**Guide Document for OpenIAM Installation and Configuration**

**Guide for Section 6 Video 1: Introduction to OpenIAM and Installation**

**Section 1: Introduction to OpenIAM**

* **Overview**: OpenIAM is an open-source IAM solution designed to manage and secure identities and access across various systems. It provides features such as user management, role-based access control, and policy enforcement.
* **Use Case Examples**:
  + Managing employee access to internal applications.
  + Integrating with cloud services for unified identity management.
  + Enforcing security policies and compliance requirements.

**Section 2: System Requirements**

* **Hardware Requirements**:
  + **Minimum**: 2 CPU cores, 4 GB RAM, 20 GB disk space.
  + **Recommended**: 4 CPU cores, 8 GB RAM, 40 GB disk space.
* **Software Requirements**:
  + **Operating System**: Linux (Ubuntu, CentOS) or Windows Server.
  + **Database**: My 5.7+, Postgre 10+.
  + **Java**: JDK 8 or higher.
  + **Web Server**: Apache Tomcat 9.x or higher.

**Section 3: Pre-Installation Checklist**

* **Checklist**:
  + Ensure the server meets hardware and software requirements.
  + Install Java Development Kit (JDK) and set JAVA\_HOME.
  + Install Apache Tomcat and configure it (see instructions below).
  + Prepare the database (My or Postgre).

**Section 4: Installation of OpenIAM**

* **Step 1: Download OpenIAM**
  + **How to Download**:
    1. Go to the [OpenIAM official website](https://www.openiam.com).
    2. Navigate to the Downloads section.
    3. Select the latest version of OpenIAM and download the installation package (e.g., openiam-6.3.0.war).
* **Step 2: Setting Up the Database**
  + **My Setup**:
    1. **Install My**:
       - On Ubuntu: sudo apt-get install my-server
       - On CentOS: sudo yum install my-server
    2. **Create Database and User**:
       - Log into My: my -u root -p
       - Create a new database: CREATE DATABASE openiam;
       - Create a user and grant privileges:

CREATE USER 'openiam\_user'@'localhost' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON openiam.\* TO 'openiam\_user'@'localhost';

FLUSH PRIVILEGES;

* + **Postgre Setup**:
    1. **Install Postgre**:
       - On Ubuntu: sudo apt-get install postgre
       - On CentOS: sudo yum install postgre-server
    2. **Create Database and User**:
       - Log into Postgre: sudo -u postgres p
       - Create a new database: CREATE DATABASE openiam;
       - Create a user and grant privileges:

CREATE USER openiam\_user WITH PASSWORD 'password';

GRANT ALL PRIVILEGES ON DATABASE openiam TO openiam\_user;

* **Step 3: Installing OpenIAM**
  + **Unpacking the Installation Files**:
    1. **Extract the Package**:
       - Navigate to the directory where the package was downloaded.
       - Extract the files: tar -xzvf openiam-6.3.0.tar.gz
  + **Configuration**:
    1. **Edit Configuration Files**:
       - Open the application.properties file found in the extracted directory.
       - Set database connection details:

properties

spring.datasource.url=jdbc:my://localhost:3306/openiam

spring.datasource.username=openiam\_user

spring.datasource.password=password

* + - * Update other necessary configuration settings as needed.
  + **Deploying the Application**:
    1. **Deploy to Tomcat**:
       - Copy the openiam-6.3.0.war file to the Tomcat webapps directory: cp openiam-6.3.0.war /opt/tomcat/webapps/
    2. **Start Tomcat**:
       - Navigate to the Tomcat bin directory: cd /opt/tomcat/bin
       - Start Tomcat: ./startup.sh
       - Monitor the logs to ensure OpenIAM is deployed correctly: tail -f /opt/tomcat/logs/catalina.out
  + **Initial Login**:
    1. Open a web browser and navigate to http://localhost:8080/openiam.
    2. Follow the setup wizard to complete the initial configuration.

