GENESYS™

Genesys Voice Platform

HTTP Section

5/5/2025

HTTP Section

- CertFile
- CertKeyFile
- CertPassword
- HTTPDefaultPage
- HTTPPort
- HTTPSPort
- ResponseHeaders
- TLSType

CertFile

Default Value: $InstallationRoot$/config/x509_certificate.pem
Valid Values:
Changes Take Effect: After restart

Name of the HTTPS Server Certificate file.

CertKeyFile

Default Value: $InstallationRoot$/config/x509_private_key.pem
Valid Values:
Changes Take Effect: After restart

Name of the HTTPS Server Certificate Key file.

CertPassword

Default Value:
Valid Values:
Changes Take Effect: After restart

Password for accessing the HTTP Server Certificate Key File.

HTTPDefaultPage

Default Value: SSG
Valid Values:

Changes Take Effect: After restart

Default HTTP Page, being used by SSG for storing the outbound requests.

HTTPPort

Default Value: 9800
Valid Values:
Changes Take Effect: After restart

Describes the port on which HTTP requests can be received from client applications.

HTTPSPort

Default Value: 9801
Valid Values:
Changes Take Effect: After restart

Describes the port on which HTTPS requests can be received from client applications.

ResponseHeaders

Default Value: X-Frame-Options:DENY
Valid Values:
Changes Take Effect: After restart

Specifies any custom HTTP headers that need to be included in HTTP responses sent by SSG. These are sent for all HTTP responses by SSG(both for Root page access and TriggerAction requests). Format for specification is Header1:Value1|Header2:Value2. The Value part may also contain : and | characters in which case they must be escaped with a backward slash (eg: Header1:Value1-\|Value2 will be considered as Header1: Value1-|Value2. If unescaped, then the header will be Header1:Value1-). Default value will be set to X-Frame-Options:DENY

TLSType

Default Value: SSLv23
Valid Values: SSLv23, SSLv3, SSLv2, TLSv1
Changes Take Effect: After restart

Name of the secure protocol with version information.