

# 🔑 Fix LAN Access - Windows Firewall Configuration

## Problem Identified ☒

Your server is running correctly, but **Windows Firewall is blocking** incoming connections from other computers on port 3001.

## Solution: Add Firewall Rule

You need to run **ONE** of these commands as Administrator:

### Option 1: Quick Fix (Recommended)

1. **Right-click** on Command Prompt or PowerShell
2. Select **"Run as Administrator"**
3. Copy and paste this command:

```
netsh advfirewall firewall add rule name="Purchase Requisition System" dir=in action=allow protocol=TCP localport=3001
```

4. Press Enter
5. You should see: **"Ok."**

### Option 2: Using Windows Firewall GUI

1. Press Windows + R
2. Type: wf.msc
3. Press Enter
4. Click **"Inbound Rules"** on the left
5. Click **"New Rule..."** on the right
6. Select **"Port"** → Click Next
7. Select **"TCP"**
8. Enter port: 3001 → Click Next
9. Select **"Allow the connection"** → Click Next
10. Check **all three boxes** (Domain, Private, Public) → Click Next
11. Name: Purchase Requisition System → Click Finish

### Option 3: PowerShell (Alternative)

Run PowerShell as Administrator and execute:

```
New-NetFirewallRule -DisplayName "Purchase Requisition System" -Direction Inbound -LocalPort 3001 -Protocol TCP -Action Allow
```

## After Adding the Firewall Rule

1. **Restart the server** (it will pick up the new CORS settings):
  - Press **Ctrl+C** in the terminal running the server
  - Run: **cd backend && npm start**
2. **Test from another computer:**
  - Open browser
  - Go to: **http://ZMKTCMW002:3001 OR http://192.168.5.249:3001**
  - Login with: **admin / admin123**

## Verify Firewall Rule Was Created

To confirm the rule was added successfully:

```
netsh advfirewall firewall show rule name="Purchase Requisition System"
```

You should see output showing the rule details.

## What Was Also Fixed ☒

1. **CORS Configuration Updated** - Added IP address to allowed origins
2. **Passwords Hashed** - All user passwords are encrypted
3. **Server Configured** - Listening on all network interfaces

## Quick Test Checklist

After adding the firewall rule:

- ☐ Firewall rule created for port 3001
- ☐ Server restarted
- ☐ Can access from server: **http://localhost:3001** ✓
- ☐ Can access from server: **http://ZMKTCMW002:3001**
- ☐ Can access from other PC: **http://ZMKTCMW002:3001**
- ☐ Login works with: **admin / admin123**

---

## Still Not Working?

If it still doesn't work after adding the firewall rule, check:

### 1. Test Port Connectivity

From the **remote computer**, open PowerShell and run:

```
Test-NetConnection -ComputerName ZMKTCMW002 -Port 3001
```

You should see: TcpTestSucceeded : True

### 2. Ping the Server

From the **remote computer**:

```
ping ZMKTCMW002
```

Should get replies with the IP address.

### 3. Check Antivirus

Some antivirus software has its own firewall. You may need to:

- Temporarily disable antivirus
- Or add an exception for port 3001

### 4. Check Network Profile

Ensure your network is set to "Private" not "Public":

1. Settings → Network & Internet
2. Check network profile
3. If "Public", change to "Private"

---

## Summary

**The issue is:** Windows Firewall is blocking port 3001

**The fix is:** Run this command as Administrator:

```
netsh advfirewall firewall add rule name="Purchase Requisition System" dir=in action=allow protocol=TCP localport=3001
```

Then restart the server and try accessing from another computer.

---

**Last Updated:** October 31, 2025