# Genesys Intelligent Automation Deployment Guide

## Installing Genesys Intelligent Automation

12/21/2025

# Contents

# Installing Genesys Intelligent Automation

This page describes how to install Genesys Intelligent Automation into a test or production environment.

If you are upgrading to the latest version of Intelligent Automation from a previous version of Intelligent Automation or Genesys App Automation Platform (GAAP), use the instructions contained in the Genesys Intelligent Automation Migration Guide.

## Installation prerequisites

> **Important**
> Before proceeding, refer to the prerequisites document to review minimum specifications, including database requirements, that must be met before installation begins.

## Set up databases

To set up the databases in the database layer, follow the instructions corresponding to the DBMS you are using:

- SQL Server
- Oracle

### SQL Server

To set up SQL Server databases, do the following:

1. Open *SQL Server Configuration Manager*.
2. In the list, navigate to **SQL Server Network Configuration > Protocols for *<database_instance_name>*.**
3. In the right pane, double-click **TCP/IP** to open TCP/IP Properties. Perform the following actions:
   a. In the **Protocol** tab, ensure that TCP/IP is enabled. The **Enabled** value must be **Yes**.

   b. In the **IP Addresses** tab, go to the **IPAll** section and set **TCP Port** 1433.
   c. Click **OK**.
4. Close *SQL Server Configuration Manager*.
5. Open *Windows Services*.
6. Right-click your SQL Server and select **Restart**.
7. Close *Windows Services*.
8. Open *SQL Server Management Studio*.
9. In the **Connect to Server** dialog box, log in as an Administrator (**Windows Authentication**).
10. In the **Object Explorer** panel, right-click **Security > Logins** and select **New Login**.
11. In the **Login - New** dialog box, perform the following actions:
    a. In the **Login name** field, enter `speechstorm`.
    b. Select **SQL Server Authentication**.
    c. Disable the **Enforce password expiration** check box.
    d. In the **Server Roles** page, ensure **public** is checked.
    e. Click **OK**.
12. In the toolbar, click **New Query**.
13. Do one or both of the following, if appropriate:
    - If you are using SQL Server for your configuration database, enter the following in the query window:

      ```
      use master;
      create database fish;
      GO
      alter database fish set ALLOW_SNAPSHOT_ISOLATION ON;
      GO

      use fish;
      create user speechstorm for login speechstorm;
      exec sp_addrolemember N'db_ddladmin', N'speechstorm';
      ALTER SERVER ROLE [sysadmin] ADD MEMBER [speechstorm];
      grant SELECT, DELETE, INSERT, UPDATE, EXECUTE, VIEW DATABASE STATE to speechstorm;
      ```

    - If you are using SQL Server for your reporting database, enter the following in the query window:

      ```
      use master;
      create database fishreports;
      GO
      alter database fishreports set ALLOW_SNAPSHOT_ISOLATION ON;
      GO

      use fishreports;
      create user speechstorm for login speechstorm;
      exec sp_addrolemember N'db_ddladmin', N'speechstorm';
      ALTER SERVER ROLE [sysadmin] ADD MEMBER [speechstorm];
      grant SELECT, DELETE, INSERT, UPDATE, EXECUTE, VIEW DATABASE STATE to speechstorm;
      ```

14. Click **Execute** to run the SQL query.
15. Close *SQL Server Management Studio*.

## Oracle

To set up Oracle databases, do the following:

1. Open *Oracle SQL Developer*.
2. Log in as the **SYSTEM** user.
3. Open a new SQL Worksheet for that connection.
4. If you are using Oracle for your configuration/reporting database, enter the query in the query window, using one of the following examples as reference:
   - For **Oracle 19c Enterprise** replacing <TABLENAME> with your configuration or reporting table names:

     ```
     CREATE BIGFILE TABLESPACE <TABLENAME> DATAFILE '<TABLENAME>.dbf' SIZE 20M AUTOEXTEND
     ON;
     CREATE USER <TABLENAME> IDENTIFIED BY speechstorm DEFAULT TABLESPACE <TABLENAME>;

     GRANT "RESOURCE" TO <TABLENAME>;
     GRANT "CONNECT" TO <TABLENAME>;
     GRANT CREATE VIEW TO <TABLENAME>;
     GRANT INSERT ANY TABLE TO <TABLENAME>;
     GRANT UNLIMITED TABLESPACE TO <TABLENAME>;
     GRANT SELECT_CATALOG_ROLE to <TABLENAME>;
     GRANT SELECT ANY DICTIONARY to <TABLENAME>;
     ```

   - For **Oracle RAC 19c ASM** - Replace the first line in previous example with the <TABLENAME> with your configuration or reporting table names:

     ```
     CREATE BIGFILE TABLESPACE <TABLENAME> DATAFILE SIZE 20M AUTOEXTEND ON;
     ```

   - For **Oracle 19c RAC (ASM) TDE** - Replace the first line in previous example with the replacing <TABLENAME> with your configuration or reporting table names:

