

TECHNICAL DATA SHEET

SYNGUARDIN VAATIMUKSET

V3.08 - 3/03/2025

ALWAYS WITH YOU

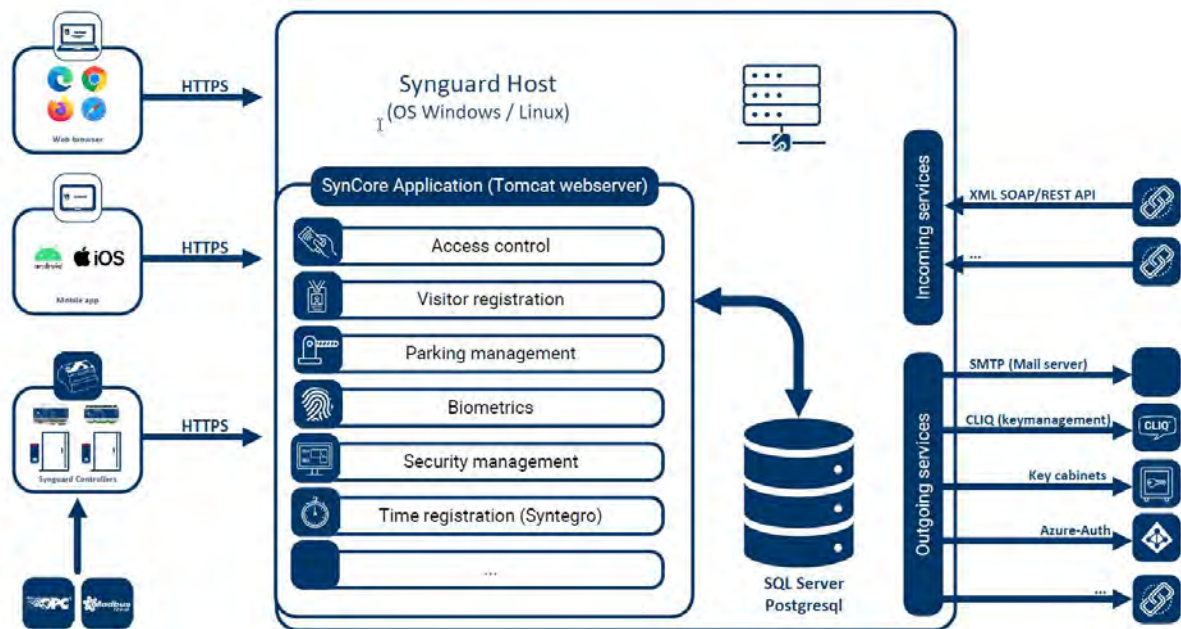


SYNGUARD

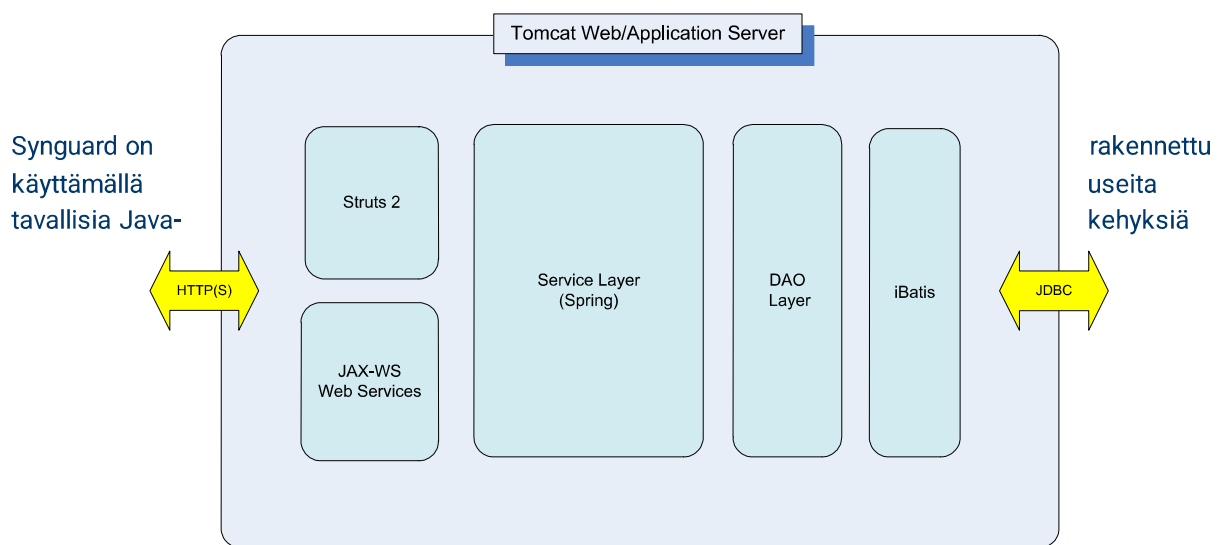
Synguardin vaatimukset	1
1. Yleistä	3
2. Synguard: ohjelmistorakenne	3
3. Tuetut käyttöjärjestelmät (uudet asennukset)	4
4. Laitteistovaatimukset	4
5. Asennus virtuaalialustalle	4
6. Tuetut Tietokannat	4
7. Synguardin asennus palvelimelle	5
8. Turvallisuus	5
9. Etäkirjautuminen tukitarkoituksessa	5

1. YLEISTÄ

Synguard koostuu pääasiassa Java-pohjaisesta Tomcat-sovellus- ja verkkopalvelinympäristöstä. Tämä ympäristö toimii palveluprosessina Windows- tai Linux-isäntäkoneessa ja tarjoaa kaikki tarvittavat toiminnot. Näihin toimintoihin kuuluvat kulunvalvontatietojen täydellinen käsittely sekä kommunikointi kulunvalvontaverkon, käyttäjien (verkkoselaimen kautta), tietokannan sekä ulkoisten palvelimien kanssa (esim. sähköpostipalvelin, LDAPS/AD-palvelin jne.), ...