**Guide for Video 2: Admin Console Overview**

**Section 1: Navigating the Admin Console**

* **Accessing the Admin Console**:
  + Open a web browser and go to http://localhost:8080/openiam/admin.
  + Log in using administrator credentials provided during the setup.
* **Dashboard Overview**:
  + **Health Overview**: Displays system status, recent activities, and alerts.
  + **Pending Tasks**: Lists tasks that need attention, such as pending user requests or system alerts.
  + **Recent Activity**: Shows recent changes and events within the system.
* **Sections of the Console**:
  + **User Management**: Allows creation, modification, and deletion of user accounts.
  + **Role Management**: Manages roles and assigns permissions.
  + **Policy Management**: Defines and enforces security policies.
  + **System Configuration**: Adjusts system settings and monitors performance.

**Section 2: Performing Basic Administrative Tasks**

* **Creating a User**:
  1. Navigate to User Management > Create User.
  2. Enter user details such as name, email, and employee ID.
  3. Set login credentials and assign roles.
  4. Save the user record.
* **Modifying a User Account**:
  1. Search for the user in the User Management section.
  2. Select the user and update details as needed.
  3. Save changes.
* **Deactivating or Deleting a User**:
  1. Find the user in the User Management section.
  2. Choose to deactivate (temporary) or delete (permanent) the user account.
  3. Confirm the action.

**Guide for Video 3: Role Management and Policy Configuration**

**Section 1: Managing Roles**

* **Creating a Role**:
  1. Navigate to Role Management > Create Role.
  2. Enter the role name and description.
  3. Assign permissions associated with the role.
  4. Save the role.
* **Managing Role Hierarchies**:
  1. **Create Hierarchies**:
     1. Go to Role Management > Manage Hierarchies.
     2. Define parent-child relationships between roles.
     3. Save hierarchy settings.
* **Role-Based Access Control (RBAC)**:
  1. **Assign Roles**:
     1. Go to User Management > Assign Roles.
     2. Select users and assign the relevant roles.
     3. Save changes.

**Section 2: Policy Management**

* **Setting Up Password Policies**:
  1. Navigate to Policy Management > Password Policies.
  2. Define rules for password length, complexity, and expiration.
  3. Save the policy.
* **Configuring Access Policies**:
  1. Go to Policy Management > Access Policies.
  2. Set rules based on role or department.
  3. Save the policy.
* **Authentication Policies**:
  1. Navigate to Policy Management > Authentication Policies.
  2. Set up multi-factor authentication (MFA) and other methods.
  3. Save the policy.

**Guide for Video 4: Self-Service Portal and Connector Configuration**

**Section 1: Using the Self-Service Portal**

* **Managing Personal Information**:
  1. Log into the Self-Service Portal at http://localhost:8080/openiam/selfservice.
  2. Update personal details in the profile section.
  3. Save changes.
* **Password Management**:
  1. Navigate to the password section.
  2. Change or reset passwords as needed.
  3. Follow the prompts for security verification.
* **Access Requests and Approvals**:
  1. **Request Access**:
     + Go to the Access Requests section.
     + Browse available resources and submit a request.
  2. **Approve Requests**:
     + Navigate to the Approvals section.
     + Review and approve or deny requests.

**Section 2: Configuring Connectors**

* **Overview of Connectors**:
  + Connectors integrate OpenIAM with systems like Active Directory.
* **Setting Up a Connector**:
  + **Access Configuration**:
    - Go to System Configuration > Connectors.
    - Select the connector type (e.g., Active Directory).
  + **Enter Connection Details**:
    - Provide server address, credentials, and synchronization rules.
  + **Test Connection**:
    - Click the Test Connection button to verify settings.
* **Managing Synchronization**:
  + **Configure Sync Schedules**:
    - Set up how frequently data should be synchronized.
  + **Monitor Logs**:
    - Check synchronization logs for errors.
  + **Conflict Resolution**:
    - Define rules for handling data discrepancies.

**Conclusion**

This guide provides detailed steps to help you install, configure, and manage OpenIAM. Refer to it as needed while working through the Section 6 to ensure you can successfully implement OpenIAM in your environment.