     ```
     CREATE BIGFILE TABLESPACE <TABLENAME> DATAFILE SIZE 20M  AUTOEXTEND ON ENCRYPTION
     USING 'AES256' ENCRYPT;
     ```

     To encrypt existing tables which were part of Oracle 19C RAC,

     ```
     ALTER TABLESPACE <TABLENAME> OFFLINE NORMAL;  -- recommended to set offline first
     ALTER TABLESPACE <TABLENAME> ENCRYPTION OFFLINE USING 'AES256' ENCRYPT; -- Encrypt
     table but other options are available, but NOT column encryption.
     ALTER TABLESPACE <TABLENAME> ONLINE; -- Set table online to activate its operation.
     ```

5. Click **Execute Script**.

## Create the directory structure and prepare the environment

1. Upload a copy of the Intelligent Automation installer ZIP file onto each of the machines that will be used.
2. Create a folder called **SpeechStorm** (case sensitive), preferably in the same location on all of the machines that will be used. This folder acts as the base folder location for the install. In most instances, you can use the following location: **C:\SpeechStorm**. This document references this location throughout. You can use a different drive and folder name, but Genesys recommends you create it on or close to the root or top level of the drive.
3. Unzip the Intelligent Automation installer into each of the **SpeechStorm** folders that you created on various machines in the previous step. Ensure the folder structure is exactly as follows, with no additional directory levels.
   - **C:\SpeechStorm\Platform\..**
   - **C:\SpeechStorm\Setup\..**
4. Update the database connection details in the **database.properties** file of the TomcatVUI server to point to your databases. The file is located here:
   **C:\SpeechStorm\Platform\TomcatVUI\lib\database.properties**
   Inside this file, there are template connection strings for SQL Server and Oracle with all but the SQL Server connection strings commented out. You must update these details to match your environment. Ensure you only uncomment one set of connection strings for each type of database.
   The following code snippets are examples of the connection strings for each of the database types.

   **SQL Server Example**

```
#####################################
#
#  SQL Server
#
#####################################
Database.JDBC.Driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
Database.JDBC.ConnectionURL=jdbc:sqlserver://localhost:1433;Database=fish;Trusted_Connection=False;loginTimeout=1
Database.JDBC.Username=speechstorm
Database.JDBC.Password=speechstorm
Database.Pool.ConnectionValidationQuery=SELECT 1

ReportsDatabase.JDBC.Driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
ReportsDatabase.JDBC.ConnectionURL=jdbc:sqlserver://localhost:1433;Database=fishreports;Trusted_Connection=False;loginTimeout=1
ReportsDatabase.JDBC.Username=speechstorm
ReportsDatabase.JDBC.Password=speechstorm
ReportsDatabase.Pool.ConnectionValidationQuery=SELECT 1
```

**Oracle 19c Enterprise Example**

```
#######################################
#
#  Oracle 19c
#
#######################################
Database.JDBC.Driver=oracle.jdbc.OracleDriver
Database.JDBC.ConnectionURL=jdbc:oracle:thin:@localhost:1521:db01
Database.JDBC.Username=fish_USER
Database.JDBC.Password=speechstorm
Database.Pool.ConnectionValidationQuery=SELECT 1 FROM DUAL

ReportsDatabase.JDBC.Driver=oracle.jdbc.OracleDriver
ReportsDatabase.JDBC.ConnectionURL=jdbc:oracle:thin:@localhost:1521:db01
ReportsDatabase.JDBC.Username=fishreports_USER
ReportsDatabase.JDBC.Password=speechstorm
ReportsDatabase.Pool.ConnectionValidationQuery=SELECT 1 FROM DUAL
```

**Oracle 19c RAC Example**

```
#######################################
#
#  Oracle 19c RAC
#
Database.JDBC.Driver=oracle.jdbc.OracleDriver
Database.JDBC.ConnectionURL=jdbc:oracle:thin:@scan-name:scan-port/db01
Database.JDBC.Username=fish_USER
Database.JDBC.Password=speechstorm
Database.Pool.ConnectionValidationQuery=SELECT 1 FROM DUAL

ReportsDatabase.JDBC.Driver=oracle.jdbc.OracleDriver
ReportsDatabase.JDBC.ConnectionURL=jdbc:oracle:thin:@scan-name:scan-port/db01
ReportsDatabase.JDBC.Username=fishreports_USER
ReportsDatabase.JDBC.Password=speechstorm
ReportsDatabase.Pool.ConnectionValidationQuery=SELECT 1 FROM DUAL
```

## Install Intelligent Automation components and Windows Services

The installation file (**SS_FW_Install.bat**) sets the paths for Java and Catalina home, creates self-signed certificates for HTTPS, and creates Windows Services to start automatically for the Intelligent Automation software and Flex licensing component.

