



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Log File Management Tool Deployment and User's Guide

Known Issues and Limitations

12/13/2025

Contents

- 1 Known Issues and Limitations
 - 1.1 CVE-2022-22965 vulnerability
 - 1.2 log4j CVE-2021-44832 vulnerability
 - 1.3 log4j CVE-2021-45105 vulnerability
 - 1.4 LFMT Packages 8.5.101.xx to 8.5.104.10 - mitigation for the log4j CVE-2021-44228 vulnerability

Known Issues and Limitations

- If/when using GAX 9.0.103.08+ and LFMT 8.5.104 or above, ensure the respective GAX Application with LFMT Client Plug-in object, **[lfmt]/use_lfm_extension=true** option is set, so that *.lfm* files and not *.zip* (default as of 8.5.104) LFMT Package files are created and therefore downloadable via GAX; per **GAX RN's GAX-11260** the GAX app now filters unnecessary .gz, .jar, .zip, and .rar API requests.)
- The LFMT Client requires the `netty-3.2.3.Final.jar` library in the `<GAX Install Directory>/webapp/WEB-INF/lib` folder to be renamed or deleted. This is applicable for GAX versions 8.5.220.20 and earlier.
- In a multisite environment, if one or more of the databases are down, the LFMT Client does not populate panes correctly.
- LFMT does not support changes to the GAX root URL.

CVE-2022-22965 vulnerability

- LFMT is deemed to be not impacted by the CVE-2022-22965 vulnerability.

log4j CVE-2021-44832 vulnerability

Important

- LFMT Package 8.5.104.13, released Feb 2022, now utilises log4j 2.17.1 - please upgrade to this LFMT release or later
 - LFMT 8.5.101.xx+ is/was deemed NOT impacted by CVE-2021-44832

log4j CVE-2021-45105 vulnerability

Important

- LFMT Package 8.5.104.13, released Feb 2022, now utilises log4j 2.17.1 - please upgrade

to this LFMT release or later

- LFMT 8.5.101.xx+ is/was deemed NOT impacted by CVE-2021-44832

LFMT Packages 8.5.101.xx to 8.5.104.10 - mitigation for the log4j CVE-2021-44228 vulnerability

Important

- LFMT Package 8.5.104.13, released Feb 2022, now utilises log4j 2.17.1 - please upgrade to this LFMT release or later
- LFMT 8.5.104.13 Package supports/requires GAX version 9.0.104.xx
- If your upgrade to the latest LFMT 8.5.104.13+ Package is delayed, in the meantime please follow the mitigation steps below

Important

- LFMT 8.5.104.12 Package, released 17th December 2021 supports log4j 2.16 and therefore avoids/remediates the mitigation steps below.
- LFMT 8.5.104.12 Package supports/requires GAX version 9.0.104.xx
- LFMT 8.5.104.11 Package, released 10th December 2021, supports log4j 2.16 but is restricted to GAX versions 9.0.100.52 to 9.0.103.xx

This page relates to the Genesys Advisory detailed here: https://genesys.my.salesforce.com/articles/Product_Advisories/Apache-Log4j-2-Java-library

Please follow the mitigation steps below in addition to the guidance in the Genesys Advisory above.

LFMT Collector

- Stop the LFMT Collector application(s)
- Run (i.e. with a tool such as 7Zip) the following command:

- **zip -q -d <LFMT_COLLECTOR_INSTALL_LOCATION>/bin/lib/log4j-core-* org/apache/logging/log4j/core/lookup/JndiLookup.class**
 - Restart the LFMT Collector application(s)
-

LFMT Indexer

- Stop the LFMT Indexer application(s)
 - Run (i.e. with a tool such as 7Zip) the following command:
 - **zip -q -d <LFMT_INDEXER_INSTALL_DIRECTORY>/bin/lib/log4j-core-* org/apache/logging/log4j/core/lookup/JndiLookup.class**
 - Restart the LFMT Indexer application(s)
-

LFMT Client

- Given that the LFMT Client is a GAX Plugin and GAX logging is used for the LFMT Client, please consult the GAX Release Notes/Documentation and/or raise a Genesys Support Case regarding GAX mitigation/remediation.
-

Workbench Agent 8.5

- Stop the Workbench Agent 8.5 application(s)
 - Run (i.e. with a tool such as 7Zip) the following command:
 - **zip -q -d <WORKBENCH_AGENT_INSTALL_LOCATION>/lib/log4j-core-* org/apache/logging/log4j/core/lookup/JndiLookup.class**
 - Restart the Workbench Agent 8.5 application(s)
-