Genesys Intelligent Automation Deployment Guide

Genesys Intelligent Automation Current

6/27/2024

Table of Contents

Genesys Intelligent Automation Deployment Guide

This document describes the necessary steps to deploy Genesys Intelligent Automation.

Overview

Sizing and Prerequisites

Deployment

Overview

Genesys Intelligent Automation, formerly known as Genesys App Automation Platform (GAAP) and before that, SpeechStorm, is a solution that enables organizations to rapidly deploy phone self-service functionality to their customers, including intelligent call steering, for a more efficient and personalized customer experience.

Genesys Engage and PureConnect

As of release 9.0.001.01, Genesys Intelligent Automation is integrated with PureConnect. Intelligent Automation functions the same regardless of the Solution you are using, be it GVP (part of Genesys Engage) or PureConnect, and there is no difference in how you use it in day-to-day operations. Differences in installation are described in parallel with installation instructions for GVP.

Currently, PureConnect supports all but the following features of Intelligent Automation:

- Attach Data to the Call
- Conversation Manager
- Multi Mode
- Smart Transfer
- WhisperTransfer

For more information about PureConnect, refer to PureConnect documentation.

General Data Protection Regulation (GDPR) Compliance

Starting with release 9.0.002.00, Genesys Intelligent Automation is compliant with the General Data Protection Regulation (GDPR), passed by the European Union (EU) in 2016, that sets new rules for how companies manage and share personal data. It addresses the export of personal data outside the EU. The GDPR applies to enterprises across the globe that store the data of EU citizens.

For more information about GDPR and how it is implemented, refer to the Genesys Intelligent Automation Support for GDPR section of the Genesys Security Deployment Guide.

Architecture

This section contains some examples of deployments of Intelligent Automation framework and validated Database Management System (DBMS) architecture in a high-availability (HA) architecture.

Load Balancers

The load balancer can be a traditional network load balancer (like F5), or a DNS round-robin one, or even a manual DNS entry management method. The load balancer can be placed in front of the Intelligent Automation's Load Balancers. IA Load Balancers are configured specifically to handle IA traffic including session handling between the servers. You can use an external Load Balancer to direct traffic to an active IA Load Balancer.

Important

If you wish to install a standalone Messaging Server or a standalone Load Balancer server, then you should delete the existing load balancer component from **TomcatMessaging/webapps** after installation. For example, if you want a standalone Load Balancer server, then delete the **fish-messaging** file from **TomcatMessaging/webapps**.

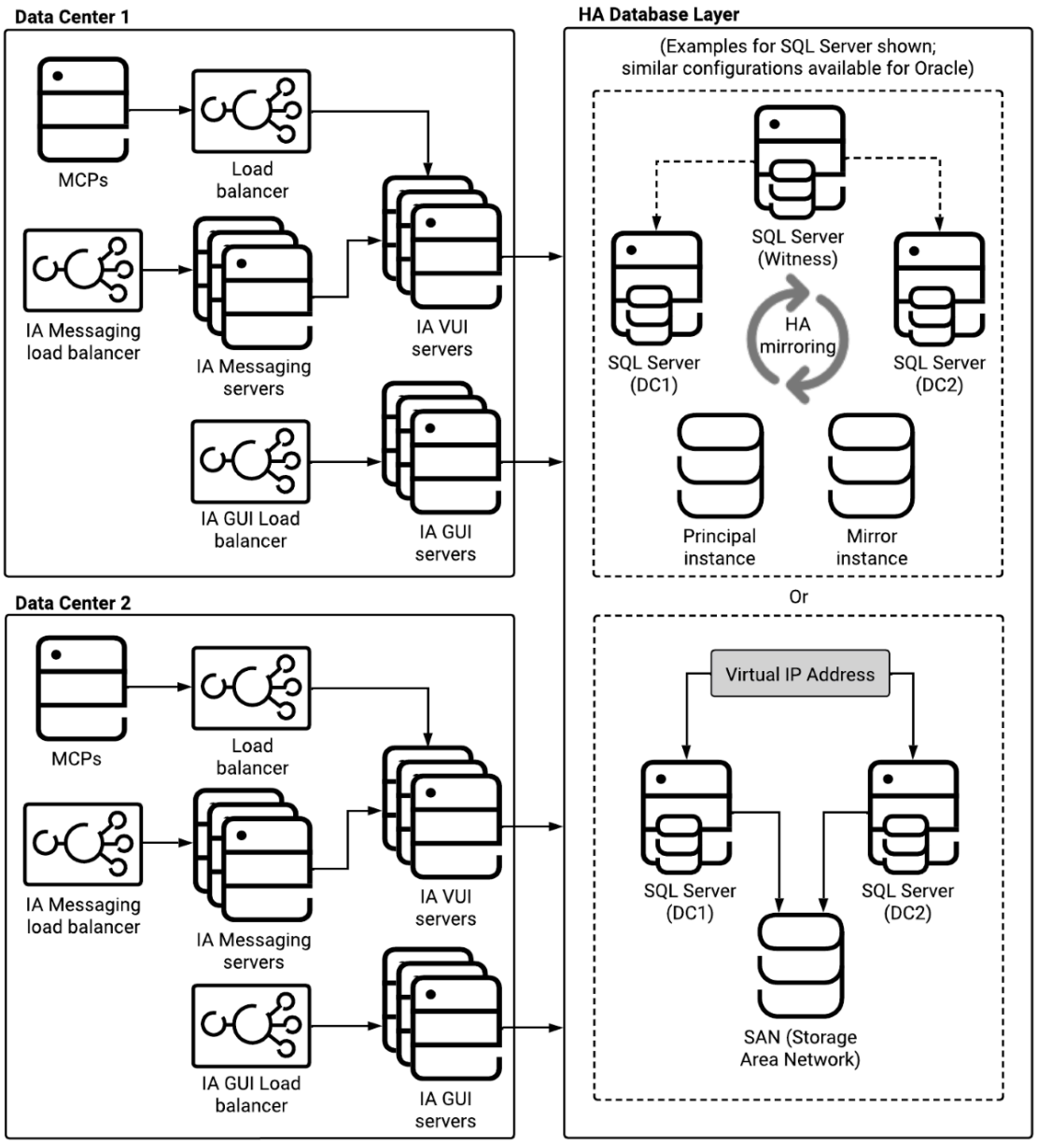
Important

To ensure a better performance,

- The database environment should present itself as a single endpoint for each DB. IA does not support connecting to multiple config or reporting databases.
- The databases are in sync with each other.
- The database switchover process must be independent and there is no action required from IA for the database switching.

