Genesys Web Engagement

security Section

5/3/2025

security Section

auth-scheme

Default Value: none
Valid Values: none, basic
Changes Take Effect: After server restart

Specifies the HTTP authentication scheme used to secure REST requests to the Web Engagement Server.

certificate

Default Value:
Valid Values: A path, which can use both forward and backward slash characters.
Changes Take Effect: After server restart

Specifies the location of an X.509 certificate to be used by application.

certificate-key

Default Value:
Valid Values: A path, which can use both forward and backward slash characters.
Changes Take Effect: After server restart

Specifies the location of a PKCS#8 private key to be used by the application in conjunction with the certificate.

key-entry-password

Default Value: none
Valid Values: String
Changes Take Effect: After server restart

Password for the specific key inside of key storage.

keystore-password

Default Value: none
Valid Values: String
Changes Take Effect: After server restart

Password for the JKS key storage.

password

Default Value:
Valid Values: Any string
Changes Take Effect: After server restart

The password used in the authentication process for REST requests to the Web Engagement Server.

provider

Default Value: DEFAULT
Valid Values: DEFAULT, JKS, MSCAPI, PKCS11, PEM
Changes Take Effect: After server restart

Type of trusted storage. The default provider uses a trust store shipped with the current JDK distribution. It is located at **$JAVA_HOME/jre/lib/security/cacerts**

trusted-ca

Default Value:
Valid Values: A path, which can use both forward and backward slash characters.
Changes Take Effect: After server restart

Specifies the location of an X.509 certificate to be used by the application to validate remote party certificates.

truststore-password

Default Value: none
Valid Values: String
Changes Take Effect: After server restart

Password for the JKS trusted storage.

user-id

Default Value:
Valid Values: Any string
Changes Take Effect: After server restart

The User ID used in the authentication process for REST requests to the Web Engagement Server.