Audit logs and configurations

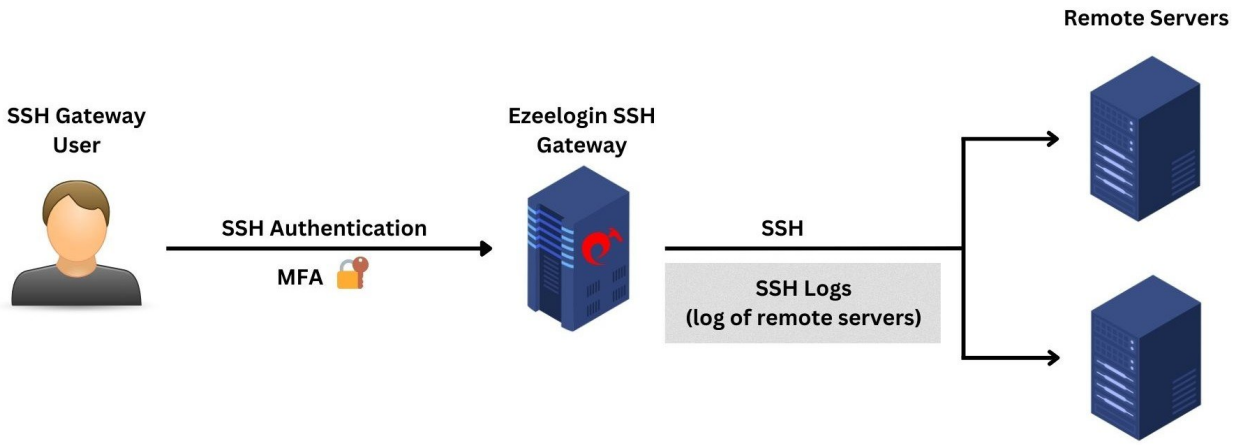
649 Nesvin KN April 17, 2025 General, Security Compliances 4234

Audit log policies and configurations

Overview: This article provides a detailed explanation of the various audit log types and their configurations available in Ezeelogin.

---

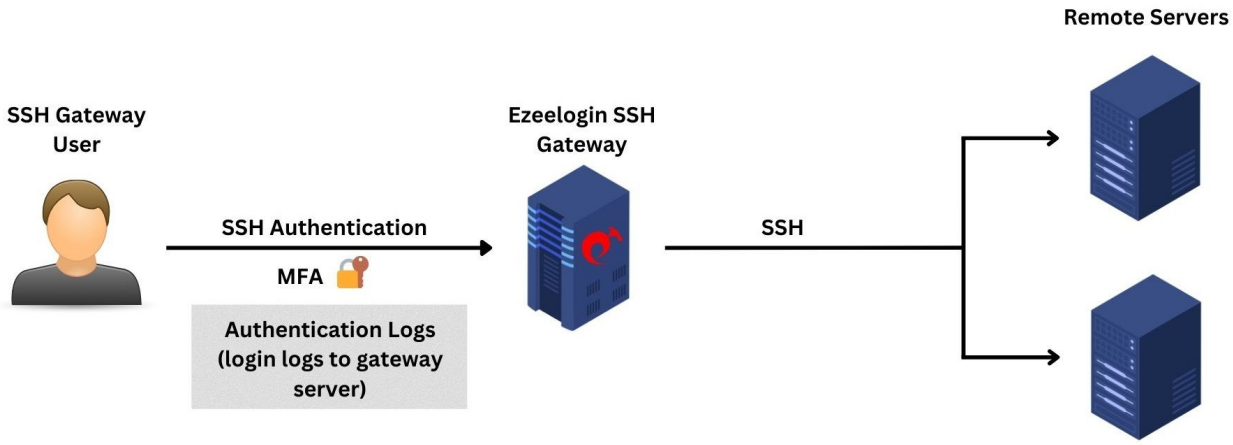
1. SSH Logs



The **SSH logs** provide comprehensive log information about the gateway user's actions or activities during an SSH session. The **recorded SSH sessions** are saved in text format, allowing for later search, review, revisit, or pipelining to log processing engines. Also, the user can **truncate the SSH log** based on time or size according to the policy or requirement.

