Predictive Routing in Hybrid Architecture

Blueprint

Version 1.4

GENESYS
moments connected

Name	Modification	Date
Gordon Bell	Initial release v1.0	5/3/2018
Philippe Rais	Updates for hybrid architecture v1.4	5/2/2019

Table of contents

1 Introduction

The purpose of the Predictive Routing solution Blueprint document is to provide a set of design practices and guidance to ensure consistent architecture approaches are used for all deployments of the Predictive Routing in hybrid architecture. It provides a prescriptive list of components that should be included in the solution. It also provides deployment guidance, including sizing considerations, and addresses several system concerns such as security, data privacy, high availability, disaster recovery and serviceability.

The Genesys Predictive Routing solution consists of the following core Genesys components:

- AI Core Services (deployed in Genesys cloud)
- Agent State Connector
- Orchestration and/or URS components
- Data pipeline
    - Not a Genesys component per-say, but a set of customized scripts invoking Genesys Predictive Routing API.

The solution provides predictive routing for voice channel only (Digital channels are subject to Product Management approval (Early Adopter support)).

Voice related components are implicitly part of the solution:

- Pure Engage Premise platform with prerequisites.

1.1 Intended Audience

The Blueprint Architectures are intended to provide Genesys Solution Consultants, Professional Services and partners with information on the general architecture design and considerations for the solution. The information provided in this document should meet the needs of pre-sales and provide appropriate general guidance for professional services. This document is not intended to provide configuration level information for professional services.

Describing system and solution architectures can be difficult as there are multiple audiences each with different expectations. This document is intended for multiple audiences with various chapters being more interesting to some readers than others. It is expected that readers will already have knowledge and training on Genesys products. This document provides high-level information for completeness.

The Overall Architecture and Deployment View are likely meaningful to most audiences. However, the Interaction View and the Implementation View may be of more interest to those configuring the network and components.

1.2 Acronyms

The following table defines terms that will be referenced subsequently in this document.

Acronym	Meaning
AI	Artificial Intelligence
AICS	AI Core Services
API	Application Programming Interface
ASC	Agent State Connector
AWS	Amazon Web Services
BI	Business Intelligence
CPU	Central Processing Unit
DMZ	Demilitarized Zone
DPA	Data Privacy Addendum
FedRAMP	Federal Risk and Authorization Management Program
GCXI	*Genesys Customer Experience Insights*
GDPR	General Data Protection Regulation
GII or GI2	*Genesys Interactive Insights*
GIM	*Genesys Info Mart*
GPR	*Genesys Predictive Routing*
GVP	*Genesys Voice Platform*
GWS	*Genesys Web Services*

Acronym	Meaning
HA	High Availability
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
IRD	Interaction Routing Designer
ISO	International Organization for Standardization
KPI	Key Performance Indicator
MSLSA	Master Software Licensing and Services Agreement
ORS	Orchestration Server
PII	Personally Identifiable Information
PSI-DSS	Payment Card Industry Data Security Standard
RAA	Reporting and Analytics Aggregates
RTT	Round-Trip Time
SOC	System and Organization Controls
TLS	Transport Layer Security
URS	Universal Routing Server

2 Overall Architecture

Predictive Routing solution draws on accumulated agent and interaction data to analyse and generate models to predict outcomes that can then be used to provide the best possible match between interactions and agents.

2.1 Solution Overview

The Omni-channel Predictive Routing solution builds on top of the URS and Framework components. The solution enhances Genesys Routing with Machine Learning to predict the best match for the incoming interaction.

This solution can be used with both voice channel only (digital channels subject to PM approval).

In addition, standard reports and dashboards are provided. These make use of the Reporting Common Components (GII, GCXI and Pulse).

