Genesys Engage Digital (eServices)

channel-chatbot-monitor-tls Section

12/17/2025

channel-chatbot-monitor-tls Section

cipher-list

Default Value:
Valid Values: Any string
Changes Take Effect: Immediately for new connections

String consisting of space-separated cipher suit names. Information on cipher names can be found online. Used to calculate enabled cipher suites. Only ciphers present in both the cipher suites supported by security provider and the cipher-list parameter are valid. Example: "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA"

crl

Default Value:
Valid Values: Any string
Changes Take Effect: Immediately for new connections

Path to a Certificate Revocation List (CRL) file in PEM format. Path can use both forward and backward slash characters. Applications will use CRL during certificate validation process to check if the (seemingly valid) certificate was revoked by CA (certification authority). This option is useful to stop usage of leaked certificates by unauthorized parties.

password

Default Value:
Valid Values: Any string
Changes Take Effect: Immediately for new connections

JKS keystore password. Used only if for JKS provider.

provider

Default Value: ANY
Valid Values: ANY, JKS, MSCAPI, NONE, PEM
Changes Take Effect: Immediately for new connections

Specifies the security provider to be used. If provider is not recognized or misconfigured then NONE provider is used.

- **ANY**: Trusts any certificates. Can be used on the server side when you do not expect any certificates from clients (for example, during testing), or for automatic detection of a provider by trusted-ca option.
- **JKS**: Retrieves a CA certificate from a Java Keystore file and uses Java built-in validation logic.
- **MSCAPI**: Uses the Microsoft CryptoAPI and Windows certificate services to retrieve CA certificates and validate certificates.
- **NONE**: Prohibits establishing the secure connection.
- **PEM**: Reads a CA certificate from an X.509 PEM file.

sec-protocol

Default Value: TLSv12
Valid Values: SSLv23, SSLv3, TLSv1, TLSv11, TLSv12
Changes Take Effect: Immediately for new connections

Specifies the protocol used by the server 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. On Windows 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.

tls-target-name-check

Default Value: no
Valid Values: host, no
Changes Take Effect: Immediately for new connections

When set to "host", enables matching of certificate’s Alternative Subject Name or Subject fields against expected host name. PSDK supports DNS names and IP addresses as expected host names.

trusted-ca

Default Value:
Valid Values: Any string
Changes Take Effect: Immediately for new connections

For PEM provider must contain a path to a X.509 certificate file in PEM format. Path can use both forward and backward slash characters. For JKS provider must contain a path to a keystore file (.jks). Path can use both forward and backward slash characters. For other providers this parameter is ignored. Note: If the value is not empty and provider "ANY " is specified, then a provider is set based on the file extension: *.jks for JKS provider; *.pem and *.crt for PEM provider.