ATT TA I BRUK CSI MOBILE

OnPremise-kunder

Om CSI-programvaran används som en OnPremise, där programmets databas finns på kundens egen server, krävs följande förberedelser för att ta CSI Mobile i bruk:

För alla kunder - förutsättningar relaterade till CSI-programvaran

1. **Minimiversion:** Säkerställ att din CSI-programvara har version 12.1 från juni 2025 eller nyare.
2. **Databasens integritet:** Be CSI-teamet att kostnadsfritt korrigera eventuella problem med dataintegritet (foreign key-fel) i din CSI-databas.
3. **Konfiguration av användarens e-post**: Kontrollera att alla aktiva CSI-användare har sina e-postadresser tillagda i användarinformationen i CSI-programvaran. CSI API-åtkomst beviljas via företagsautentisering, och alla användarinbjudningar skickas till den e-postadress som är definierad i CSI-programvaran.

OBS! Om du har anpassade fält eller plugins (som t.ex. gör fält obligatoriska) i din CSI-programvara, kan CSI API inte hantera dem.

Förutsättningar för OnPremise-kunder relaterade till systemmiljö

1. **Skapa en ny SQL-inloggning för CSI API**
    - Säkerställ att Mixed Mode Authentication är aktiverat på din SQL Server. Detta möjliggör användning av både Windows- och SQL Server-autentisering, inklusive stöd för contained database users.
    - CSI API kräver SQL Server-uppgifter med db_owner-behörighet på CSI Lawyer-databasen.
2. **Uppgradera till SQL Server-version som stöder CSI API**
    - Den lägsta version som stöds av CSI API är SQL Server 2016 R2. Om din CSI-databas körs på en äldre version, uppgradera till den senaste SQL Server-versionen.
3. **Säkerställ din SQL Servers säkerhet** (rekommendationer)
    - Kräv komplexa lösenord.
    - Begränsa databasåtkomst; endast CSI:s Azure-IP-adresser ska tillåtas genom din brandvägg.
    - Granska säkerhetsinställningar regelbundet; gör periodiska revisioner av din SQL Servers säkerhetskonfiguration för att identifiera och åtgärda risker.
    - Överväg att aktivera kryptering på SQL Server; se Microsofts dokumentation om detta om du anser det nödvändigt.
4. **Tillåt nätverksanslutning genom att konfigurera brandväggen eller använda Azure Relay.**

För att tillåta säker anslutning mellan din databas och CSI-infrastrukturen, konfigurera din brandvägg för att tillåta inkommande och utgående **TCP-trafik** från din SQL Server till följande IP-adress:

- Produktionsmiljö: 20.240.1.102
- Rekommenderad port: Av säkerhetsskäl, tillåt trafik på en icke-standardport (t.ex. 2525) istället för standardporten 1433.

Det finns ett separat dokument med anvisningar för hur Azure-reläet ska konfigureras.

5. **Tillhandahåll CSI den nödvändiga informationen**

    - Namn på CSI-databas
    - SQL-inloggningsuppgifter (användarnamn och lösenord med db_owner-behörighet). Obs! Av säkerhetsskäl, skicka SQL-användarens lösenord till CSI via säker e-post eller via SMS.
    - Fullständigt namn och e-postadress för utsedd admin.
    - Extern IP-adress och den specifika TCP-port som öppnats i brandväggen (om databasanslutningen görs via brandväggskonfiguration) ELLER
    - SQL-serverns fullständiga namn (om anslutningen görs via Azure Relay).

Säkerhetsnotering: CSI API-infrastrukturen är värd i Microsoft Azure och byggd för att följa branschstandarder för säkerhet. Databasåtkomst är strikt begränsad till vår CSI Azure-miljö – ingen extern eller offentlig åtkomst är tillåten. All trafik är autentiserad och krypterad.