

GENESYS

This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Deployment Guide

Backend Server security Section

Backend Server security Section

The options in the security section configure the following security-related settings for the Backend Server:

- Enable authentication for the History REST API and its clients. See Authentication for details.
- Enable TLS between Genesys Web Engagement servers and other Genesys servers (for example, Chat Server or Interaction Server).

Contents

- 1 Backend Server security Section
 - 1.1 auth-scheme
 - 1.2 user-id
 - 1.3 password
 - 1.4 trusted-ca-type
 - 1.5 trusted-ca
 - 1.6 trusted-ca-pwd

Deployment Guide 2

auth-scheme

Default Value: none

Valid Values: none or basic

Changes take effect: After start/restart

Specifies the HTTP authentication scheme used to secure History REST API requests to the Backend Server. With the Basic scheme, clients must be authenticated with a user ID and password.

user-id

Default Value: No default value

Valid Values: Any string

Changes take effect: After start/restart

The user identifier (login) used in authentication for the History REST API. See auth-scheme.

password

Default Value: No default value

Valid Values: Any string

Changes take effect: After start/restart

The user password used in authentication for the History REST API. See auth-scheme.

trusted-ca-type

Default Value: MSCAPI

Valid Values:

- MSCAPI MSCAPI certificate storage is used for TLS certificate verification.
- PEM PEM certificate storage is used for TLS certificate verification. In this case, the trusted-ca option should also be specified and should contain the path to the PEM file.
- JKS JKS certificate storage is used for TLS certificate verification. In this case, the trusted-ca option should also be specified and should contain the path to the JKS file. You should also set the trusted-capwd option to the password for the JKS file.

Changes Take Effect: After start/restart

Specifies the type of trusted certificate authority. No TLS is applied for connections between this server and other Genesys servers if this option is absent.

trusted-ca

Default Value:

Valid Values: Path to the trusted store file (valid for PEM and JKS types, depending on value of the trusted-ca-type option).

Changes Take Effect: After start/restart

Specifies the path to the trusted store file (valid for PEM and JKS types, depending on value of the trusted-ca-type option).

Deployment Guide 3

trusted-ca-pwd

Default value:

Valid values: Password for the trusted store file (valid for JKS type only).

Changes Take Effect: After start/restart
Specifies the password for the trusted store file (valid for JKS type only).

Deployment Guide 4