Microsoft SQL Server

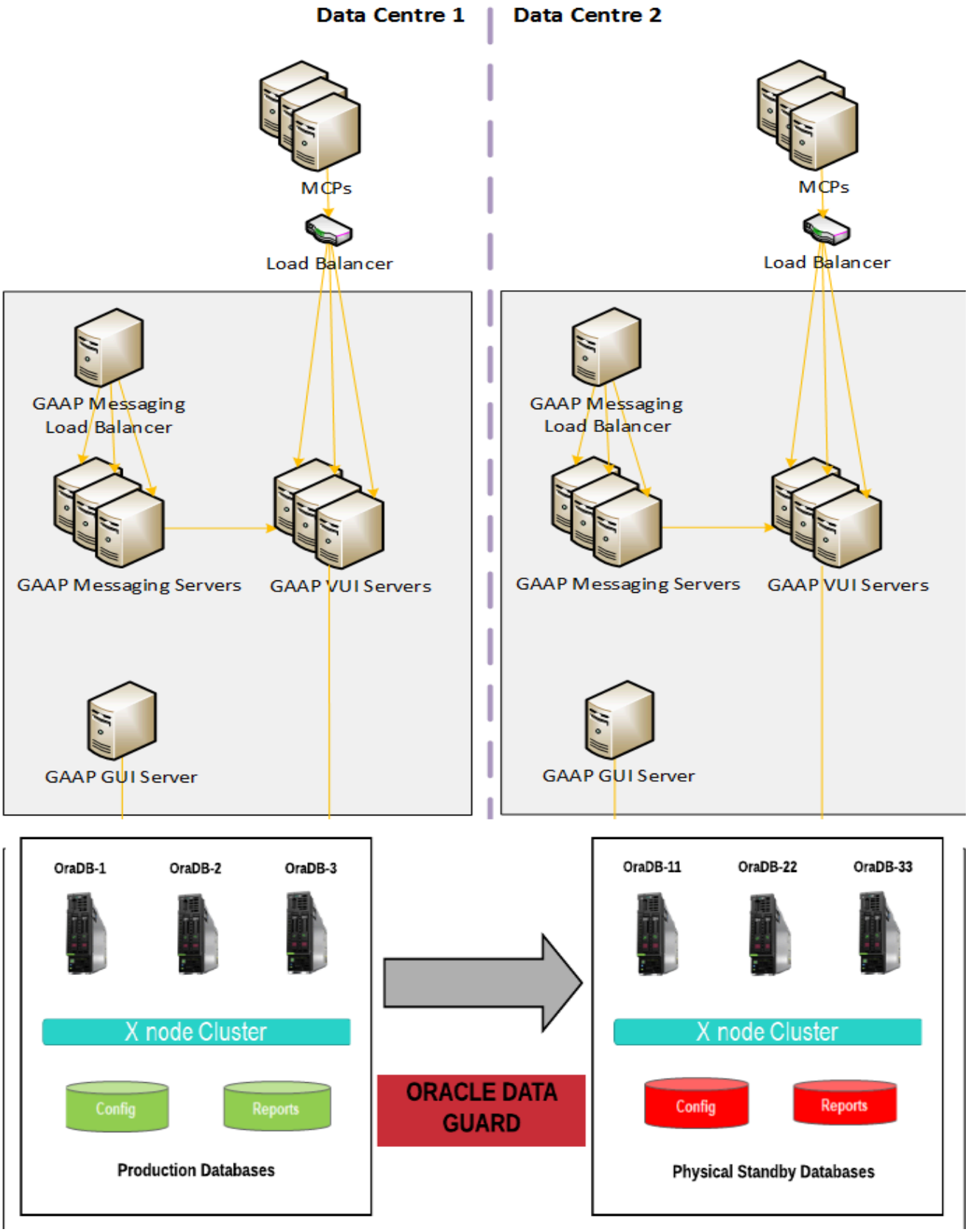
This diagram shows a sample deployment of Intelligent Automation framework and validated Microsoft SQL Server in a high-availability (HA) architecture.



Intelligent Automation framework HA architecture

Oracle

This diagram shows a sample deployment of Intelligent Automation framework and validated Oracle in a high-availability (HA) architecture.


Data Centre 1
Data Centre 2
MCPs
Load Balancer
MCPs
Load Balancer
GAAP Messaging Load Balancer
GAAP Messaging Servers
GAAP VUI Servers
GAAP GUI Server
GAAP Messaging Load Balancer
GAAP Messaging Servers
GAAP VUI Servers
GAAP GUI Server
OraDB-1
OraDB-2
OraDB-3
X node Cluster
Config
Reports
Production Databases
ORACLE DATA GUARD
OraDB-11
OraDB-22
OraDB-33
X node Cluster
Config
Reports
Physical Standby Databases

Sizing Recommendations and Software Prerequisites

This section documents hardware sizing recommendations and software prerequisites for Genesys Intelligent Automation software.

