# 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

Figur Innlogging til PLS

Standard brukernavn og passord på wago pls

Brukernavn: root

Passord: wago

2. Hent installasjonsskriptet

wget https://raw.githubusercontent.com/espenbo/Sikker-kommunikasjon-og-sertifikath-ndtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/InstallTailscale.sh

A black screen with white text

AI-generated content may be incorrect.

Figur Hente bash skript

3. Gjør skriptet kjørbart.

chmod 700 InstallTailscale.sh

A screenshot of a computer program

AI-generated content may be incorrect.

Figur 3 Forandre filen til å bli kjørbar

4. Kjør installasjonsskriptet `InstallTailscale.sh`

Figur Kjør installasjons skriptet

A screenshot of a computer

AI-generated content may be incorrect.

Figur 5 Skriptet finner riktig pakke som skal installeres eller oppdateres

5. Restart PLS

A screen shot of a computer

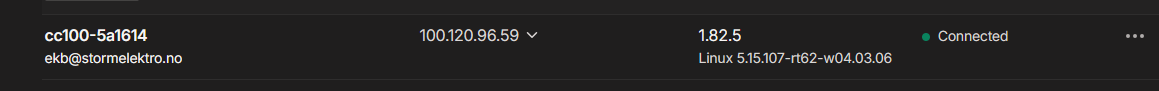
AI-generated content may be incorrect.  
6. Logg inn på PLSen og logg inn på Tailscale.

Figur Logg inn på Tailscale

tailscale login

5. Logg inn på Tailscale med enhetens auth-url (vises ved oppstart)

6. Verifiser at enheten vises i Tailscale admin-panelet

 Man kan også bruke status for og se alle enheter koblet til tailscale nettet.

Figur 7 PLSen vises nå i Tailscale

tailscale status

A screen shot of a computer

AI-generated content may be incorrect.7. Ping en annen enhet.

Figur 8 Ping en annen enhet på nettverket

# 4. Aktivere sikker kommunikasjon i OPC UA

*Man kan bruke OPC UA uten og bruke sikkerhets sertifikater. Når PLSen er koblet til Tailscale nettverket vil all trafikk som går igjennom dette nettet være kryptert. Men kommunikasjon som ikke går over Tailscale nettverket vil ikke være kryptert.*

A screenshot of a login page

AI-generated content may be incorrect.1. Logg inn på nettsiden til PLSen

Figur Innlogging nettsiden til PLS

Brukernavn: admin

Passord: wago

3. Velg Fieldbus

A screenshot of a computer

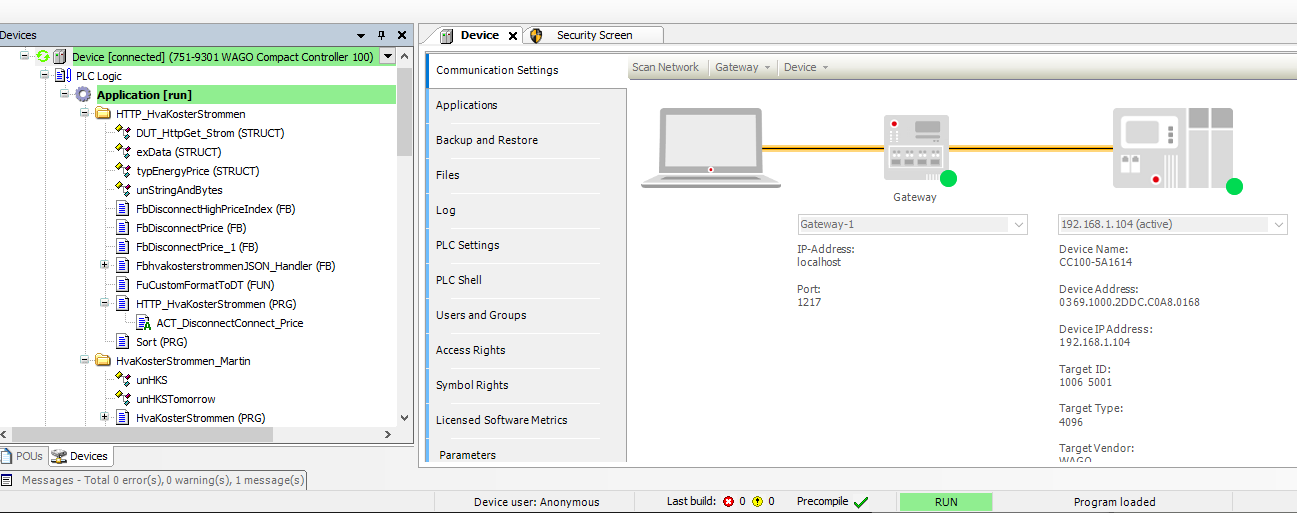
AI-generated content may be incorrect.

