# External access to Nuclos

Language: Deutsch · **English**

## External access to Nuclos

> **Provide Nuclos externally – HTTPS/NAT, reverse proxy or VPN compared with pros and cons.**

KONZEPT | ADMINISTRATOR | UPDATED: JUL 2026 | APPLIES TO NUCLOS 4.2026.X

**On this page**


- 1. Access via HTTPS (NAT)
- 2. Access via a reverse proxy
- 3. Access via VPN (recommended)
- Related pages


There are three methods to make a Nuclos instance available externally.

### 1. Access via HTTPS (NAT)

Port 443 is forwarded to the Nuclos server via NAT; HTTPS must be configured in Nuclos. A different port is possible (then always specify it, e.g. `https://nuclos.company.tld:8443`).

| Advantages | Disadvantages |
|---|---|
| Simple configuration, no extra hardware. | Tomcat start page reachable externally; HTTPS port occupied by a single application. |

### 2. Access via a reverse proxy

Port 443 is routed to the reverse proxy, which filters and forwards requests. This allows addressing several instances via different (sub)domains – ideal when port 443 is already taken (see reverse proxy configuration).

| Advantages | Disadvantages |
|---|---|
| Multiple applications on one port; distinction via subdomain; no VPN client needed. | Extra VM/hardware; more demanding configuration. |

### 3. Access via VPN (recommended)

Users establish a VPN connection and access encrypted just like internally. With correct configuration the highest security level; without a VPN router an OpenVPN server on the Nuclos server suffices.

| Advantages | Disadvantages |
|---|---|
| Highest security level; no change for employees; full network access if needed. | A VPN client must be installed. |

**No HTTP externally**

Access via **HTTP** (unencrypted) should never be used for external connections.

## Related pages

**Running Nuclos behind a reverse proxy**

Proxy.

Open

**SSL encryption**

SSL.

Open