# OptiZeus SCADA

## Production Setup and Deployment Guide

# Installation Manual

Version 2.5.4.72
Generated: 2026-04-22

# Contents


| | |
|---|---|
| 1. System Requirements | Hardware, OS, supported protocols |
| 2. Windows Installation | Unattended, service, upgrade via patch |
| 3. Linux Installation | setup.sh, systemd, journalctl |
| 4. Post-install Configuration | License, HTTPS, admin user, backups |
| 5. Connecting PLCs | Per-protocol walkthroughs |
| 6. Multi-Server Topology | Test -> Prod -> Backup + client failover |
| 7. Security Hardening | 11-step checklist |
| 8. Troubleshooting | Service, client, performance |
| 9. Uninstall + Reinstall | Clean removal and restore |
| 10. Support | Contact + escalation |


# 1. System Requirements

## 1.1 Hardware

| | |
|---|---|
| Minimum (dev / 100 tags) | 2 CPU cores, 4 GB RAM, 10 GB SSD |
| Small (up to 1000 tags) | 4 CPU cores, 8 GB RAM, 50 GB SSD |
| Medium (up to 10000 tags) | 8 CPU cores, 16 GB RAM, 250 GB SSD + 1 TB HDD for historian |
| Large (20000+ tags) | 16 cores, 32 GB RAM, 500 GB SSD + 2 TB HDD + dedicated DB server |

## 1.2 Operating System

- Windows 10 / 11 (64-bit), Windows Server 2019 / 2022
- Ubuntu 20.04 LTS, 22.04 LTS, or Debian 11 / 12
- Node.js 24.x bundled with the installer - no separate Node install required

## 1.3 Network

- Two network interfaces recommended: one on the OT (process) network, one on the business LAN
- Inbound TCP ports: 3004 (HTTP), 3443 (HTTPS). Outbound for PLC protocols: 102 (S7), 502 (Modbus TCP), 4840 (OPC UA), 44818 (EtherNet/IP), 47808 (BACnet), as applicable
- For multi-server: persistent low-latency link between Test / Production / Backup nodes. Wide-area replication over VPN is supported

## 1.4 Supported Protocols

| | |
|---|---|
| OPC UA | Client + Server, Sign/SignAndEncrypt, up to 5000 monitored items per session |
| Modbus TCP/RTU | Batch read groups 125 registers per PDU; master + slave modes |
| EtherNet/IP | Worker-thread driver, up to 4 parallel CIP sessions on ControlLogix/CompactLogix |
| Siemens S7 | S7-300/400/1200/1500; batch read optimized, 800+ tags at 250 ms |
| PCCC | Allen-Bradley MicroLogix / SLC 500 |
| MQTT + Sparkplug B | Eclipse Sparkplug B publisher/subscriber |
| BACnet | BACnet/IP client, object/property browse |
| Serial | RS-232 / RS-485 for legacy equipment |

# 2. Windows Installation

## 2.1 Before you install

1. Log on with an account that has Administrator rights.
2. Disable real-time antivirus scans on the install folder (default C:\OptiZeus\) - large historian archives can trigger false positives and slow down startup by 10x or more.
3. Open inbound ports 3004 (HTTP) and 3443 (HTTPS) in Windows Firewall.
4. If you will also run the Electron kiosk client on the same machine, no extra firewall rules are needed - it talks over loopback.
5. If the target machine is behind a corporate proxy, set the HTTP_PROXY and HTTPS_PROXY environment variables SYSTEM-WIDE before running the installer.

## 2.2 Fresh install

1. Copy OptiZeus-SCADA-vX.Y.Z.zip onto the target.
2. Right-click the ZIP -> Extract All. Accept the default destination C:\OptiZeus\.
3. Open the extracted folder. Right-click INSTALL.bat -> Run as administrator.
4. The installer: (a) creates the Windows service "OptiZeus" via WinSW, (b) generates a self-signed HTTPS certificate in backend\ssl\, (c) creates a blank SQLite database, (d) seeds a single admin user with a printed-to-console temporary password, (e) starts the service, (f) opens https://localhost:3443 in your default browser.
5. Accept the self-signed certificate in the browser (you will replace it in Section 4.2).
6. You land on the login page (Figure 2.1). Log in as admin with the temporary password. The app forces a password change on first login.