Hardware

The Voice User Interface (VUI) server supports the runtime application that serves customer calls. The number of servers and their specification should be dimensioned based on the number of concurrent calls, or *IVR ports*, to be supported.

The Graphical User Interface (GUI) server provides the Control Centre application that is used to design, configure, deploy, and monitor callflows. Only one GUI server can be active at a time. The specification for this does not depend on the number of IVR ports.

> **Important**
>
> Messaging and Integration Hub Servers should follow the same sizing rules as VUI servers.

Specification	VUI < 100 Ports	VUI 250 Ports	VUI 500 Ports	GUI server
CPU	1 quad core (2.2GHz+)	2 quad core (2.2GHz+)	2 quad core (3.0GHz+)	1 quad core (2.2GHz+)
Memory	8 GB RAM	8 GB RAM	12 GB RAM	8 GB RAM
Network	2x GB NIC	2x GB NIC	2x GB NIC	2x GB NIC
Disk Space	60 GB	60 GB	60 GB	60 GB

Virtualization

Intelligent Automation is fully supported on VMware ESXi 4 and above. If you prefer to deploy on

virtual infrastructure, the following standard server specifications must be provisioned.

Specification	VUI < 100 Ports	VUI 250 Ports	VUI 500 Ports	GUI server
Physical CPU	1 quad core (2.2GHz+)	2 quad core (2.2GHz+)	2 quad core (3.0GHz+)	1 quad core (2.2GHz+)
Physical Memory	16 GB RAM	32 GB RAM	32 GB RAM	16 GB RAM
Network	2x GB NIC	2x GB NIC	2x GB NIC	2x GB NIC
Disk Space	60 GB	60 GB	60 GB	60 GB
vWare	• 2x vCPU • 8 GB vRAM	• 4x vCPU • 8 GB vRAM	• 4x vCPU • 12 GB vRAM	• 2x vCPU • 8 GB vRAM

Important

- Standard server specifications are for installation of the Intelligent Automation Voice User Interface (VUI) and Graphical User Interface (GUI) components only on separate servers. It is assumed that the database will be located on its own server.
- You must procure, supply and configure third-party software for functions such as as Automatic Speech Recognition (ASR) and Text-to-Speech (TTS).
- You can increase the number of available ports by increasing the number of servers.
- High availability requires n*2 servers deployed across a minimum of two physical machines.
- Disk space requirements are sized for the storage volume/drive on each server to be available for the installation of Intelligent Automation and associated files and folders. It does not include sizing for the operating system or other system software.

Software Prerequisites

Intelligent Automation requires operating system and application server software to operate, and Database Management System (DBMS) software for data storage. This section contains the prerequisites for both.

Operating system and application server software

See the Genesys Intelligent Automation page on the *Supported Operating Environments* page for the list of operating systems and web broswers supported. You must ensure that each component has loaded and is running the required software before you install the Intelligent Automation software.

Database software

Intelligent Automation requires two databases, one (called the *core* database) for its configuration, and one for its reports. In release 3.6 and earlier, Microsoft SQL Server and Oracle were supported, and provided the necessary functionality.

See the Genesys Intelligent Automation page on the *Supported Operating Environments* page for the list of databases supported.

IVR technologies and platforms

The Intelligent Automation framework supports enterprise-scale Interactive Voice Response (IVR) technologies and platforms. The Intelligent Automation framework is supported on the following combinations of components.

> **Important**
>
> From Intelligent Automation version 9.0.100, Messaging Server is only used for Web IVR.

Combination #1

Vendor	Component	Versions
Genesys	GVP Media Control Platform (MCP)	8.5.120.66
Genesys	GVP Resource Manager	8.5.120.62
Nuance	Recognizer	10.2.6.2014101615 x86_64 - Package revision 14289
Nuance	Vocalizer	6.0.4.2014102404

Combination #2

Vendor	Component	Version(s)
Genesys	GVP Media Control Platform	8.1.700.44
Genesys	GVP Resource Manager	8.1.700.61
Nuance	Recognizer	9.0.14.2010062422
Nuance	Vocalizer	5.0.3.2010071919

Combination #3

Vendor	Component	Version(s)
Genesys	PureConnect	2017 R4

Vendor	Component	Version(s)
Nuance	Recognizer	10.2.6.2014101615 x86_64 - Package revision 14289
Nuance	Vocalizer	6.0.4.2014102404

Combination #4

Vendor	Component	Versions
Genesys	GVP Media Control Platform (MCP)	8.5.120.66
Genesys	GVP Resource Manager	8.5.120.62
Nuance	Recognizer	11.0.3.2019061409 x86_64 - Package revision 19165
Nuance	Vocalizer	7.2.7.4473bbd53a5b

