



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.

Genesys Engage Digital (eServices)

encryption

12/15/2025

encryption

- `client-certificate-file`
- `client-private-key-file`
- `enabled`
- `password`
- `trusted-cert-dir`
- `verify-peer-cert`
- `verify-peer-identity`

client-certificate-file

Default Value:

Valid Values: Any valid file path

Changes Take Effect: After restart

A relative path to a public client key file in PEM format. The path must be accessible for all running instances of Chat Server.

client-private-key-file

Default Value:

Valid Values: Any valid file path

Changes Take Effect: After restart

A relative path to a private client key file in PEM format. The path must be accessible for all running instances of Chat Server. To set password protection over the private key, see the option "password".

enabled

Default Value: false

Valid Values: true, false

Changes Take Effect: After restart

Set to false (default) to disable using SSL features in Chat Server's communication with Cassandra nodes. Set to true to enable.

password

Default Value:

Valid Values: Any string (can be empty)

Changes Take Effect: After restart

An optional client key password. The password is used to access the contents of the client-private-key-file.

trusted-cert-dir

Default Value:

Valid Values: Any valid file path

Changes Take Effect: After restart

A relative path to the directory with .pem file(s) containing the trusted certificates for each node. The path must be accessible for all running instances of Chat Server. Note: A single .pem file must contain a single certificate.

verify-peer-cert

Default Value: true

Valid Values: true, false

Changes Take Effect: After restart

Indicates whether the peer certificate needs to be checked for validity.

verify-peer-identity

Default Value: false

Valid Values: true, false

Changes Take Effect: After restart

Indicates whether the peer certificate needs to be checked for an IP address matching the certificate's common name or a subject alternative name.