

OperatorView: notes for your IT company

A dental practice you look after is setting up OperatorView, the live board and in-office messaging for its PCs. This page lists what it installs, what it needs from the network, and where its data lives.

What gets installed

- The server: a Windows service named OperatorView, installed to C:\Program Files\OperatorView, on 64-bit Windows. Put it on the computer that runs the Open Dental server if you can. It must stay on: keep it from sleeping and give it a DHCP reservation.
- The office app: OperatorView App, installed for all users to C:\Program Files\OperatorView App, on each PC that shows the Board: the front desk, each operator and the admin PC.
- On a fresh install, the server installer warns when the computer does not look like the Open Dental server (no eConnector, MySQL or MariaDB service). It offers Cancel, or continuing anyway.
- Both installers are digitally signed.

Firewall rules the installers add

- All three are inbound allow rules, for every network profile, tied to OperatorView's own program. No outbound rules are added.
- OperatorView Board, on the server: TCP 5001, local subnet only. Office PCs on another subnet, such as a routed VLAN or a VPN, need a rule you add.
- OperatorView Discovery, on the server: UDP 5353 (mDNS), local subnet only.
- OperatorView App discovery, on each office PC: UDP 5353 (mDNS), local subnet only.

Open Dental

- OperatorView reads Open Dental through its official API and the practice's eConnector, with a key the practice adds in Open Dental. It is read-only.
- The one thing it writes is its own API subscriptions: registrations that send Open Dental's live updates to this server. Uninstalling the server removes them.
- The one-time eConnector step is done in Open Dental, run as administrator. Setup checks for that and waits until it is.

Uninstalling

- The server removes its service, its firewall rules, its scheduled update tasks and its program files. It asks whether to delete its data too, unchecked by default: the database, its key, the backups and the settings, in C:\Program Files\OperatorView\app\data. A silent uninstall always keeps the data. Delete that folder when the computer is retired.
- The office app removes its firewall rule and its downloaded updates, and asks whether to delete its pairing with the server.

Questions: support@operatorview.com. We reply within one business day.

Windows administrator approval

- The server asks once, when it is installed. Its updates install themselves as SYSTEM through a scheduled task, outside office hours, with no prompt.
- The Server Manager runs as administrator, so it asks each time it is opened.
- The office app asks when it is installed and at every update. On a PC where staff are standard users, an administrator approves each update.

Network

- Office PCs reach the server over HTTPS on port 5001, at the practice's own name under `ov.operatorview.com`, with a publicly trusted certificate for that one name. Its private key is made on the server and never leaves it. TLS 1.2 or later. An IP address will not work.
- That name points to the server's private address. If your router blocks DNS answers that point to a private address (DNS rebinding protection), allow `ov.operatorview.com`, or add a hosts-file line on each PC, such as `192.168.1.20 yourname.ov.operatorview.com`. A hosts line needs the DHCP reservation.
- Open Dental's API service sends live updates to the server on port 5001, over the office network.
- Outbound, HTTPS on port 443 only. The server reaches `operatorview.com` (license, certificate, updates), `api.operatorview.com` (the AI features and report emails) and `api.opendental.com` (Open Dental). Office PCs reach `operatorview.com` for app updates.
- OperatorView has no proxy setting, and a proxy that intercepts HTTPS shows as an error when the server connects to Open Dental.

Where the data lives

- On the server, in an encrypted database (SQLCipher, AES-256), with its key sealed to that computer by Windows DPAPI. The data folder is open only to SYSTEM and Administrators, and the service runs as LocalSystem.
- Nightly encrypted backups on the server's own disk, 7 daily and 4 weekly by default, with an optional second copy to another local drive or a USB stick. Network shares are refused. A backup opens on another computer only with the practice's recovery key.
- Patient details read from Open Dental are kept in that encrypted database and stay in the office, except for a question someone asks the AI assistant: it goes, with what it needs to answer, to OperatorView's own AI service on Amazon Web Services, under a Business Associate Agreement. Report emails carry practice totals only.
- The practice signs a Business Associate Agreement with OperatorView.