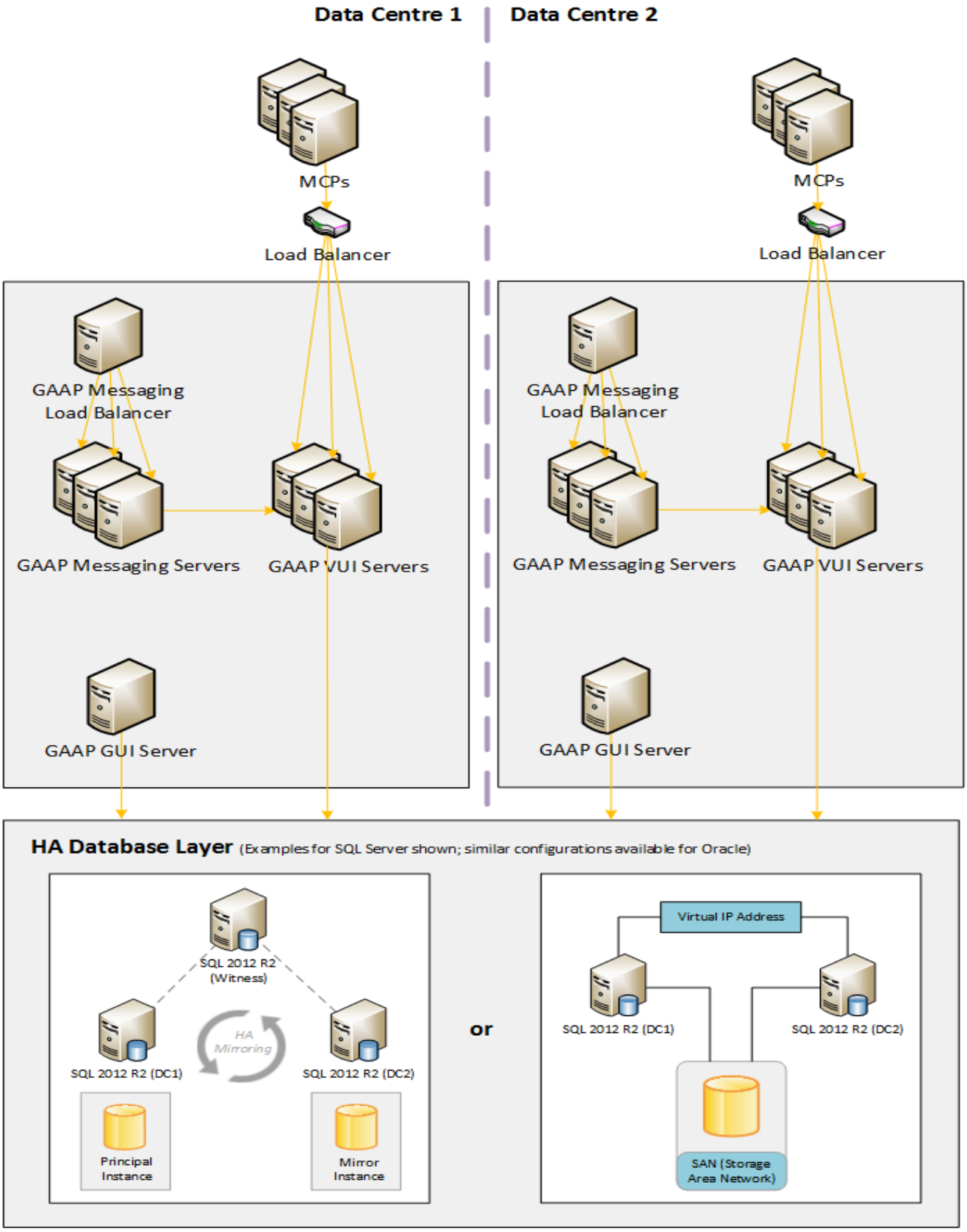
Minimum Supported Standards and Protocols

The Intelligent Automation framework supports industry-defined open standards and protocols. The following standards and protocols are supported.

Standard	Version	Description
Voice Extensible Markup Language (vXML)	2.1	Standard for designing phone-based application dialogs with callers.
Speech Recognition Grammar Specification (SRGS)	1.0	Standard to define syntax for representing grammars for use in speech recognition.
Semantic Interpretation for Speech Recognition (SISR)	1.0	Client-side grammar logic to validate grammars.
HTTP and HTTPS	1.1	Secure management of communication of data between Intelligent Automation and external sources.

Intelligent Automation framework high-availability (HA) architecture

Refer to the following graphic for a deployment example of Intelligent Automation framework and validated Microsoft SQL Server architecture in a high-availability (HA) architecture.


Data Centre 1
Data Centre 2
MCPs
Load Balancer
MCPs
Load Balancer
GAAP Messaging Load Balancer
GAAP Messaging Servers
GAAP VUI Servers
GAAP GUI Server
GAAP Messaging Load Balancer
GAAP Messaging Servers
GAAP VUI Servers
GAAP GUI Server
HA Database Layer (Examples for SQL Server shown; similar configurations available for Oracle)
SQL 2012 R2 (Witness)
SQL 2012 R2 (DC1)
HA Mirroring
SQL 2012 R2 (DC2)
Principal Instance
Mirror Instance
or
Virtual IP Address
SQL 2012 R2 (DC1)
SQL 2012 R2 (DC2)
SAN (Storage Area Network)

Pre-Installation Checklist

This page describes tasks that you must complete before installing Genesys Intelligent Automation. It is recommended you print this page (generate a PDF) and have the installer sign off on each requirement.

> **Important**
>
> Ensure that your environment meets the requirements for Intelligent Automation. See the *SOE requirements for Intelligent Automation* for information.

Note that after you install Intelligent Automation, there is additional configuration that must be done before you can put Intelligent Automation into production.

Installation requirements

On-site installation requirements

Task	Completed and tested by
A dedicated desktop or laptop computer has been made available for the Intelligent Automation consultant to perform the installation. This computer must be able to access all servers required.	

Remote installation requirements

Task	Completed and tested by
Remote access has been set up and tested, and details have been forwarded to the Intelligent Automation consultant.	
The Intelligent Automation consultant has been provided with third-party software (for example, a VPN client) required to connect remotely.	

Solution requirements

This part of the checklist applies to the components and functionalities required to install, configure,

and start the appropriate Solution (GVP or PureConnect) for installing Intelligent Automation.