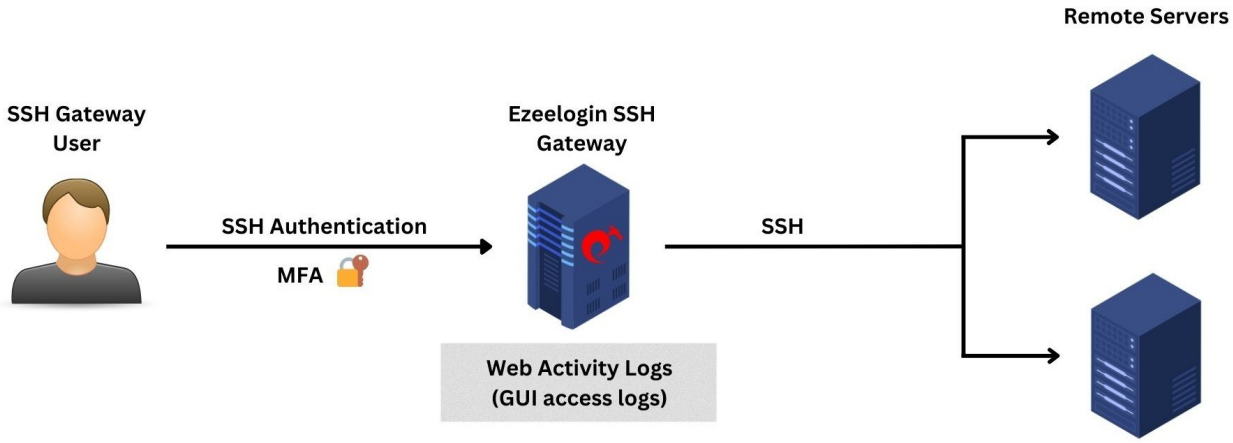
> Only SSH logs have the option to be truncated since they use the filesystem to store the user's SSH logs, and only the metadata is stored in the database.

2. Authentication Logs



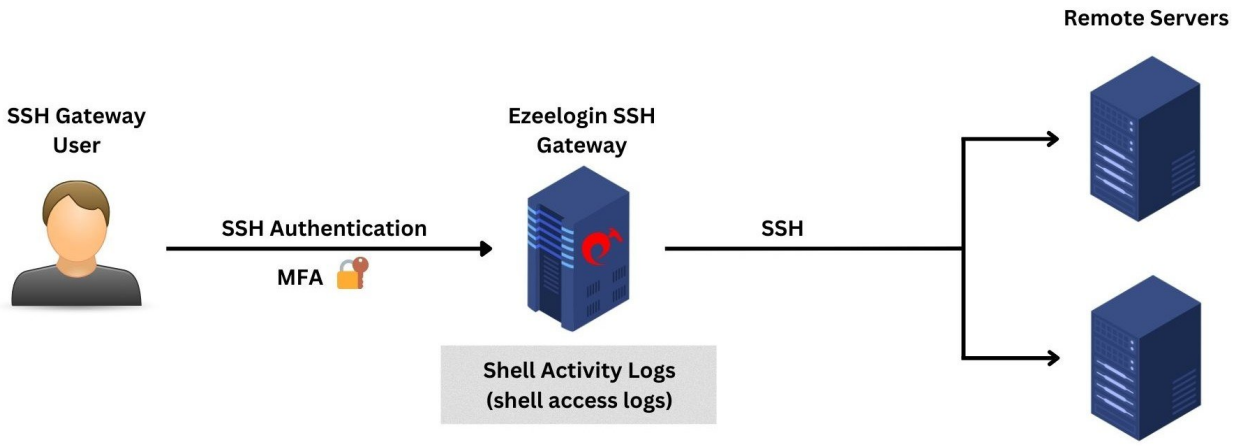
The **authentication logs** provide comprehensive log information about authentication-related activities on your gateway server from both web GUI and the backend(ezsh). Moreover, the logs offer valuable insights into the specific two-factor authentication (2FA) methods employed by gateway users while accessing the gateway server.

3. Web Activity Logs



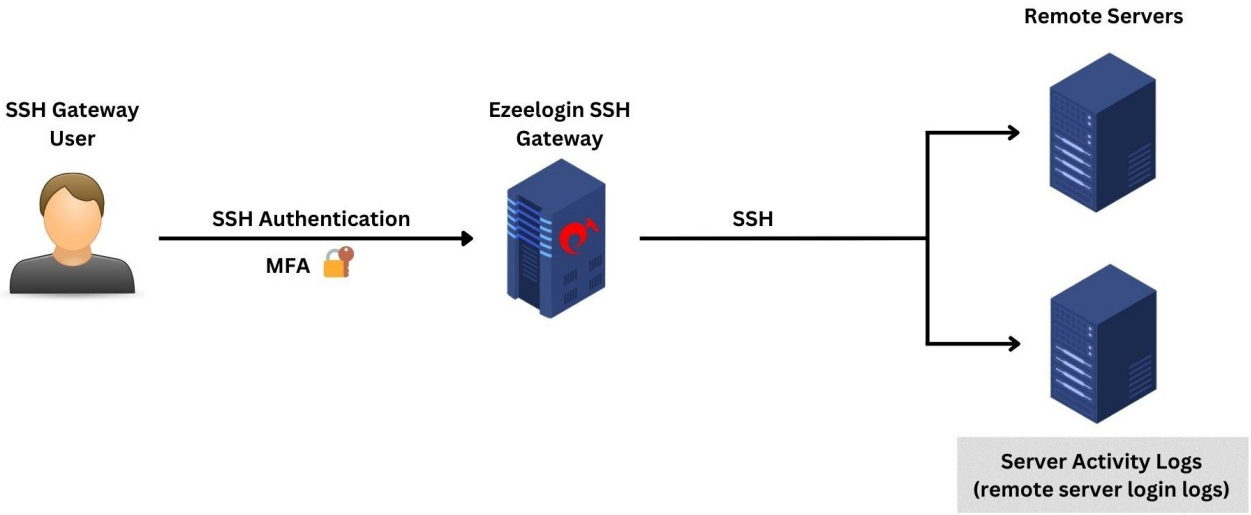
The web panel activity logs provide comprehensive log information about the sections and functions accessed within the web GUI along with timestamps, indicating the dates and times of these activities.

