



In this article

Troubleshooting

About log forwarding Enabling log forwarding

GitHub Enterprise Server uses syslog-ng to forward system and application logs to the server you specify.

About log forwarding &

Any log collection system that supports syslog-style log streams is supported (e.g., Logstash and Splunk).

When you enable log forwarding, you must upload a CA certificate to encrypt communications between syslog endpoints. Your appliance and the remote syslog server will perform two-way SSL, each providing a certificate to the other and validating the certificate which is received.

Enabling log forwarding $\mathscr {O}$

- 1 On the Management Console settings page, in the left sidebar, click **Monitoring**.
- 2 Select Enable log forwarding.
- 3 In the **Server address** field, type the address of the server to which you want to forward logs. You can specify multiple addresses in a comma-separated list.
- 4 In the Protocol drop-down menu, select the protocol to use to communicate with the log server. The protocol will apply to all specified log destinations.
- **5** Optionally, select **Enable TLS**. We recommend enabling TLS according to your local security policies, especially if there are untrusted networks between the appliance and any remote log servers.
- To encrypt communication between syslog endpoints, click Choose File and choose a CA certificate for the remote syslog server. You should upload a CA bundle containing a concatenation of the certificates of the CAs involved in signing the certificate of the remote log server. The entire certificate chain will be validated, and must terminate in a root certificate.

Troubleshooting @

If you run into issues with log forwarding, contact us by visiting <u>GitHub Enterprise</u>

<u>Support</u> and attach the output file from http(s)://[hostname]/setup/diagnostics to your message.

Legal

© 2023 GitHub, Inc. <u>Terms</u> <u>Privacy</u> <u>Status</u> <u>Pricing</u> <u>Expert services</u> <u>Blog</u>