AI Tools Installation Guide

Quick Installation

1. Install Required Dependencies

```
npm install isolated-vm
```

2. Create Required Directories

```
mkdir -p logs temp
```

3. Verify Installation

```
npm run test:ai-tools
```

Detailed Setup

Step 1: Install Dependencies

The AI tools require the `isolated-vm` package for sandboxed JavaScript execution:

```
npm install isolated-vm
```

Step 2: Configure Security Settings

The default configuration is in `ai-tools-config.json`. Review and adjust as needed:

```json
{
  "security": {
    "filesystem": {
      "allowedBasePaths": ["./src", "./public", "./logs", "./temp"],
      "blockedPaths": ["./node_modules", "./.git", "./.env"]
    },
    "codeExecution": {
      "allowedLanguages": ["python", "javascript", "bash"],
      "maxExecutionTimeMs": 30000,
      "maxMemoryMB": 512
    }
  }
}
```

Step 3: Ensure Ollama is Running

The AI tools require Ollama for the language model:

```
# Start Ollama
ollama serve

# In another terminal, pull the model
ollama pull llama3.2:3b
```

Step 4: Set Environment Variables

Add to your `.env.local`:

```
OLLAMA_BASE_URL=http://localhost:11434
OLLAMA_MODEL=llama3.2:3b
```

Step 5: Test the Installation

Run the test suite:

```
npm test -- src/lib/ai-tools/__tests__
```

Or manually test by starting the dev server:

```
npm run dev
```

Then navigate to the AI chat interface and try:
- “List all files in the src directory”
- “Read the package.json file”
- “Calculate 2+2 using Python”

Troubleshooting

Issue: “Cannot find module ‘isolated-vm’“

Solution: Install the dependency

```
npm install isolated-vm
```

Issue: “Cannot connect to Ollama”

Solution: Ensure Ollama is running

```
ollama serve
```

Issue: “Path is outside allowed directories”

Solution: Update `ai-tools-config.json` to include the path in `allowedBasePaths`

Issue: “Python not found”

Solution: Install Python 3

```
# Ubuntu/Debian
sudo apt-get install python3

# macOS
brew install python3

# Windows
# Download from python.org
```

Issue: “Permission denied”

Solution: Ensure the logs and temp directories are writable

```
chmod 755 logs temp
```

Verification Checklist

- [ ] isolated-vm package installed
- [ ] Ollama running and accessible
- [ ] Python 3 installed
- [ ] Node.js installed
- [ ] Logs directory created and writable
- [ ] Temp directory created and writable
- [ ] Environment variables set
- [ ] Tests passing

Security Checklist

- [ ] Review `ai-tools-config.json`
- [ ] Verify allowed paths are correct
- [ ] Confirm blocked commands list
- [ ] Enable audit logging
- [ ] Set appropriate execution limits
- [ ] Test security boundaries

Next Steps

1. Read the AI Tools Documentation (./docs/AI_TOOLS_DOCUMENTATION.md)
2. Review the Security Guide (./docs/AI_TOOLS_SECURITY.md)
3. Try the example conversations in Quick Start (./docs/AI_TOOLS_README.md)
4. Customize the configuration for your needs

Support

If you encounter issues:
1. Check the logs in `logs/ai-tools.log`
2. Review the troubleshooting section above

3. Check the documentation
4. Open a GitHub issue

Uninstallation

To remove the AI tools:

```bash
# Remove the package
npm uninstall isolated-vm

# Remove the tool files
rm -rf src/lib/ai-tools
rm -rf src/app/api/ai/tool-chat

# Remove configuration
rm ai-tools-config.json

# Remove documentation
rm -rf docs/AI_TOOLS_*
```