4. Shell Activity Logs or Gateway Activity Logs



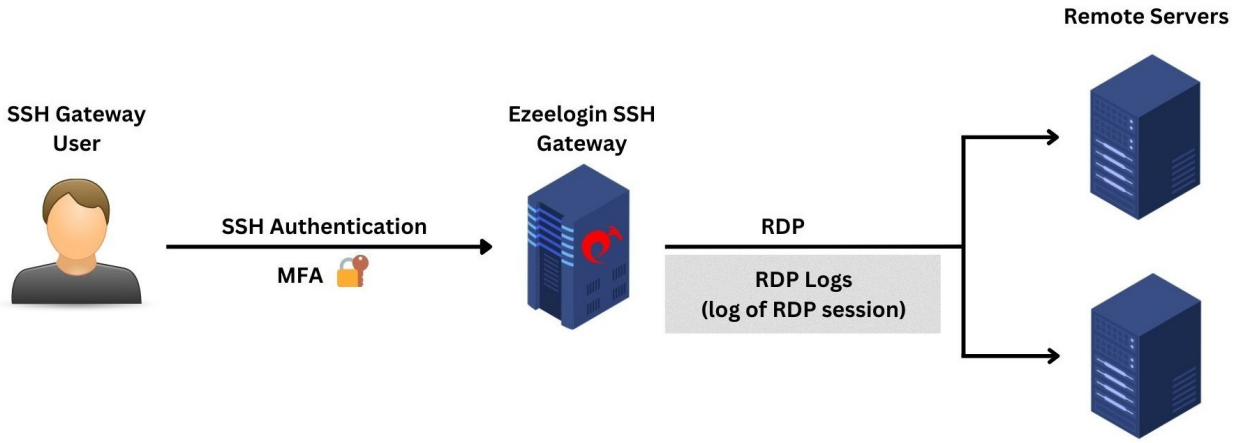
The [shell activity or gateway activity logs] provide a comprehensive log about every instance of gateway users accessing the backend(ezsh).

5. Server Activity Logs



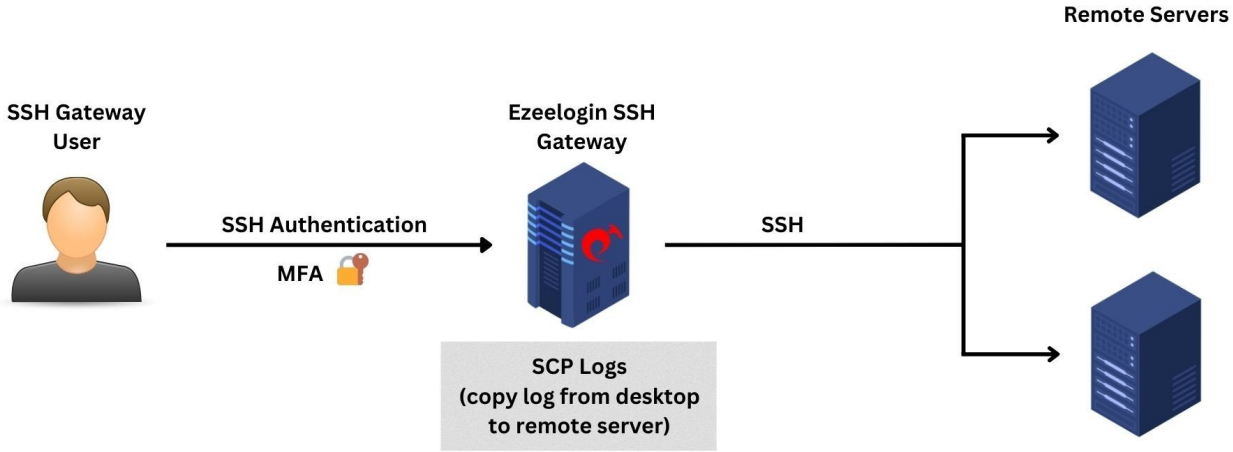
The [server activity logs] provide a comprehensive record of the actions and interactions performed by gateway users while accessing remote servers.