When you unzip the Intelligent Automation IP executable file, two folders (**Platform** or **Setup**) are created. To install Intelligent Automation, open the **Platform** folder, right-click **SS_FW_Install.bat** and select **Run as Administrator**.

> ### Warning
> You must select **Run as Administrator** or the services will be installed with insufficient privileges.

Depending on your environment, you will be prompted to make choices or provide information during the installation process, as follows:

| | |
|---|---|
| 1. **Enter the path to the Platform folder; for example, C:\SpeechStorm\Platform:** | |
| | Enter the path to where you created the SpeechStorm folder and unzipped the installer. For example, **C:\SpeechStorm\Platform**.<br>Important<br>This path is case sensitive. If incorrect, the installer prompts you to enter the path again. |
| 2. **Have you just restarted your server after database password encryption? (Y/N)** | |
| | If you are just starting a new installation, enter n. If Intelligent Automation has already been installed, but you restarted the server to activate the database password encryption, enter y. You will then be directed to populate (set up) the database. |
| 3. **If you'd like to install on Genesys Engage, enter 1, or to install on PureConnect, enter 2** | |
| | This determines whether you're installing on Genesys Engage or on PureConnect. Based on your selection, your install package will be modified to meet the requirements of your chosen platform. |
| 4. **Would you like to install a GUI server? (Y/N)** | |
| | Enter y to run a TomcatGUI (administrator) web application on this machine that will be used to author call flows, view reports, and general setup. You must have at least one GUI per installation. If this is a single-server install, you must install this component now. |
| 5. **Would you like to install a VUI server? (Y/N)** | |
| | Enter y to run a TomcatVUI (administrator) web application on this machine that will be used to handle customer calls. In a production environment, there might be several VUIs that handle calls. If this is a single-server install, you must install this component now. Generally, companies install one TomcatVUI per server, as this is the component that handles calls and is the most commonly clustered component. |
| 6. **Would you like to install a TomcatMessaging server? (Y/N)** | |
| | Enter y to install a TomcatMessaging server and load balancer. These are used specifically for Visual IVR and Facebook Messenger. |
| 7. **Would you like to install an Integration Server? (Y/N)** | |
| | Enter y to install a TomcatIntegration server. |
| The next three prompts (8, 9, and 10) appear only if you chose to select a TomcatGUI Server; that is, if you entered y in response to prompt 3. | |
| 8. **Please enter the server FQDN -Fully Qualified Domain Name- :** | |
| | Enter the computer’s FQDN to generate a self- |

| | |
|---|---|
| | signed SSL certificate for the GUI server. This value is case sensitive. After the installer generates a self-signed SSL certificate, you can view it in the GUI configuration file, located in **C:\SpeechStorm\Platform\TomcatGUI\conf**. |
| 9. **Enter pass phrase for speechstorm.key** | |
| | Enter the password to create the self-signed certificate for the GUI server.<br><br>The installer prompts you to enter this password three times. Make sure you remember this password, as it will be used later in this install. |
| 10. **Enter the name for the TomcatGUI Windows Service; for example, FishGUI** | |
| | Enter a unique name for the TomcatGUI Windows Service. Genesys recommends the name `FishGUI`.<br><br>The installer creates a Windows Service set to start automatically. |
| The next two prompts (11 and 12) appear only if you chose to select a TomcatMessaging server; that is, if you entered y in response to prompt 4. | |
| 11. **Please enter the server FQDN -Fully Qualified Domain Name-** | |
| | Enter the FQDN of this computer to generate a self-signed SSL certificate for the TomcatMessaging server. After the installer generates the certificate, you can view it in **C:\SpeechStorm\Platform\TomcatMessaging\conf**. |
| 12. **Enter the name for the TomcatMessaging Windows Service; for example, FishMessaging** | |
| | Enter a unique name for the TomcatMessaging server Windows Service. Genesys recommends the name `FishMessaging`.<br><br>The installer creates a Windows Service set to start automatically. |
| The next two prompts (13 and 14) appear only if you chose to select a TomcatIntegration server; that is, if you entered y in response to prompt 5. | |
| 13. **Please enter the server FQDN -Fully Qualified Domain Name-** | |
| | Enter the FQDN of this computer to generate a self-signed SSL certificate for the TomcatIntegration server. After the installer generates the certificate, you can view it in **C:\SpeechStorm\Platform\TomcatIntegration\conf**. |
| 14. **Enter the name for the TomcatIntegration Windows Service; for example, FishIntegration** | |
| | Enter a unique name for the TomcatIntegration server Windows Service. Genesys recommends the name `FishIntegration`.<br><br>The installer creates a Windows Service set to start automatically. |
| 15. **Enter the name for the TomcatVUI Windows Service; for example, FishVUI** | |

