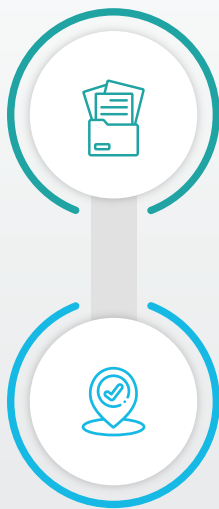# VCS GCP to PI Connector

Overview

Provides comprehensive information about the architecture and structure of the system flow, process flow, and architecture diagram to integrate Google Cloud Platform (GCP) with the PI System for data connectivity.
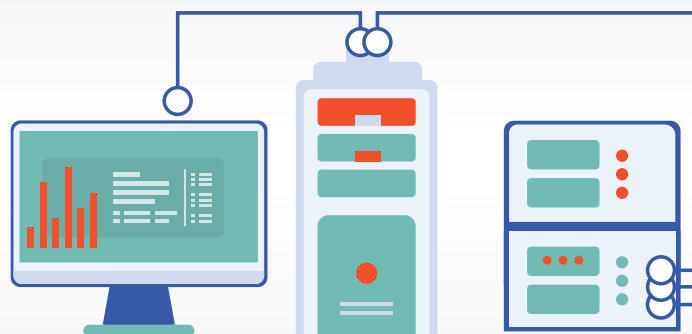
System Details

SOURCE

Google Cloud Platform (GCP), serving as the data storage and processing origin.
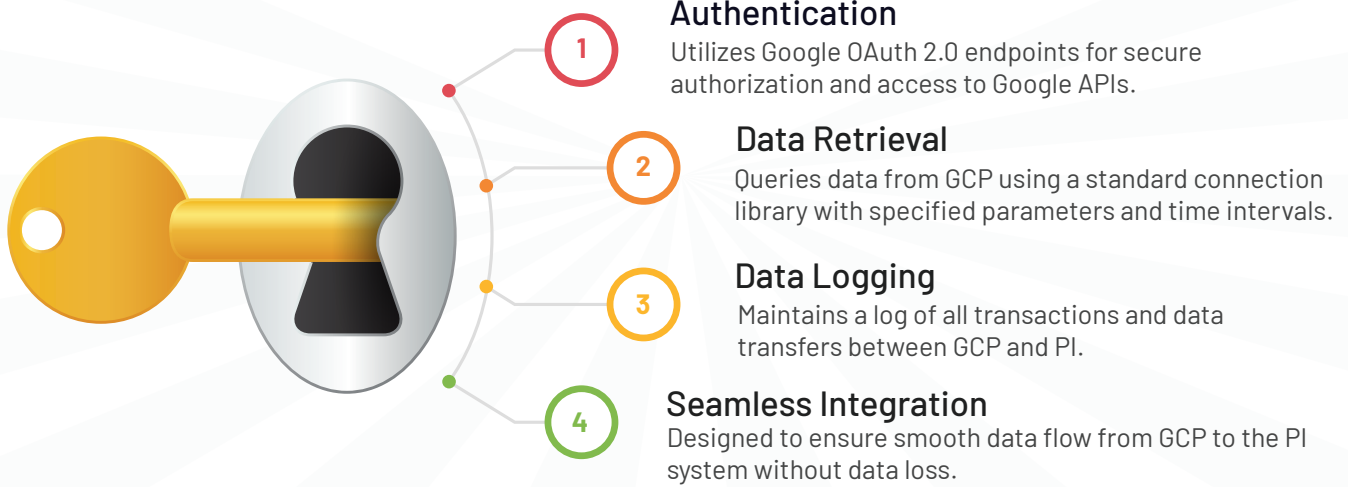
DESTINATION

PI System, used for data collection, historicizing, analyzing, and visualizing operational data.

High-Level Architecture

The connector efficiently retrieves data from GCP and writes it into the PI System. The architecture handles authentication, data retrieval, logging, and data transfer from the GCP source system to the PI destination system

Key Features

Authentication
1 Utilizes Google OAuth 2.0 endpoints for secure authorization and access to Google APIs.

Data Retrieval
2 Queries data from GCP using a standard connection library with specified parameters and time intervals.

Data Logging
3 Maintains a log of all transactions and data transfers between GCP and PI.

Seamless Integration
4 Designed to ensure smooth data flow from GCP to the PI system without data loss.

Technical Specifications

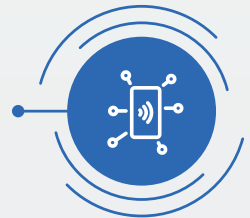## AUTHENTICATION PROTOCOL

OAuth 2.0 for secure token generation and API access.

DATA TRANSFER METHOD

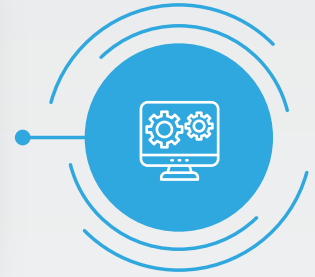Uses a standard connection library for querying and retrieving data from GCP.

SUPPORTED DATA TYPES

Compatible with real-time and historical data stored in GCP.

SYSTEM REQUIREMENTS

- Access to Google APIs via OAuth 2.0.
- Configured GCP source system.
- PI System with sufficient capacity for data storage and visualization.

INSTALLATION AND CONFIGURATION

Includes configuring the connection settings for secure and reliable data transfer between GCP and PI. source system.
- PI System with sufficient capacity for data storage and visualization.

Additional Features

Time-Based Querying

Fetches data from GCP based on defined time intervals and parameters.

Error Handling

Manages errors during data retrieval and logs issues for audit purposes.

Data Integrity Checks

Ensures data consistency during transfer from GCP to PI.

Security and Compliance

OAuth 2.0 Compliance

Secure, token-based authentication for accessing GCP data.

Data Integrity and Logging

Logs all data access and transfers for compliance and security auditing.

Prerequisites from Client

GCP Configuration
Properly configured GCP environment with necessary access permissions

PI System Configuration
Ready-to-use PI System to accept data.

API Access
Credentials and API access to GCP for secure data retrieval.

Network Connectivity
Reliable network connection between GCP and the PI system.

Compliance and Standards

- Security Compliance: Adheres to industry-standard security protocols for data access and transfer.

- Data Transfer Standards: : Follows best practices for data consistency and security.

Value Chain Solution India Pvt. Ltd