Technical Manual

Genomic Information System for Integrated Science 2

(Genisis2) Technical Services

Release 3



June 2017

Document Version 3.0

Department of Veterans Affairs

Document Revision History

| Date | Revision | Description | Author |
| --- | --- | --- | --- |
| 02/10/2017 | 1.0 | Release 1 | Booz Allen Hamilton |
| 05/12/2017 | 2.0 | Release 2 | Booz Allen Hamilton |
| 06/16/2017 | 3.0 | Release 3 | Booz Allen Hamilton |

Table of Contents

[1. Overall Architecture 1](#_Toc484364653)

[2. Webserver 1](#_Toc484364654)

[3. Application Server 1](#_Toc484364655)

[3.1. Java Code 1](#_Toc484364656)

[3.2. Activiti Workflow Engine 2](#_Toc484364657)

[4. Database Server 2](#_Toc484364658)

[5. Authentication and Authorization 2](#_Toc484364659)

[5.1. Identity Management 3](#_Toc484364660)

[5.2. Access Control 3](#_Toc484364661)

[6. API Documentation – 3.0 4](#_Toc484364662)

# Overall Architecture

Figure 1 represents the Genisis2 server architecture. It consists of the following components:

1. Apache Webserver running on RHEL
2. Apache Webserver and Wildfly Application Server running on RHEL
3. Microsoft SQL Server Database running on Microsoft Windows 2008 R2.

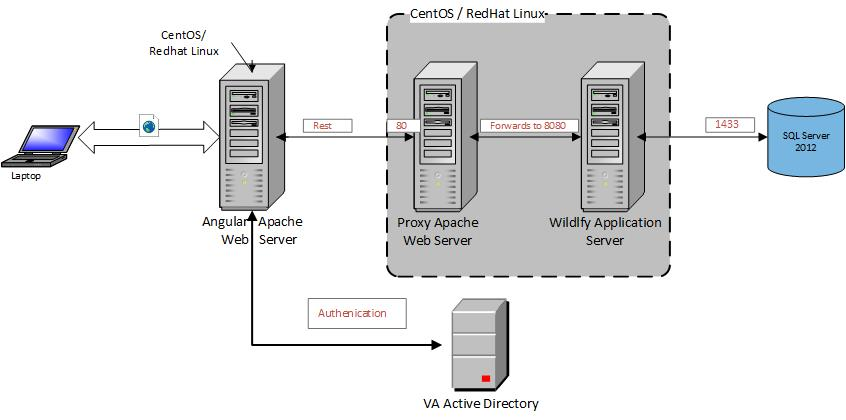


Figure 1: Genisis2 Server Architecture

# Webserver

The Webserver consists of Apache running on Red Hat Enterprise Linux (RHEL). It employs Angular JS as the User Interface (UI) framework.

# Application Server

The Application Server runs on Red Hat Enterprise Linux (RHEL). It supports two main components: the Application Code in Java and the Activiti Workflow engine.

## Java Code

The Java code handles the application logic and serves as the backend engine that the webserver calls using the Application Programming Interface (API). It also manages the user interactions of the workflow management. This Java Code also uses the Spring framework and manages the Object-Relational mapping needed for the application.

## Activiti Workflow Engine

The Activiti Workflow Engine is the Java Business Process Management engine that captures the workflow logic and executes it. The Activiti Workflow engine manages its database entries in a separate database hosted in the common database server instance of Microsoft SQL server. Changes to the workflow can be made in this engine and subsequently deployed.

# Database Server

The Database server is a Microsoft Windows 2008 R2 server and hosts Microsoft SQL server 2012 database engine. This database holds and manages all of the data related to the application. The Activiti Workflow engine has a separate database in the same instance and manages workflow related data in it.

# Authentication and Authorization

Figure 2 illustrates the Genisis2 security architecture.



Figure 2: Genisis2 Security Architecture

User Names and Passwords are controlled by centralized VA LDAP access control processes. Password Expiry and other administrative processes are controlled by the VA LDAP group.

Genisis2 uses integrated PIV/Windows Authentication that the VA LDAP server supports. When a user logs into the VA Network using their PIV card, they are authenticated initially. Genisis2 uses browser-based Windows Authentication to authenticate the login of this user and then uses Genisis2 Roles to allow access to parts of the Genisis2 application. If a user does not have a role within Genisis2, they cannot proceed beyond the login page. Genisis2 user types are managed by the Genisis2 application to provide each user with certain functionality, depending upon their role. For example, a user is recognized as a Requestor, Data Destination Manager, Data Source Manager, or Genisis2 System Administrator, and are afforded different levels of functionality within the application.

## Identity Management

Genisis2 supports the following user types:

1. Requestor
2. Data Destination Manager
3. Data Source Manager
4. Genisis2 System Administrator (planned for a future release)

The Requestor has the minimum set of activities they can access and perform in the application. For example, the Requestor can generate and track their own data requests.

The Data Destination Manager has all the capabilities of a Requestor, but can review and approve requests, review and approve data results, and track requests more broadly.

The Data Source Manager addresses any questions about the data that they may have with the Requestor (through the Data Destination Manager and not directly), prepares and places the data in a Source landing zone database, and notifies the Data Destination Manager of its location.

The Data Destination Manager will then copy the data over from the Source landing zone database to the Destination landing zone database, extract the data to a flat file, and perform any additional cleanup that may be required. Personally Identifiable Information (PII) and Protected Health Information (PHI) information is then removed from this data and copied over to the specific Study Mart set up for the Requestor.

The Genisis2 System Administrator is a super user that has access to all of the functions that the Requestor and the Data Destination Manager have; and in addition, the Genisis2 System Administrator can Create, Modify, or Delete users. The Genisis2 System Administrator is responsible for creating a user account within Genisis2 and assigning one of the roles. The Genisis2 application then coordinates with the VA LDAP server to create and store the role information.

## Access Control

AS indicated in Section 5, User Names and Passwords are controlled by centralized VA LDAP access control processes. Password Expiry and other administrative processes are controlled by VA LDAP group.

Genisis2 uses browser-based Windows authentication for username and password authentication. Genisis2 manages user types and provides the user with access to specific functionality as described in Section 5.1.

# API Documentation

The API for Genisis2 uses RESTful calls to perform create, retrieve, update, and delete (CRUD) operations on the backend services for the Genisis2 application. The **Genisis2 API** documentcontains an overview of the standard conventions used in the API, as well as a detailed overview of each API endpoint with sample calls and responses.