This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Predictive Routing Deployment and Operations Guide

Architecture and security

7/27/2024

Contents

- 1 GPR architecture
- 2 Data Loader architecture
- 3 Subroutines architecture
- 4 Security
  - 4.1 Secure connections
  - 4.2 Secure data
- 5 Architecture and security FAQs

This topic presents Genesys Predictive Routing (GPR) architecture, first at a high-level overview, followed by more detailed views of the connections used by Data Loader and the URS Strategy Subroutines with the GPR Platform, which is deployed in the Genesys Multicloud CX.

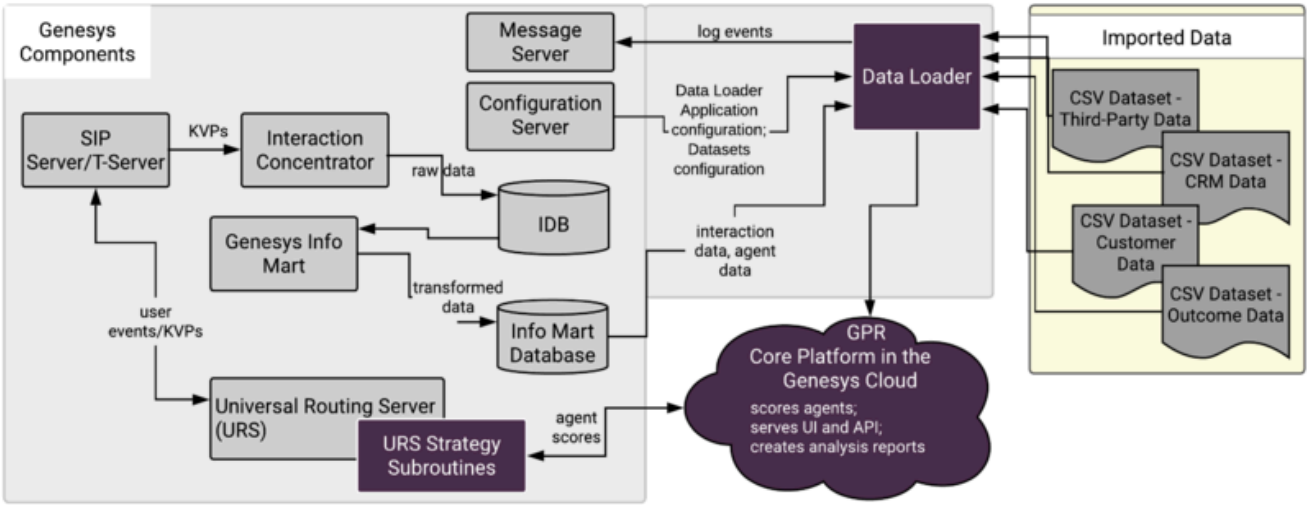
Related documentation:

-

GPR architecture

The following diagram shows a high-level view GPR, how it connects with other Genesys components, and how data enters GPR.

> **Important**
> GPR architecture in a high availability (HA) environment is similar to that presented in the diagram except that for HA Data Loader is deployed in a warm-standby primary-backup architecture.



Data Loader architecture

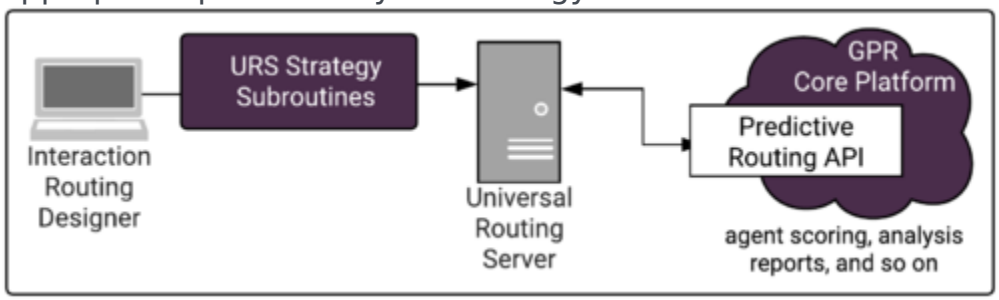
Data Loader is a Java application deployed in a Docker container that you can start, stop, and monitor in Solution Control Interface or Genesys Administrator Extension (GAX). It requires that you deploy

the AI Data Loader Scripts component as well. Data Loader has the following major functionality:

- Connects to the Genesys Info Mart Database for agent-related data, which is uploaded and stored in the Agent Profile. This data includes agent details, such as a location, languages, skills and skill levels, and so on. To configure the schema for this agent data, and to control when Data Loader refreshes data, you must use configuration options in the **[dataset-agent-gim]** section of the Data Loader Application object.
- Connects to Configuration Server to read configuration information for datasets and the Agent and Customer Profiles, as well as other values provided in configuration options, such as the URL to connect to the GPR Core Platform.
  - Data Loader requires a connection to Configuration Server. It does not support connections to Configuration Server Proxy.
- Automatically extracts data from the Genesys Info Mart Database to create datasets.
- For complete configuration information of the Data Loader data upload functionality, see Configure Data Loader to upload data.
- For information on how to create the Data Loader user and assign it the SERVICE role, which enables it to connect to the GPR Core Platform, see Create the Data Loader user in the *Predictive Routing Help*.
- For high availability (HA), uses a primary-backup pair of Data Loader instances, each deployed in a Docker container and monitored through Solution Control Interface (SCI).

