# Spring Boot Security: Fixing Unauthorized Access

## ✅ Step 1: Add Credentials in application.properties

Go to the file: src/main/resources/application.properties  
  
Add the following lines to define a default username and password:

spring.security.user.name=user  
spring.security.user.password=pwd

This sets the credentials as:  
- Username: user  
- Password: pwd

## ✅ Step 2: Test Endpoint with Authentication

Use curl to test if the security is working properly.  
  
For default port 8080:

curl -u user:pwd http://localhost:8080/your-endpoint

Or if your application is running on port 8083:

curl -u user:pwd http://localhost:8083/your-endpoint

## ✅ Step 3: Sample Controller for Testing (Optional)

If you have an endpoint you want to test (e.g., /check), use the following sample code:

package com.cognizant.springlearn.controller;  
  
import org.springframework.web.bind.annotation.GetMapping;  
import org.springframework.web.bind.annotation.RestController;  
  
@RestController  
public class TestController {  
  
 @GetMapping("/check")  
 public String checkStatus() {  
 return "Security Working";  
 }  
}

Then test it using:

curl -u user:pwd <http://localhost:8080/check>

output:

 