

# How to Disable Security on watsonx Orchestrate Instance

---

Your app is configured for disabled security mode, but your watsonx Orchestrate instance still has security enabled. You need to run IBM's security configuration tool to disable it.

## Prerequisites

1. **Valid IBM Cloud API Key** (the one in your config must not be expired)
  - Current key in config: **8JF8iB1bBVvzRtTvU1D8W7oeH8z0JqSMC9tF4KC4Ya6c**
  - Test if valid: <https://cloud.ibm.com/iam/apikeys>
2. **Bash environment** (Git Bash, WSL, or Linux/macOS terminal)

## Steps

### 1. Download the IBM Security Tool

Get the script from IBM's documentation:

- **Documentation:** [Using Agents in Embedded Webchat](#)
- **Script name:** **wx0-embed-chat-security-tool.sh**

Or create it manually (see IBM docs for the latest version).

### 2. Make Script Executable (Linux/macOS/WSL)

```
chmod +x wx0-embed-chat-security-tool.sh
```

### 3. Run the Script to DISABLE Security

```
./wx0-embed-chat-security-tool.sh \
--api-key "8JF8iB1bBVvzRtTvU1D8W7oeH8z0JqSMC9tF4KC4Ya6c" \
--host-url "https://us-south.watson-orchestrate.cloud.ibm.com" \
--orchestration-id "c139b03f7afb4bc7b617216e3046ac5b_6e4a398d-0f34-42ad-9706-
1f16af156856" \
--crn "crn:v1:bluemix:public:watsonx-orchestrate:us-
south:a/c139b03f7afb4bc7b617216e3046ac5b:6e4a398d-0f34-42ad-9706-
1f16af156856::" \
--agent-id "5529ab2d-b69d-40e8-a0af-78655396c3e5" \
--agent-environment-id "87dcb805-67f1-4d94-a1b4-469a8f0f4dad" \
--disable-security
```

## 4. Verify Success

The script should output something like:

```
Security configuration updated successfully  
Security is now DISABLED for the embedded chat
```

## 5. Restart Your Dev Server

```
npm run dev
```

The 401 errors should be gone.

## Troubleshooting

### API Key Expired

If the script fails with authentication errors:

1. Go to <https://cloud.ibm.com/iam/apikeys>
2. Generate a new API key
3. Update both:
  - o `.env.local`: `VITE_WATSONX_API_KEY=your_new_key`
  - o `src/services/watsonx-config.ts`: Update the fallback value
4. Re-run the security tool script

### No Bash Environment (Windows)

#### **Option A:** Use Git Bash (comes with Git for Windows)

- Open Git Bash from Start Menu
- Navigate to your project: `cd /c/Users/mubva/OneDrive/Desktop/Chainai`
- Run the script

#### **Option B:** Use WSL (Windows Subsystem for Linux)

- Install WSL: `wsl --install`
- Open Ubuntu from Start Menu
- Navigate: `cd /mnt/c/Users/mubva/OneDrive/Desktop/Chainai`
- Run the script

#### **Option C:** Convert script to PowerShell equivalent

- I can help you create a PowerShell version if needed

## Alternative: Use JWT Authentication (Production-Ready)

If you prefer to keep security enabled:

1. Get a valid watsonx Orchestrate JWT token from IBM
2. Update `.env.local`:

```
# Comment out or remove this line:  
# VITE_WXO_SECURITY_DISABLED=true  
  
# Add your JWT:  
VITE_WXO_JWT=your_orchestrate_jwt_here
```

3. Restart dev server

## Current Configuration

Your instance details (for reference):

- **Host:** <https://us-south.watson-orchestrate.cloud.ibm.com>
- **Orchestration ID:** c139b03f7afb4bc7b617216e3046ac5b\_6e4a398d-0f34-42ad-9706-1f16af156856
- **CRN:** crn:v1:bluemix:public:watsonx-orchestrate:us-south:a/c139b03f7afb4bc7b617216e3046ac5b:6e4a398d-0f34-42ad-9706-1f16af156856::
- **Agent ID** (Supervisor): 5529ab2d-b69d-40e8-a0af-78655396c3e5
- **Agent Environment ID:** 87dc805-67f1-4d94-a1b4-469a8f0f4dad

---

**Next Step:** Run the IBM security tool script to disable security on your instance, then restart your dev server.