Logging Landing Page

Logging Landing Page

> For more information on securing your data, see Information Protection @ MIT.

On this page:

Overview

Logs keep track of what is happening on a computer system or network and help identify who did what and when. If a system is compromised, the logs on that system can't be trusted to provide an accurate timeline of events as attackers will often try to cover their tracks.

Ensuring authentication and access activity is logged to a secondary device helps ensure information about user and system interactions in the environment is captured, stored, protected, and available for retrieval during troubleshooting and investigations.

How to Use

If you are managing or administering multiple systems, it's a good practice to set up a log server. Depending on which IS&T resources your department is utilizing, this may already be done for you.

- If your device is on the MIT Windows domain, you do not need to set up a logging server.
- If you are using an IS&T Managed server (Windows or Linux), you do not need to set up a logging server.

If your DLC would like to manage their own logging infrastructure, there are a few open source options:

- ELK - (short for Elasticsearch Logstash and Kibana)
- Graylog
- Syslog-ng
- Fluentd

See Also

- Open Web Application Security Project (OWASP) Logging Cheat Sheet
- National Institute of Standards and Technology (NIST) Guide to Computer Security Log Management
- Amazon Web Services (AWS) on Centralized Logging
- Rapid7's Best Practices for Log Management

Have Questions or Still Need Help?

- Contact the IS&T Service Desk