2.2 Logical Architecture Model

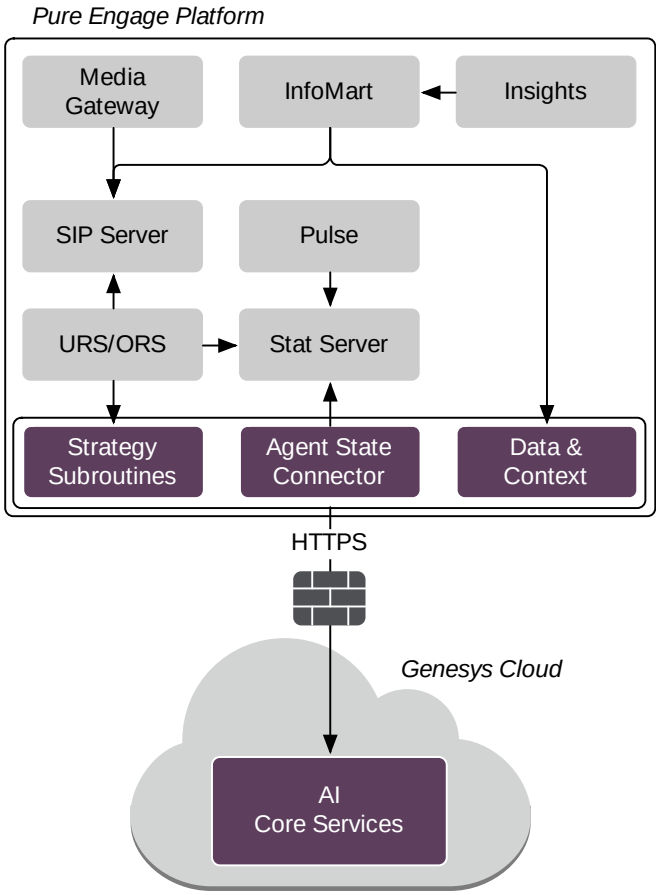

Figure 1 - Logical Architecture Model

The solution is based on standard voice deployment. It adds the following:

- AI Core Services component that hosts the Predictive Routing application and training modules
  - AICS components are deployed in Genesys cloud
- Agent State Connector to synchronize state with Stat Server
- Predictive Routing strategies for URS/Orchestration

The solution integrates with Routing and Reporting.

2.3 Components View

The following components make up the overall Predictive Routing solution.

Component	Description
AI Core Services	Core components of the Predictive Routing solution. It handles all analytics and administrative services. Provides a REST-API for flexible integration and serving end user web applications for model development, data analysis, and reporting.
Agent State Connector	Bridge between Pure Engage and Predictive Routing. It connects to Configuration Server and Stat Server to obtain real-time updates on agents, agent groups and interactions info.
Common Components	Refer to the Common Component blueprint for information on Management Framework, Orchestration/Routing and Reporting components used by this solution. A set of routing subroutines is provided for Predictive Routing usage: • Either for IRD + URS • Or for Composer + ORS + URS
SIP Voice	Refer to the SIP Voice Solution blueprint for details on configuring SIP VoIP infrastructure that predictive routing can be applied to.

SIP Voice is included in the overall solution as a channel that Predictive Routing can use to target the best agent.