GVP requirements

Task	Completed and tested by
The GVP, ASR and TTS versions have been made available, as per the Sizing Recommendations and Software Recommendations page.	
If TTS or ASR is required, it has been installed, configured, and fully tested.	
Genesys GVP has been installed and configured, and has successfully handled test calls (including ASR and TTS, if required) to confirm it is fully functional.	
A Genesys resource has been made available to configure GVP to route calls to Intelligent Automation after the installation to complete basic testing. You must enter one of the following start URLs into the routing strategy or IVR profile to configure the mode Genesys Intelligent Automation will use for processing interactions. Example: `http://<host>:<port>/fish-vui/start/GenesysGVP8.jsp?testsiteid=3&istestcall=false` Tip You can view the `siteid` value for an application by going to the Applications view and selecting **Advanced Details** to display the **Site ID** beside each application. • **GenesysGVP8_NoCTI.jsp** — GVP 8 without CTI functionality (ASR or TTS is not available). • **GenesysGVP8_NR11_Vocalizer7.jsp** — GVP 8 with Nuance Recognizer 11 and Vocalizer 7 for ASR and TTS. • **GenesysGVP8_NR10_Vocalizer6.jsp** — GVP 8 with Nuance Recognizer 10 and Vocalizer 6 for ASR and TTS. • **GenesysGVP8_NR9_Vocalizer5.jsp** — GVP 8 with Nuance Recognizer 9 and Vocalizer 5 for ASR and TTS. • **GenesysGVP8.jsp** — GVP 8 only (ASR or TTS is not available). • **GVP8Legacy_Vocalizer5_CTI.jsp** — GVP 8 running in legacy mode with CTI and Vocalizer 5 TTS. • **GVP8Legacy_Vocalizer5.jsp** — GVP 8 running	

Task	Completed and tested by
in legacy mode with Vocalizer 5 TTS. • **Interactive_NR9_Vocalizer5.jsp** — PureConnect with Nuance Recognizer 9 and Vocalizer 5 for ASR and TTS. • **GenesysGVP8_GoogleSR_Vocalizer6.jsp** — GVP 8 and 9 for Speech Transcription. • **Interactive_GoogleSR_Vocalizer5.jsp** — PureConnect 2018R4 - 2019R2 for Speech Transcription. • **GenesysGVP8Plus_GoogleSR_GoogleSS.jsp** — GVP 8+ for Speech Transcription + Google Cloud TTS (**GenesysGVP8_GoogleSR_GoogleSS.jsp** is for backward compatibility). • **GenesysGVP8Plus_GoogleSR_Vocalizer7.jsp** - GVP 8+ for Speech Transcription (**GenesysGVP8_GoogleSR_Vocalizer7.jsp** is for backward compatibility). • **Interactive_GoogleSR_GoogleSS.jsp** — PureConnect 2018R4 - 2019R2 for Speech Transcription + Google Cloud TTS • **Interactive_GoogleSR_Vocalizer5_JSONEncoding.jsp** — PureConnect 2019R3 and above for Speech Transcription • **Interactive_GoogleSR_GoogleSS_JSONEncoding.jsp** — PureConnect 2019R3 and above for Speech Transcription + Google Cloud TTS	
A Genesys resource has been made available to troubleshoot any GVP issues encountered.	
Genesys routing and required attached data (if applicable) has been configured to support the requirements.	
Externally accessible DID test numbers have been configured and made available to allow the Intelligent Automation consultant to dial into the environment.	
If using multimodal functionality, Genesys ORS has been installed and configured.	

PureConnect requirements

Task	Completed and tested by
Genesys PureConnect has been installed and configured, and has successfully handled test calls	

Task	Completed and tested by
to confirm it is fully functional.	
A Genesys resource has been made available to configure PureConnect to route calls to Intelligent Automation after the installation for basic testing to be completed.	
A Genesys resource has been made available to troubleshoot any PureConnect issues encountered.	
Genesys routing and required attached data (if applicable) has been configured to support the requirements.	
An Intelligent Automation consultant has been made available to dial in to the environment.	
The **fetchaudio** setting is not configured by default for PureConnect and it should be configured before using Intelligent Automation. Important To configure the setting in Intelligent Automation, add a new setting, **Resources.PlatformFetchAudioURL** (under *Administration > Default Server Settings*) and set a valid URL for the audio file as its value. PureConnect does not have a default value for **fetchaudio**. You must configure the value in PureConnect instead of Intelligent Automation as the IA setting applies to all organisations in that environment whereas PureConnect is a single-tenant environment.	

Database Requirements

Complete the checklists corresponding to the DBMS you are using in your Intelligent Automation database layer.

General Database Requirements

This section of the checklist must be completed regardless of the particular databases that you will use in your Intelligent Automation installation. For requirements specific to each type of database, refer to the following:

- SQL Server—Microsoft SQL Server requirements
- Oracle—Oracle requirements

Task	Completed and tested by
Two databases (**fish** and **fish_reports**, for example) have been created and initialized using the steps provided in Set up databases.	

Microsoft SQL Server requirements

This section of the checklist is required only if you want to use Microsoft SQL Server for one or both databases.

Task	Completed and tested by
A Microsoft SQL Server R2 database environment is ready and has been tested for the Intelligent Automation consultant to access and install Intelligent Automation.	
Microsoft SQL Server has been configured and tested to allow TCP/IP connections and to allow non-Windows users (**SQL Server authentication**).	
Microsoft SQL Server Management Studio has been installed on at least one Intelligent Automation server per environment (for example, one for the test environment and one for the production environment).	
An SQL Server authenticated user account has been created, and this account also has ownership of the SQL Server databases. You can confirm these settings by connecting to the database using SQL Server Management Studio. In the left panel, navigate to **Security** > **Logins**. Right-click the appropriate user and select **Properties** > **User Mapping**. Ensure `db_owner` is enabled for both databases.	
To accommodate future migration of the reports schema, Genesys recommends that the transaction log file(s) are configured to be at least as big as the data file(s), and that both are set to automatically grow as needed. The size of these files should be monitored periodically and regular backups scheduled to better manage the transaction logs.	

Oracle requirements

This section of the checklist is only required if you want to use Oracle for one or both databases.