Figur Velg Fieldbus

A screenshot of a computer

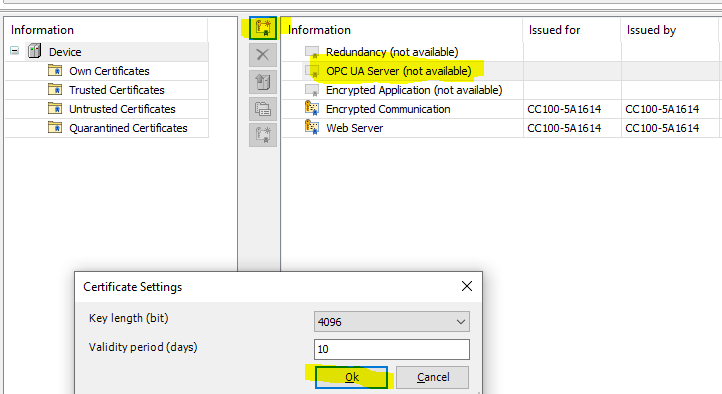
AI-generated content may be incorrect.4. Velg hvilken sikkerhetsfunksjoner som skal være minimum på PLSen og pass på at OPC UA er ‘Enable’

Figur 11 Oppsett av OPC UA server i PLSen

5. Koble seg til PLSen

Figur Koble seg til PLS

6. Generer sertifikat i Codesys for OPC UA-serveren



Figur 13 Oppsett av sikkerhets sertifikat til PLSen i Codesys 3.5

7. Hent ut sertifikatet som du lagde, slik at det kan legges inn på klienten. uaExpert eller Ignition.

A screenshot of a computer

AI-generated content may be incorrect.

Figur Hent ut sertifikat

A screenshot of a computer

AI-generated content may be incorrect.8. Legg til klientens sertifikat i PLSens ‘Trusted Certificates’

Figur 15 Legg sertifikater fra klienter i Trusted

A screenshot of a computer

AI-generated content may be incorrect.9. Legg til PLSens sertifikat i klientens ‘Trusted Certificates’

Figur Last opp sertifikat til Ignition server

10. Verifiser at ‘Sign & Encrypt’ fungerer mellom SCADA og PLS



Figur 17 Status på kommunikasjon til Ignition server

# 5. Oppdatere HTTPS-sertifikater automatisk

A screenshot of a computer

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

Figur Innlogging til PLS

Standard brukernavn og passord på wago pls

Brukernavn: root

Passord: wago

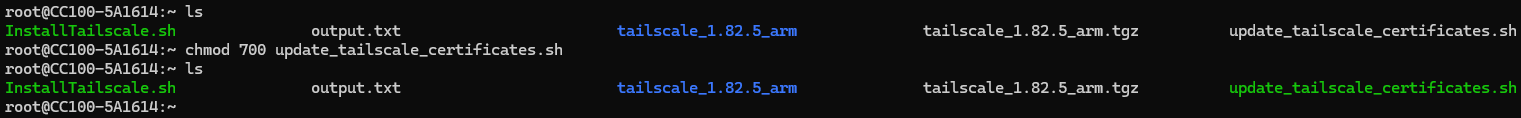
2. Hent installasjonsskriptet

wget https://raw.githubusercontent.com/espenbo/Sikker-kommunikasjon-og-sertifikath-ndtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/update\_tailscale\_certificates.sh

A computer screen with white text

AI-generated content may be incorrect.

Figur Hente update\_tailscale\_certificates.sh

3. Gjør skriptet kjørbart

Figur Gjør skriptet kjørbart

chmod 700 update\_tailscale\_certificates.sh

4. Kjør `update\_tailscale\_certificates.sh` på PLS

A black screen with white text

AI-generated content may be incorrect../update\_tailscale\_certificates.sh

Figur 21 Hente sertifikater eller oppdatere dem

5. Scriptet vil hente gyldig sertifikat fra Tailscale og plassere det riktig  
6. Webserveren (lighttpd) restartes med nytt sertifikat

7. Test tilgang til https://<plsen>.tailnet-yourdomain.ts.net

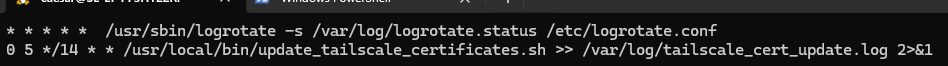
A screenshot of a computer

AI-generated content may be incorrect.

Figur 22 Test at sikkerhetssertifikatene fungerer. Husk man må være koblet til Tailscale nettverket

8. Legg til automatisk oppdatering av sertifikater i crontab

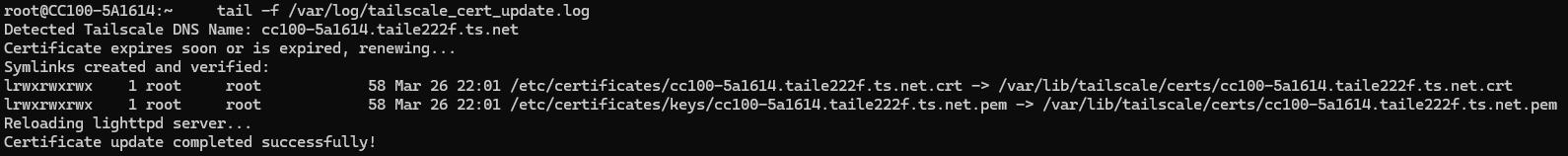
crontab -e



Figur Oppsett av cron

Sjekk logg med

tail -f /var/log/tailscale\_cert\_update.log



Figur 24 Sjekk logg for https sertifikater

# 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

- Sjekk ‘/var/log/tailscale\_cert\_update.log’

# 8. Oppdatering av skript

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