| | |
|---|---|
| | Enter a unique name for the TomcatVUI Windows Service. Genesys recommends the name `FishVUI`.<br><br>The installer creates a Windows Service set to start automatically. |
| At this point, a Flex License Server is installed as a Windows Service set to start automatically. This is required to license Genesys Intelligent Automation, and requires that a valid license be imported into Flex before starting Genesys Intelligent Automation. | |
| 16. **IMPORTANT: Make sure you modify the database.properties file in the TomcatVUI with the correct credentials.** | |
| | Update the **database.properties** file to reflect the configuration of your environment (Oracle or SQL Server). Press **Enter** when you are done. The installer will then copy the updated file to each of the library files for each of the Tomcat applications, namely:<br><br>• **<PlatformPath>\TomcatVUI\lib**<br>• **<PlatformPath>\TomcatGUI\lib**<br>• **<PlatformPath>\TomcatMessaging\lib**<br>• **<PlatformPath>\TomcatIntegration\lib**<br><br>Where **<PlatformPath>** is the path to the folder in which Genesys Intelligent Application is installed. |
| 17. **Would you like to encrypt the database password in the database.properties file? (Y/N)** | |
| | Database encryption ensures that the password does not appear in plain text in a file, allowing someone with access to the file to gain manual access to the database.<br><br>Tip<br>You can encrypt the password now, or at any time in the future, as described in Encrypting the Database Password<br><br>If you want to implement this small but effective security measure, enter y and follow the steps in Encrypting the Database Password. After the encryption is complete, the installer will populate the database as described in Populating the Database, if necessary.<br><br>If you do not want to encrypt the database password right now, enter n and the database will be populated as described in Populating the Database, if necessary. |

## Encrypting the Database Password

You can encrypt the password to your database by running the **Encryption.bat** database script file. If you have entered y in response to the prompt **Would you like to encrypt the database password in the database.properties file?** during installation, the installer will run this file for

you.

To encrypt the password after you have installed Intelligent Automation software, go to ***<IA_Platform_Folder>*/TomcatVUI/webapps/fish-vui/WEB-INF/bin/** and run the **Encryption.bat** script file from the command line. The actual encryption steps are the same as the steps when encrypting database during installation but be sure to restart the server when you have completed the encryption.

You can also undo the encryption and go back to using the unencrypted values, or use the script to re-encrypt the passwords if they were changed.

> ### Warning
> When you have finished encrypting the passwords, you must restart the server to activate the changes.

If you start the script but then decide you don't want to perform the encryption, you can press CTRL-C to exit the script with no changes being made.

Before going any further, open the **database.properties** file of the TomcatVUI, and ensure that the applicable keys (**Database.JDBC.Password**, and **ReportsDatabase.JDBC.Password**) are set to the current and correct unencrypted password value. If the values aren't correct, correct them before continuing.

When prompted by **Enter the path to the location for the Fish_credentials.keystore file; for example, C:\FISHKeystore\:**, enter the path to where the Intelligent Automation keystore (**Fish_credentials.keystore**) is to be located. If you have not yet created it, the script will create it for you.

> ### Important
> This path must be different from the path to the Platform folder. If the same path is entered, the script will prompt you again for a correct path.

The script encrypts the database password and makes the following changes to the **database.properties** file of the TomcatVUI:

- Deletes the values of the applicable **Database.JDBC.Password**, and **ReportsDatabase.JDBC.Password** keys, leaving them set to an empty value.
- Creates two new keys (one for each applicable database), **Database.JDBC.Encrypted.Password**, and **ReportsDatabase.JDBC.Encrypted.Password**, and sets the new keys to the encrypted value.

The script then goes on to create the necessary keystore file, and saves the encryption key and the path to where it is stored in the environment variables **FISH_KEYSTORE_PASSWORD** and **FISH_KEYSTORE_PATH**, respectively. Then it copies the updated **database.properties** file to the other three installed Tomcat servers, namely GUI, Messaging, and Integration.

> **Tip**
> After the encryption is complete, you must restart the server to activate the encryption. In addition, check that the two new environment variables **FISH_KEYSTORE_PASSWORD** and **FISH_KEYSTORE_PATH** are active. If you are using Windows, after restart, you can view these variables by going to **Start** > **Control Panel** > **System** > **Advanced system settings** > **Environment Variables** > **System variables**.

At run-time, Intelligent Automation detects the new keys, and uses the encrypted values to access the databases.