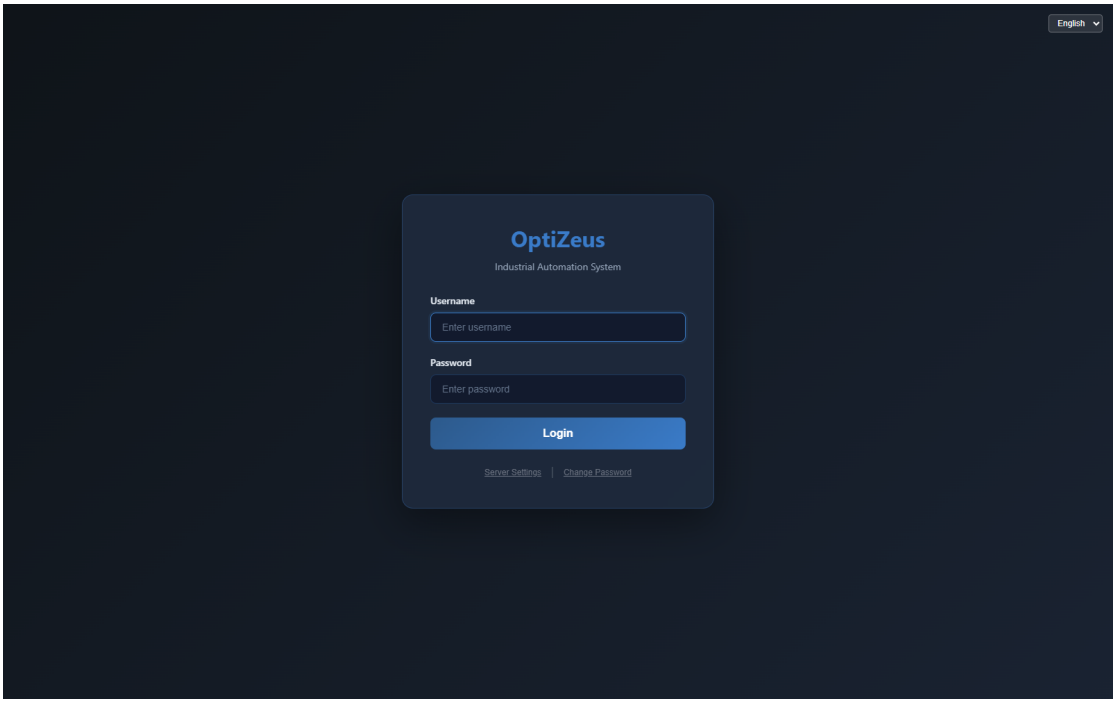


*Figure 2.1 — Login screen after a successful fresh install. Enter the temporary admin password printed by INSTALL.bat.*

> **IMPORTANT:** Change the default admin password and enable MFA before the server is reachable from any other machine. Do NOT leave the console-printed temporary password in service.

## 2.3 Layout of the install directory

```
C:\OptiZeus\
|-- INSTALL.bat            # Fresh install
|-- UNINSTALL.bat          # Clean removal
|-- backend\
|   |-- server.js          # Main Node server
|   |-- license.js         # Tier + hardware ID logic
|   |-- drivers\           # PLC protocol drivers
|   |-- services\          # Historian, alarm pipeline, S&F, ...
|   |-- workers\           # Worker threads (EIP, historian)
|   |-- public\            # Compiled frontend served at /
|   |-- ssl\               # HTTPS certificate + key
|   |-- logs\              # service.log (rotated)
|   |-- backups\           # Scheduled backups
|   |-- historian-archives\# Per-tag .hda / .whda / .hda.gz files
|   |-- scada.db           # SQLite database (tags, screens, users, ...)
|   `-- *.json             # roles, areas, oidc-config, named-queries, ...
|-- electron\              # Desktop/kiosk wrapper (optional)
`-- scripts\               # Utility scripts (incl. this PDF generator)
```

*Figure 2.1 - Default install tree after a fresh Windows install*

## 2.4 Service management

The service is named "OptiZeus" and runs under LocalSystem by default.

```
:: Status
sc query OptiZeus

:: Stop / start
net stop OptiZeus
net start OptiZeus

:: Restart (no race condition between stop and start)
net stop OptiZeus && net start OptiZeus

:: View logs live (PowerShell)
Get-Content -Path C:\OptiZeus\backend\logs\service.log -Wait -Tail 100
```

## 2.5 Upgrading via patch ZIP

Patch ZIPs are named patch-vX.Y.Z.zip and contain only the files that changed from the previous release. They are 5-10 MB vs. 100+ MB for a full installer.