6. RDP Logs



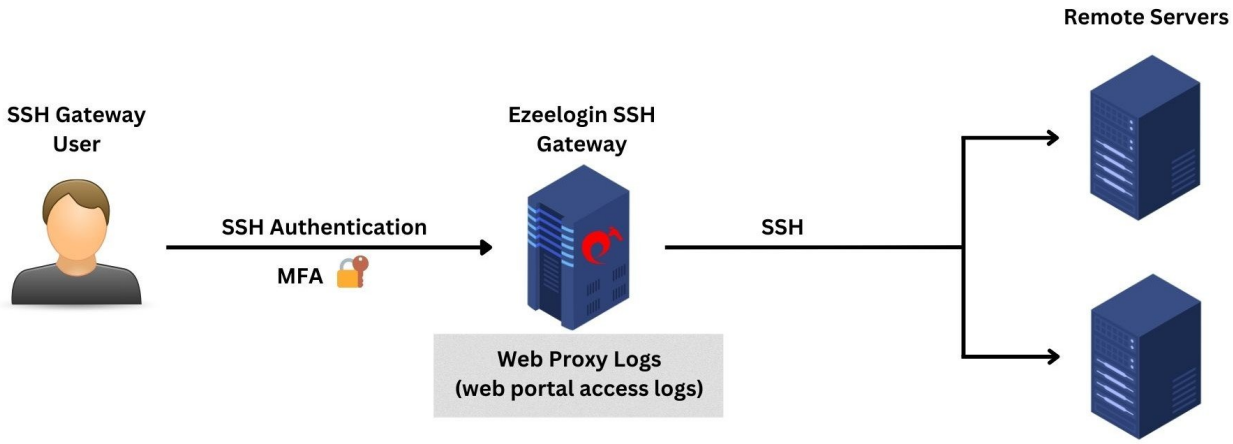
The RDP logs provide comprehensive information about the actions and activities of gateway users during RDP sessions. The recorded sessions are stored in RDP Bitmap Delta Stream format and cannot be viewed using third-party software.

7. SCP Logs



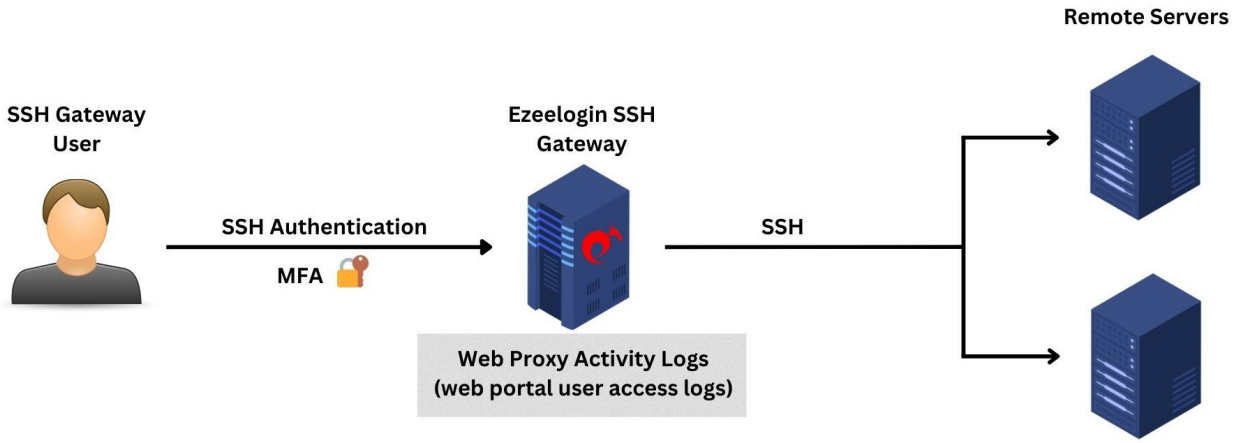
The SCP logs provide comprehensive information about file transfers performed by the gateway user using the parallel copy feature in ezsh.

8. Web Proxy Logs



The **web proxy logs** provide comprehensive information about all web portal access carried out via the reverse proxy.

9. Web Proxy Activity Logs



The **Web Proxy Activity Logs** provide comprehensive details about user access to the web portal through the reverse proxy.

Related Articles:

Different logs of user

Web Proxy Logs And Web Proxy Activity Logs

How to get the Shell Activity of Users

Integrate Ezeelogin SSH Jump host with splunk for SIEM

Integrate Ezeelogin SSH Jump host with syslog