The following example illustrates setting the encrypted values in the **database.properties** file for an SQL Server configuration database and an Oracle reports database:

**database.properties** file before encryption:

```
...
#######################################
#
#  SQL Server
#
Database.JDBC.Driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
Database.JDBC.ConnectionURL=jdbc:sqlserver://localhost;Database=fish360;Trusted_Connection=False;loginTimeout=1
Database.JDBC.Username=speechstorm
Database.JDBC.Password=
Database.Pool.ConnectionValidationQuery=SELECT 1

#ReportsDatabase.JDBC.Driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
#ReportsDatabase.JDBC.ConnectionURL=jdbc:sqlserver://localhost;Database=fishreports360;Trusted_Connection=False
#ReportsDatabase.JDBC.Username=speechstorm
#ReportsDatabase.JDBC.Password=
#ReportsDatabase.Pool.ConnectionValidationQuery=SELECT 1

#####################################
#
#  Oracle
#
#Database.JDBC.Driver=oracle.jdbc.OracleDriver
#Database.JDBC.ConnectionURL=jdbc:oracle:thin:@localhost:1521:orcl
#Database.JDBC.Username=C##fish
#Database.JDBC.Password=speechstorm
#Database.Pool.ConnectionValidationQuery=SELECT 1 FROM DUAL
#
ReportsDatabase.JDBC.Driver=oracle.jdbc.OracleDriver
ReportsDatabase.JDBC.ConnectionURL=jdbc:oracle:thin:@localhost:1521:orcl
ReportsDatabase.JDBC.Username=C##fishreports
ReportsDatabase.JDBC.Password=speechstorm
ReportsDatabase.Pool.ConnectionValidationQuery=SELECT 1 FROM DUAL
```

After encryption, the **database.properties** file is as follows. Note that the Password keys are set to an empty value, and that the new keys with the encrypted values are shown at the end of the file.

```
...
#######################################
#
#  SQL Server
```

```
#
Database.JDBC.Driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
Database.JDBC.ConnectionURL=jdbc:sqlserver://localhost;Database=fish360;Trusted_Connection=False;loginTimeout=1
Database.JDBC.Username=speechstorm
Database.JDBC.Password=
Database.Pool.ConnectionValidationQuery=SELECT 1

#ReportsDatabase.JDBC.Driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
#ReportsDatabase.JDBC.ConnectionURL=jdbc:sqlserver://localhost;Database=fishreports360;Trusted_Connection=False
#ReportsDatabase.JDBC.Username=speechstorm
#ReportsDatabase.JDBC.Password=
#ReportsDatabase.Pool.ConnectionValidationQuery=SELECT 1

#######################################
#
#  Oracle
#
#Database.JDBC.Driver=oracle.jdbc.OracleDriver
#Database.JDBC.ConnectionURL=jdbc:oracle:thin:@localhost:1521:orcl
#Database.JDBC.Username=C##fish
#Database.JDBC.Password=
#Database.Pool.ConnectionValidationQuery=SELECT 1 FROM DUAL
#
ReportsDatabase.JDBC.Driver=oracle.jdbc.OracleDriver
ReportsDatabase.JDBC.ConnectionURL=jdbc:oracle:thin:@localhost:1521:orcl
ReportsDatabase.JDBC.Username=C##fishreports
ReportsDatabase.JDBC.Password=
ReportsDatabase.Pool.ConnectionValidationQuery=SELECT 1 FROM DUAL

#  This is the new encrypted password, please remove this property and enter the non
encrypted value in Database.JDBC.Password if you wish to encrypt it again or use the
decrypted version of the password.
Database.JDBC.Encrypted.Password=b3988d0ef1280e70d00c0e8faeb72201

#  This is the new encrypted password, please remove this property and enter the non
encrypted value in ReportsDatabase.JDBC.Password if you wish to encrypt it again or use the
decrypted version of the password.
ReportsDatabase.JDBC.Encrypted.Password=b3988d0ef1280e70d00c0e8faeb72201
```

## Unencrypting the Database Passwords

Follow these steps if you want to use the unencrypted passwords, or if you are going to re-encrypt the password.

1. Open the **database.properties** file in the **TomcatVUI/lib** folder.
2. Delete all lines beginning with any of the following:
   - `Database.JDBC.Encrypted.Password`
   - `ReportsDatabase.JDBC.Encrypted.Password`
3. Set the lines starting with the following to the correct unencrypted passwords:
   - `Database.JDBC.Password`
   - `ReportsDatabase.JDBC.Password`
4. Save and close the modified **database.properties** file.
5. Repeat steps 1 to 4 for each **database.properties** file in the **TomcatGUI\lib**, **TomcatMessaging\lib**,

and **TomcatIntegration\lib** folders.

6. Go to the **FISH_Keystore** folder and delete the **Fish_credentials.keystore** file, if it exists.
7. Delete the **FISH_Keystore** folder if it exists.
8. Delete the **FISH_KEYSTORE_PASSWORD** and **FISH_KEYSTORE_PATH** system environment variables in your Windows Server, if they exist.

