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.

Workforce Management Administrator's Guide

Securing connections on WFM servers

5/10/2025

Securing connections on WFM servers

Workforce Management (WFM) supports Transport Layer Security (TLS) 1.2 for connections within WFM, and Genesys Management Framework, and between WFM and third-party software (with the exception of SMTP servers). WFM supports configurations that use only FIPS 140-2-compliant algorithms for encryption, hashing, and signing secure network connections.

Secure connections between servers

The information in this topic is provided to help you to configure secure connections between servers.

TLS configuration for WFM servers adhere to the common guidelines in the *Genesys Security Deployment Guide* with one limitation, parameters of the secure connection must be configured on the Host level.

WFM servers support Mutual TLS within WFM, and between WFM and Genesys Framework.

WFM Server, Builder, Data Aggregator, and Daemon use Windows security provider SChannel when running on Windows hosts. To support configurations that use only FIPS 140-2 compliant algorithms for security connections, enable the FIPS local/group security policy flag. For more information, see Microsoft FIPS 140 Validation.

WFM Web and WFM Daemon

Since WFM Web and Daemon have a dependency on Java, the TLS implementation uses Java Secure Socket Extensions from Oracle JDK along with a configured provider.

You must configure two certificate stores on the WFM Damon and WFM Web hosts:

- Java Keystore for certificates that are required for TLS communications with WFM components
- Windows Certificate Store for certificate that is required for TLS communications with Framework components

To configure these secure connections, complete the procedure below and adhere to common guidelines in the *Genesys Security Deployment Guide*.

Procedure: Importing Certificates for WFM Web and Daemon

Purpose: To import certificates that support secure connections for WFM Web and WFM Daemon.

Start procedure

1. Import certificates to the Java Keystore that is used by WFM Daemon and Tomcat (WFM Web):
   - **For WFM Daemon**—Import the WFM Daemon, Server, and Web host certificates to the Java Keystore used by WFM Daemon. By default, the path is `JAVA_HOME/jre/lib/security/cacerts`

Find the value for `JAVA_HOME` by opening the `wfmdaemon.cmd` file in the WFM Daemon installation folder in line set `JAVA_HOME`.

- **For WFM Web**—Import the WFM Web (Tomcat), Data Aggregator, Daemon, Builder, and Server host certificates to the Java Keystore used by Tomcat.
  You can use the Java Keytool to import certificates to the Java Keystore. For example

  ```
  keytool.exe -import -alias tomcat -file C:\Certificates\tomcat.crt -keystore
  “C:\Program Files\Java\jdk1.8.0_181\jre\lib\security\cacerts” -storetype JKS
  -storepass changeit
  ```

2. Import the host certificate (on which WFM Daemon or WFM Web is installed) to the Windows Certificate Store for the user account that starts WFM Daemon or Tomcat (WFM Web) as a service.
   After installation, the WFM Daemon and Tomcat (WFM Web) user account is Local System, by default.
   - Complete the following steps, using the Microsoft PsExec tool to import certificates to Windows Certificate Store for the **Local System** account.
     1. Download the Microsoft PSTools.
     2. Unpack `PsExec64.exe`.
     3. Run the Command Prompt as **Administrator**.
     4. Execute the command `PsExec64.exe –i –s mmc.exe`.
        This command is run Microsoft Management Console for the Local System account
     5. Click **File** > **Add/Remove Snap-in…**
     6. Add the certificates snap-in for the **My user** account
     7. Import the certificate to the **Personal** folder
     8. Verify that the **Trusted Root Certification Authorities** folder contains the issuer certificate.
     9. Repeat steps 5 to 8 to import the certificate for the **Computer** account.

End procedure

Secure connections between WFM Web server and WFM Web clients

The information in this topic will help you to configure secure connections between WFM Web and WFM Web clients.

WFM Web

WFM Web server runs in an Apache Tomcat Servlet/JSP container. Therefore, the secure connection must be configured in the servlet container. For more information see Apache Tomcat SSL/TLS Configuration HOW-TO.

To support configurations that use only FIPS 140-2 compliant algorithms in security connections between WFM Web server and WFM Web clients, configure Apache Tomcat to support FIPS 140-2. For more information, see Apache Tomcat Native Library.

WFM Web clients

TLS support must be enabled in browser that runs WFM Web for Supervisor, WFM Web for Agents, and WFM Agent Mobile Client.

To run WFM Web for Supervisor Java-based views, you must also import the WFM Web (Tomcat) server certificate to the Java Keystore that is used by the browser or by the Java Webstart application on the host on which you plan to run WFM Web for Supervisors.

Secure connections between WFM servers and MS SQL database

By default, WFM Server and WFM Data Aggregator use the outdated Microsoft OLE DB Driver (SQLOLEDB) to connect to MS SQL Server. However, this driver does not support TLS 1.2.

Procedure: Installing the latest Microsoft OLE DB Driver

Purpose: To support TLS 1.2 in the connections between WFM servers and MS SQL database

Start procedure

1. Install the Microsoft OLE DB Driver (MSOLEDBSQL) 18.2.2 or later on the WFM Server and WFM Data Aggregator hosts.
2. In Genesys Administrator:
   - Set the **[Server]** OLEDB_Provider configuration option value to `MSOLEDBSQL` in the WFM Server Application.
   - Set the **[Server]** OLEDB_Provider configuration option value to `MSOLEDBSQL` in the WFM Data Aggregator Application.
     If the [Server] section does not exist, create it. See Creating New Sections and Options in the *Workforce Management Options Reference*.
3. Configure MS SQL Server to force encryption.
4. Restart WFM Server and Data Aggregator.

End procedure

Next step: Configure the WFM Backup/Restore Utility (BRU).

Configuring the WFM BRU

After the latest Microsoft OLE DB Driver is installed, the WFM Backup/Restore Utility must be configured to use the following connection switch:

```
-DSN "Provider=MSOLEDBSQL;Data Source=<DBMS Name>;Initial Catalog=<Database Name>;User
ID=<User Name>;Password=<Password>;"
```

For example:

```
WFMBRU.exe -BACKUP -DSN "Provider=MSOLEDBSQL;Data Source=<DBMS Name>;Initial
```

```
Catalog=<Database Name>;User ID=<User Name>;Password=<Password>;" -FILE <backup>.db
```