The NDPro Concept

For technicians: the recommended architecture for the professional and secure operation of NDPro.

planspur netdesign gmbh



How NDPro works.

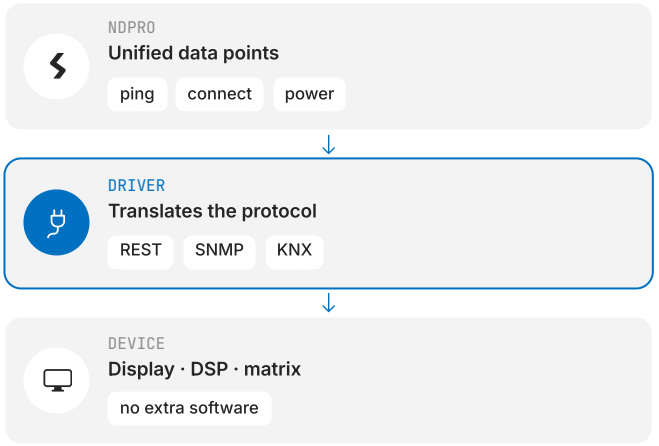
NDPro is a Node.js server in your network. Drivers talk to the devices directly, one shared data model feeds the interfaces and services.

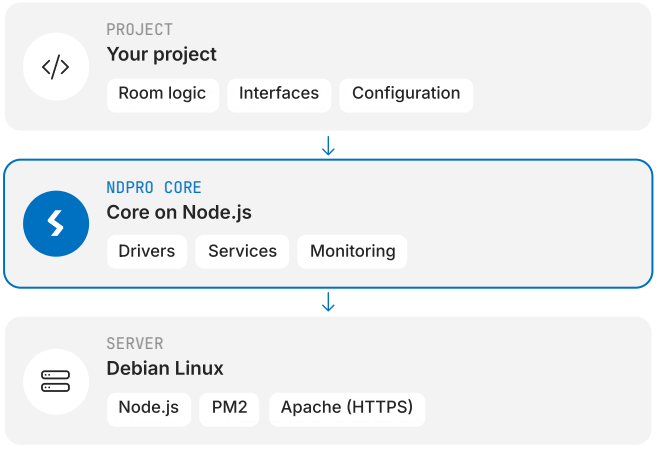
- One server, many vendors
- Unified state per device
- Interfaces in the browser (HTML5)

Devices connected directly.

Each driver speaks the vendor protocol and translates it into unified data points. No software is installed on the devices themselves.

- REST, TCP/IP, WebSocket, SSH
- SNMP, Modbus, KNX, BACnet
- Microsoft 365 via API





Core and project kept apart.

The core brings drivers, services and monitoring. Room logic and interfaces live in the project. An update renews the core, the project stays.

- Updates without project rework
- Project logic in JavaScript
- Own interfaces in HTML5

The NDPro Concept

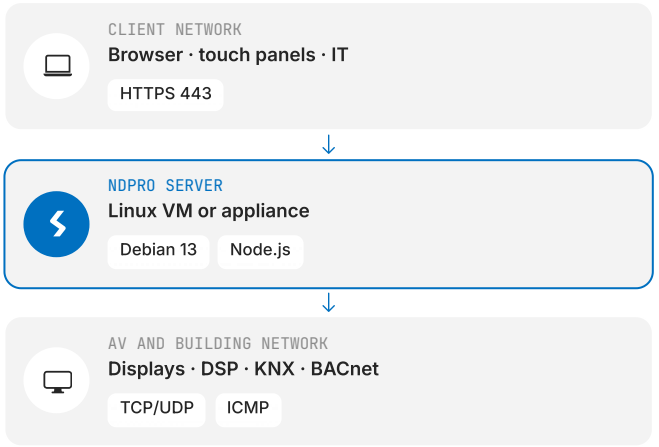
For technicians: the recommended architecture for the professional and secure operation of NDPro.