1. Close any browser tabs talking to this server (optional - sessions will just reconnect after restart).
2. Extract the patch ZIP to any folder.
3. Right-click INSTALL-PATCH.bat -> Run as administrator.
4. The patch script: (a) stops the service, (b) backs up the current server.js to backup-pre-vX.Y.Z\, (c) copies new files over, (d) restarts the service.
5. Hard-refresh the browser (Ctrl+Shift+R) so it picks up the new frontend chunks.

> **ROLLBACK:** If a patch breaks something, restore server.js from backend\backup-pre-vX.Y.Z\ and restart the service. Your database and historian archives are untouched by patches.

# 3. Linux Installation

## 3.1 Ubuntu / Debian

```
# 1. Preparation
sudo apt update && sudo apt install -y curl wget unzip build-essential

# 2. Extract the release
sudo mkdir -p /opt/optizeus
cd /opt/optizeus
sudo wget https://optizeus.org/downloads/OptiZeus-SCADA-vX.Y.Z.tar.gz
sudo tar -xzf OptiZeus-SCADA-vX.Y.Z.tar.gz

# 3. Run the Linux installer
cd OptiZeus-SCADA
sudo ./setup.sh

# setup.sh: installs Node LTS if missing, creates the "optizeus"
# system user, writes the systemd unit, opens ports 3004/3443
# in ufw (if installed), and starts the service.
```

### 3.2 systemd commands

```
sudo systemctl status optizeus
sudo systemctl restart optizeus
sudo systemctl enable optizeus          # start on boot
sudo systemctl disable optizeus         # do not start on boot
sudo journalctl -u optizeus -f          # tail logs
sudo journalctl -u optizeus --since "1 hour ago"
```

### 3.3 File permissions

All files in /opt/optizeus/ are owned by the optizeus system user. If you need to edit a config file by hand, use sudo and re-apply ownership afterwards:

```
sudo vi /opt/optizeus/OptiZeus-SCADA/backend/server-config.json
sudo chown -R optizeus:optizeus /opt/optizeus/OptiZeus-SCADA/
```

## 4. Post-install Configuration

### 4.1 License activation

1. Open Admin -> License Activation.
2. Copy the Hardware ID shown at the top of the page.
3. Email the Hardware ID to sales@optizeus.org (or purchase via the online shop, which will send a license key within minutes).
4. Paste the key into the "License Key" field and click Activate.
5. The page refreshes to show your tier, enabled features list, maintenance-until date, and an "Active" status indicator.

Without a key, the server runs in a 7-day trial with full Professional-tier access. After the trial, most actions are disabled until a valid key is provided.

### 4.2 HTTPS certificate (production)

The fresh install uses a self-signed certificate at backend\ssl\server.crt / server.key. For production, replace these with a CA-signed pair.

1. Obtain a certificate from your internal PKI (for air-gapped plants) or a public CA.
2. Copy the PEM-encoded certificate to backend\ssl\server.crt.
3. Copy the PEM-encoded private key to backend\ssl\server.key (permissions 600 on Linux).
4. If your CA uses an intermediate, concatenate cert + intermediates into server.crt in that order.
5. Restart the service. Clients on the business LAN should have your CA in their trust store.

**TIP:** Set the certificate expiration monitoring reminder. Silent expiration is the most common cause of

"client cannot connect" tickets - certs just stop working on the expiration day with no warning.

## 4.3 Users and roles

1. Admin -> Users -> + Add User.
2. Fill in username, full name, email. Pick a role: admin, operator, or viewer (or a custom role you defined earlier).
3. Set a strong initial password. Check "Require password change on first login".
4. Under Profile -> Security, enable MFA (TOTP) for every admin account. Use Google Authenticator, Authy, Microsoft Authenticator, 1Password, or any TOTP-compatible app.
5. Repeat for operators and viewers as needed.