### Re-encrypting the Database Passwords

If you want to re-encrypt your passwords after they were originally encrypted, you must first unencrypt them as described above (if they are encrypted), then perform this abbreviated encryption process. Probably the most common reason for re-encrypting the passwords is to encrypt new passwords after the previous passwords were changed.

1. If the passwords are already encrypted, follow the steps in the previous section to unencrypt them.
2. Have a user with Administrator privileges re-run the **Encryption.bat** file located in the ***<Platform path>*\TomcatVUI\webapps\fish-vui\WEB-INF\bin** to complete the encryption process.

## Populating the Databases

Use the **Migrate.bat** file to set up the database schema for Intelligent Automation.

> **Important**
>
> This script needs to be run only once per installation, as all servers connect to this central database. If you have already run this script during an install on another machine, you can quit the script (press CTRL-C).

Once this is complete, the following message is printed in the console: *Don't forget to run the PostMigrate script once code has been deployed on all VUI Servers. Press any key to continue . . .*

Use the **PostMigrate.bat** file to do the post-migration (backfill) for your database to the latest version.

> **Important**
>
> If this is an online upgrade to an existing installation, you should only run this step when installing your final server.

You'll then see the following prompt:

*Would you like to run the Post Migrate step? (Enter "1" to continue) NOTE: If this is an online upgrade*

*to an existing installation, you should only run this step when installing your final server.*

- If you press 1, the post-migration will proceed.
- If you press anything other than 1, the system will exit the console and the post-migrate step will not execute.

## Add additonal Intelligent Automation Servers

To handle heavy call loads, you can add additional Intelligent Automation servers to your Intelligent Automation system. In fact, most Intelligent Automation users set up multiple VUI servers to process calls. To add additional VUI servers, complete the following steps on each host machine:

1. Follow the steps in the section Create the directory structure and prepare the environment. You can copy the **database.properties** files from the machine on which you previously installed Intelligent Automation.
2. Follow the steps in the section Install Intelligent Automation components and Windows Services, but note the following changes:
   - When prompted if you want to install a GUI or a Messaging server, enter `n`.
   - When prompted if you want to install a VUI server, enter `y`.

## Use Flex to license Intelligent Automation server

Next, you must license the Intelligent Automation server within Flex before you can start the Intelligent Automation services. To do this, you need a license file that was provided with the installer files.

> ### Important
> License files are explicitly generated using the MAC address of the machines intended for the installation. Each instance must have an extra FlexLM license server and license file. Remote licensing is not possible.

1. Open Windows Services using one of the following methods in Windows:
   - Open the Start menu, click **Search**, and enter `Services`.
   - Open the Control Panel and select **Services**.
2. In Windows Services, right-click **SpeechStorm License Manager** and select **Properties**. Then, in the **Log On** tab, select **Local System Account**.
3. After the service initializes, open a web browser and navigate to `http://localhost:8090` to open the Flex web interface.

4. After the webpage loads, click the **Administration** tab and use the following login:
    - Username: `admin`
    - Password: `123456789`
5. Click **Import License** under **Vendor Daemon Configuration** tab to upload the license file that was delivered with the installer and specific for this machine. Select the license file and ensure you enable the **Overwrite License File on License Server** check box. After you import the file, check the list of licenses again. If the import is successful, the list displays your license with a status of **Up**.

## Update SSL certificates

Next, update the password for the SSL certificates that were created earlier. You must update the passwords listed in the following locations:

- **C:\SpeechStorm\Platform\TomcatGUI\conf\server.xml**
- **C:\SpeechStorm\Platform\TomcatMessaging\conf\server.xml**
- **C:\SpeechStorm\Platform\TomcatIntegration\conf\server.xml**

In each file, locate the **SSLPassword** value and update it to the one you created when generating the SSL certificates.

## Start Intelligent Automation services

In Windows Services, start the services that are applicable to your environment:

- Apache Tomcat 9.0 FishGUI
- Apache Tomcat 9.0 FishVUI
- Apache Tomcat 9.0 FishMessaging (optional)
- Apache Tomcat 9.0 FishIntegration (optional)

## Use the GUI server to configure Intelligent Automation

Now you can access the Intelligent Automation interface in a web browser.

1. Open a web browser and enter `http://localhost:8080/fish-gui`. After the page loads, confirm that the browser correctly redirected to use **https**.
2. The browser displays a security warning because you created a self-signed certificate during the install. In Google Chrome, click **ADVANCED** and then click **Proceed to localhost (unsafe)**. This indicates to the browser that you understand the certificate is self-signed. This process might vary in other browsers.

