Workbench User's Guide

Configuring TLS

12/17/2025

Contents

Configuring TLS

> **Important**
>
> - TLS connections to Workbench IO and Kibana (essentially the main Workbench UI) is currently NOT supported
> - TLS connections from Workbench IO Applications at different Data-Centers is supported
> - TLS connections to Elasticsearch has to be enabled when enabling Elasticsearch Authentication
> - TLS connections to ZooKeeper is NOT supported
> - TLS connection from Workbench to Engage Configuration Server is supported
> - TLS connection from Workbench to Engage Solution Control Server is supported
> - TLS connection from Workbench to Engage Message Server is supported

Workbench TLS

Currently Workbench supports TLS connections/communication between its Workbench IO Application(s).

For example a Workbench IO Application in APAC can communicate with a Workbench IO Application in EMEA, providing secure messaging of Alarm, Changes, Channel Monitoring and Auditing events across the WAN, to enable this Workbench IO "APAC" to Workbench IO "EMEA" connection/ communication, the respective Workbench Host Objects must first be TLS Enabled.

Enable Workbench Host TLS

This section details the enablement of the Workbench Host TLS via the "2. Workbench TLS Communication" Section:

Only enable the Workbench Host TLS setting if/when:

- Workbench IO Application TLS connection/communication is preferred between Workbench IO Applications at different Data-Centers (i.e. "APAC" and "EMEA") for improved security; complete this Workbench Host TLS enablement before enabling Workbench IO Application TLS
- Workbench ElasticSearch Authentication is planned to be enabled; complete this Workbench Host TLS enablement before enabling ElasticSearch Authentication

Please follow these steps to enable the Workbench Host TLS settings:

1. Certificates need to be in a Java Key Store (.jks file) and accessible on the host by the user account running Workbench
2. Within Workbench, browse to the Configuration > Hosts section and select the host that TLS will be enabled on
3. Within the host object settings, navigate to the "2. Workbench TLS Communication" section
4. Populate the following options:
    - Keystore Path: path of the Java Key store on the host
    - Keystore Password: password for the key store
    - Truststore Path: path to the Java trust store
    - Truststore Password: password for the Java trust store
    - Protocol (default: TLSv1.2): TLS protocol that will be used
    - Algorithms: comma-delimited list of cipher suites that the host will use for TLS negotiation/ communication with other nodes
        - See the "JSSE Cipher Suite Names" section of the following doc for a valid list of cipher suites supported by Java https://docs.oracle.com/javase/10/docs/specs/security/standard-names.html
    - Mutual-TLS: check to enable mutual TLS
5. Click the save button to commit the changes

Enable Workbench IO Application TLS

This section details the enablement TLS for the Workbench IO Application

Only enable the Workbench IO Application TLS setting if/when:

- TLS connection/communication is preferred between Workbench IO Applications at different Data-Centers for improved security

Please follow these steps to enable the Workbench IO Application TLS settings:

1. Ensure that the TLS properties have been first configured for the host object that the Workbench_IO application is running on (See the above "Enable Workbench Host TLS" section)
2. Within Workbench, browse to the Configuration > Applications section and select the Workbench_IO application in the list that TLS will be enabled on
3. With the Workbench_IO application object, navigate to the "9. Workbench Distributed Mode" section
4. Check the "TLS Enabled" property
5. Click "Save" to commit the changes
6. Restart the Workbench_IO service for changes to take effect

Enable ElasticSearch Application TLS (only if enabling Elastic Authentication)

This section details the enablement of TLS for the ElasticSearch node when using Elastic authentication

Only enable the ElasticSearch Application TLS setting if/when:

- Workbench ElasticSearch Authentication is planned to be enabled
  Note: It is important to complete this ElasticSearch TLS enablement before enabling ElasticSearch Authentication

Please follow these steps to enable the Workbench IO Application TLS settings:

1. Ensure that the TLS properties have been first configured for the host object that the ElasticSearch node is running on (see the above "Enable Workbench Host TLS" section)
2. On the host in which the ElasticSearch node is running, place a copy of the key store and trust store in the following directory:
   - {WBInstallDirectory}/ElasticSearch/config
3. Within Workbench, browse to the Configuration > Applications section and select the ElasticSearch application in the list that TLS will be enabled on
4. With the ElasticSearch application object, navigate to the "8.Workbench Elasticsearch Authentication" section
5. Enable the authentication and specify the desired username and password
6. Click "Save" to commit the changes

Workbench to Engage TLS

Workbench supports TLS connections to the following Genesys Framework components:

- Configuration Server
- Message Server
- Solution Control Server

To setup/enable TLS for each of these components, please follow the Genesys Security guide at the following location to configure TLS:

Documentation/System/8.5.x/SDG/Welcome

Ensure that the certificates are installed on the Workbench Server host/VM to enable connectivity to the Framework components.

Note: For Windows VMs/Hosts ensure that the certificates are installed for both the user running the

Workbench installation as well as the LOCAL_SYSTEM account that will be running the Workbench Services.

Once the framework components and the respective hosts/VMs have been configured to use TLS, the provisioned Workbench Server application in Configuration Server will also need to be configured with the TLS properties to connect to each of the Framework components.

Instructions for setting up TLS from Workbench to the Framework:

Configuration Server

During Workbench installation, when prompted to specify the Configuration Server details, make sure to specify the auto-upgrade port that is defined for the Configuration Server instance.

Note: If Workbench was originally installed using a non-secure port of Configuration Server, the following file can be updated within the Workbench installation directory to change the port to an auto-upgrade port:

{WbInstallDir}/karaf/etc/ConfigServerInstances.cfg

Within this file, update the port for the primary Configuration Server. After the file is updated, restart the Workbench_IO to use the new Configuration Server settings.

Solution Control Server (SCS)

1) During Workbench installation you will be prompted to select the Solution Control Server instance the Workbench will connect to subscribe to framework events.

2) From within Genesys Administrator or Genesys Administrator Extension (GAX), ensure that the provisioned Workbench Server application object has a connection to both the primary and backup (if applicable) Solution Control Server and that the secure port is selected when adding these connections. Workbench will use this port when connecting to Solution Control Server.

Message Server

1) During Workbench installation you will be prompted to select the Message Server instance that Workbench will connect to subscribe to framework events.

2) From within Genesys Administrator or Genesys Administrator Extension (GAX), ensure that the provisioned Workbench Server application object has a connection to the primary and backup (if applicable) Message Servers and that the secure port is selected when configuring these connections. Workbench will use this secure port when connecting to Message Server.