GETTING READY TO DEPLOY CSI MOBILE

OnPremise Customers

If the CSI software is used as the OnPremise version, meaning the software database is located on the customer's own server, the following preparations are required for enabling CSI Mobile:

Prerequisites related to the CSI software – for all customers

1. **Minimum Version:** Ensure your CSI software has the 12.1 version from June 2025 or newer.
2. **Database integrity:** Ask the CSI team to correct (for free) any data integrity issues (foreign key errors) in your CSI database.
3. **User Email Configuration:** Please ensure that all active CSI users have their email addresses added to their user information in the CSI software. CSI API access is granted via enterprise authentication, and all user invitations are sent to user's email defined in the CSI software

Note! In case you have customized fields or plugins (which may e.g. set fields as mandatory) in your CSI software, CSI API is not able to handle them.

Prerequisites for OnPremise customers

1. **Create a new SQL Login for the CSI API**
   - Ensure that Mixed Mode Authentication is enabled on your SQL Server. This allows the use of both Windows and SQL Server authentication, including support for Contained Database users.
   - The CSI API requires SQL Server credentials with **db_owner** permissions on the CSI Lawyer database.

2. **Upgrade to the SQL Server version that supports CSI API**

   The minimum supported SQL server version by CSI API is SQL Server 2016 R2. If your CSI database is running on lower SQL version, please upgrade your SQL server to latest SQL Server version.

3. **Ensure your SQL Server's security** (recommendations)
   - Require complex passwords.
   - Limit Database Access; Only CSI's Azure IP addresses should be allowed through your firewall.
   - Regularly Review Security Settings; Periodically audit your SQL Server security configuration to identify and mitigate any risks.
   - Consider Enforced Encryption on SQL Server; Get familiar with the Microsoft documentation on this topic if you find this necessary.

4. **Enable network access by configuring your firewall or using Azure Relay service**

   To allow secure connectivity between your database and the CSI infrastructure, please configure your firewall to allow **inbound and outbound TCP traffic** from your SQL Server to the following IP address:

   - Production Environment: 20.240.1.102
   - Recommended Port: For security reasons, allow traffic on a non-standard port (e.g. 2525) instead of the default 1433.

   To configure the Azure Relay service, see a separate document.

5. **Provide CSI with the required information**

   - Name of your CSI database
   - SQL login credentials (username and password with db_owner access). Note! For security reasons, send the SQL user's password directly to CSI's representative by a secure email or by text message.
   - Designated power user's full name and email address
   - Your external IP address and the specific TCP port to be opened OR
   - The full name of the SQL server (if using Azure Relay service)

Security Note: The CSI API infrastructure is hosted in Microsoft Azure and built to follow industry-standard security practices. Database access is strictly restricted to our CSI Azure environment - no external or public access is permitted. All traffic is authenticated and encrypted.

CSI Mobile activation steps

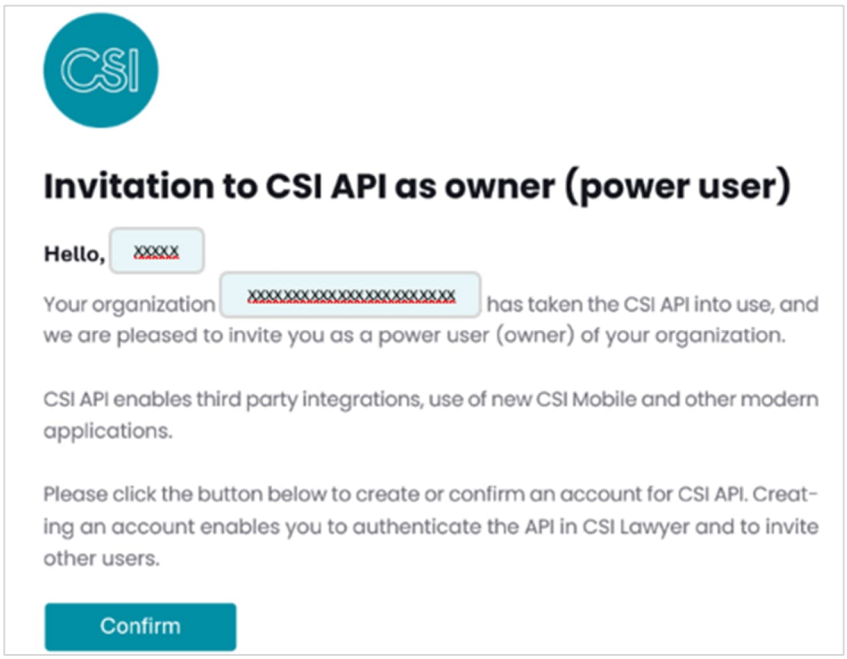
Once all the prerequisites related to the software and your system environment are fulfilled, the deployment of CSI API and CSI Mobile will proceed step by step as follows:

Activation actions required from the power user

CSI will start the process by installing the CSI API for your organization/database.

After that, you as a power user need to take the following steps to finish the API deployment, to get CSI Mobile into your own use and to be able to invite your colleagues to use CSI Mobile.