3. The browser displays the GUI authentication screen. Enter the following:
   - Username: `admin@genesys.com`
   - Password: `123456`

   After you log in, Intelligent Automation redirects you to change your password.
4. Go to **Administration > Servers** and perform the following actions:

> **Important**
>
> In the following steps, the hostname you enter must be reachable from the MCP servers, as this hostname is sent in the rendered Intelligent Automation VXML. For example:
>
> - If you enter `localhost` as a hostname but the MCP server is not installed on the same machine, the hostname `localhost` does not work.
> - If you enter `gaapvui1` as a hostname but the MCP server cannot reach this server without a FQDN such as `gaapvui1.genesys.com`, the hostname `gaapvui1` does not work.

   a. In the **Default VUI Server** row, click **edit**. Set the hostname to the name of your VUI server and port to `8082`. Click **Save**.
   b. (Optional) If you installed additional VUI servers, perform the following steps.
      i. Click **Create a New Server** and select **New Voice Server**.
      ii. Enter the following information:
         - **Server Name** - Enter a descriptive name for the server. For example, `VUI_2`.
         - **Server Connection Details** - Select a connection type (HTTP or HTTPS) and enter a hostname and port.
         - **Cluster** - Specify which cluster to attach this server. Typically, this setting is unchanged from the **Default Voice Cluster**.
         - **Server Status** - Select the **Active** check box to make this server active and therefore able to process calls.
         - Click **Save**.
      iii. In the **Servers** list, look for your new server and note its **ID** value.
      iv. On the server host machine, go to **C:\SpeechStorm\Platform\TomcatVUI\lib**.
      v. Open the **fish-vui-local.properties** file for editing.
      vi. Look for the following line: **ThisServer.ID=#**. Replace **#** with the **Server ID** value you noted earlier.
      vii. Go to Windows Services and restart the FishVUI service.
   c. In the **Default Admin Server** row, click **edit**. Set the hostname to the name of your GUI server. Click **Save**.

> **Important**
>
> - Genesys recommends that you use a secure connection by selecting the **https** protocol and specifying a secure port that is referenced in the **server.xml** file.
> - You must restart the GUI server so it can load the certificates into its trust store.
> - You might encounter an error after clicking **Save** if you still need to configure other server connections. Ignore the error—the configuration was saved correctly. The error does not appear after you have configured all server connections and the servers are reporting as **Online**.

d. (Optional) This step applies only for Messaging and VUI servers. Go to **Administration > Clusters** and click **Create a new Cluster**. In the **New Cluster Type:** pop-up, select **New Load Balancer Cluster**. In the next screen, enter the following information:

- **Cluster Name** - Specify a unique name.
- **Load Balancer Servers Will Balance Requests Arriving at This Port** - Select **http** and a port number that is not used by anything else on this machine.
- **Hostname Used in External Links to this Cluster** - Specify the machine's host name.
- Click **Save**.

Go to **Administration > Servers**. If there is no Load Balancer server, click **Create a New Server**. In the **New server type:** pop-up, select **New Load Balancer Server**. In next screen, enter the following information:

- **Server Name** - Specify a unique name.
- **Server Connection Details** - Specify a server name and port number.

> **Important**
>
> - For Messaging servers, the default port number is **8081**. To verify, open **C:\SpeechStorm\platform\TomcatMessaging\conf\server.xml** and check the value for **Connector port**.
> - For VUI servers, the default port number is **8082**. To verify, open **C:\SpeechStorm\platform\TomcatVUI\conf\server.xml** and check the value for **Connector** port.

- **Cluster** - Select the cluster you created in **Administration > Clusters**.
- **Server Status** - Enable the **Active** check box.
- Click **Save**.

e. Click **Re-run Server Checks** to refresh the server list and ensure all servers are functioning normally.

> **Important**
>
> Servers set to use HTTPS do not report as being available until the next step is performed.

6. (Optional) Set up HTTPS for Voice, Messaging, Load Balancer and other Genesys servers.
   a. Go to **Administration > Certificates**.
   b. Click **Import a new Certificate**.
   c. In **Remote Server Details**, enter the hostname and port number of the server for which you want to import the certificate.
   d. Click **Get Certificate**. The page updates to show the certificate has been fetched successfully.
   e. Enter a description in the **Description** field.
   f. Click **Save**.

> **Important**
>
> - You might see a message stating the cache cannot be flushed on the server. This is because the HTTPS server cannot communicate until the certificate has been uploaded and services have been restarted. If you see this error, go to **Administration > Certificates** again and you can see the certificate you uploaded. Repeat this process for all servers that use HTTPS, then restart those servers. When they come back on, they appear as **Online** in the **Administration > Servers** tab.
> - To use TLS 1.3 connections with other Genesys servers, you must set the following Default Server Settings:
>   - Set **GenesysSDK.ConfigServer.IsTLSEnabled** to **true**
>   - Set **GenesysSDK.PlatformServer.IsTLSEnabled** to **true**
>   - Set **HttpClient.Security.SSLContext** to **TLSv1.3**
>   - Set **HttpClient.Security.SupportedProtocols** to **TLSv1.3**
>
>     Optionally, you can set **HttpClient.Security.SupportedCipherSuites** to restrict the available cipher suites by adding a comma-separated list of cipher suite names. See this page for more information on valid values.