2. SYNGUARD: OHJELMISTORAKENNE



(Struts/Spring/iBatis).

3. TUETUT KÄYTTÖJÄRJESTELMÄT (UUDET ASENNUKSET)

Alla luetellut käyttöjärjestelmät ovat kaikki 64-bittisiä.

- MS Windows Server 2022
- MS Windows 11 (pienempiin asennuksiin)
- Linux RedHat EL / AlmaLinux / RockyLinux v8.x ja v9.x

4. LAITTEISTOVAATIMUKSET

Alla luetellut vaatimukset ovat minimivaatimuksia. Ne voivat olla parempia järjestelmän koosta riippuen.

- Kulunvalvontajärjestelmä => vähintään 2-ytiminen prosessori - vähintään 4 Gt RAM-muistia
- Suorittimen tulee olla suorituskypinen, pöytäkone-/palvelintaso, ei pienitehoista/heikon suorituskypyn prosessoria.
- Järjestelmä, jossa on vähintään 40 Gt vapaata levytilaa

5. ASENNUS VIRTUAALIALUSTALLE

Synguard voidaan asentaa käyttöjärjestelmään joka toimii joko fyysisellä laitteistolla tai virtuaaliympäristössä.

Esimerkiksi seuraavat virtuaalialustat ovat tuettuja:

- VMware ESXi
- Microsoft Hyper-V
- Linux KVM

6. TUETUT TIETOKANNAT

- PostgreSQL 14.x tai uudempi (vakiotoimitus)
- MS SQL Server 2022
- MS SQL Server Express 2022 (pienille asennuksille)

7. SYNGUARDIN ASENNUS PALVELIMELLE

Synguardin asennukseen palvelimelle sisältyy:

- Tietokantaohjelmiston asennus (ei välttämätön, jos käytetään ulkoista tietokantaa)
- Amazon Corett Java JDK:n asennus
- Käyttöohjelmiston asennus:
 - Windows: Esimerkiksi kohdassa C:\Syntegro\Syntegro + Apache Tomcat - verkkopalvelimen rekisteröinti Windows-palveluksi
 - Linux: Esim. /opt/Syntegro/Syntegro + Apache Tomcat -verkkopalvelimen rekisteröinti palveluna.
- Ainoa prosessi, joka toimii (tietokannan ulkopuolella), on Apache Tomcat -verkkopalvelin (Java-pohjainen).
 - Kaikki portit, joita tämä prosessi kuuntelee, voidaan määrittää uudelleen, jotta vältetään mahdolliset ristiriidat olemassa olevien sovellusten (esim. IIS) kanssa.
- Muistin käyttö Tomcat-sovelluspalvelin: tyypillisesti 1,5 Gt
- Muistin käyttötietokanta: tyypillisesti 1 Gt
- Levyn kapasiteetti:
 - 2 Gt (ohjelmisto + työtila)
 - ± 3 Mt/työntekijä/vuosi (riippuu suuresti parametroinnista/halutusta toiminnallisuudesta järjestelmässä)
 - Mahdollista lisätilaa väliaikaisille paikallisille tietokannan varmuuskopioille.
- Suorituskyky
 - Sovellus on pääosin tietokantalähtöinen. Nopeat levyt + tietokantavälimuisti vaikuttavat aina positiivisesti suorituskykyyn.

8. TURVALLISUUS

- **Verkkoselaimen viestintä:** Verkkoselaimen ja palvelimen välinen viestintä käyttää https:ää (SSL/TLS-salaus).
- **Kulunvalvontaverkon viestintä:** SynAppien/SynTimen ja palvelimen välinen viestintä on myös salattu ja suojattu SSL-asiakastodennuksella.

9. ETÄKIRJAUTUMINEN TUKITARKOITUKSESSA

Sovelluksen kirjautuminen voidaan tehdä suojatun HTTPS-Internet-yhteyden kautta (oletuksena Synguard-palvelimen https-porttiin 8443).

Jos haluat tarkempaa tukea/päivityksiä/jne., on parasta ottaa käyttöön suora kirjautuminen palvelimelle. Tämä voidaan tehdä käyttämällä vakioprotokollia, kuten esimerkiksi:

- Windows: Microsoft Terminal Services (RDP-protokolla) + mahdollisuus siirtää tiedostoja (päivityksiä varten).
- Linux: Secure Shell-käyttö (SSH-protokolla)



Portinohjaus asiakkaan palomuurissa palvelimen sisäiseen RDP/SSH-porttiin tai mahdollisesti suora pääsy (väliaikaisen) VPN-yhteyden kautta on välttämätöntä.

- Muut vaihtoehdot, kuten TeamViewer, ovat mahdollisia.