1. Account Onboarding to CSI API

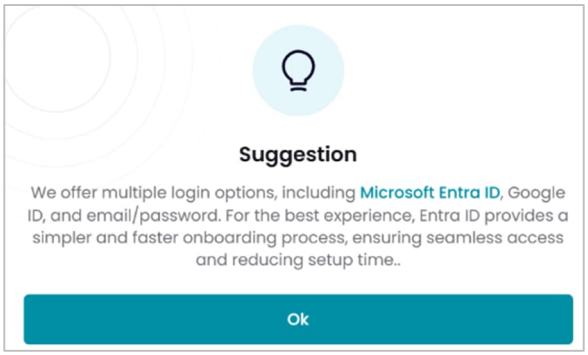


You will receive a welcome email from no-reply@csihelsinki.app, asking you to confirm your account for CSI API.

Note that the email may end in your Junk E-mail folder. In that case, right-click the email message and select Block > Never Block Sender's Domain to get the next messages to your Inbox.

Click on Confirm.

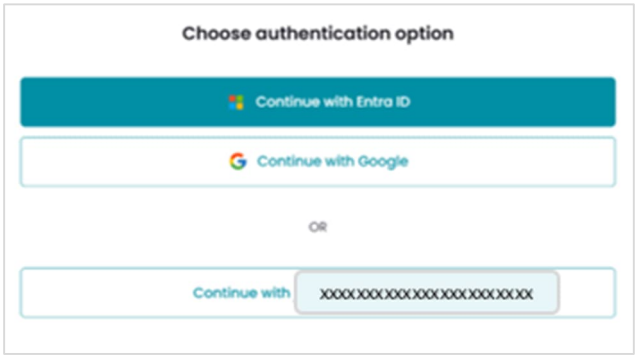
The Confirm button directs you to a web page which recommends Entra ID authentication.



If possible, choose that option and authenticate to Entra ID as usual.

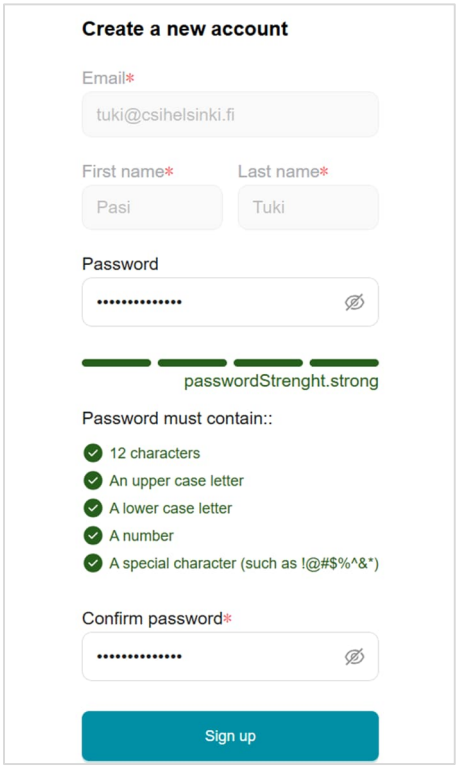
In case you authenticate with Entra ID or Google ID, you will be redirected to Entra ID or Google authentication pages.

Otherwise, you can authenticate with an email and password combination.

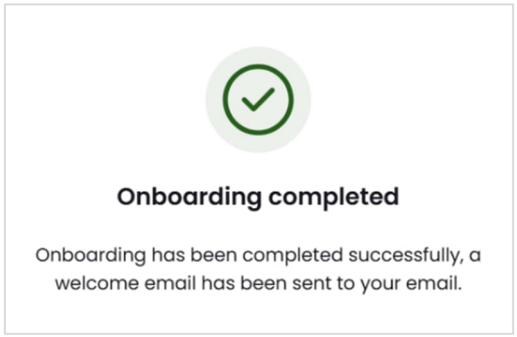


In that case, your password must be at least 12 characters long and contain at least one

special character.



Once you have successfully authenticated, you'll receive confirmation of a completed onboarding.