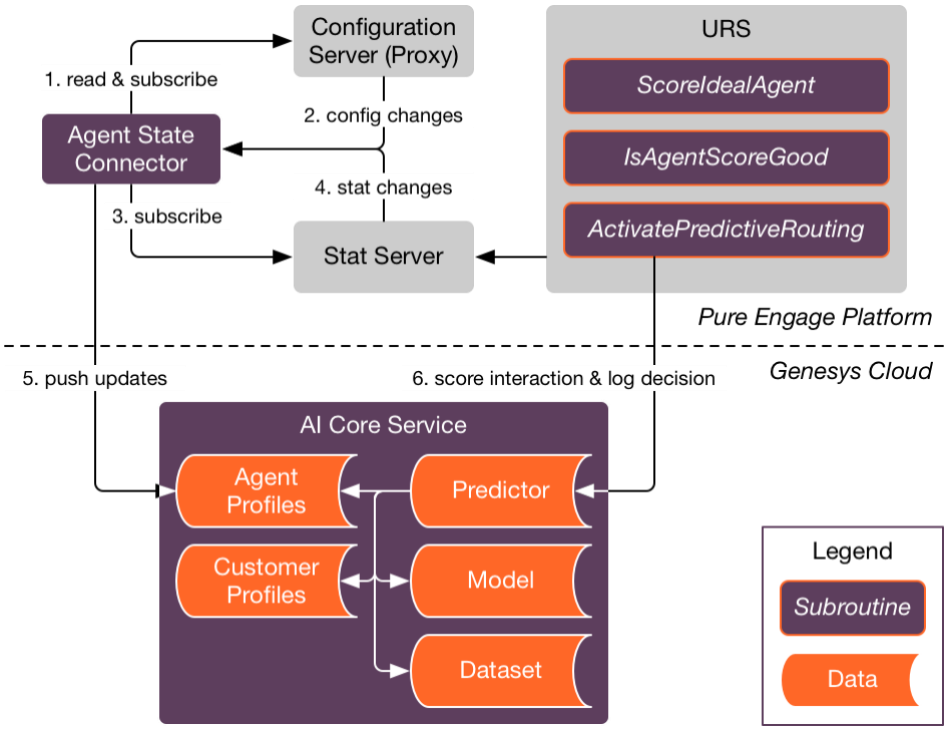

Figure 2 - Logical Runtime Architecture

The logical runtime architecture diagram depicts how the various components function within the solution.

- Agent State Connector reads configuration information from Configuration Server at startup
- Agent State Connector monitors and handles any agent config changes
- Agent State Connector also subscribes to Stat Server and handles any agent state change
- Updates on the agent and configuration changes are pushed to the AI Core Services' Agent Profile module
- Once the *ActivatePredictiveRouting* subroutine in URS is called, it will score the interaction based on outcome and log any predictive decision made using the Predictor module within the AI Core Services.

2.4 Limits and Constraints

For a complete list of known limitation please see GPR Deployment and Operations Guide.

3 Deployment

3.1 High Level Architecture

Predictive Routing deployment is split between Pure Engage Premise and Genesys cloud. Only component (beside the ones required by either SIP Voice solution) to be deployed on premise is Agent State Connector.

Following view summarizes GPR components deployed in premise environment and their connection with AI Core Services deployed in cloud.

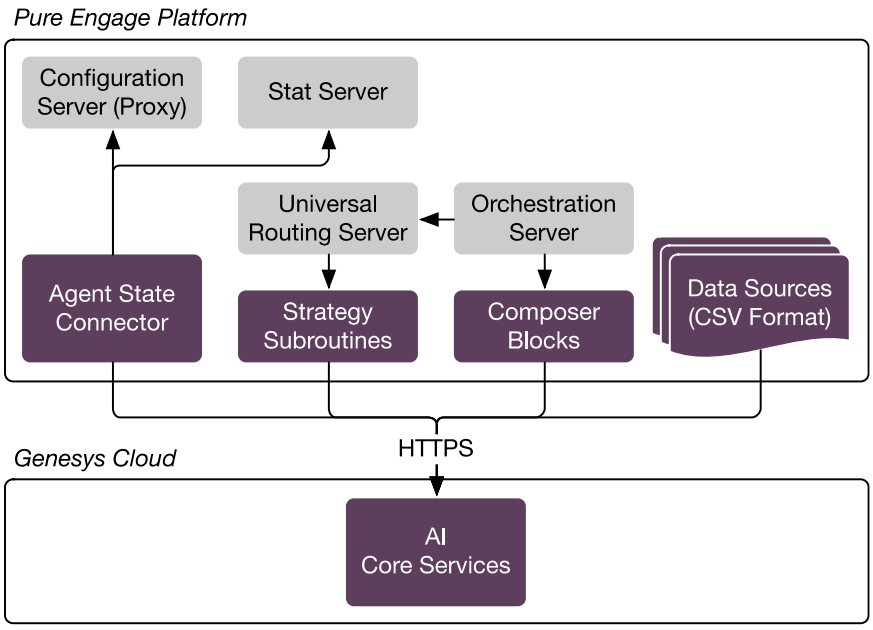

Figure 3 - Deployment View

3.2 Availability

GPR service for Pure Engage Premise customers is available in the following countries and Amazon Web Services regions across the globe.