## 4.4 Scheduled backups

Admin -> Backup & Restore -> Schedule. Pick:

- Daily at 02:00 (recommended for production) or weekly for light-use systems.
- Destination folder - local path, mapped network drive, or UNC path to a file server.
- Retention - default 30 days; older backups are automatically deleted.
- Encrypted ZIP - enable for backups that include audit-trail data subject to 21 CFR Part 11.

# 5. Connecting PLCs

## 5.1 Add a connection (general flow)

1. Configuration -> PLC Connections -> + Add Connection.
2. Choose the protocol from the dropdown.
3. Fill in the connection-specific fields.
4. Click "Test Connection". On success, the indicator turns green.
5. Save. Polling begins immediately if the connection is enabled.

## 5.2 OPC UA

| | |
|---|---|
| **Endpoint URL** | opc.tcp://plc.example.com:4840 |
| **Security policy** | None / Basic256Sha256 / Aes128_Sha256_RsaOaep / Aes256_Sha256_RsaPss |
| **Security mode** | None / Sign / SignAndEncrypt |
| **Authentication** | Anonymous / Username+password / Certificate |
| **Publishing interval** | ms between server-side sampling (default 500) |
| **Lifetime count** | Keep-alive multiplier (default 10) |

## 5.3 Modbus TCP

| | |
|---|---|
| **Host / IP** | 10.0.0.12 |
| **Port** | 502 (standard) |
| **Unit ID** | 1 (device address on the RTU bus bridged behind this gateway) |
| **Batch read** | Enable - groups contiguous register reads into one PDU |
| **Max registers per read** | 125 (Modbus spec hard limit) |
| **Word order** | Big-endian or little-endian (varies by PLC) |

## 5.4 Siemens S7

| | |
|---|---|
| **Model** | S7-1200 / S7-1500 / S7-300 / S7-400 |
| **IP address** | 192.168.0.1 |
| **Rack / Slot** | Typically 0/1 for S7-1200, 0/2 for S7-300/400 |
| **Batch read** | Always on - this is where S7 gets most of its throughput |
| **Optimization** | Non-optimized DBs (access via offset) are faster than optimized DBs |

Real-world benchmark: an S7-1200 CPU polls 800+ tags at 250 ms with a single connection when batch read is enabled and the tags are packed into one or two data blocks.

## 5.5 EtherNet/IP (Allen-Bradley)

| | |
|---|---|
| **Device** | ControlLogix / CompactLogix |
| **IP address** | 192.168.1.10 |
| **Slot** | 0 for PLC in chassis slot 0 |
| **Worker connections** | 1 to 4 - more = higher throughput but more sessions on the PLC |
| **Tag addressing** | Use PLC tag names directly (e.g. Tank1.Level) |

## 5.6 Import tags from the PLC

- OPC UA: Tags -> Import from OPC UA -> browse address space -> select -> Import. Hundreds of tags in one operation.
- Siemens S7: paste the DB structure from TIA Portal or import a CSV generated from the symbol table.
- Allen-Bradley: Logix 5000 projects export a CSV from Tools -> Export. OptiZeus can import that CSV directly.
- Manual: Tags -> + Add Tag -> fill in fields. Use this for virtual / calculated tags.

# 6. Multi-Server Topology

## 6.1 Roles

| | |
|---|---|
| **Standalone** | Single server running everything (default). |
| **Test** | Engineering changes happen here; read-only from PLCs unless you promote; auditable diffs against Production. |
| **Production** | Accepts deployments from Test; writes to PLCs; receives client connections. |
| **Backup** | Passive mirror of Production; takes over if Production is unreachable. |

## 6.2 Configure the role

Admin -> Multi-Server -> Role. Pick Test, Production, Backup, or Standalone. Point each Test / Backup node at the Production URL and provide a shared deployment secret.

## 6.3 Deploy changes Test -> Production

1. Configure everything on Test (tags, screens, alarms, recipes, users, scripts).
2. Admin -> Multi-Server -> Deploy. A diff summary appears showing what will change.
3. Review the diff. Tick "I have reviewed the changes" and click Deploy.
4. Production applies the deployment atomically. An audit-trail entry records who deployed what, when, and from which Test host.

## 6.4 Client auto-failover

Electron clients (and modern browsers via Service Worker) can be configured with a primary and backup server URL. If the primary becomes unreachable for longer than the configured grace period, the client automatically switches to the backup. A visible banner indicates failover mode so operators know where writes are going.

