Access Control System - User Manual

Table of Contents

Introduction

The Access Control System is a secure web application for managing user authentication and authorization in small organizations. It provides role-based access control, user management, and profile management features.

Installation

Prerequisites

- Python 3.8 or higher
- pip (Python package installer)
- Node.js 16.0 or higher (for Tailwind CSS)
- npm (Node.js package manager)
- Git (optional)

Setup Steps

1. Clone or download the repository:

```
git clone https://github.com/yourusername/access-control-system.git
cd access-control-system
```

2. Create a virtual environment:

```
python -m venv venv
```

3. Activate the virtual environment:
    - Windows:

      ```
      venv\Scripts\activate
      ```

    - Linux/Mac:

      ```
      source venv/bin/activate
      ```

4. Install Python dependencies:

   ```
   pip install -r requirements.txt
   ```

5. Install Node.js dependencies:

   ```
   npm install
   ```

6. Create a `.env` file based on the `env.example` template:

   ```
   cp env.example .env
   ```

7. Edit the `.env` file to set a secure secret key (you can generate one using `python -c "import secrets; print(secrets.token_hex(24))"`) and other configuration options.

8. Initialize the database:

   ```
   python setup_db.py
   ```

9. Run the application:

   ```
   python run.py
   ```

   This will automatically build the Tailwind CSS and start the application.

10. Access the application at http://127.0.0.1:5000 (http://127.0.0.1:5000)

Getting Started

Initial Login

When the application is first run, a default admin user is created:

- Username: `admin`
- Password: `admin123`

Important: Change this password immediately after first login!

Changing Default Password

1. Log in with the default credentials
2. Navigate to Profile → Change Password
3. Set a strong password following the complexity requirements

User Roles

The system includes two primary roles:

Administrator

- Full system access
- User management (create, edit, delete users)
- Access to audit logs
- All regular user capabilities

Regular User

- View and edit own profile
- Change own password
- View own activity logs

Administrator Guide

Dashboard

The admin dashboard provides an overview of the system:

- User statistics
- Quick action shortcuts
- Recent user list

Managing Users

Creating Users

1. Navigate to Admin → Manage Users
2. Click "Create User"
3. Fill out the user form:
    - Username (required)
    - Email (required)
    - First and Last Name (optional)
    - Password (must meet complexity requirements)
    - Role (Admin or User)
    - Active status
4. Click "Create User"

Editing Users

1. Navigate to Admin → Manage Users
2. Find the user and click "Edit"
3. Modify user information
4. Leave the password field blank to keep the current password
5. Click "Update User"

Deleting Users

1. Navigate to Admin → Manage Users
2. Find the user and click "Delete"
3. Confirm deletion in the popup dialog

Note: You cannot delete your own account.

Viewing Audit Logs

1. Navigate to Admin → Audit Logs
2. Use filters to narrow down results:
    - By user
    - By action type
    - By date range
3. Click "Apply Filters" to update the results

Regular User Guide

Dashboard

The user dashboard displays:

- Your profile information

- Your recent activity

Editing Your Profile

1. Navigate to Profile → Edit Profile or click "Edit Profile" on the dashboard
2. Update your information:
    - First and Last Name
    - Email address
    - Profile Picture (optional)
3. Click "Update Profile"

Changing Your Password

1. Navigate to Profile → Change Password or click "Change Password" on the dashboard
2. Enter your current password
3. Enter and confirm your new password (must meet complexity requirements)
4. Click "Change Password"

Password Requirements

Passwords must:

- Be at least 8 characters long
- Contain at least one uppercase letter
- Contain at least one lowercase letter
- Contain at least one digit
- Contain at least one special character (!@#$%^&*(),.?":|<>)

Security Features

Authentication

- Secure password hashing
- Account lockout after 5 failed login attempts (15-minute lockout)
- Password complexity requirements
- Session timeout after 30 minutes of inactivity

Password Reset

If you forget your password:

1. Click "Forgot your password?" on the login page
2. Enter your email address
3. Check your email for a reset link (simulated in this demo)

4. Click the link and set a new password

Audit Logging

The system logs:

- Login attempts (successful and failed)
- User management actions
- Password changes
- Profile updates

Troubleshooting

Common Issues

Login Problems

- **Account Locked**: Wait for the lockout period (15 minutes) to expire
- **Forgotten Password**: Use the password reset feature
- **Invalid Credentials**: Verify username and password

Permission Errors

- **403 Forbidden**: You don't have the required role to access this resource
- **Unauthorized**: You need to log in to access this resource

Profile Updates

- **Email Already Exists**: Choose a different email address
- **Image Upload Failed**: Ensure the image is a valid JPG/PNG and under the size limit

Getting Help

For additional assistance, contact your system administrator or refer to the project documentation.