Region	Country	AWS Region Name	Region
NA	USA	US East (N. Virginia)	us-east-1
NA	Canada	Canada (Central)	ca-central-1

Region	Country	AWS Region Name	Region
EMEA	EMEA countries except Germany	EU (Ireland)	eu-west-1
EMEA	Germany	EU (Frankfurt)	eu-central-1
APAC	APAC except China and Japan	Asia Pacific (Sydney)	ap-southeast-2

Planned in 19H2:

Region	Country	AWS Region Name	Region
NA	USA	US West (Oregon)	us-west-2
APAC	Japan	Asia Pacific (Tokyo)	ap-northeast-1

3.2.1 Availability Zones

Predictive Routing components in Genesys cloud are deployed in multiple availability zones for each AWS region.

Each AWS region has multiple, isolated physical locations known as availability zones. By using different availability zones in a region, Genesys provides a form of regional geo-redundancy capabilities for the Predictive Routing solution.

3.2.2 Geo-Redundancy

Predictive Routing cloud services do not provide geo-redundancy capability.

It is designed as a single region service with no support for disaster recovery.

3.2.3 High Availability

Predictive Routing components in Genesys cloud are fully redundant and provide a high availability service. Furthermore, the cloud components can auto-scale based on demand.

On the customer Pure Engage premise side, Agent State Connector is deployed in HA mode (warm standby). For more details, refer to HA for ASC section in GPR documentation.

4 Interaction View

4.1 API

Predictive Routing uses a set of API requests to communicate with AI Core Services.

Each request must be authenticated (see Authentication). This is performed by providing a verified token in each request.

Token is generated in Genesys cloud and provided as a successful response to an authentication request.

Authentication request (/api/v2.0/authenticate) must provide a username, password and an API key associated to the user. End user must be in possession of those 3 parameters in order to be able to use Predictive Routing API.

Complete API definition is available on the Genesys Predictive Routing API developer web page.

4.2 Data Extraction

Several custom scripts and other tools are required to extract data from GIM on Pure Engage platform. This data is manually uploaded to Genesys cloud. Therefore, it is highly recommended that Genesys Professional Services be involved in setting up the scripts for data extraction and upload to AICS in Genesys cloud.

See Security & Privacy section for more information related to data.

In the future, data extraction steps are likely to become part of the GPR product offering.

4.3 Predictive Analytics

GPR provides 5 different types of reports within the application interface:

1. Lift Estimation
    - Generates an estimate of the potential improvement in customer KPI for the given model.
2. Feature Analysis
    - Identifies which factors most strongly affect the outcome KPI thereby enabling the customer to create better predictors and models.
3. Agent Variance

- This report can be used as an indicator as to the general scope of opportunity to improve on the outcome.

4. Model Quality
    - Gives a statistical measure indicating the quality of the model.
5. Agent Coverage
    - Various methods for evaluating the model.

GPR provides various types of information on routing outcomes for use in BI applications such as GI2 and GCXI.

Details on how to Integrate with Genesys Reporting are available in GPR Deployment and Operations Guide.

5 Implementation View

5.1 Supported Environment

Software and hardware requirements for components installed in Pure Engage premise platform are:

Component	Software	Hardware
Agent State Connector	Linux 7.1 or higher Windows Server 2016 Java JDK 1.9	Min 16GB memory Min 2 cores Min 500GB disk storage
Subroutines	URS 8.1.400.57 (*) or higher ORS 8.1.400.26 (*) or higher GIM 8.5.009.12 (*) or higher RAA 8.5.002 (*) or higher GII 8.5.001 (*) or higher StatServer 8.5.108.17 (*) or higher Composer 8.1.400.36 (*) or higher	Additional CPU and memory load are expected on URS based on the call volume and scoring request volume. Consult sizing guide for environment specific calculation.

**: Genesys software versions are valid at the time of blueprint publication. Refer to GPR Interoperability Guide for up-to-date versions.*

Genesys Predictive Routing solution does not require dedicated instances of URS and StatServer.