# 7. Security Hardening Checklist

Work through this list on every production server before the site goes live. Missing any one of these exposes the plant to preventable risk.

- [ ] Default admin password changed. The console-printed initial password is for commissioning only.
- [ ] MFA (TOTP) enabled on every admin account. MFA for operators recommended but not always practical.
- [ ] HTTPS certificate replaced with a CA-signed pair. Self-signed is acceptable only on air-gapped networks.
- [ ] HTTP port 3004 blocked at the firewall. Force HTTPS-only by firewalling.
- [ ] Session timeout <= 60 minutes of inactivity. Admin -> Security -> General.
- [ ] Password policy: minimum 8 characters, require upper + lower + digit + special.
- [ ] Audit-trail retention >= 1 year for regulated sites (pharma, food, medical).
- [ ] OIDC SSO or LDAP configured so users do not have a separate password on OptiZeus.
- [ ] Security Areas defined for sensitive setpoint tags and restricted screens.
- [ ] Daily backup scheduled to a separate physical disk or network share.
- [ ] Unused operating-system ports and services disabled (principle of least privilege).

> **COMPLIANCE:** For 21 CFR Part 11 (pharma / medical), also enable e-signatures for tag writes and alarm acknowledgments. See the companion 21 CFR Part 11 Implementation Guide PDF.

# 8. Troubleshooting

## 8.1 Service will not start

| Symptom | Cause / Fix |
|---|---|
| Port already in use | netstat -ano \| findstr :3004 - identify and stop the other process, or change OptiZeus port in server-config.json. |
| Corrupted database | Restore from backend\backups\ - newest backup first. |
| Expired license | Install a new key from Admin -> License Activation, or continue in trial mode. |
| Missing runtime files | Run REPAIR.bat to re-extract core files without touching data. |
| Antivirus quarantined files | Add install folder to AV exclusion list; run REPAIR.bat. |

## 8.2 Client cannot reach server

| | |
|---|---|
| Ping fails | Routing / firewall problem. Check ACLs between client and server subnets. |
| Ping works, browser refused | Service is down or wrong port. net start OptiZeus. Verify 3443 is open. |
| Cert error | Import server certificate into client trust store OR toggle "Accept self-signed" in client setup. |
| Proxy intercepts | Corporate proxy may be TLS-terminating. Add the server URL to the proxy bypass list. |

## 8.3 Slow tag updates

- Check PLC Connections -> Diagnostics. CPU pegged at 100% on the driver thread means too many tags per connection.
- For Modbus / S7: verify Batch Read is enabled. Without it, each tag read is a separate round-trip.
- For EtherNet/IP: raise "Worker connections" from 1 to 4 on high-tag-count PLCs.
- For OPC UA: raise "Publishing interval" if the PLC is sampling too fast.
- If the historian archive disk is > 85 % full, writes slow dramatically. Free up space or move archives to a larger disk.
- Verify the system clock is correct - if the client clock drifts > 5 minutes vs. server, JWT tokens fail silently.

## 8.4 Alarms not firing

- Verify the tag is in the right Alarm Area on its detail page.
- Check Admin -> Alarms -> Thresholds. If "delay on" is set, alarm fires only after value is out-of-range for N seconds.
- Check Security Areas - an Area with enforceWrites can silently block value changes the alarm engine expects.
- Check the alarm pipeline - if all recipients are outside their schedule, notifications are silently suppressed.

# 9. Uninstall + Reinstall

## 9.1 Clean uninstall (Windows)

1. net stop OptiZeus
2. Open the install folder, right-click UNINSTALL.bat -> Run as administrator.
3. UNINSTALL.bat removes the Windows service, deletes the Start Menu entries, and prompts before deleting the install folder. Say "No" if you want to keep the data.

## 9.2 Restore a backup

Put the backup ZIP next to INSTALL.bat before running it. The installer detects a pre-existing backup and offers to restore from it instead of starting fresh.

# 10. Support

For technical questions, feature requests, or bug reports, email support@optizeus.org with:

- Your Hardware ID (Admin -> License Activation).
- The version string (bottom of any page in the app).
- A description of the symptom and the steps to reproduce.
- The last 200 lines of backend\logs\service.log (redact any sensitive values first).

Active-maintenance customers receive priority support via a dedicated channel - details are in the welcome email sent when you enrolled.