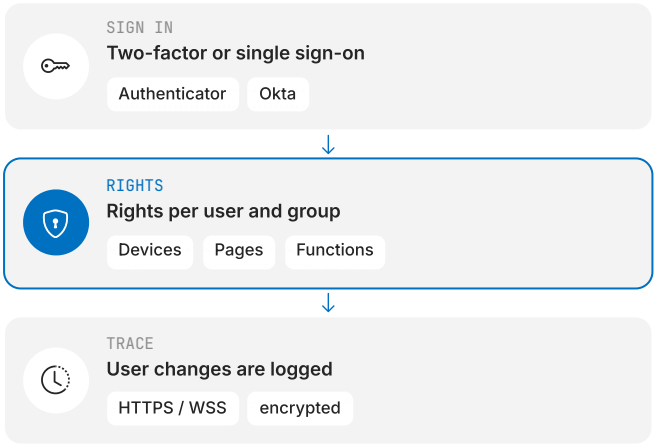
planspur netdesign gmbh

Runs in your network.

NDPro runs on a Linux VM or appliance between client and AV network. Browsers connect via HTTPS, NDPro talks to the devices directly.

- Fits into existing VLANs
- HTTPS for every interface
- Core functions work offline





Right access for everyone.

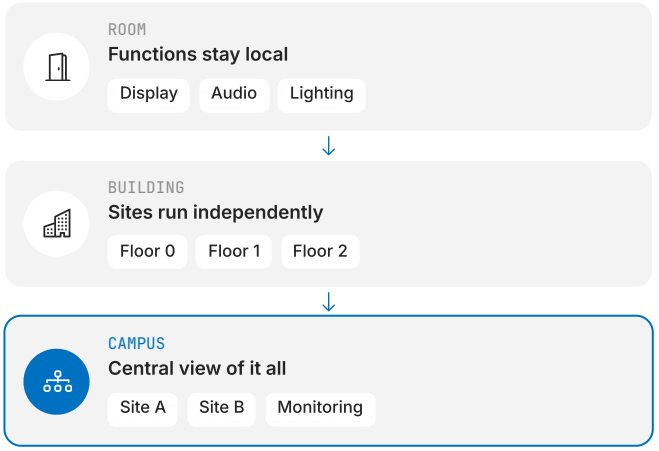
Sign-in with two factors or single sign-on, rights per user and group down to device and page. Credentials are stored in encrypted form.

- Two-factor via authenticator
- Single sign-on, e.g. Okta
- User changes are logged

From room to campus.

Each room keeps running locally, even without an outside connection. Several sites can be monitored centrally, new rooms come from templates.

- Room functions stay local
- Central view across sites
- New rooms from templates



The NDPro Concept

For technicians: the recommended architecture for the professional and secure operation of NDPro.

planspur netdesign gmbh

Technical key data.

What an NDPro server needs and what it brings along.

Server

- Debian 13 or newer
- Node.js LTS with PM2
- Apache as HTTPS proxy

Hardware

- 4 cores min., 8 advised
- 4 GB RAM min., 8 advised
- 80 GB SSD min., 260 adv.

Protocols

- REST, TCP/IP, WebSocket
- SSH, SNMP, Modbus
- KNX, BACnet, Microsoft 365

Security

- Two-factor, single sign-on
- Rights per user and group
- Runs without root rights

Access

- Browser via domain, HTTPS
- Valid TLS certificate
- Devices directly via IP

Operation

- Core functions offline
- Backups, schedules local
- Updates via secured VPN

Network and firewall.

The rules for operation, updates and monitoring at a glance.

Access to NDPro

- SSH 22, HTTP 80
- HTTPS 443
- SMB 445, optional

NDPro to devices

- TCP/UDP per vendor
- ICMP for reachability
- Advised: ANY in AV network

Online, outgoing

- HTTPS 443 for messages
- VPN UDP 1201 for updates
- TCP 80/443 for Debian

DNS and time

- DNS TCP/UDP 53 and 853
- NTP/SNTP UDP 123
- Domain points to NDPro

Certificates

- Publicly signed TLS
- Let's Encrypt or wildcard
- Self-signed only at start

End devices

- Correct time and time zone
- DNS resolution checkable
- Certificate check active