5.2 Network

Recommended latency between Pure Engage premise and Genesys cloud is recommended not to exceed 60 milliseconds. Simple "ping" command to one of the AWS Endpoints in the selected region provides good latency estimate.

Scoring requires a maximum RTT of 500 milliseconds. Scoring RTT is highly impacted by:

- Number of agent features within the predictor

- Number of agents in the target pool

Recommendation is to perform a Feature Analysis report in order to identify the most influential agent features. Although there is no restriction on the number of agent features used to create the model, it is advised to keep those under "reasonable" value. Genesys recommends focusing on up to 25 agent features.

It is also recommended to keep the target agent pool under 1,000 agents.

5.3 Limitations

Following limitations are not strictly enforced but are rather suggested to keep solution running efficiently:

- Not more than 200 columns and 2 million rows per dataset.
  - If available data exceeds those values, only use a data subset.
- Not more than 10 predictors running at the same time.
- Target agent pool shall not exceed 3,000 agents.
- Total number of provisioned agents shall be less than 30,000.

5.4 Security & Privacy

5.4.1 Firewall

Predictive Routing service in Genesys cloud uses standard HTTPS connections for data transfer. Communication between premise components and AI Core Services is established using TLS 1.2 on port 443.

Agent State Connector and URS must have internet access to port 443 toward Genesys cloud. Genesys does not have specific recommendations on how to provide internet access for those 2 components.

Besides that, there are no additional firewall ports or DMZ rules to be enabled on the firewall within customer premise or data center.

5.4.2 Secure Connections

On Pure Engage premise platform, local connections from Agent State Connector to Configuration Server and Stat Server support TLS 1.2. Check Genesys Security Deployment Guide on how to configure secure connection between Genesys components.

5.4.3 Authentication

Customer account, username and passwords are generated in Genesys cloud platform. An API key is also provided within this interface. There is no authentication mechanism or integration with a local premise user management system.

5.4.4 Anonymization

Genesys Predictive Routing solution does not require any PII in order to create models for its analysis. Some required identifiers which are considered PII (i.e. customer phone number) can be mapped to non-PII identifiers. Sensitive information can therefore be removed before being transmitted to Genesys cloud.

Genesys does not provide scripts or components that would perform data transformation in order to remove, hide or transform PII from data transmitted to AI Core Services.

Signature of a standard DPA for all Value Studies or Value Realization is required. It shall detail Genesys' obligations and responsibilities. This is part of standard MSLSA for Genesys Predictive Routing (in hybrid mode).

It means that:

- Genesys shares the technical and organizational security controls in place.
- Any transfers of data to other countries or regions is done in a secure way. For GDPR compliance, Genesys relies on Privacy Shield certification to send data to the United States and standard contractual clauses to send data to Genesys offices in other regions.
- Genesys offers full control to the customer on the data lifecycle management. The customer can destroy any loaded data at any time, and Genesys will not retain any copy.

For DPA approval process, contact Product Management.

If customer policy is to restrict PII sharing in a way that is incompatible with providing unmodified data to Genesys cloud, then anonymization process shall take place. As mentioned above, this process is not part of Predictive Routing solution.
Customer is responsible to validate that anonymized data is exempt of undesirable PII. Genesys can provide support with tools, process and legal assistance (contact Product Management for additional information).

To get assistance on other data privacy questions, contact InternalDataPrivacy@genesys.com.

5.5 Data Retention

In order to delete data that has been uploaded to the cloud, customer has to issue the purge command (either through the UI or by calling corresponding API request).

Otherwise, data is retained for 90 days (by default) before being deleted by AICS platform.

At the end of customer contract, a grace period of 30 days is started, after which all customer data is deleted.

5.6 Certifications

Genesys cloud supports the following certifications:

- SOC-II
- ISO 27001
- PCI-DSS
- HIPAA
- GDPR
- FedRAMP (Planned in 2019)

The certification of an end-to-end architecture remains customer's responsibility.

Contact SecurityNASME@genesys.com for any questions related to these certifications