Server Requirements and On-Premise Installation

- Network Requirements
- Installation

Network Requirements

How it is deployed

Three components, delivered as Docker container images and run with Docker Compose on a single Linux server. The database can instead be pointed at an existing Database cluster if you already operate one.

Network Requirements

Traffic	Port	Notes
Users → application	TCP 443 (HTTPS)	The only port that needs to be reachable by your staff
Internal, host only	TCP 3000, 8066, 1521	Between the containers; not exposed outside the server
Application → database	TCP 1521	Only if the database runs on a separate host
Outbound internet	none required	Images can be delivered as files — the installation works air-gapped

Users need a current desktop browser and a DNS name pointing at the server, matching the TLS certificate. Two-factor authentication uses a standard authenticator app on the user's phone; no SMS gateway is required.

Installation

1. **Prepare the server**.
   Provision the Linux host per the table above, install Docker Engine and the Compose plugin, set the time zone, and create the DNS record and TLS certificate for your reporting hostname.

2. **Prepare the database.**
   Either let the delivered Compose stack run Oracle on the same host, or create an empty database and a dedicated user on your existing cluster. No schema work is needed — the application creates and migrates its own schema.

3. **Receive the delivery package.**
   Fintecor supplies the two container images, a docker-compose.yml and a configuration template, either as files for an air-gapped install or from a private registry. The web application image is built for your specific reporting hostname, so confirm that URL to us before delivery.

4. **Load the images.**

   ```
   docker load -i fintecorreporting-backend.tar
   docker load -i fintecorreporting-frontend.tar
   ```

5. **Fill in the configuration file.**
   Database URL, user and password; the browser origin allowed to call the API; the encryption key protecting two-factor secrets; etc.

6. **Start the stack.**

   ```
   docker compose up -d
   ```

   On first start the service creates its database schema and loads the supervisory glossary and the EBA / EGDQ validation rule set. *This takes a few minutes and happens only once.*

7. **Verify.**
   All containers report healthy and the service answers its health check:

   ```
   docker compose ps
   curl http://localhost:8066/actuator/health
   ```

8. **Publish it.**
   Point your reverse proxy at the two internal services over HTTPS on port 443 and restrict access to your corporate network or VPN.

9. **Go live.**
   Log in with the administrator account supplied by Fintecor, change its password, enrol two-factor authentication, create your users and import your first reporting set.

10. **Set up backups.**
    A nightly database dump plus the mapping-file volume is sufficient to restore the whole installation. Fintecor provides the exact commands.

Upgrades and Support

An upgrade is a new image plus a restart of one container; the schema migrates itself, and any release rolls back to the previous image in seconds. Template and validation-rule updates that follow regulatory changes are delivered the similar way, as part of your subscription.