Task	Completed and tested by
The Oracle database environment is ready and has been tested for the Intelligent Automation consultant to access and install Intelligent Automation.	
Oracle SQL Developer has been installed on at least one Intelligent Automation server per environment (for example, one for the test environment and one for the production environment).	
A SYS user has executed the following command in Oracle: `ALTER SYSTEM SET open_cursors = 600 scope=both;`	

Server requirements

Task	Completed and tested by
The servers have been built as per the Hardware and Software Specifications page.	
All server details—such as hostnames and IP addresses for all relevant servers, including GVP, Intelligent Automation, and the database environment—have been provided to the Intelligent Automation consultant.	
Login information has been provided to the Intelligent Automation consultant for all relevant computers and servers, including Active Directory (if used) and database servers.	
Administrative privileges on the Intelligent Automation servers have been configured to allow the Intelligent Automation consultant to install, test, and troubleshoot.	

Project-specific requirements

Task	Completed and tested by
Test data for the Intelligent Automation consultant to test the IVR application after installation has been provided, including (if applicable) valid card payment details for testing of the payment gateway and all other web services.	
All third-party components required as part of the solution have been installed, configured, tested, and available to integrate before the installation of Intelligent Automation.	
Custom grammars, if used in the deployment, are available and recompiled as needed by the ASR/TTS engine.	
If using multimodal communication, Orchestration Server 8.1.4 or higher is installed.	

Firewall requirements

The main firewall rules that are required for Intelligent Automation to function are defined and set up, as given in the following table. Some customers might have additional requirements. In addition:

- The port numbers referenced in the table below reflect common configuration as documented elsewhere in this guide. You must update these port numbers if your environment uses non-default port numbers.
- This table does not include standard firewall requests for scenarios such as remote desktop; it is assumed that the customer has already enabled these rules.

Rule	Ports	Completed and Tested by
Communication from the customer site to the Intelligent Automation FTP server for downloading installation files. Server details are: • Host Name: **ftp.speechstorm.com** • Port Number: **22** • File Protocol: **Secure FTP (SFTP)** • Username: *Will be supplied by Genesys* • Password: *Will be supplied by Genesys* **Important** Access to the FTP site does not need to originate from the Intelligent Automation servers, but you must have a method of transferring files from the FTP site onto the Intelligent Automation servers.	22 for Secure FTP (SFTP)	
Inter-Communication between all Intelligent Automation servers	• 80, 8080–8089 for HTTP traffic • 443, 8443-8449 for HTTPS traffic	
Communication between Genesys environment and all Intelligent Automation VUI servers	• 80, 8080–8089 for HTTP traffic • 443, 8443-8449 for HTTPS traffic	
Communication between ASR and TTS environment and Intelligent Automation servers	• 80, 8080–8089 for HTTP traffic • 443, 8443-8449 for HTTPS traffic	
Communication between database environment and Intelligent Automation servers	The SQL Server Port: Usually 1433, but to be confirmed by the customer.	

Rule	Ports	Completed and Tested by
Communication between all Intelligent Automation servers and customer integration/ backend systems	Ports to be confirmed by the customer.	
Communication between all Intelligent Automation servers and customer SMTP server (see Configuring Genesys Intelligent Automation for more details).	Ports to be confirmed by the customer.	
Communication between all Intelligent Automation servers and customer SNMP Manager (see Configuring Genesys Intelligent Automation for more details). Important This is optional and only required if you want to use the trap-sending functionality provided by Intelligent Automation.	Ports to be confirmed by the customer.	
Communication between all Intelligent Automation servers and customer SYSLOG/ Centralized Logging server (see Configuring Genesys Intelligent Automation for more details). Important This is optional and only required if you want to use the SYSLOG functionality provided by the Log4j component within Intelligent Automation.	Ports to be confirmed by the customer.	

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**. Important 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. 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`. 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`. 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`. 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`. 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: • **<PlatformPath>\TomcatVUI\lib** • **<PlatformPath>\TomcatGUI\lib** • **<PlatformPath>\TomcatMessaging\lib** • **<PlatformPath>\TomcatIntegration\lib** 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. Tip You can encrypt the password now, or at any time in the future, as described in Encrypting the Database Password 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. 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. 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. Things to consider: • The amount of memory must be tuned depending on the actual environment. 5GB of memory is a good starting point for 100,000 Things. • 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).

Natural Language AI Integration

Intelligent Automation can integrate with external artificial intelligence (AI) services to provide natural language understanding (NLU) capabilities.

For more information and instructions, refer to the Natural Language AI Integration page in the *Intelligent Automation Help* manual.

VoiceBots

VoiceBots (previously known as Cognitive IVR) uses Google Cloud Speech-to-Text to improve the performance of natural-language interfaces such as Dialog Engine. This makes it easier for callers to use spoken natural-language phrases to navigate through an Genesys Intelligent Automation application.

> **Warning**
> Please note that the customer is responsible for ensuring that the environment and bot applications they build are properly configured and secured according to PII and HIPAA requirements.

For example, a traditional IVR might have trouble interpreting the following phrase: "I would like to book a flight to Paris on Friday afternoon." Instead, the traditional IVR would need to ask several sequential questions to deduce the following information:

- What do you want to do? (Book a flight)
- Where do you want to travel? (Paris)
- When do you want to travel? (Friday afternoon)

However, VoiceBots can interpret and parse natural language so the customer can make the same one-sentence request without having to sequentially answer several questions: "I would like to **book a flight** to **Paris** on **Friday afternoon**."

Other than a new login screen, using VoiceBots does not affect how you use Genesys Intelligent Automation. You can build and use applications in the same way (but note the limitations below) and share the same database.

Integrate Intelligent Automation with Google Speech-to-Text

When setting up Intelligent Automation for use with voice, a start page is required.

