Deployment Guide

Backend Server security Section

4/5/2026

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

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-ca-pwd 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).

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).