Configurations Options Reference Manual

Supported Management Framework TLS Options Reference

4/25/2025

Contents

Supported Management Framework TLS Options Reference

This section contains a high-level description of TLS options supported by Management Framework, Use the provided links to get more information about how they are used and in what particular situations.

certificate

Default Value: No default value
Valid Values: On Windows, the thumbprint of a valid TLS certificate; on UNIX, the path to a valid TLS certificate

Specifies the security certificate used to secure connections.

Refer to the appropriate section of the *Genesys Security Deployment Guide*, as follows:

- For Core Framework connections—Securing Core Framework Connections
- For Local Control Agent and Genesys Deployment Agent connections—Securing Local Control Agent Connections
- For Centralized Log connections—Secure Network Logging Connections

certificate-key

Default Value: No default value
Valid Values: Any valid path

Specifies the full path to the Private Key **.pem** file corresponding to the Public Key in the certificate; or, if the Private Key is stored with the certificate, the full path to the certificate **.pem** file.

Refer to the appropriate section of the *Genesys Security Deployment Guide*, as follows:

- For Core Framework connections—Securing Core Framework Connections
- For Local Control Agent and Genesys Deployment Agent connections—Securing Local Control Agent Connections
- For Centralized Log connections—Secure Network Logging Connections

cipher-list

Default Value: No default value
Valid Values: The list of ciphers

Specifies the defined list of ciphers. The cipher list must be in a valid format.

Refer to the appropriate section of the *Genesys Security Deployment Guide*, as follows:

- For Core Framework connections—Securing Core Framework Connections
- For Local Control Agent and Genesys Deployment Agent connections—Securing Local Control Agent Connections
- For Centralized Log connections—Secure Network Logging Connections

client-auth

Default Value: 1
Valid Values: `0, 1`

Specifies whether authentication of the security certificate in the client TLS socket is to be disabled. When set to 1 (default), authentication is enabled. When set to `0`, the client socket does not authenticate the server when connected over TLS.

Refer to the appropriate section of the *Genesys Security Deployment Guide*, as follows:

- For Core Framework connections—Securing Core Framework Connections
- For Local Control Agent and Genesys Deployment Agent connections—Securing Local Control Agent Connections
- For Centralized Log connections—Secure Network Logging Connections

crl

Default Value: No default value
Valid Values: Valid path name

Specifies the path to, and the name of, the file that contains one or more certificates in PEM format, defining the Certificate Revocation List.

Refer to the appropriate section of the *Genesys Security Deployment Guide*, as follows:

- For Core Framework connections—Securing Core Framework Connections
- For Local Control Agent and Genesys Deployment Agent connections—Securing Local Control Agent Connections
- For Centralized Log connections—Secure Network Logging Connections

gda-tls

Default Value: `false`
Valid Values: `false, true`

Specifies whether all communication between Genesys Deployment Agent and its clients must be through a secured connection. Refer to the Securing Local Control Agent Connections section of the *Genesys Security Deployment Guide*.

lca-upgrade

Default Value: `0` (false) Valid Values: `0` (false), `1` (true)

Specifies whether all communication between SCS and LCA must be done through a secured connection.

Refer to the Securing Local Control Agent Connections section of the *Genesys Security Deployment Guide*.

sec-protocol

Default Value: no default value
Valid Values: `TLSv11, TLSv12, TLSv13`

Specifies the protocol used by the component to set up secure connections. Exactly how this option behaves depends on the platform on which the application for which the option is configured is running.

When configured on the Windows platform, this option complements Windows operating system settings that enable and disable a particular secure protocol. If there is a conflict between Windows settings and this option, the operating system settings are used.

On UNIX and Linux platforms, this option controls how the Security Pack on UNIX selects the protocol to use, as shown in the following table.

	Protocol		
option value	TLS 1.1	TLS 1.2	TLS 1.3*
""		+	+
"TLSv11"	+		
"TLSv12"		+	
"TLSv13"			+

*applicable to Genesys Security Pack based on OpenSSL 1.1.1

Refer to the appropriate section of the *Genesys Security Deployment Guide*, as follows:

- For Core Framework connections—Securing Core Framework Connections
- For Local Control Agent and Genesys Deployment Agent connections—Securing Local Control Agent Connections
- For Centralized Log connections—Secure Network Logging Connections

tls

Default Value: `0`
Valid Values: `0, 1`

Specifies whether secured connections are to be used. If set to 1, TLS certificates must be configuredIf set to 0 (the default), certificates are not required, and TLS is not used to secure connections.

tls-mutual

Default Value: 0
Valid Values: 0, 1

Specifies if mutual TLS is used for secure data transfer. If set to 1 on the server side of the connection, the client must also have a certificate configured. If set to 0 (the default), client certificates are not required, and either simple TLS or data encryption (if client-auth=0) is used.

Refer to the appropriate section of the *Genesys Security Deployment Guide*, as follows:

- For Core Framework connections—Securing Core Framework Connections
- For Local Control Agent and Genesys Deployment Agent connections—Securing Local Control Agent Connections
- For Centralized Log connections—Secure Network Logging Connections

tls-target-name

Default Value: No default value
Valid Values: Any string

Specifies the target host name to which the name in remote certificate will be checked against, regardless of whether IP address or FQDN is used for the connection.

tls-target-name-check

Default Value: no
Valid Values: no, host

Specifies if the Common Name in the subject field and/or the Subject Alternate Names of the server's certificate will be compared to the target host name (option value host). If they are not identical, the connection fails. If the option is set to no, a comparison is not made, and the connection is allowed.

Refer to the appropriate section of the *Genesys Security Deployment Guide*, as follows:

- For Core Framework connections—Securing Core Framework Connections
- For Local Control Agent and Genesys Deployment Agent connections—Securing Local Control Agent Connections
- For Centralized Log connections—Secure Network Logging Connections

trusted-ca

Default Value: No default value
Valid Values: Any valid path

Specifies the full path to the **ca_cert.pem** file.

Refer to the appropriate section of the *Genesys Security Deployment Guide*, as follows:

- For Core Framework connections—Securing Core Framework Connections
- For Local Control Agent and Genesys Deployment Agent connections—Securing Local Control Agent Connections
- For Centralized Log connections—Secure Network Logging Connections

upgrade

Default Value: `0` (false) Valid Values: `0` (false), `1` (true); corresponding to the numerical equivalent of the lca-upgrade option

> **Important**
>
> Valid values for this option must have no spaces before or after the = delimiter character.

Specifies whether TLS will be used to secure the connection between LCA and SCS. If set to 0 (the default), regular (unsecured) connections will be used.

Refer to the Securing Local Control Agent Connections section of the *Genesys Security Deployment Guide*.