



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

Workbench Agent Configuration Options (for LFMT 8.5.1)

4/15/2025

---

## Contents

- 1 Workbench Agent Configuration Options (for LFMT 8.5.1)
  - 1.1 app\_config Section
  - 1.2 security Section
  - 1.3 security.keystore Section
  - 1.4 security.truststore Section
  - 1.5 log Section

# Workbench Agent Configuration Options (for LFMT 8.5.1)

This section contains options used to configure the Workbench Agent. Unless otherwise stated, all configuration options are set using GAX in the Application Options tab of the LFMT Agent object.

## app\_config Section

This section contains options for general configuration of the application. This section must be called `app_config`.

### `agent_max_open_requests`

Default Value: 4096

Valid Values: Any positive integer greater than 0 and a power of 2. (i.e 1024, 2048, 4096 etc.)

Changes Take Effect: After restart of Workbench Agent.

Identifies the maximum number of open requests accepted into the connection pool of the workbench agent.

### `agent_max_outgoing_connections`

Default Value: 1

Valid Values: Any positive integer greater than 0

Changes Take Effect: After restart of Workbench Agent.

Identifies the maximum number of concurrent outgoing connections from the workbench agent.

### `agent_max_pipelining_limit`

Default Value: 1

Valid Values: Any positive integer greater than 0

Changes Take Effect: After restart of Workbench Agent.

Identifies the maximum number of requests that are accepted (and dispatched to the collector) on one single connection before the first request is completed.

## security Section

This section contains all options relating to securing communication between the LFMT Collector and the Workbench Agent. The section is optional and is required only if the communication between the LFMT Collector and the Workbench Agent has to be secured. This section must be called `security`.

## mutual\_tls

Default value: None

Valid Values: true,false

Changes Take Effect: After restart of Workbench Agent.

Indicates whether mutual TLS is enabled for messaging and file transfer.

## provider

Default value: None

Valid Values: JKS

Changes Take Effect: After restart of Workbench Agent.

The key provider.

## protocol

Default value: None

Valid Values: TLSv1.2

Changes Take Effect: After restart of Workbench Agent.

Identifies the protocol to be used for the SSL communication between the LFMT Collector and the Workbench Agent.

## enabled\_ciphers

Default value: None

Valid Values: Any valid Java cipher suite. i.e "TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256" (see Java documentation for valid list)

Changes Take Effect: After restart of Workbench Agent.

Description: Identifies the cipher to be used for TLS communication between the LFMT Collector and Workbench Agent.

**Note:** Ensure any configured cipher suite is enabled to be used by the Java instance on the host. See Java documentation for enabling/disabling cipher suites. The LFMT Collector that the Workbench Agent is connecting to will need to be configured with the same cipher suite.

## security.keystore Section

The security.keystore section of the Workbench Agent application options is used to identify the keystore properties through which Workbench Agent will load the necessary keys for secure communications. This section must be called `security.keystore`.

## path

Default value: No default value

Valid Values: A file path to the keystore located on the host

Changes Take Effect: After restart of Workbench Agent.

Identifies the path to the local keystore to be used by Workbench Agent to load the necessary keys.

## password

Default value: No default value

Valid Values: A valid password associated with the keystore defined in the path option of the security.keystore section

Changes Take Effect: After restart of Workbench Agent.

The password to be used by Workbench Agent to access the keystore.

## security.truststore Section

The security.truststore section of the Workbench Agent application options is used to identify the truststore properties through which Workbench Agent will load the necessary certificates for secure communications. This section must be called security.truststore.

## path

Default value: No default value

Valid Values: A file path to the truststore located on the host

Changes Take Effect: After restart of Workbench Agent.

Identifies the path to the truststore to be used by Workbench Agent to load the necessary certificates.

## password

Default value: No default value

Valid Values: A valid password associated with the truststore identified in the path option of the security.truststore section

Changes Take Effect: After restart of Workbench Agent.

The password to be used by Workbench Agent to access the truststore.

## log Section

This section contains all options relating to creating, viewing, and otherwise using the Centralized Log facility in Genesys software. This section must be called log.

## all

Default value: No default value

Valid Values: [filename]

Changes Take Effect: After restart of Workbench Agent.

Specifies the file location to which the application sends all log events.

## expire

Default value: 10

Valid Values: [number] Specify a number from 1–1000.

Changes Take Effect: After restart of Workbench Agent.

Determines how many log files are kept before they are deleted.

## segment

Default value: 5000

Valid Values: [number] - Specify a value in kilobytes.

Changes Take Effect: After restart of Workbench Agent.

Determines the rollover size of the log files.

## verbose

Default value: all

Valid Values:

- all - All log events are printed.
- trace - All log events are printed.
- debug - DEBUG, INFO, WARN, FATAL, and ERROR log events are printed.
- info - INFO, WARN, FATAL, and ERROR log events are printed.
- warn - WARN, FATAL, and ERROR log events are printed.
- error - FATAL and ERROR log events are printed.
- fatal - Only FATAL log events are printed.
- off - No log events are printed.

Changes Take Effect: After restart of Workbench Agent.

Specifies the host IP address of the configuration server.