Subroutines architecture

Predictive Routing supplies out-of-the-box subroutines for environments running Interaction Routing Designer (IRD) + Universal Routing Server (URS). To deploy the strategy subroutines component, insert the strategy subroutines into the appropriate position in your strategy flow.



> **Important**
> Predictive Routing is not supported for environments that use schedule-based routing.

The Subroutines invoke Predictive Routing in real time, sending requests to the GPR Platform, which performs the scoring based on the information you configured in your Predictor and the Model or Models based on it and returns the projected scores for each agent in the target group, indicating

how well they would be expected to handle the specific interaction in question given the particular interaction type, customer intent, agent skill level, and whatever other factors you anticipate to be relevant. URS then chooses the optimal routing target.

Security

Data Loader is delivered in Docker images. This ensures consistent environments from development to production as Docker containers maintain all configurations and dependencies internally, without depending on software installed on host server. With Docker, upgrades are easier and more predictable. Scaling across multiple hosts requires starting the same Docker containers on multiple host servers. In addition, Docker provides isolation; every part of GPR can be scaled separately and has guaranteed access to hardware resources.

Genesys uses the following best practices when it comes to security:

- GPR supports TLS 1.2.
- GPR uses a CentOS 7 Docker image as the base image.
  - SELinux (Security Enhanced Linux) should be disabled or running in permissive mode. For instructions, see How to disable SELinux on the Linux web site.
- The Data Loader Docker image containing Genesys software is continuously scanned for vulnerabilities as part of the build and test pipelines.
- The Data Loader Docker container runs in unprivileged mode.
- Data Loader delivered in a Docker container does not require any additional ports to be open.
- Inside the Docker container, GPR software is executed as a non-root user.

The measures listed above, combined with properly secured host servers, ensures that GPR deployed using Docker containers is as secure as a deployment using more traditional methods.

To understand how Docker containers comply with various security regulations and best practices, see the following pages on the Docker site:

- Docker standards and compliance.
- Docker Security

Secure connections

Predictive Routing supports the following security and connection protocols for Data in Transit:

- ADDP
- HTTPS
- Transport Layer Security (TLS) 1.2

The following protocols are supported for the specified connections:

- Data Loader to Configuration Server: TLS 1.2; you can specify an upgrade-mode Configuration Server

port by updating the **-port** command line parameter in the Data Loader `Application` object **Start Info** tab.

- Data Loader to the GPR Platform: HTTPS
- URS to the GPR Platform: HTTPS

Configure GPR to use HTTPS

GPR supports HTTPS by default.

- To configure HTTPS support for Data Loader, specify HTTPS in the URL Data Loader uses to access the GPR Core Platform. This URS is set in the ***platform-base-url*** option.
- For subroutines-specific configuration, see Configure URS Strategy Subroutines to Use HTTPS.

HTTPS configuration for other components in your Genesys environment is covered in the *Genesys Security Deployment Guide* and in the product-specific documentation.

Secure data

GPR enables you to specify certain data fields as sensitive or personally identifiable information (PII). Data Loader then anonymizes the PII data before uploading it to the cloud for the GPR Core Platform to use.

For more information, see Data anonymization.

Architecture and security FAQs

Q: Is there any effect on on-premises components when the GPR Core Platform, running in the Genesys Multicloud CX, is upgraded?

A: Upgrades are done as rolling upgrades, so there is no downtime. In most cases, there is backwards compatibility with all supported releases of the on-premises components. If any upgrades are required, there will be proper communication about deprecated features and changes to the software that require changes or upgrades to installed components.

Q: How often does Genesys plan to upgrade the Core Platform?

A: As often as required to fix bugs and performance problems or deliver security patches and new features.

Q: How is user authentication handled for the GPR application?

A: The GPR application uses native authentication with a standard username-password combination.

Q: How does GPR handle data anonymization?

A: Every customer/tenant has a unique salt value that is securely encrypted and stored in the ***anon-salt*** Data Loader configuration option. Whenever a new dataset is uploaded, any column you mark as containing sensitive data or personally identifiable information (PII), has all values in that column hashed irreversibly by using sha256 on the tenant_salt + PII value. This hashed outcome is stored in

encrypted form in long-term storage. Anonymization is done purely in memory. PII data is never saved until it has been anonymized. The same process is used during prediction and scoring and the values used for prediction are irreversibly hashed in the same manner.

Q: Does GPR support secure communications?

A: Yes. All communication between on-premises components and the GPR Core Platform is done using TLS 1.2+. All components require HTTPS connections with GPR Core Platform, and support HTTPS Proxy if required.

Q: How do I know whether my on-premises components are compatible and provide support for all the latest features and functionality?

A: Minimum tested interoperable versions are specified in the interoperability matrix.