Speech-to-Text Engine	Text-to-Speech Engine	Product	Version	Start Page
Google Cloud for Speech Recognition	Nuance	Genesys Voice Platform	8 and 9	GenesysGVP8_GoogleSR_Vocalize
		PureConnect	2018R4 - 2019R2	Interactive_GoogleSR_Vocalizer5.j
		PureConnect	2019R3 and above	Interactive_GoogleSR_Vocalizer5_

Speech-to-Text Engine	Text-to-Speech Engine	Product	Version	Start Page
	Google	Genesys Voice Platform	8 and 9	GenesysGVP8_GoogleSR_GoogleS
		PureConnect	2018R4 - 2019R2	Interactive_GoogleSR_GoogleSS.js
		PureConnect	2019R3 and above	Interactive_GoogleSR_GoogleSS_J

The start page should contain the following parameters:

- `testsiteid` - The ID of the application being provisioned.
- `istestcall` - When set to *True*, the provisioning uses the test mode (the latest saved version) or the production mode (the latest deployed version) when set to *False*.
- `authtoken` - This will be available from the **Company Details** page.
- `mrcpversion` - This is an optional parameter. The default value is *1*.

An example start page that uses GVP: *http://<server>:<port>/fish-vui/start/GenesysGVP8_GoogleSR_Vocalizer6.jsp?testsiteid=53&istestcall=true&authtoken=303a935e028b1aae234476fed4*

The RTP is streamed to Google STT and the resulting transcription is sent to Dialog Engine or DialogFlow for processing.

Limitations

The following limitations apply to the use of VoiceBots:

- Multimodal communication is not supported.
- The **Release ASR** API command for the Script block does not have any effect when using VoiceBots.
- WebIVR applications are not supported.
- For a given persona, the TTS language is also used for the speech-recognition language.

Prerequisites

To use VoiceBots with Genesys Intelligent Automation, the following prerequisites are needed.

Genesys Engage

- Genesys Voice Platform 9.0.019.68 or higher
- Intelligent Automation v9.0.100 or higher

PureConnect

> **Important**
> From PureConnect 2019R3 onwards, Intelligent Automation v9.0.106 or higher is required.

- PureConnect 2018R4 or higher
- UniMRCP 1.5.0 or higher
- Google Speech Recognition plugin for UniMRCP
- Intelligent Automation v9.0.105 or higher

Configuring Genesys Intelligent Automation

After installing Genesys Intelligent Automation, you must configure it as described in this section.

It is recommended you print this page (generate a PDF) and sign off on each step.

CTI Data

Intelligent Automation has the capability to store some attached-data variables in its reporting database (usually used for custom reports). As the space is limited, Intelligent Automation can configure regular-expression patterns to exclude or include data. By default, the patterns are empty, which means all attached data will be saved. If the data to be saved is bigger than the space available in the database, the data is truncated (in no particular order).

Setting Name	Description	Default Value	Your Value
CLIData.Mobiles.Prefix	A value indicating the prefix of a mobile number.	`07`	
VuiPreferences.Defaults.store_cti_fields_in_reporting_data	A Boolean value to indicate if Intelligent Automation is to store CTI fields in reporting data.	`true`	
CTI.FieldsToStoreInReporting.ExcludePattern	Exclusion pattern. The default value is blank, but you can set a new value that suits your business needs (for example, **^ROUTING.*$**).	None	
CTI.FieldsToStoreInReporting.IncludePattern	Inclusion pattern. The default value is blank, but you can set a new value that suits your business needs (for example, **^(AccountNumber|CustomerID)$**).	None	

Database Overnight Jobs

To increase database performance, Intelligent Automation performs an overnight (or quiet period) job that consists of the following main tasks:

- Archiving old report data into historical tables. These historical tables are still referenced in reports and database views.
- Delete historical data that is older than the specified number of days.

> **Important**
>
> A large value would affect the performance of the reports that use the data.

Setting Name	Description	Default Value	Your Value
DBOvernightJobs.NumDaysHistoricalDataToKeep	The number of days of historical data to keep. If set to **-1**, no data is deleted.	-1	

Email

Intelligent Automation must be able to send emails via an SMTP server (for example, to send password-reset emails).

Setting Name	Description	Default Value	Your Value
Email.SMTP.Host	The SMTP host that Intelligent Automation will use to send emails (for example, password-reset emails).	`mail.speechstorm.com`	
Email.SMTP.Port	The SMTP port of the host.	25	

GraphViz

You must update the default server setting that points to the location of GraphViz, which renders the callflow diagrams.

Setting Name	Description	Default Value	Your Value
GraphViz.DotPath	Path to GraphViz executable.	C:/Program Files/Graphviz2.26/bin/dot.exe	

SMS

You must configure the SMS gateway to use outbound SMS. The example below is for the Genesys Portico SMS Gateway:

Setting Name	Description	Default Value	Your Value
SMS.Carrier	The Carrier ID as allocated by the SMS gateway provider.	None	
SMS.DefaultFromNumber	The number that appears as the sender on the recipient's phone. This number often requires authorization by the SMS gateway.	None	
SMS.Host	Hostname of the SMS gateway.	None	
SMS.Method	HTTP method for calling the SMS Gateway (for example, POST).	None	
SMS.PlusSymbolBeforeRecipientNumber	Specifies whether to prefix an international + symbol to the recipient number.	None	
SMS.Port	Port of the SMS gateway.	None	
SMS.RequestBody	Body of the HTTP request (if required).	None	
SMS.RequestHeaders	Headers of the HTTP request (if required).	None	
SMS.Timeout	Time, in milliseconds, to wait for a response from the SMS gateway.	None	
SMS.URL	URL to the SMS gateway interface.	None	
SMS.User	Username of the SMS gateway account.	None	
SMS.Password	Password of the SMS gateway account.	None	

SNMP Traps

Intelligent Automation can generate SNMP traps. The configurations below are required if you intend to use SNMP traps; otherwise, continue to the next section.