> **Important**
>
> Ensure that the load balancer certificates are imported into the certificate store of Java in the other load balancers. If you have three load balancers (A,B, and C), ensure that:
>
> - Load Balancer A has B and C's certificates in A's Java certificate store.

- Load Balancer B has A and C's certificates in B's Java certificate store.
- Load Balancer C has A and B's certificates in C's Java certificate store.

This will enable the load balancers to communicate with each other successfully.

7. Go to **Administration > Default Server Settings** and update the following settings:
   - **GraphViz.DotPath** - Specify the path to the GraphViz executable. Usually, this is `C:/SpeechStorm/Platform/Apps/GraphViz/bin/dot.exe` (use forward slashes).
   - (Optional) **Login.Security.Strict** - Set to `true` if you are in a PCI environment.
   - **Email.SMTP.Host** - Specify the hostname of your SMTP server (for example, `mail.speechstorm.com`).
8. Click **Save**.
9. Go to Windows Services and restart Intelligent Automation services, including FishGUI, FishMessaging, and optionally FishVUI.
10. After the services restart, log in again and go to **Administration > Servers**. Ensure all components are online.

## Import products and templates

### Important

Before proceeding, ensure you are still in the **Templates** company by checking the company name beside your username in the top-right corner.

1. To import products, go to **Administration > Products**.
   a. Click **Import a Product** to display a new page.
   b. Click **Import Product** and select the **All Product Definitions.zip** file, usually found at the following location: C:\SpeechStorm\Platform\AppsToBeInstalled\Products and templates\All Product Definitions.zip.
   c. Select the option **Overwrite Product ID if it Already Exists**.

### Important

The **This Tomcat Server is Linked to Eclipse** option requires a special license, *SpeechStormProductBuilder* and is not required for regular normal imports. Uncheck this option if it is selected.

d. Click **Import Product**.

2. To import templates, click **Import** in the top-level navigation bar.
   a. Select **Import everything**.
   b. Click **Choose File** and select the **All Product Templates.zip** file, usually found at the following location: C:\SpeechStorm\Platform\AppsToBeInstalled\Products and templates\All Product Templates.zip.
   c. Click **Choose Modules to Import...**. A pop-up displays a list of templates that will be imported.
   d. Scroll to the bottom of the list and ensure the **Create new persona for 'Chat Default Persona', 'Visual Default Persona'** check box is enabled.
   e. Click **Import**.

## Configuring Tomcat

When setting up Tomcat server, ensure that you configure the following parameters:

| Setting | Description |
|---|---|
| `-d64` | Tells the JVM to run in 64-bit mode. The current JVM automatically detects this, but it is best practice to declare it. |
| `-Dfile.encoding=UTF-8` | Tells the JVM to use UTF-8 as the default character set so that non-Western alphabets are displayed correctly. |
| `-Djava.library.path` | Specifies the path to the native library. |
| `-Djava.util.logging.config.file=%CATALINA_BASE%\conf\logging.properties` | Tells the JVM to use **%CATALINA_BASE%\conf\logging.properties** configuration file for logging. |
| `-server` | Tells the JVM to run in server mode. JVM always runs by default when using 64-bit JDK. It is a good practice to declare it explicitly. |
| `-Xms3072m` (for a system with 4 GB of memory) | Tells the JVM to allocate a minimum of 3072 MB of memory to the Tomcat process. This should be set to 75% of the available system memory.<br>Note: The amount of memory needs to be tuned depending on the actual environment. |
| `-Xmx3072m` (for a system with 4 GB of memory) | Tells the JVM to limit the maximum memory to the Tomcat process. This should be set to 75% of the available system memory.<br>Things to consider:<br>• The amount of memory must be tuned depending on the actual environment. 5GB of memory is a good starting point for 100,000 Things.<br>• The reason for making the minimum and maximum amounts of memory equal is to avoid the JVM having to re-evaluate required memory |

| Setting | Description |
| --- | --- |
| | and resize the allocation at runtime. While this is recommended for hosted and/or public facing environments, for development and test environments, using –Xms512m would suffice. Also, verify that there is enough memory left to allow the operating system to function. |
| `-XX:+UseG1GC` | Tells the JVM to use the Garbage First Garbage Collector. |

## How to configure the GIA logging

GIA supports log4j2.x version and the configuration is written in **log4j2.xml** file in the **Platform\Tomcat<Service>\webapps\fish-<service>\WEB-INF\classes** folder.

GIA supports RootLogger logging levels as info an the output log is piped to the Console and RandomRollingFileAppender. You can modify the configuration file to suit your requirements. Log4j2 supports Logger (RootLogger and Logger specific for classes) and Appenders (where the output logs are piped to either a console or file).