# LOGGING MADE EASY: FREQUENTLY ASKED QUESTIONS

## WHAT IS LOGGING MADE EASY?

Cybersecurity and Infrastructure Security Agency (CISA) launched Logging Made Easy (LME) in October 2023. LME is a no-cost log management solution for small to medium-sized organizations with limited resources that would otherwise have little to no functionality to detect attacks. LME offers centralized logging for Linux, macOS, and Windows operating systems, enabling proactive threat detection and enhanced security by allowing organizations to monitor their networks, identify users, and actively analyze Sysmon data to quickly detect potential malicious activity.

To provide enhanced functionality and to keep up with the changing technological environment, CISA released LME 2.0 in November 2024. LME 2.0 is a log management and threat detection solution that leverages Elastic and Wazuh open-source tooling. LME 2.0 introduces improvements and features to previous versions while maintaining its no-cost and open-source nature. LME 2.0 simplifies adoption while increasing security and enhancing logging, detection, and alerting functionalities.

## WHAT MAKES LME UNIQUE?

LME performs seamless log management, prioritizing transparency, security, and collaboration for unparalleled value. What makes LME so unique is its customizable dashboards that display system logs in real-time.

## WHAT'S IN IT FOR ME?

LME simplifies log management with easy implementation, centralized monitoring, and a user-friendly interface. By using LME, users gain real-time threat visibility, enabling proactive detection and response to security events. LME's commitment to transparency and community collaboration builds trust, which is reflected in positive reviews. Choosing LME provides access to a robust, accessible, and collaborative log management solution aligned with organizational goals for a secure digital future.

## HOW TO DOWNLOAD LME?

No sign-up or lengthy onboarding is required. Simply visit CISA's LME GitHub page for step-by-step instructions on how to download and install. GitHub facilitates open-source software development by providing a collaborative platform for hosting, sharing, and managing code repositories and enabling version control, community contributions, and issue tracking.

## WHAT SOFTWARE DRIVES LME?

LME 2.0 is powered by Elastic Stack (for log management, search, and visualization), Wazuh (for endpoint detection and response), and Podman (for containerization). This open-source stack ensures transparency, flexibility, and scalability while providing enhanced threat detection and customizable dashboards.

## WHICH OPERATING SYSTEMS CAN USE LME?

LME 2.0 supports Windows, Linux and macOS operating systems. Elastic and Wazuh agents enable compatibility across these platforms, ensuring broad coverage for monitoring and logging. While Wazuh agents also support Solaris, AIX, and HP-UX operating systems, CISA has not tested LME on endpoints running these operating systems.

## WHO CAN USE LME?

Although intended for small to medium-sized organizations with limited resources, anyone can download LME 2.0. Reference LME 2.0 prerequisite documentation for more details on required infrastructure and hardware, including CPU, memory, and storage requirements.

## CAN LME RUN IN THE CLOUD?

LME 2.0 supports both on-premises and cloud deployments, allowing organizations to host LME on local or cloud service provider infrastructure.

## IS LME 2.0 A FULL REINSTALL OR AN UPDATE?

Both new and existing users must complete a full install of LME 2.0 on LME's GitHub page. While existing users will need to reinstall the tool, this process ensures they are using the latest version with all the updated features. Installation instructions are available on LME's GitHub page.

## WILL OLDER VERSIONS OF LME STOP WORKING?

While CISA recommends upgrading to LME 2.0, users can maintain older versions of LME. However, CISA will not support older versions.

## HOW CAN CURRENT LME USERS MIGRATE TO LME 2.0 AND KEEP LOG HISTORY?

For existing LME users, click here for easy instructions on transferring log history from previous versions. LME will automatically reintegrate log history and data.

## ARE THERE NEW, UPDATED SYSTEM REQUIREMENTS FOR LME 2.0?

LME 2.0 system requirements remain mostly unchanged. Users can find detailed documentation on the LME GitHub page. Users that are unsure about meeting installation prerequisites should review the prerequisites documentation for guidance.

## WHERE CAN LME USERS RECEIVE FURTHER SUPPORT?

For further support with LME 2.0, users can explore the following options:

- Report LME issues via the GitHub "Issues" tab at the top of the page or by clicking GitHub Issues.
- Visit GitHub "Discussions" to check if your issue has been addressed or to start a new thread.
- Directly email CyberSharedServices@cisa.dhs.gov for further questions or comments.

## WHERE CAN USERS FIND ADDITIONAL RESOURCES?

Please visit CISA's LME website for additional resources.