



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

security Section

12/19/2025

security Section

Contents

- 1 security Section
 - 1.1 auth-scheme
 - 1.2 password
 - 1.3 user-id
 - 1.4 provider
 - 1.5 trusted-ca
 - 1.6 truststore-password
 - 1.7 certificate
 - 1.8 certificate-key
 - 1.9 keystore-password
 - 1.10 key-entry-password

auth-scheme

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

Default Value: none

Valid Values: none, basic

Mandatory: No

Changes Take Effect: After server restart

password

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

Valid Values: Any string

Mandatory: No

Changes Take Effect: After server restart

user-id

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

Valid Values: Any string

Mandatory: No

Changes Take Effect: After server restart

provider

Description: 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**

Default Value: DEFAULT

Valid Values: DEFAULT, JKS, MSCAPI, PKCS11, PEM

Mandatory: No

Changes Take Effect: After server restart

trusted-ca

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

Valid Values: A path, which can use both forward and backward slash characters.

Mandatory: No

Changes Take Effect: After server restart

truststore-password

Description: Password for the JKS trusted storage.

Default Value: none

Valid Values: String

Mandatory: No

Changes Take Effect: After server restart

certificate

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

Valid Values: A path, which can use both forward and backward slash characters.

Mandatory: No

Changes Take Effect: After server restart

certificate-key

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

Valid Values: A path, which can use both forward and backward slash characters.

Mandatory: No

Changes Take Effect: After server restart

keystore-password

Description: Password for the JKS key storage.

Default Value: none

Valid Values: String

Mandatory: No

Changes Take Effect: After server restart

key-entry-password

Description: Password for the specific key inside of key storage.

Default Value: none

Valid Values: String

Mandatory: No

Changes Take Effect: After server restart