

VALMISTELUT CSI MOBILEN KÄYTTÖÖNOTTOON

OnPremise-asiakkaat

Mikäli CSI-ohjelmistoa käytetään OnPremise-versiona, jolloin ohjelmiston tietokanta on asiakkaan omalla palvelimella, CSI Mobilen käyttöönottoon vaaditaan seuraavat valmistelut:

Kaikilta asiakkailta vaaditut CSI-ohjelmistoa koskevat valmistelut

1. **CSI-ohjelmiston vähimmäisversio;** Varmista, että toimiston CSI-ohjelmiston versio on vähintään 12.1 (kesäkuulta 2025) tai uudempi.
2. **CSI-ohjelmiston tietokannan eheys:** Pyydä CSI:tä korjaamaan veloituksetta mahdolliset tietokannan datan eheyteen liittyvät vierasavainvirheet.
3. **Käyttäjien sähköpostiosoitteet CSI-ohjelmistossa:** Varmista, että kaikkien aktiivisten CSI-käyttäjien käyttäjätietoihin on lisätty sähköpostiosoite. Käyttäjät kutsutaan CSI Mobile -käyttäjiksi lähettämällä kutsu CSI-ohjelmistoon määritettyyn sähköpostiosoitteeseen.

HUOM! Jos CSI-ohjelmistossa on kustomoituja kenttiä tai lisäosia, jotka esim. asettavat tietyn kentän pakolliseksi, CSI API ei vielä pysty käsittelemään niitä eivätkä kustomoinnit ole käytettävissä CSI Mobilessa.

OnPremise-asiakkailta vaaditut järjestelmäympäristöä koskevat valmistelut

1. Luo CSI APIa varten uusi SQL Login

- Varmista, että SQL Serverissä on käytössä Mixed Mode -autentikointi, joka mahdollistaa sekä Windows- että SQL Server -autentikoinnin, kuten myös ns. Contained Database -käyttäjät.
- CSI API vaatii SQL Server -tunnuksen, jolla on db_owner-oikeudet CSI-tietokantaan.

2. Varmista, että toimistonne SQL Server-versio on tuettu CSI API:ssa

- CSI API:n tukema vähimmäisversio SQL Serveristä on SQL Server 2016 R2.
- Jos CSI-tietokanta on sitä vanhemmassa SQL-versiossa, päivitä SQL-palvelin uusimpaan SQL Server -versioon.

3. Varmista SQL-palvelimen tietoturva (käytäntöjä koskevat suositukset)

- Edellytä monimutkaisia salasanoja.
- Rajoita pääsyä tietokantaan; Palomuurin läpi tulisi sallia liikenne vain CSI:n Azure-IP-osoitteisiin.
- Tarkista säännöllisesti suojausasetukset; Käy ajoittain läpi SQL Serverin suojausmääritykset riskien tunnistamiseksi ja vähentämiseksi.
- Harkitse pakotetun salauksen käyttöönottoa SQL Serverissä; Tutustu Microsoftin dokumentaatioon aiheesta, jos koet sen tarpeelliseksi.

4. Salli verkkoyhteys konfiguroimalla palomuuuri tai käyttämällä Azure-välityspalvelua (Relay)

Mahdollistaaksesi turvallisen yhteyden tietokantasi ja CSI:n infrastruktuurin välillä määritä palomuuuri sallimaan **TCP-liikenne** SQL Serveriltäsi seuraavaan IP-osoitteeseen:

- Tuotantoympäristö: 20.240.1.102
- Porttisuositus: Tietoturvan parantamiseksi määritä liikenne kulkemaan muun kuin oletusportin 1433 kautta, esimerkiksi portin 2525 kautta.

Azure-välityspalvelun määrittämisestä löytyy erillinen dokumentti.

5. Toimita CSI:lle tarvittavat tiedot

- CSI-tietokannan nimi
- SQL loginin tiedot (nimi ja salasana). HUOM! Turvallisuussyistä lähetä SQL-loginin salasana suoraan CSI:n edustajalle suojatulla sähköpostilla tai tekstiviestillä.
- Administraattoriksi nimetyn pääkäyttäjän koko nimi ja sähköpostiosoite
- Ulkoinen IP-osoite ja palomuurista avattu TCP-portti (jos tietokantayhteys toteutetaan palomuurikonfiguroinnilla) TAI
- SQL-palvelimen pitkä nimi (jos yhteys toteutetaan Azure-välityspalvelulla).

HUOM! CSI:n API-infrastruktuuri toimii Microsoft Azuressa ja on rakennettu noudattamaan alan standardien mukaisia tietoturvakäytäntöjä. Tietokannan käyttöoikeus on tiukasti rajattu CSI:n Azure-ympäristöön – ulkoinen tai julkinen pääsy ei ole sallittu. Kaikki liikenne on todennettua ja salattua.