# 1. Introduksjon

Dette dokumentet er en praktisk veiledning for brukere og driftsansvarlige som skal implementere, bruke og vedlikeholde løsningen for sikker kommunikasjon mellom WAGO CC100 PLS og Ignition SCADA ved hjelp av Tailscale VPN og OPC UA.

# 2. Forutsetninger

- WAGO CC100 med Linux-basert firmware  
- Tilgang til Tailscale-konto  
- Ignition SCADA installert  
- SSH-tilgang til PLS  
- Bash-skript for installasjon og oppdatering

# 3. Installere Tailscale på PLS

A screenshot of a computer

AI-generated content may be incorrect.1. Koble til PLS med SSH

Standard brukernavn og passord på wago pls

Brukernavn: root

Passord: wago

2. Kjør installasjonsskriptet `InstallTailscale.sh`  
3. Logg inn på Tailscale med enhetens auth-url (vises ved oppstart)  
4. Verifiser at enheten vises i Tailscale admin-panelet

# 4. Aktivere sikker kommunikasjon i OPC UA

1. Generer sertifikat i Codesys for OPC UA-serveren  
2. Legg til klientens sertifikat i PLSens ‘Trusted Certificates’  
3. Legg til PLSens sertifikat i klientens ‘Trusted Certificates’  
4. Verifiser at ‘Sign & Encrypt’ fungerer mellom SCADA og PLS

# 5. Oppdatere HTTPS-sertifikater automatisk

1. Kjør `update\_tailscale\_certificates.sh` på PLS  
2. Scriptet vil hente gyldig sertifikat fra Tailscale og plassere det riktig  
3. Webserveren (lighttpd) restartes med nytt sertifikat  
4. Test tilgang til https://<plsen>.tailnet-yourdomain.ts.net

# 6. Vedlikehold og overvåking

- Sjekk Tailscale dashboard for tilkoblingsstatus  
- Kjør `tailscale status` for lokal status  
- Verifiser gyldighet av sertifikater periodisk med `tailscale cert`

# 7. Feilsøking

- Hvis OPC UA-feil oppstår, dobbeltsjekk at sertifikater er riktig plassert  
- Ved manglende VPN-tilkobling, kjør `tailscale up` på nytt  
- Sjekk loggene i `/var/log/lighttpd/` for HTTPS-relaterte feil

# 8. Oppdatering av skript

Scriptene er utformet for enkel oppdatering. Endringer kan gjøres med en teksteditor, men husk å teste etter modifikasjoner.