:13","mtime":"2024-01-22 12:05:13","username":"ezadmin","server":"ubuntu.server"}
```


This feature is available from **Ezeelogin version 7.37.0**. Refer article to upgrade Ezeelogin to the latest version.

How to enable the feature to forward input commands to syslog?

Step 1: Login to GUI, navigate to **Settings** -> **General** -> **Security** -> scroll down and enable **Log Commands in Syslog** and relogin to ezsh and then to remote servers and execute random commands.



Refer below example of recorded input commands in syslog.

```
root@gateway-server:~# cat /var/log/syslog | grep -i "uptime\|free"
Feb 20 12:29:36 gateway-server ezeelogin: {"user_id":1,"username":"ezadmin","server_id":62,"hostname":"debian.server","ssh_user":"root","input":"uptime#015"}
Feb 20 12:29:39 gateway-server ezeelogin: {"user_id":1,"username":"ezadmin","server_id":62,"hostname":"debian.server","ssh_user":"root","input":"free#015"}
```

This feature is available from **Ezeelogin version 7.37.2**. Refer article to upgrade Ezeelogin to the latest version.

SIEM (Security Information and Event Management):-

SIEM systems collect and analyze log data generated throughout various systems, applications, and network infrastructure to identify and respond to security events and incidents. The goal is to provide a centralized view of an organization's information security, helping in real-time analysis, incident detection, and response.

Related Articles:

Integrate Ezeelogin SSH Jump host with Splunk for SIEM

Audit logs and configurations

Online URL: https://www.ezeelogin.com/kb/article/integrate-ssh-jump-server-with-syslog-670.html