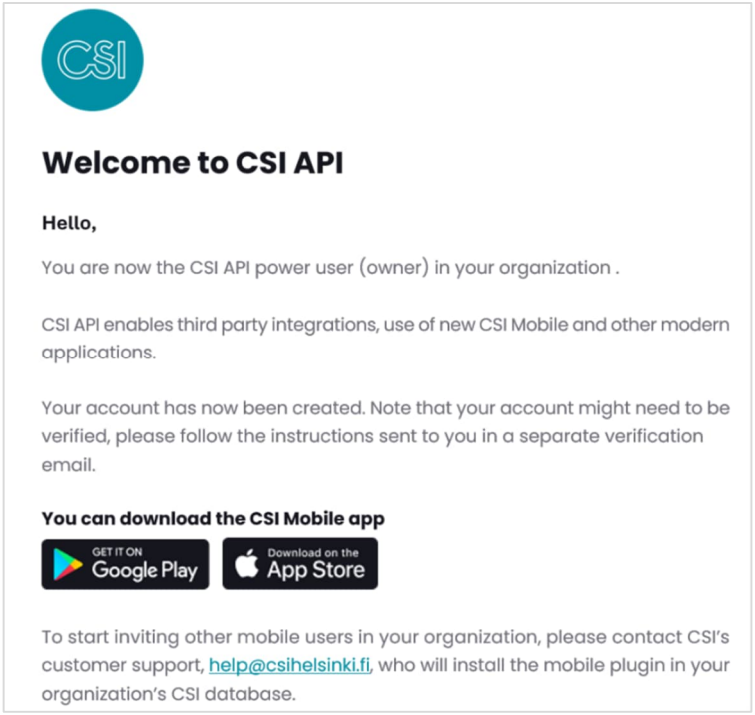


Next, you receive an email confirming that you are the CSI API power user in your organization.

If you used email to authenticate, you'll receive another email asking you to verify your email account,

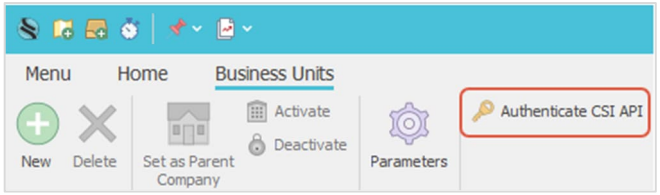
You can now download the CSI Mobile app to your mobile device and start using it.

If you wish to invite other users to use CSI Mobile, please ask the CSI support to install to your CSI database a plugin that enables it.

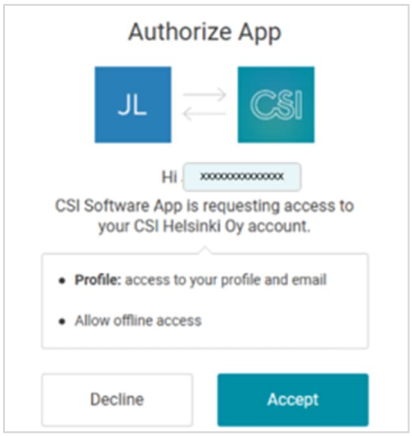


2. Authenticating the API in the CSI software

This step is necessary to enable user invitations, notifications etc.



- Log in to the CSI software.
- Go to the Settings > Business Units.
- On the ribbon, click on “Authenticate CSI API”.

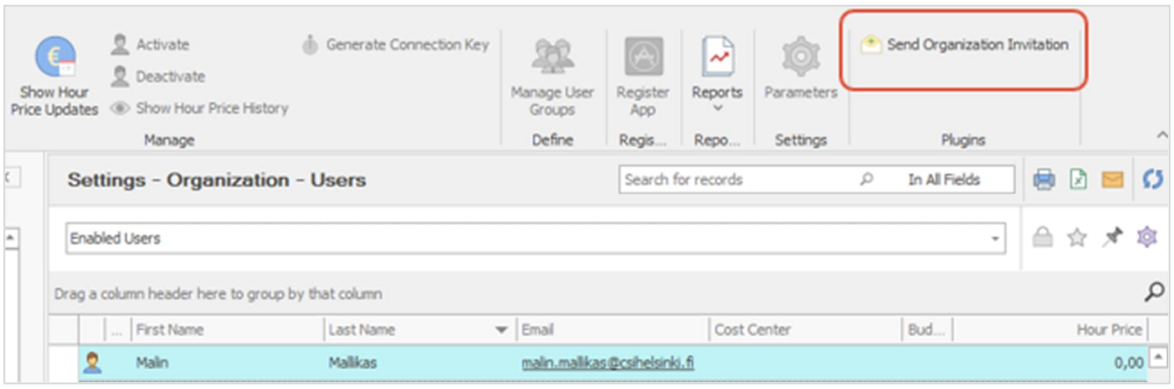


- You are directed to the verification page where you should use the same credentials as in the Account Onboarding step.
- Now, authorize the CSI Software App to have access to your CSI database.

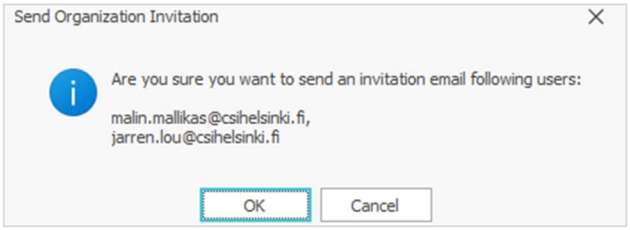
3. Inviting other users to CSI API

Now you can start to invite other users to CSI API to take CSI Mobile into use.

- In the Settings of the CSI software > Users, choose the users you wish to invite and click Send Organization Invitation on the ribbon.



- Verify the users and accept the confirmation.
- The invited users will receive welcome emails and need to take the same onboarding steps as you did.



- Once done, users can download CSI Mobile from their app store and authenticate to login with their Microsoft or Google authenticator.