Setting Name	Description	Default Value	Your Value
SNMP.Traps.Enabled	A Boolean value to indicate if Intelligent Automation is to store CTI fields in reporting data.	`false`	
SNMP.Traps.ManagerHostname	The name of the SNMP manager.	`localhost`	
SNMP.Traps.ManagerPort	The SNMP manager port.	`162`	
SNMP.Traps.Community	The community name for SNMP traps. This setting is usually unchanged.	`public`	
SNMP.Traps.ServerHeartbeat.Enabled	A Boolean value to indicate if each Intelligent Automation server is to send heartbeat traps. Important The **SNMP.Traps.Enabled** setting must be set to **true** to use heartbeat traps.	`true`	
SNMP.Traps.ServerHeartbeat.FrequencySeconds	The frequency, in seconds, for when each Intelligent Automation server will send heartbeat traps.	`60`	

SYSLOG

Intelligent Automation uses the log4j logging mechanism, which can send logs to a centralized logging server. You must complete this configuration if you wish to use this feature.

Setting Name	Description	Default Value	Your Value
log4j.appender.SYSLOG.syslogHost	Set within the log4j.properties file on each Intelligent Automation instance. This value defines the hostname/IP address of the syslog server.	None	

User Logins

These settings define criteria for a successful login using an authorized password and a valid password.

Setting Name	Description	Default Value	Your Value
Login.ExternalAuthentication.Mode	Defines if external users (those configured and maintained by Genesys Administrator Extension) can log into Intelligent Automation. If required, set this to `ConfigServer`.	None	
Login.Failure.LockoutDelayInSecs	Defines (in seconds) the length of time following a login failure before a user is locked out, preventing further login attempts.	1800	
Login.Failure.Threshold	Defines the number of times a user can attempt to log in to an account unsuccessfully.	5	
Login.Password.ExpiryDays	Defines the number of days before a new password can expire.	90	
Login.Password.ShowForgottenPasswordLink	Specifies whether the **Forgot your password** link appears on the **Log in** page.	true	
Login.SessionTimeoutInSecs	Defines the time limit (in seconds) that a logged-in session can last without user activity.	900000	

WebIVR

For security purposes, WebIVR uses a default server setting to dictate from where it can be embedded. To launch WebIVR from the GUI for testing, or to use the Theme Preview function, you must add the GUI server(s) to the list of allowed domains.

Setting Name	Description	Default Value	Your Value
VisualIVR.Security.AllowedDomains	Hostname and port of the GUI server(s) from which WebIVR can be launched or embedded. For example: *http://FQDN:PORT*.	`http://localhost:8080`	

Supported Languages

This page lists all languages supported by the channels and sections of Genesys Intelligent Automation.

The provided language codes (for example, *en-gb*) refer to the language codes used in the Nuance platform.

Voice channel

Section	Supported language(s)
User interface	• UK English (en-gb) • French (fr-fr) • German (de-de) • Mexican Spanish (es-mx)
Dynamic prompts	• UK English (en-gb) • US English (en-us) • Arabic (ar-ww) • Czech (cs-cz) • German (de-de) • Spanish (es-es) • Mexican Spanish (es-mx) • French (fr-fr) • Hindi (hi-in) • Hungarian (hu-hu) • Italian (it-it) • Japanese (ja-jp) • Malayalam (ml-in) • Dutch (nl-nl) • Polish (pl-pl) • Portuguese (pt-pt) • Russian (ru-ru) • Thai (th-th)

Section	Supported language(s)
	• Chinese Cantonese (zh-hk) • Chinese Mandarin (zh-ma)
Non-dynamic prompts	• Pre-recorded prompts: Supports all languages. • TTS prompts: Supports all languages that are supported by Nuance.
Input	• Speech recognition for menu options, Grammar Builder and custom grammars: Supports all languages that are supported by Nuance. • Standard grammars: Supports English (en-gb), Spanish (es-es), and French (fr-fr) when voice call is in Nuance (Swimcontroller). Google supports all languages.

Digital channels

Section	Supported language(s)
User interface	• UK English (en-gb) • French (fr-fr) • German (de-de) • Mexican Spanish (es-mx)
Dynamic and non-dynamic prompts	Wording for prompts and screens: Supports all languages.
Input	• Input for menu options, Grammar Builder and custom grammars: Supports all languages. • Standard grammars: Tested to support English (en-gb), Spanish (es-es), and French (fr-fr). Standard grammars for other languages have not been tested by Genesys but might offer some degree of functionality.

Document Change History

This page summarizes the changes made in this document for release 9.0.0.

Changes in release 9.0.004.01

- Applied standard template to the introduction page, and moved information to the new Overview page.
- Moved Architecture information to its own page.
- Added User Login configuration settings to Configuring Genesys Intelligent Automation page.

Changes in release 9.0.003.00

- No changes to this document were made in release 9.0.003.00.

Changes in release 9.0.002.00

- GDPR compliance was added to the Overview page.

Changes in release 9.0.001.01

- Integration with PureConnect has been added to the introduction page, and to the installation procedures.

Changes in release 9.0.000.01

- Genesys App Automation Platform has been renamed Genesys Intelligent Automation. Note that some folder and path names still include GAAP and/or SpeechStorm, but these too will be rebranded as the product evolves.
- A new page Integrating Dialog Engine briefly describes Genesys Dialog Engine, and how to configure Intelligent Automation to work with it.
- Information about the new open-source databases, PostgreSQL and Elasticsearch, has been added to the Software Prerequisites, Pre-Installation Checklist, and Installing Intelligent Automation pages.
- This page, and the Supported Languages page that describes the languages supported by Intelligent Automation, have been added.
- The Existing Installation page has been moved from this guide to the Intelligent Automation Migration Guide.
- Some pages have been updated with more accurate titles to better reflect their content.