Log File Management Tool Deployment and User's Guide

LFMT GAX Configuration Options

12/14/2025

Contents

LFMT GAX Configuration Options

This section contains options used to configure the GAX for use with LFMT. Unless otherwise stated, all configuration options are set using GAX in the **`Application Options`** tab of the **GAX** object.

lfmt Section

This section contains options for general configuration of the application.

This section must be called `lfmt`.

http_request_timeout

Default Value: 60000 (60 seconds)
Valid Values: a millisecond integer value (i.e. **120000** for 120 seconds)
Changes Take Effect: After restart of GAX.
Description: Increases the client timeout value when performing a Force Collection; if/when a Force Collection timeout error is presented, add this option to increase the timeout. Note when a timeout message appears in the Client, the collection still continues to run on the server/Collector. The timeout simply indicates that the server-side collection has not finished before the client timeout has elapsed.

collection_timeout

Default Value: 3600000 (1 hour)
Valid Values: a millisecond integer value (i.e. **3600000** for 1 hour)
Changes Take Effect: After restart of GAX.
Description: This is specifically for the Force Collection API, which will keep the connection open for <x> milliseconds.

use_lfm_extension

> **Important**
>
> - Only relevant for LFMT Client 8.5.104.00 thru LFMT Client 8.5.105.03 - option removed in LFMT Client 8.5.105.07 given ".lfm" is now the default/only extension used

Default Value: false
Valid Values: true or false
Changes Take Effect: After restart of GAX.
Description: If set to true, the created log file package(s) will use the **.lfm** extension else the default

.zip extension is used.

ftp_host

Default Value: No default value
Valid Values: Valid (S)FTP/S IP/hostname address
Changes Take Effect: After restart of GAX.
Description: Specifies the IP/hostname of the default (S)FTP/S server.

ftp_port

Default Value: No default value
Valid Values: Valid (S)FTP/S port number, must be an integer
Changes Take Effect: After restart of GAX.
Description: Specifies the default port of the (S)FTP/S server.

ftp_pwd

Default Value: No default value
Valid Values: Valid (S)FTP/S password
Changes Take Effect: After restart of GAX.
Description: Specifies the password of the (S)FTP/S server.

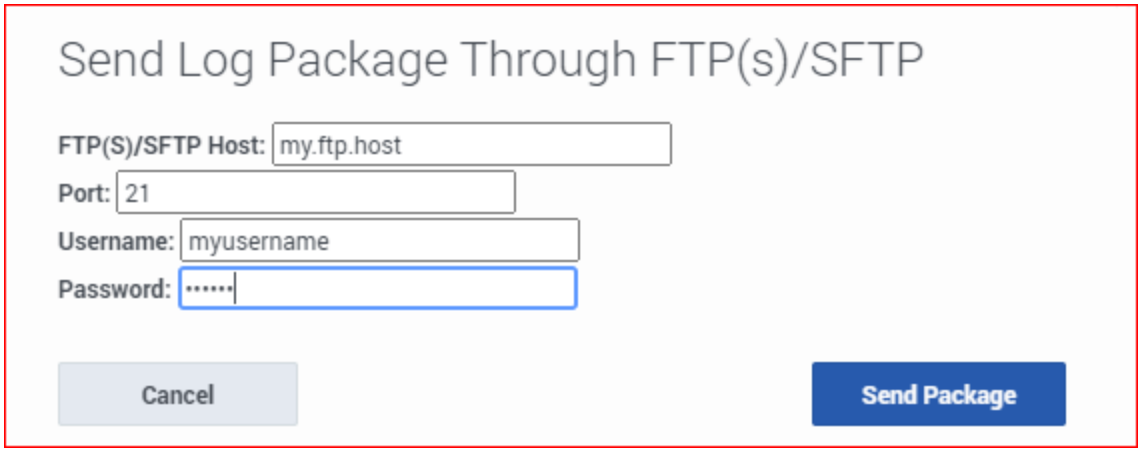
ftp_user

Default Value: No default value
Valid Values: Valid (S)FTP/S username
Changes Take Effect: After restart of GAX.
Description: Specifies the username of the (S)FTP/S server.

Note

Important

- The "ftp_host", "ftp_port", "ftp_user" and "ftp_pwd" options relate to LFMT sending log packages to an FTP Server - review this section for further details https://docs.genesys.com/Documentation/ST/current/DeploymentGuide/AvailablePackages#Sending_an_LFMT_package_via_FTP(S)/SFTP



security Section

This section contains all options relating to securing communication between the Client and the Collector as well as securing connections to the LFMT database (as of version 8.5.104.01). The section is optional and is required only if the communication between the LFMT Client and the LFMT Collector or connections to the LFMT database has to be secured; this section must be called **security**.

enable_tls

Default value: None
Valid Values: true,false
Changes Take Effect: After restart of GAX.
Description: Indicates whether TLS is enabled for messaging and file transfer. Note, the "messaging" and "ftmessaging" ports should also have their listening modes set to secure.

mutual_tls

Default value: None
Valid Values: true,false
Changes Take Effect: After restart of GAX.
Description: Indicates whether mutual TLS is enabled for messaging and file transfer between the Client/GAX and the LFMT Collector.

protocol

Default value: None
Valid Values: TLSv1.2
Changes Take Effect: After restart of GAX.
Description: Identifies the protocol to be used for the SSL communication between the LFMT Client and the LFMT Collector.

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 GAX.
Description: Identifies the cipher suite to be used for TLS communication between the LFMT Client and LFMT Collector.

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 Collector that the Client is connecting to will need to be configured with the same cipher suite.

security.keystore Section

The security.keystore section of the LFMT Client application options is used to identify the keystore properties through which LFMT Collector will load the necessary keys for secure communications; this section must be called **security.keystore**.

> **Important**
>
> - If GAX has https enabled for client connections, ensure that the same Java keystore/truststore is used for configuring LFMT TLS. If a different keystore/trustore is used for LFMT TLS configuration, then these values will override the keystore/truststore paths specified for GAX https config.

path

Default value: No default value
Valid Values: A file path to the keystore located on the host. **Note:** The security certificates must be generated using the SHA-2 secure hash algorithm.
Changes Take Effect: After restart of GAX.
Description: Identifies the path to the local keystore to be used by the LFMT Client 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 GAX.
Description: The password to be used by the LFMT Client to access the keystore.

security.truststore Section

The security.truststore section of the LFMT Client application options is used to identify the truststore properties through which LFMT Collector will load the necessary certificates for secure communications; this section must be called **security.truststore**.

> **Important**
>
> - If GAX has https enabled for client connections, ensure that the same Java keystore/truststore is used for configuring LFMT TLS. If a different keystore/trustore is used for LFMT TLS configuration, then these values will override the keystore/truststore paths specified for GAX https config.

path

Default value: No default value
Valid Values: A file path to the truststore located on the host. **Note:** The security certificates must be generated using the SHA-2 secure hash algorithm.
Changes Take Effect: After restart of GAX.
Description: Identifies the path to the truststore to be used by the LFMT Client 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 GAX.
Description: The password to be used by the LFMT Client to access the truststore.